Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet

Nouwt, J.

Publication date:
2005

Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet

Privacy voor doe-het-zelvers

Over zelfregulering en het verwerken van persoonsgegevens via internet

Sjaak Nouwt

Sdu Uitgevers Den Haag, 2005

In de IT*e*R-reeks worden de resultaten van het Nationaal Programma voor Informatietechnologie en Recht gepubliceerd. Meer informatie over IT*e*R en de in het kader van IT*e*R lopende onderzoeksprojecten is te vinden op de website: http://www.nwo.nl/iter
Een overzicht van overige publicaties in de IT*e*R-reeks vindt u achter in deze uitgave.

Redactie: Marcus van Leeuwen en Aernout Schmidt
Redactieadres: Elaw@Leiden, Centrum voor Recht in de Informatiemaatschappij, Universiteit Leiden, t.a.v. F.A.M. van der Klaauw-Koops, Postbus 9520, 2300 RA Leiden, e-mail: f.a.m.vanderklaauw@law.leidenuniv.nl, telefoon: (071) 52 77 846.

Het is mogelijk om een abonnement op de ITeR-reeks te nemen. Abonnees krijgen 50% korting op de losse verkoopprijs. Abonnementenregistratie: Sdu Klantenservice, Postbus 20014, 2500 EA Den Haag, e-mail: sdu@sdu.nl, telefoon: 070 3789880, fax: 070 3789783.

Ontwerp omslag en binnenwerk: Villa Y, Den Haag
Zetwerk: www.az-gsb.nl., Den Haag

ISBN 90-1210-913-2
NUR 820

Inhoudsopgave

Woord vooraf

Dit rapport is het resultaat van een kortetermijnonderzoek dat met subsidie van het NWO-programma IT*e*R is uitgevoerd. Het Nationaal Programma Informatietechnologie en Recht (IT*e*R) is een stimuleringsprogramma dat onderzoek naar actuele juridische vraagstukken op het gebied van informatie- en communicatietechnologie stimuleert en financiert. Het programma is een samenwerkingsverband tussen de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en de ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Justitie, Onderwijs, Cultuur & Wetenschappen, en Verkeer & Waterstaat.

In de beginfase is door Eric Schreuders een belangrijke bijdrage aan dit onderzoek geleverd. De auteur dankt hem daarvoor. Evenals de collega's 'op TILT', die in de eindfase aan de afronding van dit onderzoek hebben bijgedragen.

Tilburg, december 2004

Sjaak Nouwt

Lijst van afkortingen

BW	Burgerlijk Wetboek
CBP	College bescherming persoonsgegevens
CEN-ISSS	European Committee for Standardization-Information Society Standardization System
COPPA	Children's Online Privacy Protection Act
EER	Europese Economische Ruimte
EG	Europese Gemeenschap
EPIC	Electronic Privacy Information Center
EU	Europese Unie
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
FEDMA	Federation of European Direct Marketing
FTC	Federal Trade Commission
Gw	Grondwet
ICC	International Chamber of Commerce
ICT	Informatie- en communicatietechnologie
ICX	Centre of Excellence for e-Business in Europe
IE6	Microsoft's Internet Explorer, versie 6
IPSE	Initiative for Privacy Standardization in Europe
ITU	International Telecommunication Union
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
NEN	Nederlands Normalisatie Instituut
NLIP	Branchevereniging van Nederlandse Internet Providers
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
P3P	Platform for Privacy Preferences
PbEG	Publicatieblad Europese Gemeenschappen
PET	Privacy Enhancing Technologies
RvE	Raad van Europa
VN	Verenigde Naties
VS	Verenigde Staten van Amerika
W?WT	Which? Web Trader
Wbp	Wet bescherming persoonsgegevens
WSIS	World Summit on the Information Society

1 Inleiding

1.1 Onderwerp van het onderzoek

Dit onderzoek naar de bescherming van privacy in de nieuwe economie gaat over consumentenprivacy in het *dotcom*-tijdperk.[1] Daarmee is het terrein van dit onderzoek meteen nader afgebakend. Het onderzoek concentreert zich met name op de privacybescherming van consumenten die diensten afnemen of goederen kopen via internet en op de bescherming van hun persoonsgegevens voor zover die bijvoorbeeld verder worden gebruikt voor commerciële communicatie. Privacybescherming is een succesfactor voor de nieuwe economie omdat de consument voldoende vertrouwen moet kunnen hebben wanneer die persoonsgegevens verstrekt aan de bank, de huisarts, de credit card maatschappij, winkeliers, overheid, etc. Hierin ligt de kern van de privacy-uitdaging.[2] Daarbij is een belangrijke vraag die of er een evenwicht is tussen overheidsregulering, zelfregulering door het bedrijfsleven en individuele verantwoordelijkheden. Alle drie komen ze in dit rapport aan de orde. Privacyvertrouwen van consumenten en flexibiliteit voor bedrijven om gemak, besparingen, diensten en arbeidsplaatsen aan te bieden aan de consument vormen de grote maatschappelijke belangen in de nieuwe economie.

1.2 Veranderingen in het privacylandschap

Recent onderzoek[3] leert dat bescherming van privacy en persoonsgegevens tot voor kort veelal bestond uit een juridisch raamwerk op nationaal niveau, waarin de rechten van betrokkenen werden erkend en waarin procedures ter handhaving van deze rechten veelal verliepen via de weg van de toezichthoudende autoriteiten of de rechterlijke macht.

Deze, voor een belangrijk deel op internationale documenten en richtlijnen van de Raad van Europa en de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) berustende wetgeving wordt – hoewel de uitgangspunten voor bescherming van persoonsgegevens nog steeds actueel zijn – op de proef gesteld door een aantal nieuwe

1. Ook al spreekt men sinds het einde van de internethype ook wel van het '*dotbomb* tijdperk'.
2. Harriet Pearson, IBM, tijdens de Hearing 26 juli 2001 van de Amerikaanse Subcommittee on Commerce, Trade, and Consumer Protection, een subcommittee van de Committee on Energy and Commerce.
3. OECD Working Party on Information Security and Privacy, *Report On Compliance With, And Enforcement Of, Privacy Protection Online,* DSTI/ICCP/REG(2002)5/FINAL, 12 February 2003.

ontwikkelingen. In het OESO rapport worden de volgende ontwikkelingen in dit verband relevant geacht:

- De wereldeconomie is thans veel meer een mondiale economie dan twee of drie decennia geleden. Consumenten sluiten thans met veel gemak een economische transactie met een leverancier van goederen of diensten in andere landen.
- Het gebruik van computers waarmee persoonsgegevens kunnen worden verwerkt, heeft intussen een omvang gekregen die enkele decennia geleden niet voorzien was.
- Online systemen, zoals portaalsites, marktplaatsen en virtuele gemeenschappen zijn ontstaan die, terwijl daarop wel privacywetgeving van toepassing is, vooral functioneren op basis van door de deelnemers zelf opgestelde regels en algemene voorwaarden.
- Het concept van privacy bevorderende technologieën (PET) heeft zich ontwikkeld tot een concept voor 'privacy-by-design'.
- Het aantal internationale rechtsmacht procedures met betrekking tot online interacties is voortdurend toegenomen.

Deze ontwikkelingen hebben het juridische landschap voor de naleving en handhaving van privacyvoorschriften danig veranderd, vooral door de opkomst van alternatieve vormen van geschillenbeslechting.

Tegelijkertijd blijkt uit het OESO-onderzoek dat in elk geval in de OESO lidstaten de lidstaten en de industrie intussen volop bezig zijn geweest om alternatieve mogelijkheden te creëren ter bevordering van de naleving en handhaving van privacy en persoonsgegevens van consumenten. Deze alternatieve mogelijkheden hebben in het algemeen de volgende kenmerken:

- OESO-lidstaten en het bedrijfsleven maken steeds vaker gebruik van marktgerichte drijfveren en maatregelen die de naleving moeten bevorderen. Zo zijn privacy betrouwbaarheids- en keurmerkprogramma's ontwikkeld, waarbij deelnemende website-aanbieders zich aan bepaalde privacyregels dienen te conformeren. Doen zij dat niet, dan hebben zij ook niet het recht om een betrouwbaarheidsstempel of privacykeurmerk op hun website te voeren.
- Zij grijpen steeds vaker naar technische maatregelen om naleving van privacyregels te bevorderen. Zowel de lidstaten als het bedrijfsleven stimuleren het nemen van privacy bevorderende maatregelen, het gebruik van technische standaarden voor privacybescherming zoals P3P, toezicht en andere maatregelen die de naleving van privacyregels bij de online verwerking van persoonsgegevens moeten bevorderen. Door toepassing van 'privacy-by-design', dat wil zeggen het toepassen van privacy bevorderende technieken tijdens het ontwerpen van een informatiesysteem, tracht men de behoefte aan handhaving te verminderen.
- Internetbedrijven hebben de commerciële voordelen ontdekt van voldoende privacybescherming voor hun klanten en hen worden dan ook diverse gereedschappen, mechanismen en systemen aangeboden om hun klanten privacybescherming te kunnen garanderen. Dergelijke maatregelen bestaan bijvoorbeeld uit betrouwbaarheids-

en keurmerkprogramma's, PET, benoeming van privacyfunctionarissen, voeren van een privacybeleid, en dergelijke.
- Er bestaat voldoende potentieel voor het toepassen van bestaande nalevings- en handhavingmechanismen in een online omgeving. Zo hebben sommige lidstaten en bedrijven er voor gekozen om privacyklachten te publiceren en online toegankelijk te maken. Daarnaast zijn al enkele vormen van alternatieve geschillenbeslechting in ontwikkeling voor privacyklachten.
- Het garanderen van voldoende beveiliging wordt steeds vaker beschouwd als een essentiële maatregel ter bescherming van persoonsgegevens. Zowel overheden als particuliere organisaties bevorderen de ontwikkeling en het gebruik van technische standaarden, audits, beveiligingsbeleid en andere maatregelen ter beveiliging van de persoonsgegevensverwerking online.

Deze ontwikkelingen tonen aan dat de naleving en handhaving van de bescherming van privacy en persoonsgegevens aan het veranderen is. De tendens verplaatst zich van een strakke overheidsregulering naar een meer holistische benadering van privacybescherming. Daarbij speelt centrale overheidsregulering nog wel een rol, maar dan naast andere nalevings- en handhavingmechanismen, zoals technische en organisatorische maatregelen en zelfregulering. Teneinde in het licht van de online omgeving de bescherming van privacy en persoonsgegevens op internationaal niveau te kunnen garanderen, wordt het ook steeds belangrijker dat de bescherming van privacy en persoonsgegevens in een internationaal perspectief wordt benaderd en niet langer uitsluitend vanuit nationaal oogpunt.

1.3 Internet en consumentenprivacy

De privacy van de consument op internet beperkt zich niet tot het land van de consument. De Europese consument koopt met evenveel gemak een product in Europa als in de Verenigde Staten. Omdat de VS voor Europese consumenten interessante marktplaatsen bieden, is het van belang stil te staan bij de verschillen in privacybescherming die tussen beide bestaan.

De Europese en Amerikaanse benadering van privacybescherming verschillen in belangrijke opzichten van elkaar.[4] Hoewel in het algemeen in democratische landen de informationele privacy wordt erkend als kritische factor voor een beschaafde samenleving, heeft de VS de privacybescherming in de afgelopen decennia grotendeels overgelaten aan de vrije markt, door middel van zelfregulering. In tegenstelling daarmee beschouwt Europa het recht op privacy juist als een politieke verworvenheid, verankerd in de fundamentele rechten voor de mens.

4. Zie J.R. Reidenberg, E-commerce and Trans-Atlantic Privacy, *Houston Law Review* 38:2001, p. 717-749.

In continentaal Europa vormt het geschreven recht het belangrijkste juridische middel ter bescherming van de burger en de samenleving. Deze visie op overheidsregulering heeft tot gevolg dat de staat of overheid de belangrijkste speler is bij de inrichting van de samenleving. Dat geldt dus ook voor het opstellen van regels voor de omgang met persoonsgegevens, die invulling krijgen in de vorm van rechten en verantwoordelijkheden. De Europese burger lijkt de overheid daardoor meer te vertrouwen dan het bedrijfsleven als het om persoonsgegevens gaat.

In Europa is de bescherming van informationele privacy vooral een onderdeel van het publiekrecht. Vanaf de jaren zeventig zijn in diverse Europese landen algemene wetten ter bescherming van persoonsgegevens tot stand gekomen. In tegenstelling tot sectorale privacywetgeving worden deze wetten ook wel als omnibuswetgeving aangeduid. Zij garanderen de burger verschillende rechten ter waarborging van een behoorlijke en zorgvuldige verwerking van hun persoonsgegevens. In meer of mindere mate beschikt de Europese burger over een recht op informationele zelfbeschikking, zoals de mogelijkheid om toestemming voor een verwerking te verlenen, te weigeren of in te trekken, en om inzage en verbetering van zijn gegevens te verzoeken. Daarmee kan de burger zelf controle uitoefenen op het verzamelen en het gebruiken van hem betreffende persoonsgegevens. Tegelijkertijd legt dit verplichtingen op aan de houders die verantwoordelijk zijn voor de verwerking van die persoonsgegevens. Deze plichten hebben betrekking op het verzamelen, opslaan, gebruik en verstrekken van persoonsgegevens. De Europese benadering is daarom niet primair gericht op de belangen van het bedrijfsleven, maar voorziet eerder in een hoog niveau van bescherming voor de burger.

Veel Europese landen beschikten in de jaren tachtig over privacywetgeving. Deze wetgeving kende echter aanzienlijke verschillen, zodat harmonisatie van privacywetgeving een belangrijke doelstelling voor de EU werd, mede in het belang van de totstandkoming van de interne markt. In 1995 werd dan ook de algemene privacyrichtlijn 95/46/EG aanvaard die tot harmonisatie van privacybescherming in Europa moest leiden. Alle EU lidstaten moeten vanaf 24 oktober 1998 de richtlijn in hun nationale wetgeving hebben geïmplementeerd. Daardoor is het mogelijk met inachtneming van voldoende privacybescherming persoonsgegevens uit te wisselen tussen de lidstaten van de EU. Aldus lijkt de EU er min of meer in te zijn geslaagd haar privacystandaard, te weten die van Richtlijn 95/46/EG, aan de rest van de wereld op te leggen door strenge voorwaarden te stellen aan de doorgifte van persoonsgegevens naar derde landen. Deze standaard lijkt echter wel een deuk opgelopen te hebben door de eisen die vanuit de Verenigde Staten worden gesteld aan het verstrekken van passagiersgegevens van Europese burgers.

1.4 Het onderzoek

Het onderhavige onderzoek beoogt inzicht te bieden in de betekenis van zelfregulering voor de bescherming van persoonsgegevens, in het bijzonder van consumenten, die via internet worden verzameld. Vanuit dit perspectief van informationele privacy zullen de volgende hoofdvragen worden behandeld:

1. Waaruit bestaat het verschil tussen privacybescherming en de bescherming van persoonsgegevens?
2. Hoe denkt de burger of consument over diens privacy op internet?
3. Welke overheidsregulering en welke zelfreguleringsinitiatieven voor gegevensbescherming kunnen we onderscheiden?
4. Welke bescherming kan de techniek zelf bieden?
5. Wat kunnen zelfregulering en techniek betekenen voor de bescherming van persoonsgegevens op internet?

Deze hoofdvragen komen op de volgende wijze aan bod in dit onderzoek. Na deze inleiding wordt in hoofdstuk 2 ingegaan op de begrippen privacy en persoonsgegevensbescherming en wordt de eerste onderzoeksvraag behandeld. Vervolgens worden in hoofdstuk 3 enkele praktijkvoorbeelden uiteengezet van online verwerkingen van persoonsgegevens door commerciële bedrijven. Tevens wordt ingegaan op de resultaten van enkele privacy surveys in Europa en de Verenigde Staten. Daarmee wordt beoogd de tweede hoofdvraag van dit onderzoek te behandelen.

Het juridische kader voor de bescherming van persoonsgegevens (het eerste deel van de derde onderzoeksvraag) komt in hoofdstuk 4 aan de orde. Achtereenvolgens komen daarin eerst de belangrijkste algemene privacybeginselen ter bescherming van persoonsgegevens aan bod van de OESO en de Raad van Europa, en de Amerikaanse tegenhanger in de vorm van de Fair Information Practice Principles. Deze beginselen liggen in belangrijke mate aan de basis van het wettelijke kader ter bescherming van persoonsgegevens dat vervolgens wordt geschetst.

In hoofdstuk 5 wordt ingegaan op het tweede deel van de derde onderzoeksvraag naar de bescherming van persoonsgegevens door middel van zelfregulering, in het bijzonder via gedragscodes en keurmerken. Er wordt stil gestaan bij het instrument zelfregulering als zodanig en vervolgens worden enkele voorbeelden van gedragscodes, keurmerken en contractuele modelregelingen besproken. Mede aan de hand van het voorbeeld van het verzamelen van persoonsgegevens bij kinderen, wordt ook stil gestaan bij de betekenis van de privacy policy op internet.

In hoofdstuk 6 wordt ingegaan op diverse privacybevorderende technieken en methoden. Daarmee wordt in antwoord op de vierde hoofdvraag aangegeven in hoeverre de techniek effectief kan worden ingezet ter bescherming van persoonsgegevens van consumenten.

In hoofdstuk 7 komen de mogelijke rol en de beperkingen van zelfregulering aan de orde. Daarmee wordt de vijfde hoofdvraag beantwoord naar de betekenis van zelfregulering via gedragscodes, keurmerken en techniek voor de bescherming van persoonsgegevens op internet. Tevens worden enkele criteria geformuleerd waaraan zelfreguleringsinitiatieven ter bescherming van persoonsgegevens op internet zouden moeten voldoen.

In hoofdstuk 8 wordt een blik in de toekomst geworpen. Op het terrein van de verwerking van persoonsgegevens vinden momenteel enkele interessante ontwikkelingen

plaats die van invloed kunnen zijn op de bescherming van privacy en persoonsgegevens van consumenten.

Tot slot volgen een samenvatting en een summary.

2 Privacy en gegevensbescherming

2.1 Privacy en privacybescherming

Bij privacy, ook kan gesproken worden over persoonlijke levenssfeer of privé leven, kunnen verschillende onderdelen onderscheiden worden: de ruimtelijke privacy waartoe het huisrecht behoort, de lichamelijke privacy waartoe de integriteit van lichaam en geest behoort, de relationele privacy op grond waarvan niet alleen verschillende vormen van communicatie, maar bijvoorbeeld ook het familieleven wordt beschermd en, als laatste, de informationele privacy: het recht op bescherming van personen in verband met de informatie die over hen bekend is en ten aanzien van hen wordt toegepast.

Bij omschrijvingen van het begrip privacy wordt vaak verwezen naar noties zoals het recht om met rust gelaten te worden. Deze benadering plaatst privacy in de categorie van de afweerrechten. Het waren Warren en Brandeis[5] die privacy ruim een eeuw geleden op deze wijze op de kaart hebben geplaatst. Het is een benadering die verwantschap vertoont met de klassieke grondrechten: vrijheidsrechten van de burger tegen de overheid.

Van recenter datum is de benadering om privacy te duiden als het recht om zelf te bepalen wat er met de toegang tot, en met zijn persoonsgegevens gebeurt. Dit recht is meer actief, het is meer een actierecht: het zijn de personen zelf die hun eigen vrije ruimten bewaken en behouden. Deze benadering, ontstaan in de jaren zestig en waarvan Westin[6] de grondlegger genoemd kan worden, roept de gedachte op van de sociale grondrechten: de aanspraken op een maatschappelijk en cultureel volwaardig leven. Zo is in Duitsland in de periode 1969 tot 1983 het op de Federale Grondwet gebaseerde recht op informationele zelfbeschikking tot ontwikkeling gekomen.[7]

De visies vanuit individu zien meer op de (afzonderlijke) positie van actoren. In de privacyvisie van Johnson ligt de nadruk meer op de relatie tussen de betrokken actoren. De rol of functie die privacy speelt in het maatschappelijke verkeer ligt in deze relatiegerichte visie in de bescherming van bepaalde aspecten van individuen tegen de (positieve

5. S.D. Warren en L.D. Brandeis, 'The right to privacy', *Harvard Law Review*, 1980, no.5, p. 195. Zij spraken in navolging van Judge Cooley over 'the right to be let alone'.
6. A.F. Westin, *Privacy and Freedom*, New York, 1967, p. 7.
7. Zie T. Koopmans, 'Privacy and the dilemma's of human rights' protection', in: P. Ippel, e.a, *Privacy disputed*, Den Haag: SDU 1995, p. 45-46.

of negatieve) evaluatieve oordelen van anderen. De opvatting dat persoonsgegevens alle informatie is die van invloed is op de maatschappelijke positie van personen (zie hierover hieronder verder) houdt verband met deze relatiegerichte visie. Een precieze afbakening wordt daarbij keer op keer bepaald door uiteenlopende factoren zoals maatschappelijke omstandigheden of ontwikkelingen in techniek en technologie.[8] De relatiegerichte benadering stelt voorop dat de betekenis en inhoud van privacy dynamisch is en afhankelijk is van de omstandigheden. Volledig vaststaande kaders, begrippen of definities passen daar niet bij. Wat vandaag nog onaanvaardbaar is, kan morgen bij een weliswaar gelijkblijvend juridisch toetsingskader maar gewijzigde maatschappelijk omstandigheden wel degelijk tot de mogelijkheden behoren, of andersom.

De hier weergegeven noties van en over privacy geven nog niet noodzakelijkerwijze weer welke waarden en normen de betrokkenen (consumenten) zelf aan privacy verbinden. Toch is aandacht hiervoor niet onbelangrijk. Gevoelens over het al dan niet privacybedreigend zijn van commerciële websites zullen voor een belangrijk deel op deze waarden gegrondvest zijn. In het onderzoek *Privacybeleving van burgers in de informatiemaatschappij*[9] stonden deze waarden, normen en opvattingen achter privacy centraal. De waarden die volgens dit onderzoek achter opvattingen over privacy schuilgaan zijn:[10] zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering,[11] ongestoord leven, eigenwaarde, vrij blijven van manipulatie,[12] integriteit en autonomie.[13]

De waarde 'zelfstandigheid' ziet op het zelf kunnen besluiten, verantwoordelijkheid kunnen nemen en de mogelijkheid om gegevens voor zich te houden. 'Bewegingsvrijheid' betreft het doen en laten wat je wilt, anoniem kunnen zijn, en niet gecontroleerd worden. 'Gelijkheid' speelt bij situaties waarin mensen op basis van ongelijke of beperkte gronden geselecteerd worden. 'Vrij blijven van stigmatisering' betekent geen etiket opgeplakt krijgen en niet onderworpen worden aan oordelen, bijvoorbeeld over kredietwaardigheid, van anderen zonder daar zelf op te kunnen reageren. 'Ongestoord leven' betreft het niet gedwongen worden actie te ondernemen, bijvoorbeeld bij ongevraagd gebeld

8. Johnson spreekt er in dit verband over dat privacy 'socially or culturally' gedefinieerd is en van context tot context verschilt en derhalve dynamisch is. Zie J.L. Johnson, 'Privacy and the Judgements of others', *The Journal of Value Inquiry*, 1989, p. 157. Zie ook: A.H. Vedder, 'Privacy en woorden die tekort schieten', in: S. Nouwt en W. Voermans (red), *Privacy in het informatietijdperk*, Den Haag: SDU 1996, p. 22.
9. G.C.J. Smink, A.M. Hamstra en H.M.L. van Dijk, *Privacybeleving van burgers in de informatiemaatschappij*. Den Haag: Rathenau Instituut 1999, Werkdocument 68.
10. Smink, Hamstra en Van Dijk, *t.a.p.* p. 50-52, 58-59 en 101.
11. Ruim 2/3 van de burgers hecht hier waarde aan. Smink, Hamstra en Van Dijk, *t.a.p.* p. 101.
12. Ongeveer de helft van de burgers brengt deze waarden in verband met privacy. Smink, Hamstra en Van Dijk, *t.a.p.* p. 101.
13. Ruim 1/3 van de burgers vindt dat deze waarden deel uitmaken van het begrip privacy. Smink, Hamstra en Van Dijk, *t.a.p.* p. 101.

worden. De waarde 'eigenwaarde' wordt geschonden als burgers het idee hebben dat ze een deel van hun identiteit weggeven. 'Vrij blijven van manipulatie' ziet op het niet onbewust aangezet worden tot bepaald handelen of denken. De 'integriteit' wordt geschonden als gegevens zonder toestemming aan derden worden verstrekt. 'Autonomie' ten slotte betreft het zelf normen kunnen stellen en vrij zijn te handelen.[14] De bevindingen[15] over de waarden en opvattingen over privacy zijn enerzijds dat verschillende personen verschillende waardestelsels hanteren en verschillende waarden meer of minder belangrijk vinden. Anderzijds is het zo dat dezelfde personen in verschillende situaties andere waarden belangrijk vinden. Privacy en de waarden die daarbij een rol spelen zijn daarom in algemene zin wel in kaart te brengen, maar welke waarde of waarden een persoon als het meest belangrijk of vormend voor privacy beschouwt, verschilt van persoon tot persoon en van situatie tot situatie.[16]

2.2 Het fundamentele recht op privacy

De hierboven geduide (informationele) privacy is als grondrecht (voor Nederland) in juridische zin beschermd in artikel 10, eerste lid, en de artikelen 11 tot en met 13 van de Grondwet, in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)[17] en in artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR).[18] Constituerende regels zijn regels die het grondrecht creëren en vastleggen. Bij privacy en de bescherming van privacy valt te denken aan artikel 8 EVRM of artikel 10, eerste lid, van de Grondwet. In juridische zin zijn deze regels een *conditio sine qua non* voor het bestaan van het desbetreffende recht. Kenmerkend voor deze regels is dat een definitie van privacy niet wordt gegeven.

In deze regels wordt ook aangegeven onder welke algemene voorwaarden het beschermde goed (toch) aangetast kan worden. Een kenmerkende voorwaarde is dat de mogelijkheid tot aantasting in nadere regels dient te worden vastgelegd. Deze twee elementen van grondrechten: de vestiging van het 'absolute' recht en de mogelijkheid om onder voorwaarden een inbreuk te maken, zodat het recht niet volledig 'absoluut' is, leiden tot een systeem waarbij het legaliteitsbeginsel de boventoon voert.

In hoofdstuk 3 zal worden ingegaan op meer algemeen geformuleerde privacybeginselen.

14. Smink, Hamstra en Van Dijk, *t.a.p.* p. 50-52.
15. Smink, Hamstra en Van Dijk, *t.a.p.* p. 101-103.
16. Deze situationele invulling van privacy komt ook naar voor uit de beschrijving van A.F.Westin van drie groepen burgers in de Equifax-Harris onderzoeken. Hij spreekt daarin over de 'Privacy Fundamentalists' (25%), de 'Unconcerned' (18%) en de 'Pragmatic Majority (57%). Zie voor een eerste introductie de *Harris-Equifax Consumer Privacy Survey* 1991, 1991, Uitgevoerd in opdracht van Equifax, Georgia, USA, p. 6-7.
17. *Trb.* 1951, 154 en 1990, 156.
18. *Stb.* 1978, 177.

2.3 Persoonsgegevensbescherming

Informationele privacy en de juridische bescherming daarvan heeft naast de genoemde grondrechten, zijn juridische erkenning en uitwerking gekregen in regels ter bescherming van persoonsgegevens. In zowel de OESO privacyrichtlijnen[19], het Databeschermingsverdrag van 1981 van de Raad van Europa (RvE),[20] in de EU-Privacyrichtlijnen,[21] en in artikel 10, tweede en derde lid, van de Grondwet gaat het om de bescherming van persoonsgegevens. Deze regels geven, binnen de grenzen van de grondrechten aan, wanneer het verwerken van gegevens als rechtmatig kan worden beschouwd. De regels over het verwerken van persoonsgegevens geven in die zin ook invulling aan de mogelijkheid om inbreuk te maken op het grondrecht. De regels geven immers aan wanneer inbreuken toelaatbaar zijn. Zolang de regels over het verwerken van persoonsgegevens binnen de grondrechtelijke marge om inbreuk te maken blijven, zijn deze in principe mogelijk.

De Wet bescherming persoonsgegevens (Wbp), die overigens ook van toepassing is op verwerkingen van persoonsgegevens door middel van commerciële websites, is de algemene wet die regels bevat voor een behoorlijke en zorgvuldige omgang met persoonsgegevens.

2.4 Persoonsgegevens of niet en de juridische gevolgen

Voor de bescherming van persoonsgegevens is een belangrijke vraag in het kader van dit onderzoek of er door commerciële websites wel of geen persoonsgegevens worden verwerkt en wat daarvan de gevolgen zijn voor de mogelijkheden tot regulering.

2.4.1 Persoonsgegevens

Een ruime definitie van het begrip persoonsgegevens wordt op internationaal terrein gegeven in zowel artikel 2, onder a, van het Databeschermingsverdrag,[22] als in artikel 2,

19. *OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* October 1, 1980.
20. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, *European Treaty Series* No. 108.
21. 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*, nr. L 281 p. 31 (de algemene EU-Privacyrichtlijn); Richtlijn 97/66/EG van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (de Telecom-Privacyrichtlijn), *PbEG,* nr. L 24, p. 1; en Richtlijn 2002/58 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie, *PbEG,* nr. L 201, p. 37.
22. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, European Treaty Series No. 108. (Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg, 28 januari 1981, *Trb*. 1988, 7, goedgekeurd bij Wet van 20 juni 1990, *Stb.* 351, gewijzigd bij Wet van 27 november 1991, *Stb*. 654).

onder a, van de algemene EG-Privacyrichtlijn.[23] Het Databeschermingsverdrag spreekt in artikel 2, onder a, over: "'personal data' means any information relating to an identified or identifiable individual ('data subject')".

De Europese Privacyrichtlijn spreekt in artikel 2, onder a, met betrekking tot persoonsgegevens over: "iedere informatie betreffende een geïdentificeerde of identificeerbare persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit". De Wet bescherming persoonsgegevens spreekt, in navolging van deze definities, in artikel 1, onder a, over: "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon."

Bij persoonsgegevens gaat het volgens de genoemde definities om 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. De twee elementen 'iedere informatie betreffende' en 'geïdentificeerd of identificeerbare' staan hierbij centraal.

Met 'iedere informatie betreffende' wordt bedoeld dat het om alle gegevens gaat die over een bepaalde persoon informatie kunnen verschaffen. In veel gevallen, zoals bij gegevens over eigenschappen, opvattingen of gedragingen, zal dit duidelijk zijn. In andere gevallen zal de context waarin het gegeven wordt verwerkt en gebruikt bepalend zijn. Van belang is dan of het gegeven bepalend kan zijn voor de wijze waarop de betrokken persoon in het maatschappelijke verkeer wordt beoordeeld of behandeld. Anders gezegd: het gaat over de wijze waarop de betrokkene aan het maatschappelijke leven deelneemt. Zo kunnen gegevens over een onderneming of over telefoongesprekken persoonsgegevens zijn. Ook telefoonnummers en kentekens van auto's, en zelfs perceelnummers en IP-adressen, kunnen persoonsgegevens zijn.

Zo is het College bescherming persoonsgegevens (CBP) met betrekking tot IP-adressen van mening dat een volledig IP-adres in veel gevallen, maar niet altijd, als persoonsgegeven kan worden beschouwd. Hierdoor vallen verwerkingen van IP-adressen over het algemeen onder de reikwijdte van de privacywetgeving. De verschijningsvorm van het IP-adres is echter bepalend daarvoor. In een uitspraak van 19 maart 2001 (z2000-0340) beoordeelde de (toenmalige) Registratiekamer een door een bedrijf in de handel gebrachte CD-ROM waarop een database is opgenomen waarin bij elk IP-adres is vastgelegd in welk land (regio) dit adres wordt gebruikt en welke taal daar als voertaal wordt gesproken. Met behulp van de bijbehorende software kan een eigenaar van een website aan de hand van een concreet IP-adres aldus vaststellen welke taal de meest waarschijn-

23. 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*, nr. L 281/31-50.

lijke is om de informatie weer te geven. De Registratiekamer stelde vast dat er bij het aanmaken van de CD-ROM weliswaar sprake is van IP-adressen, maar dat deze op dusdanige wijze worden gebruikt dat deze niet tot individuele natuurlijke personen kunnen worden herleid. Deze constatering heeft ertoe geleid dat de Registratiekamer de uitspraak heeft gedaan dat er bij dit bedrijf geen persoonsgegevens zijn en dat de privacywetgeving dus niet van toepassing is.[24] De Registratiekamer sluit hiermee aan bij de opvatting van de Artikel 29 Groep, zoals neergelegd in het werkdocument *Privacy op Internet: Een geïntegreerde EU-aanpak van on-line gegevensbescherming*[25]. Daarin wijst de Artikel 29 Groep op de eenvoudige mogelijkheid voor internetaanbieders en beheerders van lokale netwerken om zonder veel moeite internetgebruikers te identificeren aan wie ze IP-adressen hebben verstrekt, doordat ze als regel systematisch de datum, het tijdstip, de duur en het verstrekte dynamische IP-adres van gebruikers in een logbestand vastleggen. Hetzelfde geldt voor internetdienstverleners die een logboek op de HTTP-server bijhouden. In deze gevallen bestaat er geen twijfel over dat men kan spreken van persoonsgegevens in de zin van artikel 2, onder a), van de richtlijn en de Wbp.

Bij gebruik van een dynamisch IP-adres is het niet altijd mogelijk om andere gegevens aan het IP-adres te koppelen waardoor identificatie van de betrokken gebruiker mogelijk wordt. Dan is er geen sprake van persoonsgegevens. Anders wordt het wanneer gebruik wordt gemaakt van verwerkingsmethoden om aanvullende informatie te verzamelen, zoals gebeurt door middel van cookies. Ook in die gevallen kan het aan de hand van deze cookies mogelijk zijn een IP-adres tot een individuele natuurlijke persoon te herleiden, waardoor sprake is van persoonsgegevens. Bij gebruik van een statisch of vast IP-adres is dat eenvoudiger en zal in de regel wel sprake zijn van een persoonsgegeven.

Bij het element 'geïdentificeerde of identificeerbare' natuurlijke persoon speelt vooral de vraag of de identiteit van de persoon zonder onevenredige inspanning vastgesteld kan worden. Twee factoren zijn hierbij vooral van belang: de aard van de gegevens en de mogelijkheden van de verantwoordelijke om de identificatie tot stand te brengen.

Wat de aard van de gegevens betreft, is een persoon identificeerbaar indien sprake is van gegevens die alleen of in combinatie met andere gegevens zo kenmerkend zijn voor een bepaalde persoon dat deze aan de hand daarvan kan worden geïdentificeerd. Niet ieder gegeven zal echter in dezelfde mate tot het identificeren van persoon (kunnen) leiden. In dit kader kan een onderscheid worden gemaakt tussen direct en indirect identificerende gegevens.

Van direct identificerende gegevens is sprake als de identiteit zonder veel omwegen eenduidig is vast te stellen. Voorbeelden zijn gegevens zoals naam, adres en geboortedatum. Die zijn in combinatie met elkaar zo uniek en kenmerkend voor een bepaalde per-

24. Bron: <www.cbpweb.nl>.
25. Groep Gegevensverwerking Artikel 29, *Werkdocument Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming*. Goedgekeurd op 21 november 2000. WP 37, p. 22.

soon dat deze kan worden geïdentificeerd. Bij indirect identificerende gegevens kunnen de gegevens via nadere stappen in verband worden gebracht met een bepaalde persoon. Bij indirect identificerende gegevens kan een onderscheid worden gemaakt tussen gegevens met een hoog onderscheidend karakter, zoals leeftijd, woonplaats en beroep, en gegevens met een laag onderscheidend karakter, zoals leeftijdsklasse, woonregio en beroepsklasse. Het onderscheidende vermogen van dergelijke (combinaties van) gegevens is mede afhankelijk van de context waarbinnen ze worden gebruikt. Ze zijn bijvoorbeeld afhankelijk van de omvang van de bevolkingsgroep waarop de gegevensverwerking betrekking heeft. Het verwijderen van de direct identificerende kenmerken biedt dan ook niet altijd voldoende garantie dat geen sprake meer is van persoonsgegevens. Door middel van vergelijking en combinatie met andere gegevens, kan in bepaalde situaties zonder bijzonder inspanning identificatie tot stand worden gebracht; ook als enkel indirect identificerende gegevens voorhanden zijn.

Naast de aard van de gegevens, spelen de mogelijkheden van de verantwoordelijke om identificatie tot stand te brengen een rol bij de vraag of er sprake is van identificerende gegevens. Een verantwoordelijke beschikt immers in meer of mindere mate over mogelijkheden tot identificatie. Bijvoorbeeld door het (kunnen) verkrijgen van aanvullende informatie. Bij de afweging is een absolute maatstaf niet aan de orde: gekeken moet worden naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs zijn in te zetten om die persoon te identificeren. Uitgegaan moet worden van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste verantwoordelijke en anderzijds om subjectivering naar bijzondere expertise.[26] Ditzelfde geldt ten aanzien van de ontvanger van gegevens. Het ontvangen van gegevens is immers het verzamelen van die gegevens en daarop is de Wbp van toepassing. Het is dus mogelijk dat bepaalde gegevens op zich wellicht geen persoonsgegevens zijn, maar vanaf het moment dat de ontvanger deze in bezit heeft wel persoonsgegevens zijn omdat het voor de ontvanger wel mogelijk is om de gegevens tot een persoon te herleiden of omdat de gegevens in handen van de ontvanger wel een rol spelen bij de wijze waarop personen in het maatschappelijke verkeer behandeld worden.

Voor wat commerciële websites betreft, kan en dient dan ook als vuistregel genomen te worden dat er daarbij sprake zal zijn van het verwerken van persoonsgegevens. Uiteraard zullen niet al die gegevens even direct identificerend of bepalend zijn voor de wijze

26. De beschrijving van het begrip persoonsgegevens is gebaseerd op de omschrijving in: B.J. Crouwers-Verbrugge, B.M.A. van Eck & E. Schreuders (red.), *Persoonsgegevens beschermd; Uitspraken van de Registratiekamer*, Den Haag: SDU 1997, p. 1-2, en in: B.M.A. van Eck, U. van de Pol & C.G. Zandee, *Persoonsgegevens beschermd, Van WPR naar Wbp; Uitspraken van de Registratiekamer*, Den Haag: SDU 1997, 2e herziene druk, p. 1-2, en de daar genoemde zaken.

waarop personen in het maatschappelijke verkeer behandeld worden. De mate waarin gegevens beschermd dienen te worden kan dan ook afhankelijk zijn van deze twee elementen. Los van een lastige discussie of er nu wel of geen sprake is van persoonsgegevens, kan de vraag ook zo benaderd worden dat bezien wordt of het aanmerken van de gegevens als persoonsgegevens voor het beoogde gebruik van die gegevens daadwerkelijk wel een belemmering is. Wellicht zal dat vaak niet het geval zijn.

2.4.2 Verwerken

Artikel 1, onder b, Wbp omschrijft 'verwerken' als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens en bevat zodoende een zeer ruime omschrijving van het begrip 'verwerken'. In de Wbp genoemde handelingen die in ieder geval als verwerkingen zijn te beschouwen zijn: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen, vernietigen,[27] verkrijgen,[28] doorvoer,[29] en doorgifte.[30]

Of er inderdaad al dan niet sprake is van verwerken, hangt overigens niet zozeer af van de definitie in artikel 1, onder b, Wbp, maar veeleer van het bepaalde in artikel 2, eerste lid, jo. artikel 1, onder c, Wbp. Volgens die artikelonderdelen is de Wbp van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen en op de niet-geautomatiseerde verwerking van persoonsgegevens die bestemd zijn om in een bestand te worden opgenomen, maar die zich nog bevinden in de fase van verzamelen.[31] Een bestand is elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.[32] Een bestand in de zin van de Wbp is vergelijkbaar met de bekende geheel handmatige persoonsregistratie van de Wet persoonsregistraties, waar in dit verband gesproken wordt over een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens die met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd.[33]

Het behoeft geen nadere adstructie dat er bij commerciële websites sprake is van 'verwerken'. De centrale vraag is dus of er sprake is van persoonsgegevens.

27. artikel 1, onder b, Wbp.
28. artikel 1, onder o, Wbp.
29. artikel 4, tweede lid, Wbp.
30. artikel 76 Wbp.
31. artikel 2, eerste lid, Wbp.
32. artikel 1, onder c, Wbp.
33. artikel 1 Wet persoonsregistraties.

2.5 Privacy of persoonsgegevensbescherming: het privacygat

Een onderscheid tussen privacy enerzijds en bescherming van persoonsgegevens anderzijds is op zijn plaats en noodzakelijk voor een goed begrip van de problematiek die in dit boek wordt beschreven.

Uit het vorenstaande blijkt dat privacy een ruim concept is en dat de bescherming van persoonsgegevens daar slechts een onderdeel van is. Dat onderdeel is de 'informationele privacy'. De bescherming van persoonsgegevens door middel van het recht is gebaseerd op de internationale verdragen en richtlijnen, zoals die hierboven ook al zijn genoemd. In de Nederlandse wetgeving zijn deze internationale rechtsbronnen vooral uitgewerkt in de Wet bescherming persoonsgegevens (Wbp). Het onderscheid tussen privacy en persoonsgegevens kan worden geïllustreerd door er op te wijzen dat de Wbp in tegenstelling tot wat vaak wordt beweerd geen privacywet is, maar een wet die het gebruik van persoonsgegevens regelt en legitimeert. De Wbp is in dit opzicht ook wel als 'het summum van repressieve tolerantie' aangeduid.[34] Of een bepaalde vorm van verwerken van persoonsgegevens is toegestaan, wordt bepaald door de voorschriften van deze wet. Dit staat in feite los van de vraag of de privacy van de betrokkene daardoor wordt geschonden.

Het begrip privacy wordt, zoals we hierboven zagen, vaak omschreven als 'het recht om met rust gelaten te worden' of 'het recht om zelf te bepalen wat met uw persoonsgegevens mag gebeuren'. Daarnaast kan, zoals we zagen, de privacy van de burger of consument verschillende waarden hebben: zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering, ongestoord leven, eigenwaarde, vrij blijven van manipulatie, integriteit en autonomie. De bescherming van privacy kan voor verschillende personen in verschillende omstandigheden verschillende waarden hebben.

De 'ruimte' die zich bevindt tussen de bescherming van persoonsgegevens en de waarde van privacy, kunnen we het 'privacygat' noemen. Het 'privacygat' bestaat uit de ruimte die zich bevindt tussen het al dan niet rechtmatig mogen verwerken van persoonsgegevens en het al dan niet ervaren van een inbreuk op de privacy door de betrokkene. Er zijn vier situaties mogelijk:

1. verwerking is rechtmatig, betrokkene ervaart het niet als een schending van diens privacy;
2. verwerking is niet rechtmatig, betrokken ervaart het wel als een schending van diens privacy;
3. verwerking is rechtmatig, betrokkene ervaart het wel als een schending van diens privacy;

34. Zie J.E.J. Prins, Acht gesprekken over privacy en aanpalende belangen. In: H. Franken e.a. (red.), *Zeven essays over informatietechnologie en recht,* Den Haag: Sdu Uitgevers 2003, p. 63 e.v.

4. verwerking is niet rechtmatig, betrokkene ervaart het niet als een schending van diens privacy.

privacy / persoonsgegevens	Verwerking rechtmatig	Verwerking niet rechtmatig
Geen schending privacy		
Wel schending privacy		

Er bestaat dus een verschil tussen de bescherming van privacy en de bescherming van persoonsgegevens. Ter bescherming van persoonsgegevens zijn in Nederland voorschriften vastgelegd in de algemene Wet bescherming persoonsgegevens en in enkele bijzondere wetten zoals de Wet Gemeentelijke basisadministratie persoonsgegevens (GBA), Wet politieregisters (en de opvolger daarvan: de Wet politiegegevens), e.d. Deze wetgeving is van toepassing zodra er sprake is van verwerking van persoonsgegevens. Het is daarbij in beginsel dus niet van belang of er ook sprake is van een schending van iemands privacy. Het enkele feit dat persoonsgegevens worden verwerkt is voldoende voor de toepasselijkheid van de wetgeving. In dit boek gaat het vooral over de bescherming van persoonsgegevens, hetgeen de informationele privacy omvat.

Bij het al dan niet ervaren van een schending van de privacy gaat het er niet zozeer om dat het verzamelen en gebruiken van persoonsgegevens als zodanig bedreigend zou zijn voor de privacy van de consument. Dat kan immers door iedere consument anders worden ervaren. De bedreiging die de verwerking van persoonsgegevens met zich meebrengt voor de privacybeleving van de betrokkene bestaat eerder uit angst voor diefstal van identiteit, financiële fraude, verspreiding van schadelijke (of smadelijke) informatie, discriminatie bij sollicitaties, weigering van verzekeringen, of de ergernis van ‘spamming’. In deze gevaren zijn weer enkele waarden van privacy te herkennen, zoals die in § 2.1 werden gesignaleerd.

2.6 Conclusie

In dit hoofdstuk is getracht een antwoord te geven op de eerste hoofdvraag van dit onderzoek: “Waaruit bestaat het verschil tussen privacybescherming en persoonsgegevensbescherming?” Daartoe is uiteengezet dat er een fundamenteel onderscheid bestaat tussen de bescherming van privacy en de bescherming van persoonsgegevens. Dit verschil is aangeduid met ‘het privacygat’. De meer fundamentele bescherming van privacy kan door consumenten op internet verschillend worden ervaren. In het algemeen zijn de volgende waarden achter privacy te onderscheiden: zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering, ongestoord leven, eigenwaarde, vrij blijven van manipulatie, integriteit en autonomie.[35]

De bescherming van persoonsgegevens is dus verwant aan, maar valt niet samen met, het meer algemene begrip 'privacy'. De wettelijke regels ter bescherming van persoonsgegevens beogen in feite niet alleen de privacy te beschermen, maar stellen de grenzen vast tot waar – onder welke voorwaarden – persoonsgegevens wél mogen worden verwerkt.

35. G.C.J. Smink, A.M. Hamstra en H.M.L. van Dijk, *Privacybeleving van burgers in de informatiemaatschappij.* Den Haag: Rathenau Instituut 1999, Werkdocument 68.

3 Praktijkvoorbeelden en de mening van de consument

3.1 Inleiding

In dit hoofdstuk wordt de tweede hoofdvraag van dit onderzoek behandeld. De tweede hoofdvraag luidt:

"Hoe denkt de burger of consument over diens privacy op internet?"

Alvorens op de beantwoording van deze vraag in te gaan, zullen eerst enkele praktijkvoorbeelden van online verwerkingen van persoonsgegevens door enkele grote (internet) ondernemingen uiteen worden gezet. Daarmee wordt getracht een beeld te schetsen van de verwerking van consumentengegevens via internet.

Teneinde vervolgens de tweede hoofdvraag te beantwoorden, wordt weergegeven hoe consumenten zelf denken over de bescherming van hun persoonsgegevens op internet. Daartoe wordt gebruik gemaakt van enkele nationale en internationale onderzoeken (privacy surveys) die onder burgers zijn gehouden teneinde hun opvattingen over privacy te inventariseren.

Op 26 juli 2001 werd door het Amerikaanse parlement een hoorzitting georganiseerd door de subcommissie *Commerce, Trade, and Consumer Protection*, van de commissie *Energy and Commerce*.[36] Tijdens deze hoorzitting kwamen diverse vertegenwoordigers van de grotere Amerikaanse industrieën aan het woord. Achtereenvolgens spraken vertegenwoordigers van *IBM*, *General Motors*, *Procter & Gamble* en *Amazon.com* over hun beleid inzake privacy en de verwerking van persoonsgegevens. Hieronder volgt een korte weergave daarvan, die een impressie geeft van de privacypraktijk van enkele grote ondernemingen op internet.

Daarna volgt een voorbeeld van het verzamelen en opslaan van persoonsgegevens door middel van Microsoft Internet Explorer. Dit voorbeeld dient vooral ter illustratie van het

36. How do businesses use customer information: Is the customer's privacy protected? Hearing before the subcommittee on commerce, trade, and consumer protection of the committee on energy and commerce, House of Representatives, One hundred seventh congress, First session, July 26, 2001, Serial No. 107–49.

feit dat er heimelijke, althans voor velen ondoorzichtige manieren van verwerken van persoonsgegevens mogelijk zijn. Ook toepassingen als 'cookies' en 'spyware' zijn daar voorbeelden van, maar daar wordt hier verder niet op ingegaan.

3.2 IBM

Namens IBM presenteerde Harriet P. Pearson, Chief Privacy Officer, IBM Corporation een Prepared Statement.

Wanneer een individu of een klein zakelijk bedrijf bijvoorbeeld een personal computer aanschaft bij IBM, vraagt IBM om gegevens zoals de aankoop, de naam van de klant, adres, telefoonnummer, e-mail adres e.d. Diegenen die de tijd nemen om zich aan te melden bij het *Owner Privileges Program* krijgen een gratis elektronische nieuwsbrief toegezonden, voorrang bij telefonische ondersteuning via een speciaal gratis telefoonnummer, en speciale aanbiedingen, waarbij gebruik wordt gemaakt van de door hen verstrekte gegevens.

IBM verzamelt ook persoonsgegevens via internet. Daarbij wordt de betrokkene wel geïnformeerd (Notice) over het privacybeleid van IBM en krijgt de betrokkene een keuze (Choice) voor het verdere gebruik van diens persoonsgegevens.

3.3 General Motors Corporation

Jacqueline L. Hourigan, Director Of Data Policies, presenteerde een Prepared Statement namens General Motors Corporation.

General Motors verzamelt persoonsgegevens langs verschillende wegen, zoals traditionele marktonderzoeken, bezoeken aan GM websites, aanmeldingen bij OnStar, verzekerings- en financieringsproducten van GMAC, en door middel van in auto's ingebouwde technologie die is ontwikkeld ter bevordering van de veiligheid en beveiliging van de klant.

3.4 The Procter & Gamble Company

Voor The Procter & Gamble Company zette Zeke Swift, Director, Global Privacy, een Prepared Statement uiteen.

Procter & Gamble maakt gebruik van internet om aan hun klanten producten en diensten te leveren. Via de website <Reflect.com>, worden producten verkocht zoals huid- en haarverzorgingsproducten, parfums, cosmetica, etc. Via de website Pampers.com, kunnen klanten zich aanmelden voor een gratis maandelijkse nieuwsbrief van het *Pampers Parenting Institute*. Teneinde deze producten en diensten te kunnen leveren, worden persoonsgegevens verzameld, zoals de naam van de klant, adres, e-mail adres of telefoonnummer, zodat het bedrijf de klant kan benaderen of producten kan toesturen. In de meeste gevallen worden deze gegevens vrijwillig verstrekt door de klant. In sommige gevallen worden additionele demografische gegevens gebruikt, die wordt verkregen van dataverwerkers, zoals Acxiom, Equifax of Experian. Deze gegevens zijn verza-

meld uit algemeen beschikbare bronnen, zoals telefoongidsen of rechtstreeks afkomstig van de klant, bijvoorbeeld door middel van door de klant ingevulde garantiecertificaten.

3.5 Amazon.com

Paul Misener, Vice President, Global Public Policy, Amazon.Com, zette in een Prepared Statement het privacybeleid van Amazon.com uiteen.

Als pionier in e-commerce, opende <Amazon.com> de virtuele deuren in juli 1995. Amazon.com verzamelt persoonsgegevens met als doel de verkoop via de website te kunnen personaliseren. Iedere klant krijgt zijn eigen unieke website te zien bij <Amazon.com>. Op die manier kan men de klant snel laten vinden wat men (waarschijnlijk) zoekt en intussen kennis laten maken met producten die de klant mogelijk ook interessant vindt. Wie een boek van Stephen King koopt, krijgt de volgende keer dat hij de website bezoekt een overzicht van andere thrillers gepresenteerd op de <Amazon.com> website. Boven aan de webpagina van <Amazon.com> treft iedere klant zijn eigen naam aan. <Amazon.com> maakt gebruik van zogeheten 'samenwerkende filtering technieken', waardoor aan de hand van aankopen uit het verleden via een vergelijking met anonieme statistische bestanden met gegevens van duizenden andere <Amazon.com> aankopen volledig geautomatiseerd valt te voorspellen dat u waarschijnlijk belangstelling heeft voor een hapjespan.

3.6 Microsoft Internet Explorer[37]

Naast de persoonsgegevens die door websites worden verzameld, zoals hierboven is beschreven, blijkt ook door de internet browser Internet Explorer van Microsoft persoonsgegevens te worden verzameld en opgeslagen. Opslag zou plaats vinden in een bestand genaamd <index.dat>.[38] Internet Explorer lijkt deze persoonsgegevens op een heimelijke manier te verzamelen.

Internet Explorer (IE) houdt een geheim overzicht bij van alle webadressen die de gebruiker recentelijk heeft bezocht. IE slaat de adressen op in 'spookbestanden', die niet via de browser, noch via Windows kunnen worden verwijderd.

Een anonieme hacker met het pseudoniem The Riddler maakt melding van een onzichtbare systeemmap, waarin Microsoft het adres kopieert van iedere website die een internetgebruiker ooit heeft bezocht met Internet Explorer. Bovendien zou ook alle e-mail die de gebruiker met Microsoft Outlook heeft verstuurd, in soortgelijke spookbestanden worden opgeslagen. De informatie is alleen toegankelijk via MS-DOS.

In verschillende Windows-versies zijn de spookbestanden met het surfgedrag traceerbaar. Of ook Outlookberichten ongemerkt worden bewaard, blijft echter onduidelijk.

37. Met dank aan Joseph Shenouda, Netdetective.
38. Bron: fuckMicrosoft.com, *Microsoft's Really Hidden Files.* Op internet: <http://fuckmicrosoft.com/content/ms-hidden-files.shtml>. Laatst gewijzigd op 9 april 2003.

In Windows 95 en 98 worden de webadressen opgeslagen in het bestand:

<C:/Windows/Temporary Internet Files/Content.ie5/Index.dat>.

In Windows 2000 heet het bestand:

<C:/Documents and Settings/GEBRUIKERSNAAM/Local Settings/Temporary Internet Files/Content.IE5/Index.dat>.

Het bestand <index.dat> kan vele megabytes groot zijn en is niet zichtbaar via de Windows-verkenner – ook niet als de optie 'Verborgen mappen' en 'Bestanden weergeven' is aangevinkt. Het spookbestand is wel met enige moeite toegankelijk via MS-DOS: ga eerst naar de betreffende map en geef dan het DOS-commando dir <index.dat>.

Het bestand <index.dat> laat zich moeilijk bekijken. Het bestand openen in Word levert een foutmelding op. Wat wel lukt is <index.dat> in MS-DOS eerst naar een andere map te kopiëren, bijvoorbeeld met de opdracht: "copy index.dat c:\". De kopie is dan wél toegankelijk via de Windows-verkenner. Wie dit bestand opent in Word ziet eerst veel onherkenbare codes; pas een paar schermpjes verder verschijnen één voor één alle webadressen.

Wat Microsoft doet met deze bestanden is onduidelijk. The Riddler constateert dat er ook andere gegevens in <index.dat> voorkomt, bijvoorbeeld de naam van een tekstbestand dat hij onlangs heeft bewerkt. Op grond hiervan beschuldigt hij Microsoft ervan al zijn doen en laten op zijn computer te volgen. Harde bewijzen kan hij echter niet leveren.
Is het bestand <index.dat> de enige plaats waar webadressen ongemerkt worden opgeslagen? De Nederlandse student Ward van Wanrooij heeft het hulpprogramma Spider <http://www.fsm.nl/ward/> ontwikkeld om de rest van de harde schijf te scannen. Het kan de gevonden webadressen desgewenst ook verwijderen.

Het bestand <index.dat> is moeilijk te vernietigen. Het verwijderen van de *cache* en de *history* via Internet Explorer is niet voldoende om dit spookbestand weg te krijgen. Via MS-DOS is het wel mogelijk, zoals beschreven staat in "Microsoft's Really Hidden Files".[39]

Verder geeft het document van The Riddler de tip om speciale schoonmaakprogramma's te gebruiken, zoals Anonymizer's WindowsWasher[40] en PurgeIE.[41] Deze bieden meer soelaas. Beiden blijken voortvarend op te ruimen en na het herstarten van de computer bleek ook het bestand <index.dat> netjes opgeschoond.

39. Bron: fuckMicrosoft.com, *Microsoft's Really Hidden Files.* Op internet: <http://fuckmicrosoft.com/content/ms-hidden-files.shtml>. Laatst gewijzigd op 9 april 2003.
40. Anonymizer.com, *Online Privacy Services.* Op internet: <http://www.anonymizer.com/washer40/washer40_desc.shtml>. Laatst bezocht op 10 juni 2003.
41. PurgeIE, *Purge Cache, Cookies and Tracks for Internet Explorer.* Op internet: <http://www.aandrc.com/purgeie/>. Laatst gewijzigd op 10 mei 2003.

Hiervoor is al even gewezen op het fenomeen 'spyware'. Spyware of spionagesoftware, is een verzamelnaam voor computerprogramma's die zich vaak onmerkbaar op de harde schijf van een computer installeren om persoonsgegevens van de gebruiker te verzamelen en door te geven aan de maker van de spionagesoftware.[42] Spyware vormt samen met spam en virussen een grote plaag voor internetgebruikers.

Spyware lijkt een groeiende bedreiging te worden voor internetgebruikers.[43] Uit een onderzoek naar spyware en andere malware van Symantec Benelux blijkt dat 76% van de onderzochte computers geïnfecteerd is met zogenaamde malware. Spyware (inclusief adware) vormt daarbinnen de grootste groep. Volgens het onderzoek is 64% van de computers hiermee besmet.

Spyware, spam en andere computervirussen liggen dus op de loer. Maar in hoeverre zijn burgers zich eigenlijk bewust van deze en andere gevaren voor privacy op internet? Daarover gaan de volgende paragrafen.

3.7 Privacy surveys

3.7.1 Nederland

Eind 1988, begin 1989 werd door SWOKA, Instituut voor strategisch consumentenonderzoek, een onderzoek gedaan naar de mening van de burger over privacybescherming.[44] In die tijd blijkt de burger privacy net zo belangrijk te vinden als goede gezondheidszorg, een schoner milieu, bestrijding van werkloosheid en bestrijding van criminaliteit. Men blijkt voor informationele privacy belangrijk te vinden en men wil graag: "weten hoe anderen aan mijn persoonsgegevens gekomen zijn", "weten wat er met mijn persoonsgegevens gebeurt", en "zelf uitmaken wie informatie over mij krijgt". De onderzoekers concluderen dat de burger het gevoel heeft de controle over de eigen gegevens te verliezen, als gevolg van het ondoorzichtiger worden van het informatiebewerkende proces.

In 1993 voerde het Centrum voor Privacyonderzoek (CPO) in opdracht van het ministerie van Economische Zaken een onderzoek uit naar de beleving van privacy door consumenten.[45] Ook daaruit blijkt dat consumenten graag controle willen houden over zaken die hen persoonlijk aangaan. Voor veel consumenten is het afschermen van het

42. Zie bijvoorbeeld: *Veilig surfen op internet*: <http://www.xs4all.nl/~rpronk/spyware.htm>.
43. Zie bijvoorbeeld het bericht "64% van de thuiscomputers besmet met spyware." Safe Internet Foundation, 23 november 2004. Op internet: < http://www.sif.nl/?page=9&catid=6&object=146663>.
44. Jan Holvast, Henny van Dijk en Gerrit Jan Schep, *Privacy Doorgelicht*. Den Haag: SWOKA 1989, naar verwezen in: J. Holvast, H. Gardeniers, *Privacy, zelfregulering en internet*, Eindrapport. Mei 2001, p. 25.
45. Centrum voor Privacyonderzoek, *Geen totale geheimhouding, maar selectieve openbaarmaking*. Amsterdam, 1993, naar verwezen in: J. Holvast, H. Gardeniers, *Privacy, zelfregulering en internet*, Eindrapport, Mei 2001, p. 26.

eigen huis en van de eigen gegevens een wezenlijk aspect van privacy. Verder betekent privacy voor veel mensen dat men zelf moet kunnen bepalen wat men doet en het recht om anders te doen of te zijn dan een ander. Een afname of het ontbreken van het zelfbeschikkingsrecht of het ten onrechte verstrekken van gegevens ervaren velen als een onaanvaardbare schending van hun privacy.

Uit 1999 stamt een onderzoek naar de privacybeleving van burgers in de informatiemaatschappij, uitgevoerd door onderzoekers van SWOKA en gepubliceerd door het Rathenau Instituut.[46] Het is een onderzoek naar de privacybeleving van burgers: hoe kijken burgers tegen privacy aan in relatie tot het gebruik van persoonsgegevens? Het onderzoek is breed opgezet, maar richt zich in een specifiek onderdeel op privacy in relatie tot informatietechnologie. Daaruit blijkt dat burgers op basis van hun houding ten opzichte van privacy in relatie tot informatietechnologie grofweg in drie groepen zijn in te delen:

1. burgers die van mening zijn dat informatietechnologie nodig is in de huidige maatschappij en die daar geen privacyproblemen van ondervinden (19%);
2. burgers die vinden dat het toenemende gebruik van informatietechnologie privacyproblemen met zich meebrengt maar die echter ook van mening zijn dat de huidige maatschappij niet meer zonder informatietechnologie kan functioneren (35%);
3. burgers die van mening zijn dat de informatietechnologie een bedreiging vormt voor de privacy en dat dit in veel gevallen zou moeten zijn te voorkomen. Het gebruik van de informatietechnologie is volgens hen niet altijd noodzakelijk (47%).

Groep 1 blijkt in vergelijking met de twee andere groepen meer mannen en hoger opgeleide burgers te bevatten.

3.7.2 Europese Unie

Op Europees niveau valt te wijzen op de 'privacy surveys' die in december 2003 zijn gepubliceerd door de Europese Commissie.[47] Een van de publicaties betreft een onderzoek onder burgers in 15 EU-lidstaten en de andere onder bedrijven in 15 EU-lidstaten.

Het onderzoek onder burgers is uitgevoerd in het kader van de Standard Eurobarometer tussen 1 en 30 september 2003. Eerder zijn soortgelijke onderzoeken uitgevoerd in 1996 en in 1991. Het onderzoek uit 2003 is het eerste dat de EU burgers ondervraagt over de bescherming van persoonsgegevens en de mate waarin zij die bedreigd achten. Vanuit dat oogpunt zijn de burgers gevraagd naar hun opvattingen over het gebruik van persoonsgegevens door banken, de politie, artsen, etc.

46. G.C.J. Smink, A.M. Hamstra, H.M.L. van Dijk. *Privacybeleving van burgers in de informatiemaatschappij*. Den Haag: Rathenau Instituut 1999, Werkdocument 68.
47. Op internet: <http://www.europa.eu.int/comm/internal_market/privacy/lawreport_en.htm#actions>.

De EU burgers zijn ook gevraagd hoe zij denken over het verzamelen van persoonsgegevens via internet. Ongeveer tweederde (64%) van alle ondervraagde EU burgers vrezen voor hun privacy als zij hun persoonsgegevens, zoals hun naam, adres en geboortedatum, achterlaten op het internet. In vijf landen geldt die vrees zelfs voor 72% of meer: Zweden, Griekenland, Ierland, het Verenigd Koninkrijk en Nederland. Aan de andere kant van de schaal vreest slechts 43% van de ondervraagde burgers in Portugal voor hun privacy. In heel de EU weet 16% van de ondervraagde burgers niet of ze voor hun privacy op internet vrezen. Dat geldt voor 24% in Portugal en voor 5% in Zweden.

Gemiddeld 34% van alle EU burgers weet voorts niet of hun nationale wetgeving hun privacy op internet wel voldoende bescherming biedt. Dit geldt voor 50% in Portugal en 48% in Spanje, tegenover 19% in Finland en 25% in Nederland.

Gevraagd naar technieken om zelf toe te passen teneinde het verzamelen van persoonsgegevens via internet te beperken, zoals cookie filters, antwoordt 72% van alle EU burgers dat men daar nog nooit van heeft gehoord. Ook de percentages voor deze vraag variëren sterk per lidstaat: in Griekenland is dat 81% en in Zweden 58%. Slechts een kleine groep EU burgers heeft wel gehoord van privacybeschermende technieken en heeft die vervolgens ook wel eens gebruikt. Dit geldt voor gemiddeld 6% binnen de hele EU, maar sommige landen springen er relatief gunstig uit: Zweden (14%), Denemarken (13%) en Nederland (12%).

Degenen die er wel van hadden gehoord, maar deze technieken nog nooit hadden gebruikt werden vervolgens gevraagd naar het waarom. Als voornaamste reden wordt door 30% van deze groep genoemd dat men niet weet hoe deze technieken te gebruiken. Dit geldt voor 35% in Griekenland en 34% in Duitsland, Spanje en Italië, en voor 16% in Ierland. Als tweede wordt door 21% genoemd dat men niet weet hoe men deze gereedschappen op de computer moet installeren. Dit geldt voor 33% in Nederland en 9% in Griekenland.[48]

Tussen 15 september en 1 oktober 2003 zijn door het EOS Gallup Europe netwerk in de 15 EU lidstaten 3013 privacyfunctionarissen van bedrijven met meer dan 20 werknemers ondervraagd. Het voornaamste doel van dit onderzoek was het meten van het bewustzijn van gegevensbescherming en het algemene beeld dat daaromtrent bestaat bij het bedrijfsleven in de EU.

Er werd verschillend gereageerd op de vraag naar de mate waarin de nationale wetgeving ter bescherming van persoonsgegevens is toegesneden op de toename van de uitwisseling van persoonsgegevens, in het bijzonder als gevolg van het gebruik van internet. In

48. Een soortgelijke situatie met betrekking tot PET bestaat in de VS. Zie bijvoorbeeld Federal Trade Commission, *Staff Workshop Report: Technologies for Protecting Personal Information*. Gepubliceerd naar aanleiding van workshops in mei en juni 2003. Op Internet: <http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf>. Zie ook: <http://www.ftc.gov/bcp/workshops/technology/>.

Finland (69%), Nederland (63%) en Griekenland (59%) bestaat veel vertrouwen in de nationale wetgeving op dit punt. Dit is anders in Portugal (28%) en Italië (31%).

Een grote meerderheid van bedrijven in de EU (91%) zegt de vereisten in de regelgeving ter bescherming van persoonsgegevens belangrijk te vinden vanuit een oogpunt van een hoog niveau van gegevensbescherming voor de consument. Een kleinere meerderheid (58%) zegt dat de eisen die voortvloeien uit de gegevensbescherming niet te streng zijn. Een uitzondering hierop is Italië (66%). Tweederde van de ondervraagden is het niet eens met de stelling dat de vereisten die uit de regelgeving voortvloeien niet noodzakelijk zijn. De meeste ondervraagden erkennen derhalve de noodzaak ervan. In Griekenland en in Italië zijn de meningen hierover echter verdeeld. Daar is ongeveer de helft het eens en de andere helft oneens met de stelling.

Het onderzoek geeft ook inzicht in de mate waarin bedrijven ervaring hebben met het beveiligen van persoonsgegevens. Daaruit kan worden opgemaakt dat er slechts weinig ervaring bestaat met het toepassen van privacy enhancing technologies (PET). Slechts eenderde (32%) van de ondervraagden geeft aan dat men PET toepast. In Nederland is dat percentage het hoogst: 47%. Bijna eenderde van de ondervraagden (28%) heeft nog nooit gehoord van PET.

Een grote meerderheid van de ondervraagden (90%) geven aan dat men geen persoonsgegevens doorgeeft naar landen buiten de EU/EER. Van de bedrijven die dat wel doen geeft de meerderheid (52%) persoonsgegevens van hun klanten of consumenten door voor commerciële doeleinden.

Uit het onderzoek blijkt voorts dat er sprake is van een gebrek aan naleving bij bedrijven in de lidstaten van de regels ter bescherming van persoonsgegevens. Volgens een meerderheid (gemiddeld 39%, vooral respondenten uit Zweden, Ierland, het Verenigd Koninkrijk, Finland, Spanje, Denemarken en Nederland) wordt dat vooral veroorzaakt door een gebrek aan kennis van de regelgeving. Anderen (gemiddeld 28%, vooral respondenten uit Griekenland, Portugal en Oostenrijk) geven als mogelijke oorzaak op dat de beperkte controle op de naleving door de toezichthoudende autoriteiten een belangrijke oorzaak is. Daardoor is het risico om 'betrapt' te worden zeer gering. Tot slot brengt een aanzienlijk aantal respondenten (gemiddeld 17%, vooral respondenten uit Luxemburg, Italië en Frankrijk) naar voren dat de aanpassing door het bedrijf aan de wettelijke eisen voor gegevensbescherming zoveel tijd kost, dat de wetgeving onvoldoende wordt nageleefd.

Tenslotte volgt uit het onderzoek onder bedrijven in de EU dat de meeste respondenten (gemiddeld 67%) van mening zijn dat het feit dat men nauwelijks klachten ontvangt tot gevolg heeft dat de naleving van de wetgeving ter bescherming van persoonsgegevens geen hoge prioriteit heeft. Dit wordt met name aangegeven door de respondenten uit Finland (82%) en Spanje (81%).

3.7.3 Verenigde Staten

Privacy surveys in Nederland en EU-brede privacy surveys zijn dun gezaaid. In de VS zijn veel meer van dergelijke onderzoeken beschikbaar die ook in meerdere mate informatie verschaffen over hoe de (Amerikaanse) internet consument aankijkt tegen de bescherming van diens persoonsgegevens.

Terwijl in de VS overheidsregulering van privacy geen traditie is, blijkt uit diverse privacy surveys onder Amerikaanse burgers dat zij veel waarde hechten aan hun privacyrechten ter bescherming van hun persoonsgegevens tegen gebruik door de overheid en door het bedrijfsleven. Hieronder volgt een weergave van de (Amerikaanse) publieke opinie over privacy, zoals dat is geanalyseerd door het Electronic Privacy Information Center EPIC.[49]

Controle over verzamelen en verstrekken van persoonsgegevens

De Amerikaanse burger vindt het opt-in systeem een van de meest belangrijke privacywaarborgen. Het opt-in systeem houdt in dat een organisatie vooraf toestemming aan de burger vraagt voor het mogen verzamelen van diens persoonsgegevens. De Business-Week/Harris Poll (maart 2000) toont aan dat 86% van de internetgebruikers verlangt dat een website via het opt-in systeem vooraf om toestemming vraagt voor het verzamelen van de naam, adres, telefoonnummer of financiële gegevens over de gebruiker. Uit hetzelfde onderzoek blijkt dat 88% het opt-in systeem wenst voor het verstrekken van hun persoonsgegevens door websites aan anderen. De Pew Internet & American Life Project Poll (augustus 2000) toont aan dat 86% van de respondenten opt-in privacy policies prefereert. De voorkeur voor opt-in systemen dateert niet van vandaag of gisteren. Reeds in 1991 bleek uit de Time-CNN Poll dat 93% van de respondenten vond dat bedrijven toestemming zouden moeten hebben van de betrokkenen alvorens hun persoonsgegevens aan derden te verkopen. Het meer recente onderzoek van het Annenberg Public Policy Center (juni 2003) toont aan dat 95% van de ondervraagden vindt dat men een (wettelijk) recht moet hebben op informatie over de persoonsgegevens waarover websites beschikken.[50] Uit hetzelfde rapport blijkt overigens dat Amerikaanse volwassen burgers in het algemeen weinig kennis hebben van de mogelijkheden om hun persoonsgegevens op internet te beschermen. Slechts 9% van de ondervraagden geeft te kennen dat men wel over de kennis daarover beschikt. Uit het onderzoek blijkt dat de meeste Amerikanen nauwelijks weten hoe websites hun persoonsgegevens gebruiken en dat zij niet weten waartoe een privacystatement op een website dient. De meeste ondervraagden denken ten onrechte dat een privacystatement betekent dat een website hun persoonsgegevens niet zal doorgeven aan andere bedrijven of websites.

49. EPIC, *Public Opinion and Privacy Page.* Op internet: <http://www.epic.org/privacy/survey/default.html>. Laatst gewijzigd op 20 maart 2003.
50. Joseph Turow, *Americans and Online Privacy: The System is Broken,* A Report from the Annenberg Public Policy Center of the University of Pennsylvania, June 2003.

De burger wenst aansprakelijkheid en beveiliging

Uit de onderzoeken blijkt voorts dat de burger in het algemeen middelen wenst om inbreuken op zijn privacy aan te kunnen pakken. Uit het Pew Internet & American Life rapport (augustus 2000) blijkt dat 94% van de Amerikaanse internetgebruikers maatregelen wenst tegen inbreuken op hun privacy. Uit de Harris Poll (februari 2002) volgt dat 84% van de respondenten van mening is dat de toegang tot hun persoonsgegevens binnen organisaties beperkt dient te zijn.

De burger wenst wetgeving en geen zelfregulering

Uit diverse surveys blijkt dat de Amerikaanse burger vindt dat het huidige model van zelfregulering onvoldoende bescherming biedt voor hun privacy. De Harris Poll (februari 2002) toont aan dat 63% van de respondenten vindt dat de huidige regelingen onvoldoende bescherming bieden. Tweederde van de respondenten in de Gallop Poll (juni 2001) is voorstander van nieuwe federale wetgeving ter bescherming van online privacy. Uit een onderzoek uitgevoerd door de Markle Foundation (juli 2001) volgt dat 64% voorstander is van regelgeving ter bescherming van consumenten op internet, terwijl 58% van mening is dat zelfregulering onvoldoende garantie biedt voor een adequate regeling van aansprakelijkheden. Blijkens de BusinessWeek/Harris Poll (maart 2000) is 57% van de respondenten voorstander van wetgeving dat het gebruik van persoonsgegevens reguleert. Uit hetzelfde onderzoek blijkt dat slechts 15% voorstander is van zelfregulering. In het onderzoek van het Annenberg Public Policy Center (juni 2003) is eveneens een sterk pleidooi te vinden voor federale wetgeving dat bijvoorbeeld websites verplicht om een geautomatiseerd privacybeleid te voeren door middel van het Platform for Privacy Preferences (P3P)[51] en dat voorwaarden stelt aan de doorverstrekking van persoonsgegevens via websites.

De burger wenst anonimiteit

Diverse surveys, uitgevoerd door het Georgia Institute of Technology's Graphic, Visualization, & Usability (GVU) Center tonen herhaaldelijk aan dat de Amerikaanse burger veel waarde hecht aan anonimiteit op internet. Uit de GVU surveys volgt dat de burger het grondig eens is met de stelling dat anonimiteit op internet belangrijk is.

De burger is tegen 'web tracking'

De Amerikaanse burger is in het algemeen tegen activiteiten als 'web tracking', het volgen van internetgebruikers teneinde gebruikersprofielen op te stellen, vooral wanneer hun persoonsgegevens vervolgens worden vergeleken met gebruikersprofielen. Volgens de BusinessWeek/Harris Poll (maart 2000) is 89% van de respondenten daartegen. Uit hetzelfde onderzoek blijkt dat 63% van de respondenten tegen 'web tracking' is ook al

51. Zie meer over P3P in § 6.6 van dit boek.

wordt de 'clickstream', d.i. de stroom van achtereenvolgens bezochte internetpagina's, niet vergeleken met hun persoonsgegevens. De Pew Internet and American Life Project (augustus 2000) laat zien dat 54% van de Amerikaanse internetgebruikers tegen tracking is. Volgens de USA Weekend Poll (juli 2000) is 65% van de respondenten van mening dat 'tracking' van de computer een inbreuk op de privacy is.

Burgers vertrouwen bedrijfsleven noch overheid

Als het gaat om de verwerking van hun persoonsgegevens hebben Amerikaanse burgers weinig vertrouwen in bedrijfsleven en in de overheid. Zij verdenken beide sectoren er van misbruik te maken van hun persoonsgegevens. Een onderzoek van de American Society of Newspaper Editors (april 2001) wijst uit dat 51% van de ondervraagden erg verontrust was en 30% enigszins verontrust over het risico dat een bedrijf hun privacy zou kunnen schenden. Uit hetzelfde onderzoek blijkt dat 52% van de respondenten er erg weinig tot geen vertrouwen in heeft dat particuliere ondernemingen hun persoonsgegevens alleen zo gebruiken zoals zij beweren. De Harris Poll (februari 2002) toont aan dat een meerderheid van de consumenten er geen vertrouwen in heeft dat het bedrijfsleven netjes omgaat met hun persoonsgegevens. Uit een onderzoek van het First Amendment Center (augustus 2002) blijkt voorts dat 60% van de ondervraagden van mening is dat de Amerikaanse overheid over te veel persoonsgegevens van burgers beschikt.

Burgers hechten veel waarde aan privacy zelfbescherming

Steeds meer burgers realiseren zich dat bestaande wet- en regelgeving niet voldoende bescherming bieden voor hun persoonsgegevens. Daardoor hechten zij steeds meer waarde aan mogelijkheden tot privacy zelfbescherming. Veel burgers blijken terughoudend te zijn geworden in het afstaan van hun persoonsgegevens, of geven bewust foutieve gegevens op, of hebben verzocht om verwijdering uit adressenbestanden voor marketingdoeleinden. Volgens de Harris Poll (februari 2002) heeft 83% van de respondenten wel eens aan een bedrijf verzocht om verwijdering van hun naam en adres uit adressenbestanden voor mailings. Uit een onderzoek van de American Society of Newspaper Editors (april 2001) blijkt dat 70% van de respondenten wel eens heeft geweigerd persoonsgegevens te verstrekken aan een bedrijf omdat die te persoonlijk van aard waren. Nog eens 62% heeft die bedrijven wel eens verzocht om verwijdering van hun naam uit een adressenbestand voor marketingdoeleinden.

Burgers zijn zich niet bewust van bestaande 'tracking' methoden

Veel internetgebruikers zijn niet in staat tot het achterhalen van de meest gebruikte methode om hun surfgedrag te volgen, te weten de 'cookie'. Het onderzoek van Pew Internet and American Life Project (augustus 2000) bracht naar voren dat 56% van de Amerikaanse internetgebruikers niet in staat waren een 'cookie' te achterhalen. Nog niet duidelijk is in hoeverre die internetgebruikers wel in staat zijn om meer geavanceerde 'tracking' methoden op te sporen, zoals 'web bugs' of 'spyware'.

Burgers willen informatie

Burgers willen informatie over hoe hun persoonsgegevens worden verzameld, gebruikt en aan wie ze worden verstrekt. Dergelijke informatie is voor 75% van de burgers absoluut essentieel of zeer belangrijk, aldus blijkt uit de BusinessWeek/Harris Poll (maart 2000).

Burgers willen ook na 11 september 2001 nog privacy

Onmiddellijk na de terroristische aanslagen van 11 september 2001 bleek uit surveys dat de Amerikaanse burger bereid is om verder gaande inbreuken op hun privacy, zoals gezichtsherkenningstechnieken en uitgebreidere verzamelingen van biometrische identificatiemethoden door politiediensten te accepteren. Bovendien gaven veel Amerikanen aan een groter vertrouwen te hebben in de overheid en dat kritiek op de overheid veelal niet terecht is. Maar na verloop van tijd blijkt de algemene steun voor deze technologieën waarmee een grotere inbreuk op de privacy mogelijk is, te zijn afgenomen. Direct na de aanvallen op 11 september 2001 bleek uit de Harris Poll dat 68% van de Amerikanen een nationaal identificatiesysteem ondersteunde. In november 2001 bleek dat uit een onderzoek van de Washington Post nog maar 44% te zijn en in maart 2002, in een onderzoek van de Gartner Group, was dat nog maar 26%, terwijl 41% er zelfs tegen is. Tegelijkertijd is ook de steun van het publiek voor andere technieken voor toezicht afgenomen.

3.8 Conclusie

In dit hoofdstuk stond de tweede onderzoeksvraag centraal: "Hoe denkt de burger of consument over diens privacy op internet?" Teneinde een indicatief antwoord te vinden op die vraag is heel kort een aantal praktijkgevallen beschreven van enkele commerciële organisaties die via internet persoonsgegevens verzamelen. Omdat IP-adressen vaak herleidbaar zullen zijn tot individuele natuurlijke personen en daarom persoonsgegevens zullen zijn, kan als vuistregel worden aangenomen dat commerciële organisaties via internet persoonsgegevens verzamelen, wanneer zij dat doen door middel van IP-adressen of cookies.

Vervolgens is stil gestaan bij een aantal privacy surveys onder burgers in Nederland, de EU en de VS. Uit het Nederlandse onderzoek blijkt dat een meerderheid van de respondenten informatietechnologie als een gevaar voor de privacy beschouwt. Uit het Europese onderzoek blijkt dat ruim tweederde van de respondenten het uit privacyoogpunt riskant vindt om persoonsgegevens achter te laten op internet. Niettemin geldt voor beide genoemde Europese onderzoeken onder burgers en bedrijven dat de reacties per land nogal eens uiteen kunnen lopen. Het lijkt daarom moeilijk om de opvatting van 'de' EU burger weer te geven.

Hoewel in de VS van oudsher een voorkeur bestaat voor zelfregulering van privacybescherming in plaats van centrale overheidsregulering, blijkt dat de publieke opinie hieromtrent momenteel een belangrijke verschuiving doormaakt. Uit diverse Amerikaanse

privacy surveys blijkt dat de Amerikaanse burger een steeds grotere voorkeur krijgt voor wetgeving boven zelfregulering. Daarnaast blijkt dat de Amerikaanse burger als consument op internet de volgende aandachtspunten bij de bescherming van persoonsgegevens belangrijk vindt:

- controle over het verzamelen en verstrekken van persoonsgegevens;
- aansprakelijkheid en beveiliging;
- anonimiteit op internet;
- geen 'web tracking';
- vertrouwen in bedrijfsleven en overheid;
- privacy-zelfbescherming;
- openheid rond bestaande 'tracking' methoden;
- informatie;
- privacy ook na 11 september 2001.

Uit het feit dat veel Amerikaanse burgers deze aandachtspunten achter de bescherming van persoonsgegevens belangrijk vinden, kan voorts worden afgeleid dat de Amerikaanse burger kennelijk weinig vertrouwen heeft in de verwerking van persoonsgegevens van consumenten via internet. De Amerikaanse internetconsument wenst meer informatie en openheid rond het verwerken van diens persoonsgegevens, meer controle over het verzamelen en verstrekken daarvan en vooral bescherming tegen misbruik door middel van centrale overheidsregulering. Het vertrouwen van de consument in een effectieve bescherming van persoonsgegevens via zelfregulering door commerciële organisaties is duidelijk tanende.
Amerikaanse burgers lijken meer aansluiting te vinden bij de EU, waar men traditioneel gezien met het oog op de bescherming van persoonsgegevens meer vertrouwt op overheidsregulering. De opvattingen lijken te veranderen, zoals blijkt uit de Amerikaanse surveys. Maar ook in de EU survey komen soms grote verschillen uit de lidstaten naar voren.

In het volgende hoofdstuk wordt ingegaan op de privacybeginselen die aan overheidsregulering ten grondslag liggen en op het juridische kader voor gegevensbescherming.

4 Juridisch kader gegevensbescherming

Hoewel diverse vormen van zelfregulering kunnen worden onderscheiden (zie de hoofdstukken 5 en 6), kan zelfregulering van privacy op het internet tevens worden beschouwd in de context van bestaande internationale en nationale wet- en regelgeving, die het juridische kader vormt ter bescherming van fundamentele rechten van de burger, zoals het recht op privacy. In antwoord op het eerste deel van de derde onderzoeksvraag wordt in dit hoofdstuk ingegaan op overheidsregulering ter bescherming van persoonsgegevens.

De juridische randvoorwaarden bestaan mede uit de beginselen voor gegevensbescherming, waarmee in dit hoofdstuk wordt gestart. Vervolgens wordt aandacht besteed aan Europese regelgeving die van toepassing is op de bescherming van de consumentenprivacy op internet. In het bijzonder wordt ingegaan in op het Handvest van de Grondrechten van de EU en op diverse EU-richtlijnen.

4.1 OESO en Raad van Europa

Een achttal internationaal erkende privacybeginselen dateert reeds uit het begin van de jaren tachtig van de vorige eeuw. Ze zijn in eerste instantie te vinden in de privacyrichtlijn van 23 september 1980 van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO).[52] Kort na de aanvaarding hiervan werd op 28 januari 1981 te Straatsburg het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens gesloten. Aangezien de OESO nauw betrokken was bij de vaststelling van de verdragstekst, is het verklaarbaar waarom de daarin opgenomen minimumnormen grotendeels overeenkomen met de inhoud van de privacybeginselen uit de OESO-richtlijn. Intussen heeft de EU in de algemene privacyrichtlijn uit 1995 (Richtlijn 95/46/EG) de privacybeginselen uit het Verdrag van Straatsburg overgenomen. De uit 1980 stammende beginselen zijn nog steeds erkend als internationale beginselen voor privacybescherming en bieden nog steeds voldoende houvast bij het verzamelen van persoonsgegevens via een willekeurig medium. Ze worden nog steeds beschouwd als het fundament voor privacybescherming in wereldwijde netwerken.[53]

52. Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris 1981.
53. OECD Working Party on Information Security and Privacy, *Privacy Online: Policy And Practical Guidance*., DSTI/ICCP/REG(2002)3/FINAL, 21 January 2003, p. 5.

Deze algemene privacybeginselen vormen tevens de grondslag voor de huidige bescherming van de informationele privacy in ons land. Het verdrag is door het Koninkrijk der Nederlanden ondertekend op 21 januari 1988[54] en door het Nederlandse parlement goedgekeurd op 20 juni 1990.[55] Het bestaande Nederlandse stelsel van privacybescherming bevat aldus een nadere uitwerking van de bedoelde beginselen.[56] De maatregelen die op nationaal niveau zijn getroffen kunnen worden beschouwd als middelen waarmee invulling wordt gegeven aan de doelen die zijn neergelegd in de afzonderlijke privacybeginselen. Over de keuze van de middelen is uiteraard discussie mogelijk, hetgeen ook wordt erkend in het Verdrag van Straatsburg.[57]

De internationaal aanvaarde privacybeginselen kunnen in twee groepen worden onderscheiden. De eerste groep heeft betrekking op de persoonsgegevens als zodanig en op de voorwaarden waaronder ze mogen worden verwerkt:

1. *Collection Limitation Principle*
   (beginsel van het beperkt verzamelen van persoonsgegevens).
   Persoonsgegevens mogen niet onbeperkt worden verzameld en zij moeten worden verkregen met wettige en eerlijke middelen, waar geëigend met toestemming of medeweten van de betrokkene.

2. *Data Quality Principle*
   (beginsel van de kwaliteit van de persoonsgegevens).
   Persoonsgegevens moeten relevant zijn voor de doeleinden waarvoor zij zullen worden gebruikt en zij moeten met het oog daarop accuraat, volledig en up-to-date zijn. Het gebruik van persoonsgegevens (het verzamelen, opslaan en verspreiden ervan) moet evenzeer met de doelstelling in overeenstemming zijn.

3. *Purpose Specification Principle*
   (beginsel van de doelspecificatie).
   Persoonsgegevens mogen slechts worden verzameld voor een van tevoren gespecificeerd doel. Het gebruik van de persoonsgegevens moet beperkt blijven tot de vervulling van de gestelde doeleinden of andere doeleinden die daarmee niet onverenigbaar zijn en die worden gespecificeerd bij elke gelegenheid waarbij het doel wordt gewijzigd.

4. *Use Limitation Principle*
   (beginsel van het beperkte gebruik van persoonsgegevens).

54. *Trb.* 1988, 7.
55. *Stb.* 1990, 351.
56. Deze stelling kan worden gebaseerd op artikel 4 van het Verdrag van Straatsburg.
57. Zie de toelichting op artikel 4 in het *Explanatory Report*, p. 16.

Persoonsgegevens mogen niet worden verstrekt, toegankelijk gemaakt of anderszins gebruikt voor andere dan de gespecificeerde doeleinden, behoudens toestemming van de betrokkene of op grond van een wettelijk voorschrift. Zodra de persoonsgegevens niet langer relevant (of in het geval van medische gegevens: noodzakelijk) zijn voor het gespecificeerde doel, mogen zij niet langer in een herleidbare vorm bewaard blijven.

De tweede categorie beginselen heeft betrekking op de verplichtingen van degenen die verantwoordelijk zijn voor de gegevensverwerking en op de rechten van betrokkenen.

5. *Security Safeguards Principle*
   (beveiligingsbeginsel).
   Persoonsgegevens moeten worden beschermd met redelijke beveiligingsmaatregelen tegen verlies van of ongeoorloofde toegang tot gegevens alsmede tegen ongeoorloofde vernietiging, gebruik, verandering of uitlekken daarvan.

6. *Openness Principle*
   (transparantiebeginsel).
   Er behoort openheid te bestaan over de aanwezigheid van persoonsgegevens, hun aard, doeleinden en de identiteit en zetel van de houder van die persoonsgegevens.

7. *Individual Participation Principle*
   (beginsel van de individuele rechtsbescherming).
   De betrokkene dient het recht te hebben om van een houder van persoonsgegevens te vernemen of deze de beschikking heeft over hem betreffende persoonsgegevens. Voorts mag de betrokkene een overzicht verlangen van zijn persoonsgegevens binnen een redelijke termijn, tegen redelijke kosten, op een redelijke wijze en in een voor hem begrijpelijke vorm. De betrokkene moet tevens de mogelijkheid hebben om, wanneer een dergelijk verzoek wordt geweigerd, te vernemen wat de reden daarvoor is en om deze weigering aan te vechten. De betrokkene moet voorts het recht hebben om de aanwezigheid en de juistheid van aanwezige persoonsgegevens te betwisten en, indien hij daarin gelijk heeft, die gegevens te laten verwijderen, herstellen, aanvullen of wijzigen.

8. *Accountability Principle*
   (aansprakelijkheidbeginsel).
   De verantwoordelijke voor de verwerking van persoonsgegevens dient aansprakelijk te kunnen worden gesteld voor het niet nemen van noodzakelijke maatregelen in verband met de invulling van de genoemde principes.

Door deze indeling in een achttal privacybeginselen ontstaat al snel de indruk dat zij strikt te scheiden zijn. Dit is echter niet het geval daar zij aan elkaar gerelateerd zijn en deels elkaar overlappen. Het onderscheid moet dus ook als een kunstmatig onderscheid worden opgevat. Het neemt echter niet weg dat voor een goed begrip van de reikwijdte van deze beginselen enige structuur hierin kan worden aangebracht.

4.2 VS: Fair Information Practice Principles

In de Verenigde Staten realiseert de Federal Trade Commission (FTC) zich dat de groei van de elektronische markt exponentiële vormen aanneemt. Tegelijkertijd beschikken online winkeliers over nieuwe technische mogelijkheden om gegevens over bezoekers van hun websites te verzamelen, op te slaan, door te geven en te analyseren. Als gevolg van dit toenemende verzamelen en gebruiken van persoonlijke gegevens, is in de VS de ongerustheid bij consumenten over hun privacy toegenomen, zoals we in het vorige hoofdstuk hebben gezien. De FTC is van oordeel dat deze ongerustheid weggenomen dient te worden teneinde het vertrouwen van de consumenten in de elektronische markt, alsmede de verdere ontwikkeling van de nieuwe economie, te kunnen bevorderen.

De FTC richt zich sinds 1995 al op het onderwerp 'online privacy'. De FTC rapporteerde over dit onderwerp aan het Amerikaanse Congres in 1998, 1999 en 2000. In 2002 rapporteerde de FTC naar aanleiding van een gehouden workshop over mobiele draadloze communicatie.[58] Door de deelnemers werd daarbij gewezen op de volgende privacybedreigingen van mobiele draadloze communicatie: het verzamelen van locatiegegevens, het volgen van het draadloos bezoeken van websites en het verzamelen van grotere hoeveelheden persoonsgegevens voor 'personalisatie' doeleinden.[59]

In het rapport *Privacy Online: A Report to Congress* (1998),[60] nam de FTC een beschrijving op van de wereldwijd geaccepteerde *fair information practice principles*. Deze door de FTC gehanteerde algemene privacybeginselen zijn de volgende:

Notice

Via websites dienen consumenten op een duidelijke en opvallende manier te worden geïnformeerd over het privacybeleid. Dat houdt onder andere in dat wordt vermeld welke persoonsgegevens worden verzameld, op welke wijze deze worden verzameld (rechtstreeks of op een minder kenbare wijze, zoals via cookies), waarvoor deze gegevens worden gebruikt, op welke wijze de consument van de andere privacybeginselen (*Choice*,

58. Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues,* February 2002. Op Internet: <http://www.ftc.gov/bcp/reports/wirelesssummary.pdf>.
59. Meer over personalisatie in hoofdstuk 8 van dit boek.
60. De privacyrapporten van de FTC zijn te vinden op internet: <http://www.ftc.gov/privacy/index.html>.

Access en *Security*) gebruik kunnen maken, of de gegevens aan derden worden verstrekt en of derden gegevens verzamelen via deze website.

Choice
Via websites dienen consumenten keuzemogelijkheden te worden geboden voor het mogen gebruiken van hun gegevens voor andere doelen dan waarvoor deze oorspronkelijk zijn verzameld (bijvoorbeeld de afhandeling van een transactie). Deze keuzemogelijkheden moeten zowel betrekking hebben op intern gebruik voor secundaire doelen (zoals marketing activiteiten) als voor extern secundair gebruik (zoals het verstrekken van de gegevens aan derden).

Access
Via websites dienen consumenten op een redelijke wijze gelegenheid te worden geboden om toegang (inzage) te hebben tot hun persoonsgegevens die via de website zijn verzameld. Tevens dienen consumenten daarbij redelijke mogelijkheden te worden geboden om gegevens te (laten) verbeteren of te verwijderen.

Security
Via websites verzamelde persoonsgegevens dienen via passende maatregelen te worden beveiligd.

Enforcement
Daarnaast onderscheidt de FTC het beginsel *Enforcement*, de erkenning van een betrouwbaar mechanisme dat in sancties kan voorzien wanneer in strijd met de overige privacybeginselen wordt gehandeld, als een kritisch element van iedere vorm van overheidsregulering of zelfregulering ter bescherming van de online privacy.

In hetzelfde rapport uit 1998 zijn de resultaten opgenomen van een door de FTC gehouden empirisch privacy-onderzoek onder commerciële websites. Vrijwel alle onderzochte websites (92%) deden mee aan het verzamelen van grote hoeveelheden persoonlijke gegevens van consumenten, terwijl slechts een gering aantal (14%) de consumenten op een of andere manier daarover informeerde.

Naar aanleiding van een vervolgonderzoek, verricht door Georgetown University, werd in het FTC rapport *Self-Regulation and Privacy Online* aan het Congres in 1999 door een meerderheid van de commissie aanbevolen om meer tijd te geven voor zelfregulerende activiteiten. Tegelijkertijd werd de industrie opgeroepen daarbij de *fair information practice principles* te implementeren.

In februari en maart 2000 verrichte de FTC opnieuw een onderzoek onder een aantal druk bezochte commerciële websites.[61] Het onderzoek concentreerde zich op twee groepen: een random groep van 335 websites en een groep bestaande uit 91 van de 100 meest bezochte websites. Dit onderzoek bevestigde nog eens de resultaten uit 1998, dat de websites een grote hoeveelheid persoonlijke informatie verzamelen over hun bezoekers. Zo verzamelen ze bijna allemaal (97% uit de random-groep en 99% uit de meest populaire websites) een e-mail adres of andere soorten identificerende persoonsgegevens.

De resultaten van het FTC onderzoek uit 2000 laten voorts zien dat het aantal websites dat althans iets over privacy vermeldt ten opzichte van 1998 is toegenomen: 88% van de random-groep en 100% van de meest populaire websites). Behalve het tellen van privacymededelingen, heeft de FTC de mededelingen ook inhoudelijk geanalyseerd in het licht van de vier *fair information practice principles*: *Notice, Choice, Access* en *Security*. Daaruit volgde dat slechts 20% van de websites uit de random-groep die persoonlijke gegevens verzamelen en 42% van de meest populaire websites alle vier de beginselen heeft geïmplementeerd. Voorts constateerde de FTC dat slechts 41% van de websites uit de random-groep en 60% van de meest populaire websites de meest eenvoudig te realiseren basisbeginselen (*Notice* en *Choice*) hebben geïmplementeerd.

Intussen zijn door de industrie diverse zelfreguleringsinitiatieven (*online privacy seal programs*) opgezet. De FTC verwacht in het algemeen dat dergelijke initiatieven de implementatie van online privacybescherming zullen vergemakkelijken. Hoewel het aantal websites dat zich bij dergelijke initiatieven heeft aangesloten ten opzichte van het jaar ervoor is toegenomen, leerde het in 2000 gepubliceerde onderzoek dat slechts 8% van de websites uit de random-groep en 45% van de meest populaire websites een privacy-logo (zoals dat van *TRUSTe*) op de website voert.

Zoals blijkt uit het rapport van 2000, acht de FTC het evident dat online privacy een enorme uitdaging blijft voor overheidsbeleid. Voorts juicht de FTC de pogingen vanuit het bedrijfsleven tot zelfregulering toe en hoopt op continuering daarvan. Uit het onderzoek trekt de FTC echter de conclusie dat deze zelfreguleringsinitiatieven vanuit het bedrijfsleven op zichzelf niet tot voldoende privacybescherming op de elektronische markt kunnen leiden. Hoewel de rol van zelfregulering van belang blijft, is de FTC van mening dat het Amerikaanse Congres in aanvulling daarop wetgevingsinitiatieven dient te nemen.

Een dergelijk initiatief zou moeten leiden tot een minimum niveau van privacybescherming door op consumenten gerichte commerciële websites. Dit minimum niveau zou moeten leiden tot een standaardpraktijk met betrekking tot het online verzamelen van persoonsgegevens en een organisatie die meer gedetailleerde standaarden moet kunnen bevorderen.

61. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress*. May 2000. Op internet: <http://www.ftc.gov/privacy/index.html>.

Wanneer commerciële websites persoonsgegevens verzamelen, zouden zij in ieder geval dienen te voldoen aan de vier *fair information practice principles: Notice, Choice, Access* en *Security*.

Vergeleken met de Safe Harbor Principles, valt op dat deze naast de beginselen *Notice*, *Choice*, *Access* en *Security* nog drie andere beginselen omvatten, te weten: *Onward Transfer*, *Data Integrity* en *Enforcement*.[62]

4.3 Handvest van de Grondrechten van de Europese Unie

De Europese Raad van 3 en 4 juni 1999 te Keulen had besloten een forum op te richten dat ermee belast was om vóór de Europese Raad van december 2000 een ontwerp-handvest van de grondrechten van de Europese Unie voor te leggen. Dit forum, "Conventie" genoemd, omvatte vijftien persoonlijke vertegenwoordigers van de staatshoofden of regeringsleiders van de lidstaten, één vertegenwoordiger van de Commissie, zestien leden van het Europees Parlement, en dertig leden van de nationale parlementen (twee per parlement). Tot voorzitter werd gekozen de heer Roman Herzog, voormalig president van de Bondsrepubliek Duitsland, die werd bijgestaan door een redactiecomité (presidium), bestaande uit de heer Nikula (Finland), gevolgd door de heer Bacelar de Vasconcelos (Portugal) en vervolgens door de heer Braibant (Frankrijk), vice-voorzitter, als vertegenwoordiger van de groep van persoonlijke vertegenwoordigers, Commissielid Vitorino, als vertegenwoordiger van de Commissie, de heer Mendez de Vigo, vice-voorzitter, als vertegenwoordiger van de groep van leden van het Europees Parlement, de heer Gunnar Jansson, vice-voorzitter, als vertegenwoordiger van de groep van leden van de nationale parlementen. Het secretariaat van de Conventie werd waargenomen door het secretariaat-generaal van de Raad.

De besprekingen van de Conventie waren openbaar en alle voorbereidende werkzaamheden zijn via internet verspreid. De ombudsman, vertegenwoordigers van het Economisch en Sociaal Comité en van het Comité van de Regio's, vertegenwoordigers van de civiele maatschappij en van de kandidaat-lidstaten zijn gehoord. Het Hof van Justitie van de Europese Gemeenschappen en de Raad van Europa hebben als waarnemers aan de besprekingen deelgenomen.

Op 17 december 1999 heeft de Conventie haar eerste vergadering gehouden. Op 26 september 2000 waren de verschillende groepen van oordeel dat zij het ontwerp-handvest konden goedkeuren. Voorzitter Herzog oordeelde op 2 oktober 2000 dat het ontwerp-handvest door alle partijen kon worden aangenomen. Vervolgens stuurde hij de tekst naar de Europese Raad. Tijdens de bijeenkomst van de staatshoofden en regeringsleiders op 13 en 14 oktober 2000 te Biarritz is besloten het Europees Parlement, de Raad van de Europese Unie en de Commissie te verzoeken het handvest goed te keuren. Het Handvest van de grondrechten van de Europese Unie is plechtig afgekondigd tijdens de

62. Zie § 5.6 in dit boek.

Europese Raad van Nice van 7 tot en met 9 december 2000 en ondertekend te Rome op 29 oktober 2004.

De preambule van het Handvest luidt als volgt:

> De volkeren van Europa hebben door onderling een steeds hechter verbond tot stand te brengen besloten een op gemeenschappelijke waarden gegrondveste vreedzame toekomst te delen.
>
> Zich bewust van haar geestelijke en morele erfgoed vestigt de Unie haar grondslag op de ondeelbare en universele waarden van menselijke waardigheid en van vrijheid, gelijkheid en solidariteit; zij berust op het beginsel van de democratie en het beginsel van de rechtsstaat. Zij stelt de mens centraal in haar optreden door het burgerschap van de Unie in te stellen en een ruimte van vrijheid, veiligheid en rechtvaardigheid tot stand te brengen.
>
> De Unie draagt bij aan de instandhouding en de ontwikkeling van deze gemeenschappelijke waarden, met inachtneming van de verscheidenheid van de culturen en tradities van de volkeren van Europa, alsmede van de nationale identiteit van de lidstaten en van hun staatsinrichting op nationaal, regionaal en lokaal niveau; zij tracht een evenwichtige en duurzame ontwikkeling te bevorderen en verzekert het vrije verkeer van personen, goederen, diensten en kapitaal, alsmede de vrijheid van vestiging.
>
> Daartoe is het noodzakelijk de bescherming van de grondrechten in het licht van de ontwikkelingen in de maatschappij, de sociale vooruitgang en de wetenschappelijke en technologische ontwikkelingen, te versterken door die rechten zichtbaarder te maken in een handvest.
>
> Onder eerbiediging van de bevoegdheden en taken van de Gemeenschap en de Unie en van het subsidiariteitsbeginsel, bevestigt dit handvest de rechten die met name voortvloeien uit de gemeenschappelijke constitutionele tradities en internationale verplichtingen van de lidstaten, uit het Verdrag betreffende de Europese Unie en de communautaire Verdragen, uit het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, uit de door de Gemeenschap en de Raad van Europa aangenomen sociale handvesten, alsook uit de jurisprudentie van het Hof van Justitie van de Europese Gemeenschappen en van het Europees Hof voor de Rechten van de Mens.
>
> Het genot van deze rechten behelst verantwoordelijkheden en plichten jegens de medemens, alsmede jegens de mensengemeenschap en de toekomstige generaties. Derhalve erkent de Unie de hieronder vermelde rechten, vrijheden en beginselen.

Artikel II-67, dat volgens de titel de eerbiediging van het privé-leven en veiligheid van zijn persoon beschermt, luidt als volgt:

> Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

De in artikel II-67 gewaarborgde rechten corresponderen met de rechten die in artikel 8 van het EVRM zijn gewaarborgd. Om rekening te houden met de technische ontwikkelingen is het woord “correspondentie” vervangen door “communicatie”.

Conform artikel II-112, lid 3, heeft dit recht dezelfde inhoud en reikwijdte als het recht in de daarmee corresponderende bepaling van het EVRM. Dit heeft tot gevolg dat de beperkingen die er rechtmatig aan kunnen worden gesteld, dezelfde zijn als die welke in het kader van voornoemd artikel 8 toegestaan zijn:

1. Eenieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voorzover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Naast dit algemene artikel, dat het privé-leven in ruime zin, als bedoeld in artikel 8 EVRM, beoogt te beschermen, kent het Handvest een specifiek artikel II-68, dat als titel de bescherming van persoonsgegevens heeft:

1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op inzage in de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.

Dit artikel is gebaseerd op artikel 286 van het Verdrag tot oprichting van de Europese Gemeenschap en op Richtlijn 95/46/EG[63], alsmede op artikel 8 van het EVRM en op het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, dat door alle lidstaten is bekrachtigd.

Het recht op bescherming van persoonsgegevens wordt uitgeoefend onder de bij bovengenoemde richtlijn gestelde voorwaarden en kan onder de bij artikel II-112 van het handvest bepaalde voorwaarden worden beperkt.

Een dergelijke scheiding tussen de bescherming van het privé-leven enerzijds en de bescherming van persoonsgegevens anderzijds, kent zowel voorstanders[64] als tegenstanders[65]. Blok wijst er op dat in Duitsland en in de VS inzake privacybescherming ook onderscheid wordt gemaakt tussen enerzijds de belangen die samenhangen met de verspreiding van persoonsgegevens en anderzijds belangen die betrekking hebben op de vrijheid van invulling van iemands privé-leven, zoals het kiezen van een partner en het krijgen van een kind.

63. Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. *PbEG* L 281 van 23.11.1995.
64. P.H Blok, De splitsing van privacy. Advies over het grondrecht op privacy in het digitale tijdperk. *Ars Aequi* 2001, nr.6, p. 435 e.v
65. Rapport Commissie "Grondrechten in het digitale tijdperk", Den Haag: Commissie Grondrechten in het digitale tijdperk, Mei 2000 (www.minbzk.nl/gdt), p. 115-135.

De Commissie Grondrechten in het digitale tijdperk adviseert in haar rapport aan de regering dat een aanpassing van het huidige artikel 10 Gw niet nodig is. Volgens de commissie zijn de regels inzake bescherming van persoonsgegevens afdoende om de gevolgen van een Grondwetswijziging in het licht van het digitale tijdperk door te laten werken in de geldende formele wetgeving. De Commissie realiseert zich dat de regelingsopdrachten van het tweede en derde lid van artikel 10 Gw uitsluitend betrekking hebben op de verwerking van persoonsgegevens. Tevens stelt de Commissie vast dat de bescherming van de persoonlijke levenssfeer zich niet beperkt tot het gebruik van persoonsgegevens. Niettemin handhaaft de Commissie in haar voorstel voor een nieuw artikel 10 Gw het recht op eerbiediging van de persoonlijke levenssfeer in het eerste lid, en de regelingsopdrachten in verband met de verwerking van persoonsgegevens in het tweede en derde lid van hetzelfde artikel.

4.4 Richtlijn 95/46/EG

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 is de algemene EU-privacyrichtlijn die de basis vormt voor de bescherming van persoonsgegevens binnen de EU. Uiterlijk 24 oktober 1998 hadden alle EU lidstaten hun nationale wetgeving aangepast moeten hebben aan deze richtlijn. In Nederland is daar invulling aan gegeven door middel van de Wet bescherming persoonsgegevens die op 1 september 2001 in werking is getreden.[66]

Zoals uit de titel van de EU privacyrichtlijn blijkt, is de bescherming van het grondrecht op privacy niet de enige drijfveer achter deze richtlijn. De richtlijn, die afkomstig is van het Directoraat-Generaal Interne Markt, dient tevens beschouwd te worden als een middel om een interne markt binnen de EU te realiseren. Realisatie van de interne markt zou bevorderd moeten worden door handelsbelemmeringen, zoals onvoldoende bescherming van persoonsgegevens, zoveel mogelijk weg te nemen.

De richtlijn bevat de algemene voorwaarde dat uitsluitend op een eerlijke en rechtmatige wijze persoonsgegevens mogen worden verwerkt. Voorts bevat de richtlijn voorschriften met betrekking tot de reikwijdte van de richtlijn, de informatieplichten, het bewaren van persoonsgegevens, de rechten van betrokkenen, vertrouwelijkheid en beveiliging.

Alvorens tot de inhoud van de richtlijn over te gaan, zij in de eerste plaats gewezen op de vraag naar de reikwijdte van de EU privacyrichtlijn, en als gevolg daarvan de reikwijdte van de nationale implementatiewetten. De Artikel 29 Groep heeft daarover een duidelijk

66. Wet van 6 juli 2000, *Stb.* 302, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

standpunt ingenomen dat, voor zover het betrekking heeft op internet, op het volgende neerkomt.[67]

Artikel 4 van de richtlijn is in artikel 4 Wbp geïmplementeerd. In artikel 4 Wbp is bepaald dat de Nederlandse wet in een tweetal bijzondere gevallen van toepassing is. In de eerste plaats is dat het geval wanneer persoonsgegevens worden verwerkt "in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland". Wanneer bijvoorbeeld een Amerikaanse multinational een vestiging in Nederland heeft, die persoonsgegevens verwerkt, is de Wbp daarop van toepassing. Volgens de richtlijn maakt het daarvoor geen verschil of de vestiging een bijkantoor is of een dochteronderneming met rechtspersoonlijkheid.[68] Wanneer een onderneming meerdere vestigingen heeft in verschillende EU lidstaten, dan dienen al die vestigingen te voldoen aan de eisen die de desbetreffende nationale regels inzake de bescherming van persoonsgegevens daaraan stellen.

Het tweede geval betreft de situatie waarin een verantwoordelijke geen vestiging heeft in de EU, maar wel gebruik maakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden. Ook in dat geval is de Wbp van toepassing. Dat geldt dus bijvoorbeeld in het geval persoonsgegevens door een Amerikaanse website aanbieder worden verzameld door middel van een computer die zich in Nederland bevindt. Daarvan is bijvoorbeeld sprake wanneer die Amerikaanse website aanbieder cookies plaatst op de computer van de internetgebruiker in Nederland. De Amerikaanse website aanbieder heeft daarmee feitelijke macht verkregen over deze gegevens. De Wbp is niet van toepassing wanneer die middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens, dus wanneer bijvoorbeeld geen cookies worden vastgelegd.

Volgens de Artikel 29 Groep heeft de EU uitdrukkelijk gekozen voor toepassing van de richtlijn c.q. nationale wet, zelfs wanneer de verantwoordelijke geen vestiging in de EU heeft (bijvoorbeeld een Amerikaanse website) maar voor de verwerking van persoonsgegevens wel gebruik maakt van geautomatiseerde middelen die zich in een van de EU lidstaten bevinden. De locatie van de geautomatiseerde middelen is in dat geval de doorslaggevende factor. Dat betekent dat de bescherming ook geldt voor Amerikaanse of Chinese burgers die een Amerikaanse website bezoeken vanaf het grondgebied van de EU.[69]

---

67. Groep Gegevensverwerking Artikel 29, *Werkdocument Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* goedgekeurd op 21 november 2000, WP 37, p. 30; maar ook: Groep Gegevensbescherming Artikel 29, *Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU,* goedgekeurd op 30 mei 2002, WP 56, p. 7. Beide documenten zijn te vinden op Internet, via: <http://www.europa.eu.int/comm/internal_market/privacy/workingroup_en.htm>.
68. Preambule 19.

Verschillende maatregelen kunnen bijdragen aan de handhaving van deze op het eerste gezicht vreemde consequentie dat de Nederlandse Wbp van toepassing is op wellicht duizenden Amerikaanse website aanbieders.[70] In de eerste plaats kan bewustwording bij zowel de Nederlandse of Europese internetgebruiker als bij de buitenlandse website aanbieder bijdragen aan het respecteren van de bescherming van persoonsgegevens. Daarnaast kunnen technologische maatregelen bijdragen aan een daadwerkelijke bescherming van persoonsgegevens in internationale verhoudingen. Het is bijvoorbeeld mogelijk om software zodanig aan te passen dat wanneer daarmee persoonsgegevens worden verzameld, dit geschiedt met inachtneming van de Europese voorschriften. Buitenlandse websites die aldus met inachtneming van de Europese voorschriften persoonsgegevens van Europese burgers verwerken, zouden bijvoorbeeld een Europees privacystempel kunnen krijgen.

Wanneer de richtlijn van toepassing is, mogen persoonsgegevens slechts eerlijk en rechtmatig worden verzameld en verwerkt. Deze voorwaarde is in het bijzonder van belang bij het verwerken van persoonsgegevens via internet, omdat in veel gevallen persoonsgegevens van internetgebruikers op 'onzichtbare' wijze worden verzameld en verwerkt. Het ontbreekt de internetgebruiker veelal aan transparantie inzake de persoonsgegevens die over hem worden verzameld wanneer die gebruiker zich op het internet bevindt. De richtlijn heeft tot gevolg dat ook voor het verzamelen van persoonsgegevens via internet de betrokkene daarover voldoende geïnformeerd moet kunnen zijn. De informatie dient met name betrekking te hebben op de identiteit van de verantwoordelijke en de doelen waarvoor de persoonsgegevens worden verzameld.

Wanneer persoonsgegevens op een eerlijke en rechtmatige wijze via internet zijn verzameld, mogen die slechts worden gebruikt ('verder verwerkt') voor zover het doel van het gebruik verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld. Voorbeelden van onverenigbaar gebruik zijn het doorgeven van transactiegegevens aan derden ten behoeve van het opstellen van kopersprofielen voor reclamecampagnes, of ook het met behulp van data mining opstellen van gedragspatronen aan de hand van lijsten van websites die door een internetgebruiker zijn bezocht.[71]

69. Groep Gegevensbescherming Artikel 29, *Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU,* goedgekeurd op 30 mei 2002, WP 56, p. 7.
70. Groep Gegevensbescherming Artikel 29, *Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU,* goedgekeurd op 30 mei 2002, WP 56, p. 15.
71. Groep Gegevensverwerking Artikel 29, *Werkdocument Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* goedgekeurd op 21 november 2000. WP 37, p. 77. Meer over data mining en persoonlijkheidsprofielen in hoofdstuk 8 van dit boek.

Voorts dient elke verwerking (ook elk gebruik) te berusten op een rechtmatige grondslag. Die grondslag dient in elk geval een van de volgende te zijn:

a) de betrokkene heeft daarvoor zijn ondubbelzinnige toestemming verleend, of
b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene, of
c) de verwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is, of
d) de verwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene, of
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, drager is opgedragen, of
f) de verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van artikel 1, lid 1, van deze richtlijn, niet prevaleren.[72]

Toestemming is dus niet altijd vereist, ook niet voor het verwerken van persoonsgegevens via internet. Wanneer een consument via internet een boek of CD bestelt, zal de verwerking van diens persoonsgegevens kunnen worden gebaseerd op de noodzakelijkheid ter uitvoering van een overeenkomst.

De informatieplicht van artikel 10 van de EU privacyrichtlijn houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens aan de betrokkenen voldoende informatie verschaft. Die informatie dient bijvoorbeeld te bestaan uit: de identiteit van de verwerker, het doel van de verwerking, de partijen voor wie de informatie bestemd is, of beantwoording van vragen vrijwillig wordt gegeven dan wel verplicht is, wat de consequenties zijn van het uitblijven van beantwoording en of een betrokkene recht heeft op kennisneming en correctie van zijn gegevens. Voorts moet de betrokkene worden geïnformeerd indien hij bezwaar kan maken tegen de verwerking. De informatie kan worden verstrekt door middel van de internetpagina van de verantwoordelijke. Teneinde te kunnen garanderen dat de consument in de gelegenheid is geweest de informatie te lezen, is het mogelijk daarvan een verplicht onderdeel te maken van het transactieproces.

72. Artikel 7 van de EU privacyrichtlijn.

Identificeerbare persoonsgegevens mogen op grond van artikel 6, lid 1, onder e) van de EU privacyrichtlijn niet langer worden bewaard dan nodig is voor het doel waarvoor de gegevens zijn verzameld. Richtlijn 2002/58/EG (richtlijn privacy en elektronische communicatie) bevat nadere voorschriften voor het bewaren van verkeersgegevens (zie hierna).

Voorts beschikken betrokkenen (consumenten, internetgebruikers) over een recht op inzage, correctie en verzet. Deze rechten gelden uiteraard ook voor persoonsgegevens die via internet zijn verzameld. De verantwoordelijke is dan ook verplicht om duidelijke en efficiënte procedures aan te bieden waardoor de betrokkenen hun rechten kunnen effectueren. De betrokkenen hebben er recht op te weten of er in zijn bestanden relevante persoonsgegevens aanwezig zijn en, zo ja, welke dan worden verwerkt, wat de bron ervan is, wat het doel is van de verwerking, welke soorten gegevens het betreft en voor welke of welke soorten partijen de te verwerken gegevens bestemd zijn. Het ligt voor de hand dat deze informatie, wanneer die via internet is verzameld, ook via internet toegankelijk te maken voor de betrokkene.[73] Betrokkenen hebben ook recht op inzage in hun gegevens wanneer die zijn verwerkt door middel van profielvorming, classificatie of categorisering of wanneer er gegevens uit andere bronnen aan zijn toegevoegd.[74]

De verantwoordelijke is verplicht passende maatregelen te treffen om de door hun klanten verstrekte informatie te beschermen tegen ongeautoriseerde inzage of overdracht. Deze verplichting geldt in het bijzonder als de verwerking gegevenstransmissie via een netwerk met zich brengt zoals in het geval van elektronische transacties op internet. De beveiligingsmaatregelen moeten zijn afgestemd op de risico's met betrekking tot veiligheid en vertrouwelijkheid, de aard van de gegevens en de stand van de techniek.

4.5 Richtlijn 97/7/EG inzake verkoop op afstand

Zoals we in de inleiding al zagen, bestaat de kern van de privacy-uitdaging voor de nieuwe economie uit het creëren van voldoende vertrouwen van de consument. Dat vertrouwen kan in belangrijke worden bevorderd door middel van openheid (transparantie) en – in samenhang daarmee – goede voorlichting aan de consument. Wie goederen en diensten online aanbiedt, zal bij het verwerken van persoonsgegevens van de consument, deze duidelijk moeten voorlichten over bijvoorbeeld de identiteit van de verwerker, het doel van de verwerking, de partijen voor wie de informatie bestemd is, of beantwoording van vragen vrijwillig wordt gegeven dan wel verplicht is, wat de consequenties zijn van het uitblijven van beantwoording en of een betrokkene recht heeft op kennisneming en

73. Groep Gegevensverwerking Artikel 29, *Werkdocument Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* goedgekeurd op 21 november 2000, WP37, p. 79.
74. Groep Gegevensverwerking Artikel 29, *Werkdocument Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming*, goedgekeurd op 21 november 2000, WP37, p. 79.

correctie van zijn gegevens. Deze informatieplicht vloeit voort uit de hierboven genoemde Richtlijn 95/46/EG.

Op grond van Richtlijn 97/7/EG[75] bestaan nog enkele andere informatieplichten voor de aanbieder van goederen en diensten op afstand. Deze richtlijn is inmiddels geïmplementeerd in het Nederlandse Burgerlijk Wetboek.[76] Op grond van artikel 7:46c, lid 1, BW moet aan de consument die op afstand, bijvoorbeeld via internet, een koopovereenkomst sluit de volgende informatie worden verstrekt:

- de identiteit en, indien de koop op afstand verplicht tot vooruitbetaling van de prijs of een gedeelte daarvan, het adres van de verkoper;
- de belangrijkste kenmerken van de zaak;
- de prijs, met inbegrip van alle belastingen, van de zaak;
- voor zover van toepassing: de kosten van aflevering;
- de wijze van betaling, aflevering of uitvoering van de koop op afstand;
- het al dan niet van toepassing zijn van de mogelijkheid van ontbinding overeenkomstig de artikelen 46d lid 1 en 46e;
- indien de kosten van het gebruik van de techniek voor communicatie op afstand worden berekend op een andere grondslag dan het basistarief: de hoogte van het geldende tarief;
- de termijn voor de aanvaarding van het aanbod, dan wel de termijn voor het gestand doen van de prijs;
- voor zover van toepassing, in geval van een koop op afstand die strekt tot voortdurende of periodieke aflevering van zaken: de minimale duur van de overeenkomst.

Dergelijke informatie komt men veelal tegen in de algemene voorwaarden. In principe is het juridisch gezien aanvaardbaar dat algemene voorwaarden via een internetpagina ter beschikking van de consument worden gesteld.[77] Van belang is dat de consument kennis kan nemen van de algemene voorwaarden, waardoor aangenomen mag worden dat de consument daarmee bekend is of ten minste geacht kan worden daarmee bekend te zijn.

Deze redenering kan analoog worden toegepast wanneer informatie over het verwerken van persoonsgegevens wordt verstrekt. Veelal gebeurt dat via zogeheten privacystatements op een internetpagina. In beginsel kan de consument dan kennis nemen van de informatie over het verwerken van diens persoonsgegevens. Met het oog op het verkrijgen van vertrouwen van de consument, in het bijzonder met betrekking tot de zorgvul-

75. Richtijn 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten. *PbEG* L 144.
76. Boek 7, Titel 1, Afdeling 9A: Overeenkomsten op afstand.
77. Zie bijvoorbeeld R.E. van Esch, 'Recente ontwikkelingen in het vermogensrecht op het terrein van de elektronische handel'. In: *WPNR: Weekblad voor Privaatrecht, Notariaat en Registratie*, 28 april 2001, jrg. 132, nr. 6443, p. 378, waar hij verwijst naar het arrest van de HR 1 oktober 1999, *NJ* 2000, 207.

dige verwerking van persoonsgegevens, verdient het aanbeveling om informatie over het verwerken van persoonsgegevens in een afzonderlijk privacystatement op te nemen en niet als onderdeel van de algemene voorwaarden.

4.6 Richtlijn 2000/31/EG inzake elektronische handel

Ook de EU Richtlijn 2000/31/EG[78] inzake elektronische handel (e-commerce) kent zogeheten transparantiebepalingen teneinde het vertrouwen van de consument in elektronische handel te bevorderen.[79] De transparantiebepalingen zijn te vinden in artikel 5 van de Richtlijn. Wie op elektronische wijze goederen of diensten aanbiedt, moet de volgende informatie voor de wederpartij (de consument) gemakkelijk, rechtstreeks en permanent toegankelijk maken:

- naam van de aanbieder;
- het adres waar de aanbieder is gevestigd;
- de adresgegevens die een snel contact en een rechtstreekse en effectieve communicatie met de aanbieder mogelijk maken, met inbegrip van diens e-mailadres;
- het nummer van inschrijving van de aanbieder in het handelsregister;
- voorzover een vergunning is vereist, gegevens over de bevoegde toezichthoudende autoriteit (bijvoorbeeld op grond van de Wet toezicht kredietwezen 1992);
- het BTW-nummer van de aanbieder.

Deze informatie mag worden gepubliceerd op een internetpagina en toegankelijk worden gemaakt door middel van een hyperlink.

Voorts is de aanbieder op grond van artikel 10, lid 1, van de Richtlijn verplicht om vóór het sluiten van de overeenkomst aan de afnemer (consument) de volgende informatie op duidelijke, begrijpelijke en ondubbelzinnige wijze te verstrekken:

- de verschillende voor de sluiting van de overeenkomst te volgen technische stappen;
- het al dan niet archiveren van de overeenkomst en de toegankelijkheid daarvan;
- de technische hulpmiddelen om invoerfouten op te sporen en te corrigeren voordat de order wordt geplaatst;
- de talen waarin de overeenkomst kan worden gesloten.

78. Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel in de interne markt (Richtlijn inzake elektronische handel), *PbEG* 2000, l 178/1.
79. Zie hierover o.a.: R.E. van Esch, 'Elektronische handel'. In: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer,* Deventer: Kluwer 2001 (vierde druk), p. 143.

Het is twijfelachtig of aan deze informatieplicht wordt voldaan wanneer de toegankelijkheid wordt vorm gegeven door middel van een hyperlink. Aan de informatieplicht wordt wel voldaan wanneer de website zo is ingericht dat de wederpartij (de consument) eerst door een aantal pagina's dient te scrollen waarop de bedoelde informatie staat vermeld, alvorens een overeenkomst met de aanbieder af te kunnen sluiten.

Op grond van het tweede lid van artikel 10 van deze richtlijn dient de aanbieder tevens aan te geven welke gedragscodes hij heeft onderschreven en dient hij informatie te verstrekken aan de consument over de wijze waarop die gedragscodes elektronisch zijn te raadplegen.

4.7 Richtlijn 2002/58/EG inzake privacy en elektronische communicatie

Richtlijn 2002/58/EG[80] inzake privacy en elektronische communicatie is de vervanger van Richtlijn 97/66/EG (Richtlijn privacy en telecommunicatie of ISDN-richtlijn). Richtlijn 97/66/EG is per 31 oktober 2003 ingetrokken.

Een belangrijke wijziging in de nieuwe richtlijn betreft de reikwijdte. Waar de oude richtlijn betrekking had op privacy en *telecommunicatie*, voorziet de nieuwe richtlijn in de bescherming van privacy bij *elektronische communicatie*. Een van de doelstellingen van deze nieuwe richtlijn is de bescherming van het recht op privacy op internet. Dat komt duidelijker tot uitdrukking in het begrip *elektronische communicatie* dan in het begrip *telecommunicatie*.

Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken in de Gemeenschap. De term *elektronische communicatiediensten* is niet gedefinieerd in deze richtlijn, maar wel in artikel 2, onder c), van de Kaderrichtlijn.[81] het voorstel voor een richtlijn inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten. De definitie luidt:

> Een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische-communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt doch niet de dienst waarbij met behulp van elektronische-communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Hij omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van Richtlijn 98/34/EG, die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische-communicatienetwerken.

80. Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), *PbEG* 2002, L 201/37.
81. Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (Kaderrichtlijn), *PbEG*, L 108 van 24.4.2002.

De nieuwe Richtlijn 2002/58/EG regelt vanuit privacy-oogpunt een viertal interessante onderwerpen, te weten: het gebruik van cookies, het verwerken van 'verkeersgegevens', het verwerken van 'locatiegegevens' en het versturen van ongevraagde elektronische communicatie (vaak 'spam' genoemd). Hier wordt kort stil gestaan bij de cookies, de verkeersgegevens en ongevraagde elektronische communicatie.

4.7.1 Cookies

Het gebruik van *cookies* is in artikel 5, derde lid, van de richtlijn geregeld. De term 'cookies' wordt hier weliswaar niet gebezigd. De richtlijn draagt de lidstaten op ervoor te zorgen dat het gebruik van elektronische-communicatienetwerken voor *de opslag van informatie of voor het verkrijgen van toegang tot informatie die is opgeslagen in de eindapparatuur van een abonnee of gebruiker*, alleen is toegestaan wanneer de betrokken gebruiker duidelijk en volledig wordt geïnformeerd over onder andere de doeleinden van deze verwerking, en het recht krijgt aangeboden om een dergelijke verwerking te weigeren. Een website aanbieder mag dus alleen een *cookie* plaatsen op de computer van de internetgebruiker wanneer dat uitdrukkelijk wordt meegedeeld en de internetgebruiker de *cookie* kan weigeren. Het weigeren van een *cookie* kan, aldus artikel 5, derde lid, van de richtlijn, echter tot gevolg hebben dat de toegang tot een bepaalde website wordt geweigerd.

4.7.2 Verkeersgegevens

Verkeersgegevens worden in de richtlijn gedefinieerd als 'gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan'. Aanbieders van elektronische-communicatienetwerken of -diensten zijn verplicht om deze verkeersgegevens van hun abonnees en gebruikers te wissen of te anonimiseren, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie. Op deze plicht tot wissen of anonimiseren bestaan echter twee uitzonderingen. Voor de facturering van abonnees en interconnectiebetalingen, mogen verkeersgegevens bewaard blijven tot het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen. In de tweede plaats mogen de netwerk- en dienstenaanbieders verkeersgegevens bewaren voor de marketing van elektronische-communicatiediensten of voor de levering van diensten met toegevoegde waarde. Een voorwaarde is wel dat de abonnee of de gebruiker daarvoor toestemming heeft gegeven, welke toestemming overigens te allen tijde kan worden ingetrokken.

4.7.3 Ongevraagde elektronische communicatie

Richtlijn 2002/58/EG bevat in artikel 13 een regeling voor het ongevraagd sturen van elektronische berichten voor direct marketing doeleinden. Deze regeling is vooral bedoeld ter bestrijding van zogeheten 'spam' berichten, die bijvoorbeeld per e-mail of per SMS in één keer naar grote groepen ontvangers kunnen worden verstuurd. Het begrip

'direct marketing' omvat niet alleen communicatie voor commerciële doeleinden, maar ook communicatie voor ideële en charitatieve doeleinden.[82]

Onder de oude richtlijn 97/66/EG gold het vereiste van toestemming vooraf (het opt-in systeem) voor direct marketing door middel van automatische oproepapparaten en door fax. Voor andere systemen, zoals e-mail en SMS-berichten gold het opt-out systeem. Onder de nieuwe richtlijn 2002/58/EG geldt het opt-in systeem ook voor e-mail. Het begrip 'e-mail' is in richtlijn 2002/58/EG zeer ruim omschreven als: 'tekst-, spraak-, geluids- of beeldbericht dat over een openbaar communicatienetwerk wordt verzonden en in het netwerk of in de eindapparatuur van de ontvanger kan worden opgeslagen tot het door de ontvanger wordt opgehaald'. Voor direct marketing die is gericht op bestaande klanten geldt het opt-out systeem, mits duidelijk en expliciet gelegenheid tot bezwaar (opt-out) wordt geboden bij het verzamelen van de elektronische contactgegevens en voorts bij elke boodschap.

4.8 Conclusie

In dit hoofdstuk is aandacht besteed aan de algemene privacybeginselen die ten grondslag liggen aan de hedendaagse wet- en regelgeving met betrekking tot privacy en persoonsgegevensbescherming. De oude uit 1980 stammende 'Europese' privacybeginselen, neergelegd in het Verdrag van Straatsburg van de Raad van Europa, zijn in 1995 nog eens bevestigd in de EU privacyrichtlijn 95/46/EG, die recentelijk in de huidige privacywetgeving van de EU-lidstaten is geïmplementeerd.

Eveneens in het midden van de jaren negentig, is in de VS een aantal vergelijkbare *fair information practice principles* geformuleerd. Vervolgens werd de Amerikaanse industrie opgeroepen om deze beginselen door middel van zelfregulering te implementeren. Uit onderzoek van de FTC blijkt echter dat in 2000 slechts een minderheid de *fair information practice principles* ook daadwerkelijk toepast bij het verzamelen van persoonsgegevens via internet. Eveneens een minderheid heeft zich aangesloten bij zogeheten privacyprogramma's als TRUSTe. Hoewel de rol van zelfregulering van belang blijft, aldus de FTC, is zij tevens van mening dat het Amerikaanse Congres in aanvulling daarop wetgevingsinitiatieven dient te nemen. Dergelijke initiatieven zouden moeten leiden tot een minimum niveau van privacybescherming voor consumenten op internet.

Wanneer deze aanbeveling van de FTC wordt opgevolgd, kan de Amerikaanse privacywetgeving zich gaan bewegen in de richting van de Europese privacywetgeving.

Het dichter naar elkaar toegroeien van beide regimes, kan er toe leiden dat de Amerikaanse privacywetgeving naar Europese maatstaven een 'passend beschermingsniveau' biedt.

82. Zie artikel Av in het wetsvoorstel tot wijziging van de Telecommunicatiewet, *Kamerstukken II*, 2002/03, 28851.

Het Europese juridische kader ter bescherming van privacy en persoonsgegevens is voortdurend in ontwikkeling. Zo is recentelijk het Handvest van de Grondrechten van de Europese Unie ontworpen. Ook dit Handvest hanteert een onderscheid tussen privacybescherming en de bescherming van persoonsgegevens. Artikel II-67 van het Handvest correspondeert met de rechten die in artikel 8 van het EVRM zijn gewaarborgd. Naast dit algemene artikel, dat het privé-leven in ruime zin, als bedoeld in artikel 8 EVRM, beoogt te beschermen, kent het Handvest een specifiek artikel II-68, dat als titel de bescherming van persoonsgegevens heeft.

Aan de basis van de bescherming van persoonsgegevens in de EU ligt de EU-privacyrichtlijn 95/46/EG. De richtlijn bevat als algemeen uitgangspunt dat uitsluitend op een eerlijke en rechtmatige wijze persoonsgegevens mogen worden verwerkt. Voorts bevat de richtlijn voorschriften met betrekking tot de reikwijdte van de richtlijn, de informatieplichten, het bewaren van persoonsgegevens, de rechten van betrokkenen, vertrouwelijkheid en beveiliging. De richtlijn is in Nederland geïmplementeerd door middel van de Wet bescherming persoonsgegevens (Wbp). De reikwijdte van de richtlijn en Wbp hebben tot gevolg dat de Wbp van toepassing kan zijn op het verwerken van persoonsgegevens door Amerikaanse website-aanbieders.

Informatieplichten moeten leiden tot meer openheid of transparantie over het verwerken van persoonsgegevens. Niet alleen de EU-privacyrichtlijn bevat informatieplichten voor commerciële website-aanbieders. Op grond van de EU-richtlijn verkoop op afstand (97/7/EG) en de richtlijn inzake elektronische handel (2000/31/EG) gelden eveneens een aantal informatieplichten. Informatie over de identiteit van de aanbieder, adresgegevens, eigenschappen en prijs van het product, etc. dient aan de consument te worden verstrekt alvorens een elektronische transactie tot stand komt. Wanneer tevens persoonsgegevens worden verzameld in het kader van een koop op afstand, strekt de informatieplicht zich tevens daartoe uit.

De EU-richtlijn inzake privacy en elektronische communicatie (2002/58/EG) bevat uit privacy-oogpunt een aantal belangrijke onderwerpen in verband met consumententransacties via internet. In het bijzonder regelt deze richtlijn het gebruik van cookies, het verwerken van verkeersgegevens, het verwerken van locatiegegevens en het ongevraagd versturen van elektronische commerciële communicatie (spam).

Het EVRM, het Handvest van de Grondrechten van de EU en de genoemde EU-richtlijnen vormen aldus het juridische kader voor het verwerken van persoonsgegevens. In het volgende hoofdstuk wordt ingegaan op zelfreguleringsinitiatieven ter bescherming van persoonsgegevens.

5 Zelfregulering ter bescherming van persoonsgegevens

5.1 Inleiding

In dit hoofdstuk wordt het tweede deel van de derde onderzoeksvraag behandeld. Deze luidt:

"Welke zelfreguleringsinitiatieven voor gegevensbescherming kunnen we onderscheiden?"

In dit hoofdstuk wordt nader ingegaan op het concept van zelfregulering en worden diverse voorbeelden van zelfreguleringsinitiatieven ter bescherming van persoonsgegevens op internet beschreven.

5.2 Zelfregulering

In zijn boek *Self-regulation in the media sector and European Community Law*, definieert Jorg Ukrow zelfregulering als: "A regulatory activity carried out by specific organisational units in order to avoid or eliminate incorrect behaviour within their internal structures, or within the structures from which they operate".[83] Dergelijke zelfreguleringsactiviteiten kunnen zeer uitgebreid zijn. Zo kunnen marktpartijen bijvoorbeeld zelf de regels en normen voor de eigen branche vaststellen en kan de zelfregulering zich tevens uitstrekken tot het toezicht op en handhaving van de regels. In die zin kan zelfregulering worden verdedigd als alternatief voor overheidsregulering.

Naast dergelijke uitgebreide vormen van zelfregulering, bestaan er verschillende andere vormen die onder meer zijn te vinden in de milieusector, media, direct marketing, gezondheidszorg, etc. Sommige zelfreguleringsvormen zijn minder uitgebreid en sluiten niet uit dat naast de zelfreguleringsinitiatieven ook overheidsregulering van toepassing kan zijn of zijn gebaseerd op samenwerking met de overheid. Zelfregulering kan dan als functie hebben dat het een nadere uitwerking biedt van overheidsregels, bijvoorbeeld in de vorm van gedragscodes.

83. J. Ukrow, *Self-regulation in the media sector and European Community Law.* Saarbrücken 1999, p. 12.

Zelfregulering is een concept waar men verschillend tegenaan kan kijken.[84] Overheid en burger benaderen zelfregulering vanuit verschillend perspectief. Als gemeenschappelijk element volgt daaruit echter dat er bij zelfregulering sprake is van een wisselwerking tussen actoren binnen de samenleving. Zelfregulering heeft slechts dan kans van slagen, wanneer alle betrokkenen er aan toe zijn en er klaar voor zijn.

In de kabinetsnota Wetgeving voor de Elektronische Snelweg (WES) van februari 1998, spreekt de Nederlandse regering haar voorkeur uit voor zelfregulering voor het internet boven overheidsregulering. De nota WES somt wel een aantal voorwaarden op waaraan die zelfregulering wel dient te voldoen, wil het een aanvaardbaar alternatief voor overheidsregulering kunnen zijn:

- De doelgroepen die in het geding zijn, zijn voldoende georganiseerd.
- Er vindt er een gelijkwaardige behartiging plaats van de relevante maatschappelijke belangen.
- Er vindt voldoende binding plaats van alle partijen.
- De handhaving van de afspraken is voldoende verzekerd.[85]

Zelfregulerende mechanismen zijn bekend in diverse verschijningsvormen. Zo worden de volgende verschijningsvormen onderscheiden[86]:
– zuivere zelfregulering;
– vervangende zelfregulering;
– geconditioneerde zelfregulering (door de wet opgedragen zelfregulering, door de wet toegestane zelfregulering, wetgeving als stok achter de deur);
– co-regulering.

Kenmerkend voor zuivere zelfregulering is dat het initiatief daartoe volledig berust bij de betrokken groep van belanghebbenden. De overheid neemt een neutrale positie in ten aanzien van het resultaat. De gedragsregels mogen echter niet in strijd zijn met de algemeen geldende rechtsregels. Voorbeelden van zuivere zelfregulering zijn geschillenregelingen, zoals de Regeling voor .nl-domeinnaamarbitrage, en de normalisatie-activiteiten van het Nederlands Normalisatie Instituut (NEN), bijvoorbeeld met betrekking tot de beveiliging van medische persoonsgegevens.[87]

84. Zie de bijdragen vanuit verschillende perspectieven in Ph. Eijlander, P.C. Gilhuis, en J.A.F. Peters (red.), *Overheid en zelfregulering. Alibi voor vrijblijvendheid of prikkel tot actie?* Zwolle: W.E.J. Tjeenk Willink 1993.
85. Nota Wetgeving voor de Elektronische Snelweg, *Kamerstukken II*, 1997/98, 25 880, nr. 2, p. 11.
86. P. Eijlander, W. Voermans, *Wetgevingsleer,* Deventer: W.E.J. Tjeenk Willink, 1999, p. 71 e.v.
87. Nederlands Normalisatie Instituut, *Nederlandse Norm Medische Informatica – Informatiebeveiliging in de zorg – Algemeen,* NEN 7510: 2004 nl (1 april 2004).

Vervangende zelfregulering is zelfregulering die zonder uitdrukkelijke verplichting tot stand komt, maar waarbij de overheid wel aandrang uitoefent om tot zelfregulering te komen. De overheid zal op de achtergrond aanwezig zijn omdat publieke belangen in het geding kunnen zijn. De wetgever is in die gevallen een reservespeler, die op enig moment kan invallen. Een voorbeeld daarvan is de persfusiegedragscode, die is gericht op het voorkomen van ongewenste dagbladconcentraties.

Zuivere en vervangende zelfregulering zijn als zodanig niet wettelijk ingekaderd. Bij geconditioneerde zelfregulering is dat wel het geval. Kenmerken daarvan zijn dat (1) de wetgever zich beperkt tot het stellen van materiële of procedurele randvoorwaarden, (2) burgers, bedrijven en maatschappelijke organisaties een aanzienlijke vrijheid hebben bij de invulling van het wettelijk kader en (3) de overheid een voorname rol speelt bij de controle op het eindresultaat. Vaak dient de wetgever bij geconditioneerde zelfregulering ook zelf in actie te komen. Daarbij kunnen zich drie varianten voordoen. In de eerste plaats kan de wet opdragen tot zelfregulering en daaraan rechtsgevolgen verbinden. Dat is bijvoorbeeld het geval in de Kwaliteitswet zorginstellingen, die aan zorgaanbieders opdraagt een systeem voor kwaliteitsbewaking op te zetten. In de tweede plaats komt het voor dat de wetgever de mogelijkheid biedt om langs een voorgeschreven procedure zelfregulering te initiëren, waardoor daaraan rechtsgevolgen worden verbonden. Zo kan een organisatie of kunnen organisaties die voldoende representatief is c.q. zijn voor een bepaalde maatschappelijke sector, op grond van artikel 25 van de Wbp een gedragscode opstellen ter bescherming van persoonsgegevens. Deze gedragscode kan vervolgens worden voorgelegd aan het College bescherming persoonsgegevens met een verzoek tot afgifte van een verklaring van overeenstemming met de wet. Ten derde komt het voor dat de wet voorziet in de mogelijkheid om alsnog met regels te komen voor het geval de zelfregulering niet tot stand mocht komen of deze in belangrijke mate tekort schiet. Wetgeving fungeert daarmee als een soort 'stok achter de deur'. Artikel 26 van de Wbp voorziet bijvoorbeeld in de mogelijkheid om bij algemene maatregel van bestuur voor een bepaalde sector nadere regels te stellen met betrekking tot de materiële normen van die wet.

Co-regulering (ook wel co-productie genoemd), is een vorm van regulering die wordt gekenmerkt door coöperatie tussen de wetgever en de markt. De wetgever en de marktpartijen zijn gelijke partners als het gaat om het starten van discussies over sociale problemen en het oplossen ervan. De wetgever is bij co-regulering niet de centrale actor die problemen definieert en oplossingen aandraagt. Bij co-regulering wordt open onderhandeld tussen de belanghebbende partijen over de aard, de uitbreiding, en de ernst van de problemen en de mogelijke oplossingen ervan.

Uit een eerdere studie[88] (over e-handelbeleid en internetbeleid) is gebleken dat er een opvallende tendens viel waar te nemen in de onderzochte landen[89], die zich oorspronkelijk op het standpunt stelden dat overheidssturing in principe niet is gewenst, maar dat de markt het voortouw dient te nemen. Er kan worden vastgesteld dat in al deze landen het besef groeit dat de overheid niet kan volstaan met uitsluitend stimuleren, maar dat het vormgeven van e-handelbeleid en internetbeleid een taak voor de overheid en de markt gezamenlijk is. Zelfs in de Verenigde Staten lijkt een tendens waar te nemen waaruit blijkt dat men de mening is toegedaan dat de overheid meer dan voorheen een sturende rol moet gaan spelen bij de vormgeving van het beleid, in het bijzonder op het terrein van de privacybescherming.[90] Uitgangspunt daarbij is het samen optrekken van overheid en markt bij het ontwikkelen van het beleid.

Bij de voornoemde constatering is het overigens wel van belang voor ogen te houden dat de term 'co-regulering' in de verschillen landen geen eenduidige invulling kent. Een blik op de diverse internationale gremia die zich met de beleidsvorming bezig houden, laat zien dat ook hier het uitgangspunt van co-regulering in toenemende mate wordt gepropageerd. Zo heeft de OESO zich tijdens een bijeenkomst in het najaar van 1999 positief uitgesproken over het concept van co-regulering. Hoewel het verleden heeft laten zien dat de individuele lid-staten zich een voorstander tonen van het – waar mogelijk – doorzetten van hun nationale beleidslijn inzake regulering in de internationale organisaties, hebben ze het uitgangspunt van co-regulering nog niet nadrukkelijk op de internationale agenda geplaatst. De oorzaak daarvan kan zijn gelegen in het feit dat het uitgangspunt pas zeer recent op de nationale beleidsagenda is gezet en nog niet rijp genoeg is voor internationale agendering. Wordt het eenmaal op de internationale agenda geplaatst dan dient men, zoals hiervoor aangegeven, nadrukkelijk rekening te houden met het feit dat het begrip co-regulering per land verschillend wordt ingevuld.

Toepassing van zelfregulering kent in het algemeen zowel voor- als nadelen. Als voordelen worden genoemd:[91]

88. Bert-Jaap Koops, Corien Prins, Maurice Schellekens, Serge Gijrath, Eric Schreuders, *Overheden over internationalisering en ICT-recht,* Den Haag: Sdu 2000. Nationaal Programma Informatietechnologie en Recht, nr. 39, p. 31-47.
89. Nederland, Duitsland, Frankrijk, en het Verenigd Koninkrijk.
90. Zie § 4.2 in dit boek.
91. P. Eijlander, W. Voermans, *Wetgevingsleer,* Deventer: W.E.J. Tjeenk Willink, 1999, p. 75. Zie bijvoorbeeld ook: B. Baarsma e.a., *Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten*, Onderzoek in opdracht van het Ministerie van Economische Zaken. Amsterdam: Stichting voor Economisch Onderzoek, april 2003. SEO-rapport no. 664, p. 17 e.v.; Jean-François Lerouge, Internet Effective Rules: The Role of Self-Regulation. *The EDI Law Review.* The Hague, Vol. 8, nr. 4, 2001, p. 197-207; E. Terryn, Gedragscodes en labels in de elektronische handel, *Computerrecht* 2003/5, p. 283-294.

1. de betere aansluiting van de regels op het handelingsperspectief van de betrokkenen;
2. de grotere bereidheid tot naleving van de zelf gestelde regels;
3. de geringere uitvoeringslasten voor de overheid;
4. de nauwere band tussen het nemen van beslissingen en het dragen van de gevolgen daarvan;
5. de grotere betrokkenheid van burgers en maatschappelijke organisaties bij het desbetreffende onderwerp, vanwege de toegenomen mogelijkheid om zelf in ruimere mate richting te geven aan het gedrag.

Als nadelen kunnen worden genoemd:
1. de toenemende macht van de sterkste of de best georganiseerde;
2. de mogelijk beperkte doordringbaarheid van de zelfreguleringscollectiviteit of -instantie voor geluiden of impulsen uit de buitenwereld;
3. de daling van het niveau van de regulering;
4. de beperkte afdwingbaarheid van de (groeps)regels;
5. de (soms) onnodige verschillen in regelgeving;
6. de toenemende uitvoeringslasten voor burgers en maatschappelijke organisaties.

Eijlander en Voermans adviseren om in de volgende gevallen het gebruik van zelfregulering, mogelijk in de vorm van wettelijk geconditioneerde zelfregulering, te overwegen: wanneer het gedrag van 'professionals' moet worden gereguleerd, in situaties waarin individuele of groepsbelangen niet te zeer verschillen van het belang dat de desbetreffende wet beoogt te dienen en in omstandigheden waarin (volledige) overheidsregulering niet of slechts zeer moeizaam te controleren en te handhaven is.[92] Met name op basis van de als laatste genoemde omstandigheden, lijkt zelfregulering voor de bescherming van de privacy op het wereldwijde internet een nuttig instrument.

Deze opvatting wordt ook gedeeld door Harriet Pearson, Chief Privacy Officer bij IBM Corporate.[93] Volgens haar en volgens IBM is het beste privacyregime voor internetconsumenten een gelaagd systeem, bestaande uit een combinatie van initiatieven van het bedrijfsleven, technologische maatregelen die consumenten zelf kunnen treffen, en overheidsregulering. De overheid dient haar regels te richten op bevordering van transparantie, bescherming van gevoelige informatie (financiële gegevens, medische gegevens en gegevens over kinderen), en effectieve bescherming bieden tegen schadelijke en fraudeleuze praktijken. Een dergelijk systeem van privacybescherming bevordert het vertrou-

92. P. Eijlander, W. Voermans, *Wetgevingsleer,* Deventer: W.E.J. Tjeenk Willink, 1999, p. 75.
93. How do businesses use customer information: Is the customer's privacy protected? Hearing before the subcommittee on commerce, trade, and consumer protection of the committee on energy and commerce. House of Representatives, One hundred seventh congress, First session, July 26, 2001. Serial No. 107–49, p. 12.

wen van de consument in de internetonderneming en is tegelijkertijd flexibel genoeg om het bedrijfsleven voldoende ruimte te laten om de consument voldoende gemak, besparingen, diensten en werkgelegenheid te bieden.

5.3 Zelfreguleringsinstrumenten

In een in 2003 gepubliceerd onderzoek van de Stichting voor Economisch Onderzoek (SEO) te Amsterdam, worden 22 verschillende zelfreguleringsinstrumenten onderscheiden.[94] Vanuit het perspectief van de gebruikers worden deze in vijf clusters onderverdeeld. Die clusters zijn:

1. techniekgerichte instrumenten
2. gedragsgerichte instrumenten
3. informerende instrumenten
4. contractuele instrumenten en
5. geschilbeslechtende instrumenten.

Als zesde cluster worden de publiekrechtelijke beroepsorganisaties onderscheiden. Een publiekrechtelijke beroepsorganisatie is een zeer vergaande vorm van zelfregulering die op de grens ligt tussen zelfregulering en overheidsregulering.

Volgens het SEO-rapport kunnen techniekgerichte instrumenten (1) worden ingezet als zelfreguleringsinstrument in technische bedrijfstakken waar producten (of delen daarvan) compatible en uitwisselbaar dienen te zijn.

De instrumenten van dit cluster zijn de volgende:

- normalisatie;
- Nederlandse Technische Afspraak (NTA);
- Regulering door techniek.

Normalisatie houdt het vaststellen van veelal technische normen in ter specificatie van een product, dienst of bedrijfsproces. Voor nationale toepassing van zo'n norm is in Nederland de tussenkomst van het Nederlands Normalisatie-instituut (NEN) of het Nederlands Elektrotechnisch Comité (NEC) vereist.

Een instrument dat een snellere manier biedt om specificaties voor een bepaalde branche op te zetten is de Nederlandse Technische Afspraak (NTA). Deze snelle procedure is sinds enige tijd door het NEN mogelijk gemaakt.

94. B. Baarsma e.a., *Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten,* Onderzoek in opdracht van het Ministerie van Economische Zaken. Amsterdam: Stichting voor Economisch Onderzoek, april 2003, SEO-rapport no. 664, p. 23 e.v.

Regulering door techniek is een instrument dat kan worden toegepast voor de handel in informatieproducten. Een voorbeeld daarvan zijn de Digital Rights Managementsystemen (DRM) waardoor intellectuele eigendomsrechten technisch beschermd kunnen worden.

Gedragsgerichte instrumenten (2) kunnen kan voor vele uiteenlopende problemen worden ingezet, zoals bij imagoproblemen in een branche.

De instrumenten van dit cluster zijn:

- gedragscode (waaronder beroepscode, branchecode en erecode);
- een zeer specifieke gedragscode: de reclamecode;
- protocol;
- herenakkoord;
- convenant;
- kartel.

Al deze instrumenten geven partijen de mogelijkheid om afspraken te maken. Gedragscodes bevatten bepaalde gedragsregels en kunnen voor verschillende terreinen worden ontwikkeld. Een voorbeeld is de Nederlandse Reclame Code. Een protocol bevat eveneens gedragsregels voor een specifieke situatie maar is meer voorschrijvend dan een gedragscode. Een herenakkoord, convenant en kartel zijn instrumenten waarvan de invulling volledig vrij staat voor de opstellers. De inhoud ervan kan wel betrekking hebben op het voorschrijven van gedrag, maar noodzakelijk is dat niet.

Informerende instrumenten (3) kunnen nuttig zijn als zelfreguleringsinstrument als de transparantie op de markt bemoeilijkt wordt door informatieasymmetrie (informatieongelijkheid) tussen aanbieder en consument. Extra informatie aan de consument kan bijvoorbeeld leiden tot een groter consumentenvertrouwen.

Dit cluster bestaat uit de volgende instrumenten:

- keurmerk;
- certificering;
- erkenningsregeling;
- ketengarantiestelsel;
- visitatie.

Een gemeenschappelijk kenmerk van certificering, een erkenningsregeling en een ketengarantiestelsel is dat informatie wordt geboden door het voeren van een bepaald keurmerk. Door middel van een keurmerk wil men laten zien dat er aan bepaalde (strenge) eisen wordt voldaan. Visitatie is een soort audit door een commissie bestaande uit externe onafhankelijke collega's, die als het ware 'op visite' gaan bij een organisatie. Visi-

taties komen alleen in de semi-overheidssector voor, zoals in het hoger onderwijs, omdat bedrijven niet graag concurrenten toelaten.

Contractuele instrumenten (4) leiden in het algemeen tot lagere transactiekosten. Wanneer aanbieder en koper over de voorwaarden van de koop moeten overleggen, kunnen transactiekosten worden verlaagd door 'overleg over contractvoorwaarden' te voeren. De aanbieder hoeft dan niet met elke koper apart te onderhandelen. Deze instrumenten leiden tot meer transparantie bij de consument, waardoor ook aan de vraagkant de transactiekosten laag kunnen blijven.

Het gaat hier om de volgende instrumenten:

- algemene voorwaarden overleg bij de SER;
- de standaardregeling.

Ondernemers- en consumentenorganisaties kunnen in het kader van de Coördinatiegroep Zelfreguleringsoverleg van de SER algemene voorwaarden afspreken waarin de rechten en plichten van consument en ondernemer zijn vastgelegd. De algemene voorwaarden gelden alleen voor het georganiseerde deel van een branche. Een standaardregeling geldt daarentegen voor de gehele branche.

Geschilbeslechtende instrumenten (5) hebben tot doel het voorkomen, beperken en oplossen van geschillen. Voordelen van deze instrumenten zijn het ontlasten van het rechtssysteem, een toegankelijke rechtsspraak en het voorkomen van lange en kostbare gerechtelijke procedures.

Dit cluster bestaat uit de volgende instrumenten:

- arbitrage;
- bindend advies;
- mediation;
- ombudsman;
- tuchtrecht.

Het verschil tussen arbitrage en bindend advies bestaat uit het al dan niet bindende karakter. Bij mediation wordt een conflict opgelost door tussenkomst van een neutrale conflictbemiddelaar: de mediator. Een door een branche zelf aangestelde ombudsman vervult een combinatie van mediation en bindend advies. Tuchtrecht waarborgt de kwaliteit van de beroepsuitoefening binnen een bepaalde beroepsgroep.

In de volgende paragrafen komen in ieder geval enkele zelfreguleringsinstrumenten aan de orde die worden toegepast in verband met de verwerking van persoonsgegevens via internet. Dit zijn in het bijzonder de gedragscodes, contractuele regelingen en keurmer-

ken. In het hoofdstuk dat hierna volgt wordt ingegaan op techniekgerichte instrumenten.

5.4 Internationaal zelfreguleringsbeleid

5.4.1 EU

Tijdens de Europese ministeriële conferentie, georganiseerd door de Europese Commissie en Duitsland van 6-8 juli 1997 in Bonn, verklaarden de aanwezige ministers dat zelfregulering een nuttig instrument zou kunnen zijn voor het reguleren van gedrag in een "Global Information Network".[95] Deze opvatting is neergelegd in Declaration 19, dat deel uitmaakt van een door de deelnemende ministers na afloop van de conferentie uitgebrachte verklaring. De tekst ervan luidt: "Ministers stress the role which the private sector can play in protecting the interests of consumers and in promoting and respecting ethical standards, through properly-functioning systems of self-regulation in compliance with and supported by the legal system."

Tegelijkertijd erkenden de ministers in dezelfde verklaring (Declaration 49-52) het belang van de beginselen voor gegevensbescherming en riepen de industrie op om technische mogelijkheden te ontwikkelen, zoals toepassingen om anoniem te kunnen internetten, e-mailen en betalen, ter bescherming van de privacy en persoonsgegevens in de "Global Information Network".

Op 25 januari 1999 is door het Europese Parlement en de Raad een meerjarig actieplan aangenomen ter bevordering van een veiliger gebruik van het internet. Dit doel zou bereikt moeten worden met het bestrijden van illegale en schadelijke informatie. Het plan stimuleert zelfregulering door het bedrijfsleven en monitoring van informatie, zoals kinderpornografie of informatie waarmee wordt aangezet tot haat op grond van iemands ras, geslacht, godsdienst, nationaliteit of etnische afkomst. Voorts wordt het bedrijfsleven opgeroepen om filters en meetinstrumenten te ontwikkelen waardoor ouders of docenten de toegankelijkheid van inhoud voor kinderen kunnen selecteren.

In een witboek getiteld 'Europese Governance (2001)'[96] richt de Europese Commissie zich op de betrokkenheid van de burgers bij de Europese Unie. Daartoe wordt onder andere voorgesteld om de Europese beleidsvorming zodanig te veranderen dat burgers en organisaties meer betrokken worden bij het ontwikkelen en uitvoeren van EU beleid. De Commissie stelt dat het meer beleidsinstrumenten wil inzetten: regulering, richtlijnen en co-regulering. De Commissie ziet vooral een raamwerk voor co-regulering als een moge-

95. Ministerial Conference, Bonn, 6-8 July 1997. Op internet: <http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html> (laatst bezocht op 26 augustus 2004).
96. Commissie van de Europese Gemeenschappen, *Europese Governance, Een witboek,* Brussel 25.7.2001. COM (2001) 428 definitief. Op Internet: < http://europa.eu.int/eur-lex/nl/com/cnc/2001/com2001_0428nl01.pdf> (laatst bezocht op 2 november 2004).

lijkheid om de kwaliteit, effectiviteit en eenvoud van regelgeving te bevorderen. Co-regulering zou moeten leiden tot een combinatie van wet- en regelgevingsinitiatieven en bijdragen van belanghebbenden vanuit hun praktijkervaringen. Door betrokkenheid van directe belanghebbenden wil men een breder draagvlak en daarmee een betere naleving van beleid realiseren, ook als het om niet bindende regels gaat. De Europese Commissie is met name van mening dat de ideeën uit het Witboek Europese Governance op mondiaal niveau kunnen worden getest, zoals de ontwikkeling van co-regulering om aspecten van de nieuwe economie te behandelen.[97]

Op 28 mei 2002 presenteerde de Europese Commissie een nieuw actieplan onder de titel: "*e*Europe 2005".[98] Het actieplan is opgesteld met het oog op de indiening ervan tijdens de Europese Raad van Sevilla van 21 en 22 juni 2002. Sinds 1997 heeft de Europese Commissie een alomvattend beleid ontwikkeld op het terrein van de elektronische handel. Enkele resultaten daarvan zijn de inmiddels door de EU aanvaarde richtlijnen voor de diensten van de informatiemaatschappij op de interne markt. Deze richtlijnen betreffen: de elektronische handel (2000/31/EG), de elektronische handtekeningen (1999/93/EG), auteursrecht en naburige rechten (2001/29/EG) en koop op afstand (1997/7/EG). Daarnaast is een aantal niet-wetgevende initiatieven ontwikkeld die zijn gericht op het bevorderen van zelfregulering. Die initiatieven liggen met name op het terrein van "e-confidence" en online geschillenbeslechting (online dispute resolution: ODR), en de lancering van het "Go-Digital" initiatief ter bevordering van de elektronische handel bij het midden- en kleinbedrijf.

De Europese Commissie werkt samen met de lidstaten aan de ondersteuning van de elektronische handel in Europa. Het doel is daarbij gericht op het bevorderen van de invoering van de elektronische handel waardoor de concurrentiepositie van Europese bedrijven verbetert. De productiviteit en groei zouden moeten toenemen door te investeren in ICT, in menselijke hulpbronnen (e-vaardigheden) en nieuwe zakelijke modellen, "*daarbij tegelijkertijd zorg dragend voor de privacy*".[99]

97. Commissie van de Europese Gemeenschappen, *Europese Governance. Een witboek*. Brussel 25.7.2001. COM (2001) 428 definitief, p. 32. Op Internet: < http://europa.eu.int/eur-lex/nl/com/cnc/2001/com2001_0428nl01.pdf> (laatst bezocht op 2 november 2004).
98. Commissie van de Europese Gemeenschappen, eEurope 2005: Een informatiemaatschappij voor iedereen. Brussel, 28.05.2002, COM (2002) 263 definitief. Op internet: <http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_nl.pdf> (laatst bezocht op 2 november 2004).
99. Commissie van de Europese Gemeenschappen, eEurope 2005: Een informatiemaatschappij voor iedereen, Brussel, 28.05.2002. COM (2002) 263 definitief, p. 16-17. Op internet: <http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_nl.pdf> (laatst bezocht op 2 november 2004).

5.4.2 OESO

Op 16 en 17 februari 1998 organiseerde de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) een workshop over privacybescherming en grensoverschrijdend gegevensverkeer voor vertegenwoordigers van de overheid, het bedrijfsleven, consumentenorganisaties en privacytoezichthouders. De workshop leidde tot de vaststelling dat een onderzoek naar beschikbare instrumenten voor gegevensbescherming – inclusief wetgeving, zelfregulering, contracten en technologieën – wenselijk was met het oog op de toepassing ervan in een netwerkomgeving en met inachtneming van de OESO Privacy Richtlijnen (1980) met betrekking tot effectiviteit, handhaafbaarheid, herstel van geleden schade en jurisdictie (rechtsmacht).

Op de Ottawa-conferentie van 7-9 oktober 1998 over "A Borderless World: Realising the Potential of Global Electronic Commerce", presenteerden de OESO-ministers een verklaring namens de regeringen van de OESO-lidstaten en de EU. Die verklaring luidde onder meer dat de ministers "*will take the necessary steps, within the framework of their respective laws and practices, to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular:*

1. *encourage the adoption of privacy policies, whether implemented by legal, self-regulatory, administrative or technological means;*
2. *encourage the online notification of privacy policies to users;*
3. *ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress;*
4. *promote user education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks;*
5. *encourage the use of privacy-enhancing technologies; and*
6. *encourage the use of contractual solutions and the development of model contractual solutions for online transborder data flows."*

Uit deze verklaring, maar ook uit andere documenten[100] blijkt dat de OESO van mening is dat online privacy het beste te beschermen is via een mix van wetgeving en zelfregulering.

5.4.3 VN/ITU

Van 10-12 december 2003 organiseerde de International Telecommunication Union (ITU), een agentschap van de Verenigde Naties, de World Summit on the Information Society (WSIS) te Genève. Tijdens deze topconferentie stond een groot aantal onderwer-

100. Zoals bijvoorbeeld in het OESO-rapport *Privacy Online: Policy and Practical Guidance*. Directorate For Science, Technology And Industry Committee For Information, Computer And Communications Policy. 21 Januari 2003. Op Internet: <http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)3-final> (laatst bezocht op 2 november 2004).

pen over de informatiemaatschappij ter discussie en werden een actieplan en een Declaration of Principles opgesteld. Een van deze beginselen betreft het creëren van een stimulerende omgeving en luidt als volgt:

> "*the rule of law, accompanied by a supportive, transparent, pro-competitive, technologically neutral and predictable policy and regulatory framework reflecting national realities, is essential for building a people-centered Information Society. Governments should intervene, as appropriate, to correct market failures, to maintain fair competition, to attract investment, to enhance the development of the ICT infrastructure and applications, to maximize economic and social benefits, and to serve national priorities.*"

Binnen deze context besteedt de Declaration of Principles ook aandacht aan reguleringsvraagstukken, waarbij ook ruimte wordt gelaten voor zelfregulering:

> "*The management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:*
> a) *Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues;*
> b) *The private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields;*
> c) *Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role;*
> d) *Intergovernmental organizations have had and should continue to have a facilitating role in the coordination of Internet-related public policy issues;*
> *e) International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.*"

Hieruit kan worden geconcludeerd dat regulering het resultaat is van samenwerking tussen publieke en private sector. Met bijvoorbeeld maatschappelijke en internationale organisaties, zoals de VN, hebben zij een belangrijke rol en verantwoordelijkheid bij de ontwikkeling van de informatiesamenleving en het besluitvormende proces dat daarmee gepaard gaat. In de Declaration of Principles wordt voorts gepleit voor coördinatie van de aanpak van internationale internet reguleringsvraagstukken. Regeringen, bedrijfsleven en maatschappelijke organisaties zouden moeten samenwerken bij het onderzoeken van en het doen van voorstellen voor de regulering van het internet in 2005.[101]

5.5 Zelfreguleringsinitiatieven ter bescherming van persoonsgegevens

In deze paragraaf worden enkele voorbeelden besproken van zelfregulering ter bescherming van persoonsgegevens op internet. Achtereenvolgens komen gedragscodes, contrac-

101. World Summit on the Information Society, *Declaration of Principles*, Document WSIS-03/GENEVA/DOC/4-E (12 December 2003), p. 7. Op Internet: <http://www.itu.int/wsis/documents/> (laatst bezocht op 2 november 2004).

tuele regelingen, het Safe Harbor programma en privacykeurmerken aan de orde. Tot slot komt de privacy policy aan bod in het kader van de bescherming van de privacy van kinderen op internet.

5.5.1 Gedragscodes

NLIP

De NLIP (Brancheverenigingen van Nederlandse Internet Providers) vertegenwoordigt een groot deel van de Internet Service Providers. Diensten die de vereniging levert zijn: vertegenwoordiging in diverse platformen, kwaliteitswaarborg en klachten- en geschillenregeling.

De *Gedragscode* van het NLIP[102] is gericht op het ondubbelzinnig vastleggen van belangrijke elementen in de relatie provider – particuliere abonnee (aanbieder – consument). Alle leden onderschrijven met hun lidmaatschap de NLIP-Gedragscode. Gelet op de wenselijkheid en het maatschappelijke belang van een 'Code of Conduct' wordt deze code unaniem onderschreven en gehanteerd door elk lid van de NLIP. De 'Code of Conduct' wordt nauw afgestemd op de 'Codes of Conduct' van Europese en internatonale internet brancheverenigingen.

De gedragscode schrijft voor dat de provider het briefgeheim met betrekking tot persoonlijke e-mail zal respecteren en hanteren. Verder zal de provider het abonnee-bestand niet aan derden ter beschikking stellen. De provider informeert de abonnee duidelijk welke gegevens eventueel wel aan derden (kunnen) worden doorgegeven. Deze gegevens zijn binnen de organisatie van provider alleen toegankelijk ten behoeve van de bedrijfsvoering. De provider is voorts verplicht zorg te dragen voor een beveiliging als bedoeld in de Wbp en TW van alle gegevensverzamelingen die mogelijk persoonsgegevens bevatten, voor zover dergelijke verzamelingen in het kader van de uitvoering van de overeenkomst in het systeem van de provider alsmede in de door hem in verband daarmee gehouden administraties aanwezig zijn. De geheimhoudingsplicht geldt ten minste twee jaar na beëindiging van de overeenkomst of zoveel langer krachtens wettelijke regelingen.

De provider en abonnee zijn voorts verplicht zich te houden aan de Nederlandse wet- en regelgeving en aan de Netiquette. Verder is de provider aangesloten bij en onderworpen aan de NLIP-Geschillencommissie. Voor het ontvangen en afhandelen van klachten hanteert de provider de NLIP-Klachtenregeling.

De diensten, producten en promotiemateriaal van de provider worden op een rechtmatige en oprechte wijze aangeboden. De providers zullen op geen enkele manier het onwettig handelen op internet stimuleren. Zij zullen zich inspannen om te verzekeren dat hun diensten- en promotiemateriaal niet misleidend zijn door inaccuraatheid, ambi-

102. NLIP – Brancheverenigingen van Nederlandse Internet Providers, *Gedragscode 2.0*, op internet: <http://www.nlip.nl/>.

guïteit, overdrijvingen, verzwijgingen of op enige andere wijze. Bij het handel drijven met klanten en andere bedrijven, zullen de leden te allen tijde op een behoorlijke, eerlijke en redelijke wijze optreden. De providers zullen hun klanten inlichten over het bestaan van deze Code en de klachtenprocedure en moeten verzekeren dat de prijzen voor hun diensten duidelijk en ondubbelzinnig opgesteld zijn. Voor particuliere aansluitingen zijn de prijzen BTW inbegrepen. Indien additionele prijzen betaald dienen te worden, dient dit meegedeeld te worden.

FEDMA

De FEDMA (Federation of European Direct Marketing) is ontstaan in 1997. FEDMA is de spreekbuis van de Europese direct marketing industrie. Haar nationale leden zijn direct marketing associaties die gebruikers, service providers en media van direct marketing vertegenwoordigen.

FEDMA's doel is het beschermen van de Europese direct marketing industrie en de belangen van haar leden, het informeren van leden, regeringen, media, bedrijven, en gebruikers over de Europese direct marketing industrie en het promoten van de Europese direct marketing industrie.

Consumenten kunnen erop vertrouwen dat hun persoongegevens en privacy zullen worden gerespecteerd in de 'online' omgeving. Zij zullen geïnformeerd worden over hoe hun persoonsgegevens zullen worden gebruikt en over hun rechten op dat gebied. FEDMA's *Code on e-commerce and interactive marketing*[103] bevat daartoe voorzieningen betreffende de bescherming van gegevens en privacy van consumenten. Zo schrijft de code voor dat marketeers hun beleid over de bescherming van persoonsgegevens en consumenten-privacy duidelijk moeten maken aan de consument. De marketeers moeten hieraan voldoen door het aanbieden van een online privacy policy of privacystatement met details van hun verplichtingen en de rechten van de consument. De verplichtingen voor de marketeer zijn bijvoorbeeld het verschaffen van informatie over het doel waarvoor de persoonsgegevens worden gevraagd en verzameld. Alleen die persoonsgegevens die noodzakelijk zijn voor de uitvoering van de specifieke doelen mogen worden gevraagd. Tevens moet op verzoek informatie verstrekt worden over de maatregelen die genomen zijn om de vertrouwelijkheid van persoonsgegevens te waarborgen. In het bijzonder moet informatie worden verschaft over hoe gegevens worden beschermd tegen onbevoegde kennisneming en misbruik en tegen elke activiteit die wijziging in status, format of toegankelijkheid tot gevolg heeft.

De rechten van de consument zijn bijvoorbeeld het toegang hebben tot een privacy beleid over de verplichtingen van het bedrijf. Deze moet beschikbaar zijn gedurende elke

103. FEDMA, *FEDMA Code On E-Commerce & Interactive Marketing*, 6 september 2000, op internet: <http://www.fedma.org/img/db/Code_of_conduct_for_e-commerce.pdf.>

transactie, die gedaan wordt met de marketeer. De consument moet kunnen verwachten dat elk verschaft persoonsgegeven verwerkt wordt op een goed beveiligde en vertrouwelijke manier. FEDMA werkt momenteel aan de ontwikkeling van een Code of Conduct ter bescherming van persoonsgegevens.

ICX

Icx (Centre of Excellence for e-Business in Europe) is een organisatie die oplossingen biedt aan alledaagse problemen die kleine en middelgrote bedrijven ondervinden bij het exploiteren van e-commerce. De *ICX Privacy Code of Conduct* vormt een duidelijke handleiding voor managers over welke stappen zij moeten nemen als zij willen voldoen aan de wetgeving over de protectie van persoonsgegevens.[104] Op die manier kunnen zij negatieve maatregelen en ongewenste publiciteit voorkomen en het vertrouwen winnen van consumenten en andere geïnteresseerde partijen.

De code is in de eerste plaats gericht tot organisaties, die zich bezighouden met commerciële activiteiten, variërend van middelgrote bedrijven tot multinationals. De code kan echter in beginsel gebruikt worden door elke vorm van organisatie.

Het doel van de gedragscode is het uitstippelen van het operationele beleid waar een organisatie zich aan moet houden. Verder behandelt het de operationele stappen die een organisatie moet nemen om te voldoen aan de EU-richtlijn 95/46/EG.

5.5.2 Contractuele regelingen

ICC

The International Chamber of Commerce is opgericht in 1919. Haar doel is het dienen van de wereldhandel door het promoten van handel en investeringen, open markten voor goederen en diensten, en het vrije verkeer van kapitaal. ICC is een pionier in de zelfregulering van e-commerce. ICC's codes betreffende adverteren en marketing worden vaak geïmplementeerd in nationale wetgeving en in codes van professionele organisaties.

Van de ICC verscheen in 1993 een *Model contract aangaande de bescherming van persoonsgegevens*.[105] Dit contract heeft de basis gevormd voor ontelbare zakelijke transacties. Het modelcontract maakte het bedrijven mogelijk om op de voor hen normale wijze zaken te doen terwijl ze daarbij een hoog niveau van gegevensbescherming kan garanderen. In september 1998, keurde de ICC een herziene versie van het model van 1993 goed.

---

104. ICX, *The ICX Privacy Code of Conduct*, July 2000, op internet: <http://www.icx.org.uk/resources/res_0452.htm>. Laatst bezocht op 18 september 2003.
105. International Chamber of Commerce, *Model clauses for use in contracts involving transborder data flows*, 23 september 1998, op internet: <http://www.iccwbo.org/home/statements_rules/rules/1998/model_clauses.asp>. Laatst bezocht op 18 september 2003.

De in het modelcontract van 1998 opgenomen clausules voor wat betreft grensoverschrijdend gegevensverkeer zijn geschreven om partijen bij te staan bij de doorgifte van persoonsgegevens vanuit een land dat export van persoonsgegevens reguleert naar een land waar de bescherming van persoonsgegevens onacceptabel is bevonden door het exporterende land. De herziening van het model contract vond plaats in het licht van veranderingen in de zakelijke praktijk en nieuwe wettelijke vereisten in bepaalde jurisdicties, in het bijzonder naar aanleiding van de EU-privacyrichtlijn 95/46/EG.

CEN-ISSS

CEN-ISSS (European Committee for Standardization-Information Society Standardization System) is gecreëerd door CEN en is gericht op zijn ICT-activiteiten. Haar missie is het verschaffen van een begrijpelijke en geïntegreerde reeks van op standaardisatie georiënteerde diensten en producten om op die manier bij te dragen aan het succes van de informatiemaatschappij in Europa.

De laatste jaren houden individuen, bedrijven en regeringen zich steeds meer bezig met de beveiliging van persoonsgegevens. Het toegenomen publieke bewustzijn en alle nieuwe regelingen hieromtrent maken het belangrijk om goed geïnformeerd te worden en te participeren in het debat.

Het CEN-ISSS ontwikkelde het *Initiative for Privacy Standardization in Europe* (IPSE)[106], waarvan de twee hoofddoelen zijn:

1. te onderzoeken of er een 'case for standardization' is, als middel om bedrijven en andere markt-partijen te helpen om de relevante wetgeving te implementeren, met name de EU-richtlijn 95/46/EG ter bescherming van persoonsgegevens;
2. op voorwaarde dat het antwoord uit de eerste vraag positief is, moet IPSE de specifieke vereisten uiteenzetten in een set van aanbevelingen door de pro's en contra's te analyseren en de mogelijkheden in kaart te brengen.

CEN-ISSS heeft recentelijk het IPSE-rapport betreffende de bescherming van persoonsgegevens (13 februari 2002) aangenomen. Dat rapport bevat de volgende zeven aanbevelingen:

1. identificeer een algemene Europese basisset van vrijwillige 'best practices' voor persoonsgegevensbescherming;
2. ontwikkel geen management standaarden, maar volg de ontwikkelingen in ISO/COPOLCO;
3. ontwikkel een algemene set van model contractbepalingen en voorwaarden voor artikel 17 van de EU-richtlijn 95/46/EG;

106. IPSE, *Data Protection and Privacy. The Initiative for Privacy Standardization in Europe*, op internet: <http://www.cenorm.be/isss/Projects/DataProtection/dp.default.htm>. Laatste update 26-03-2003.

4. inventariseer bestaande audit-praktijken voor persoonsgegevensbescherming;
5. onderzoek 'web seals' als mogelijke basis voor verdere standaardisatie;
6. rapporteer over de gevolgen van technologieën voor de bescherming van persoonsgegevens, inclusief Privacy Enhancing Technologies (PET);
7. bevorder onderwijs en promotie op het gebied van privacystandaarden.

In vervolg op het IPSE-rapport, is CEN op 3 juli 2003 gestart met een Workshop 'Data Protection and Privacy'.[107] Het doel van deze workshop is o.a. het gebruik van standaardisatie door het Europese bedrijfsleven te bevorderen met het oog op de naleving van de EU-privacyrichtlijn.

EU modelcontractbepalingen en 'Binding Corporate Rules'

Volgens Richtlijn 95/46/EG moeten de lidstaten bepalen dat persoonsgegevens vanuit de EU slechts naar derde landen mogen worden doorgegeven, wanneer in dat land sprake is van een passend beschermingsniveau. Op grond van artikel 26, lid 2, van Richtlijn 95/46/EG is het echter toegestaan om persoonsgegevens door te geven naar een derde land zonder een passend beschermingsniveau, mits waarborgen zijn getroffen, bijvoorbeeld in contractuele regelingen. In dit verband zijn door de Europese Commissie modelcontractbepalingen opgesteld ten behoeve van de verstrekking aan andere verantwoordelijken in een derde land en aan bewerkers in een derde land.[108]

Voor Nederlandse exporteurs van persoonsgegevens betekent het gebruik van contractuele regelingen, inclusief deze modelcontractbepalingen, dat tevens een vergunning van de minister van Justitie moet worden verkregen voor de doorgifte naar een derde land.

In overweging (10) van de Beschikking van 15 juni 2001 en in overweging (9) van de Beschikking van 27 december 2001, kondigt de Europese Commissie aan dat het in de toekomst zal onderzoeken in hoeverre modelcontractbepalingen die door bedrijfsorganisaties of andere belanghebbenden zijn gemaakt, eveneens voldoende waarborgen voor een passend beschermingsniveau bevatten. Op 3 juni 2003 heeft de Artikel 29 Werkgroep hierover een werkdocument gepubliceerd.[109] De strekking van het document is dat

107. CEN-ISSS, *Data Privacy Workshop*, op internet: <http://www.cenorm.be/isss/Workshop/DPP/default.htm>. Laatste update 5 mei 2003.
108. Beschikking van de commissie van 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG (kennisgeving geschied onder nummer C(2001) 1539) (Voor de EER relevante tekst)(2001/497/EG) en Beschikking van de commissie van 27 december 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG (kennisgeving geschied onder nummer C(2001) 454 (Voor de EER relevante tekst 2002/16/EG).
109. Article 29 – Data Protection Working Party, Working Document: *Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers.* Adopted 3 June 2003, WP 74.

de Artikel 29 Groep van mening is dat met inachtneming van de kaders die in het document uiteen worden gezet, een contract in de vorm van een *Intercompany Agreement* gesloten door de vestigingen van een multinational, voldoet aan de eisen van artikel 26, lid 2, van Richtlijn 95/46/EG. Dit kan de wereldwijde uitwisseling van persoonsgegevens binnen een multinational aanzienlijk vereenvoudigen. De Artikel 29 Groep is van mening dat het werkdocument een eerste stap is op weg naar doorgifte van persoonsgegevens binnen de kaders van artikel 26, lid 2, van de Richtlijn, welke doorgifte kan worden gebaseerd op zelfregulering.

5.6 EU/US Safe Harbor Agreement

De EU is er in geslaagd de belangrijkste materiële normen uit Richtlijn 95/46/EG als het ware te exporteren naar de Verenigde Staten. Daartoe werd op 26 juli 2000 bekend gemaakt dat de Europese Commissie en het Amerikaanse Department of Commerce overeenstemming hadden bereikt over het Safe Harbor programma. Het Safe Harbor programma is een belangrijke manier voor Amerikaanse bedrijven om inbreuken op hun handel met de EU te voorkomen of om gerechtelijke stappen te voorkomen door Europese autoriteiten onder EU privacyrecht. Aansluiting bij de Safe Harbor levert voor organisaties in de EU de garantie op dat het bedrijf voorziet in een passend niveau voor gegevensbescherming, zoals bedoeld in artikel 25 van Richtlijn 95/46/EG en in artikel 76 van de Wbp.

Om zich aan te kunnen sluiten bij het Safe Harbor programma, moeten Amerikaanse organisaties voldoen aan zeven Safe Harbor Principles. Ter vergelijking: de vier door de FTC erkende *fair information practice principles* waren: *Notice*, *Choice*, *Access* en *Security*. De zeven Safe Harbor Principles zijn:

Notice:
Organisaties dienen de betrokkenen te informeren over de doelen waarvoor gegevens over hen worden verzameld en verder gebruikt. Zij dienen te voorzien in informatie over de wijze waarop betrokkenen contact kunnen opnemen met de organisatie met klachten, verzoeken om informatie over derden aan wie hun gegevens worden verstrekt en de mogelijkheden die zij hebben ter beperking van het gebruik en verstrekking van hun persoonsgegevens.

Choice:
Organisaties dienen betrokkenen de keuze te bieden (opt out) voor het verstrekken van hun gegevens aan derden of voor het gebruik van hun gegevens voor andere doelen dan waarvoor ze oorspronkelijk zijn verzameld. Voor gevoelige (bijzondere) gegevens dient voor deze verstrekking en gebruik voor andere doelen vooraf de uitdrukkelijke toestemming (opt in) te worden gegeven.

Onward Transfer (Transfers to Third Parties):
Voor de verstrekking van persoonsgegevens aan derden dienen organisaties de *Notice* en *Choice* principles toe te passen. Als een organisatie de gegevens wil verstrekken aan een derde die optreedt als een 'agent'(1), is dat toegestaan wanneer wordt geverifieerd dat de derde de *Safe Harbor Principles* onderschrijft of valt onder de jurisdictie van de EU Richtlijn. Als alternatief kan de organisatie een schriftelijke overeenkomst sluiten met de derde (ontvanger) waarin is opgenomen dat de ontvanger zich ten minste aan dezelfde privacybeschermende voorwaarden zal houden.

Access:
Betrokkenen moeten inzage kunnen hebben in hun eigen persoonsgegevens. Voorts moeten zij hun persoonsgegevens kunnen verbeteren, aanvullen of (laten) verwijderen. Hierop kunnen uitzonderingen worden gemaakt wanneer dat tot een onevenredige inspanning of kosten voor de organisatie zou leiden in verhouding tot de privacyrisico's voor de betrokkene, of wanneer derden daardoor zouden worden benadeeld.

Security:
Organisaties zijn verplicht redelijke maatregelen te treffen ter beveiliging van de persoonsgegevens tegen verlies, misbruik en onrechtmatige toegang, verspreiding, wijziging en vernietiging.

Data integrity
De persoonsgegevens moeten relevant zijn met het oog op het doel waarvoor ze worden gebruikt. Een organisatie moet redelijke maatregelen treffen die dat verzekeren en dat de gegevens betrouwbaar zijn, juist, volledig en actueel.

Enforcement:
Om de naleving van de *safe harbor principles* te kunnen garanderen, is nodig (a) een onafhankelijke instantie die de klachten en geschillen van betrokkenen kan onderzoeken en oplossen en geleden schade kan worden vergoed, volgens toepasselijk recht of zelfregulering; (b) procedures ter verificatie dat organisaties zich houden aan de *safe harbor principles* waaraan zij zich hebben gecommitteerd; en (c) verplichtingen tot het oplossen van problemen die voortvloeien uit het niet naleven van de *safe harbor principles*. Sancties moeten voldoende streng zijn om de naleving van de principles te garanderen. Organisaties die niet jaarlijks hun deelname aan de *safe harbor principles* verlengen, worden niet langer opgenomen op de *safe harbor list* en de daarbij behorende voordelen kunnen niet langer worden gegarandeerd.

Teneinde nadere richting te geven aan de inhoud van deze principles, heeft de *Department of Commerce* een aantal *frequently asked questions* (FAQs) en antwoorden gepubliceerd die opheldering moeten geven over en een aanvulling betekenen op de *safe harbor principles*.

5.7 Keurmerken[110]

Keurmerken kan men onderscheiden in eerstegraads, tweedegraads en derdegraads keurmerken.[111] Een eerstegraads keurmerk komt tot stand via een proces van certificatie. Het geeft aan dat een product of dienst is gecertificeerd door een onafhankelijke instantie, die heeft geoordeeld dat is voldaan aan vooraf gespecificeerde eisen en het certificaat heeft afgegeven als bewijs daarvan. Van certificering onder accreditatie is sprake als de onafhankelijke deskundige instantie is erkend door de Raad voor Accreditatie. Certificatie onder accreditatie bevat aldus waarborgen voor de kwaliteit. Men spreekt van een tweedegraads keurmerk als het door een brancheorganisatie of een andere instelling wordt verleend. Een voorbeeld is het Keurslagerslogo. Kenmerkend is dat er geen toezicht wordt uitgeoefend door een onafhankelijke instantie op de keurmerkverlenende instelling. De derdegraads keurmerken wekken slechts de indruk dat ze keurmerken zijn, maar zijn dat niet. Een voorbeeld is het Euroshopper-logo van Albert Heijn. Dat is een keurmerk dat door het bedrijf zelf aan een product wordt gegeven zonder dat daarop externe controle wordt uitgeoefend en waarvan de betekenis voor de consument moeilijk is in te schatten.

Een privacykeurmerk is in wezen een kwaliteitslabel dat aan een website wordt verleend dat voldoet aan het naleven van een privacybeleid. In de loop der tijd zijn er uiteenlopende privacykeurmerken ontstaan, zoals TRUSTe[112], the Better Business Bureau (BBB)[113] en WebTrust[114]. Het betreft hier Amerikaanse organisaties die zich echter ook op de internationale markt willen richten. Enkele ervan zijn al in Europa actief. Tegelijkertijd worden soortgelijke initiatieven in Europa ontplooid met eveneens internationale ambities, zoals door L@belsite in Frankrijk of Web Trader, dat inmiddels is opgedoekt, maar waaraan werd deelgenomen door consumentenorganisaties uit België, Frankrijk, Italië, Nederland, Portugal, Spanje en het Verenigd Koninkrijk.

Een privacylabel wordt toegekend aan bedrijven die voldoen aan een reeks door de keurmerkorganisatie opgestelde eisen. Door periodieke controles uit te voeren, kunnen deze organisaties een zekere mate van toezicht uitoefenen op de correcte inachtneming van het (openbaar gemaakte) privacybeleid van een onderneming die het keurmerk

110. Zie ook: Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* goedgekeurd op 21 november 2000, WP37, p. 95 e.v.
111. B. Baarsma e.a., *Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten,* Onderzoek in opdracht van het Ministerie van Economische Zaken. Amsterdam: Stichting voor Economisch Onderzoek, april 2003. SEO-rapport no. 664, p. 32.
112. TRUSTe, *Make Privacy Your Choice*, op internet: <http://www.truste.org>. Laatst bezocht 18 september 2003.
113. BBBOnLine, *Privacy Program*, op internet: <https://www.bbbonline.org/privacy/>. Laatst bezocht 18 september 2003.
114. WebTrust – Consumers, op internet: <http://www.cpawebtrust.org/consumer.htm>. Laatst bezocht 18 september 2003.

voert. In sommige gevallen behandelt de keurmerkorganisatie tevens de klachten die over de bedrijven met het keurmerk op hun website worden ingebracht.

Het keuren van privacyvoorzieningen werpt volgens de Artikel 29 Werkgroep echter wel een aantal vragen op. Ten eerste stelt de werkgroep vragen bij de inhoud van een keurmerk. De bescherming van persoonsgegevens in Europa bestaat uit een aantal basisbeginselen, zoals het recht op informatie, toegang, het beginsel van noodzakelijkheid, het recht op bezwaar, de beginselen van rechtmatigheid en evenredigheid en de verplichting om de nationale instantie voor gegevensbescherming in te lichten. Omdat niet alle keurmerken even serieus genomen kunnen worden, dreigen forse maatschappelijke risico's door het gevaar van misleidende privacykeurmerken.

Een tweede vraag die de werkgroep zich stelt heeft betrekking op de controle op het privacybeleid van de website: (1) Wie voert ze uit, op welke manier en met welk soort mandaat van de gecontroleerde partij? (is de betrokkene zelf de controleur?) (2) Wie betaalt? (de bedrijven zelf die voorwerp van controle zijn?) (3) Zijn er sancties en zo ja, welke?

Niettemin is de werkgroep van mening dat deze problemen kunnen worden aangepakt, zodat privacykeurmerken wel degelijk een positieve rol in de bescherming van persoonsgegevens kunnen spelen. In de eerste plaats zou met betrekking tot de inhoud (voorwaarden) van het keurmerk gestreefd moeten worden naar een Europese norm voor privacykeurmerken dat een opgave bevat van de eisen waaraan een dergelijk keurmerk moet voldoen. Zolang het voor internetgebruikers maar voldoende duidelijk is welke keurmerken aan de Europese normen voldoen, kunnen verschillende keurmerken naast elkaar blijven bestaan.

Ten tweede, wat de controle op de privacypraktijken van websites betreft is de betrouwbaarheid van websites met keurmerken op dit punt aanzienlijk te verbeteren door hun beheerders te verplichten tot het ondergaan van periodieke audits. De beoogde Europese norm voor privacykeurmerken zou deze eis kunnen inhouden, samen met een beschrijving van de wijzen waarop dergelijke verplichte controles mogen worden uitgevoerd: bijvoorbeeld in eigen regie aan de hand van een voorgeschreven checklist of door andere partijen.

5.8 Privacy policies en de privacy van kinderen

De Amerikaanse COPPA

Een bijzondere context waarbinnen privacy policies in de VS moeten worden toegepast is die van websites voor kinderen.[115] In de VS is het verzamelen van persoonsgegevens van

115. Zie ook: Sjaak Nouwt, Kid's Privacy on the Internet, Collecting Children's Personal Data on the Internet and the Protection of Privacy, *Multimedia und Recht*, 11/2002, p. 703-709; J. Holvast en J. Nouwt, Privacy van kinderen op internet is al bij wet geregeld, *Nederlands Juristen Blad*, 2002, afl. 22, p. 1063-1065; J. Nouwt, Kinderen, internet en privacy, *Privacy & Informatie* 2003, nr. 2, p. 59-65.

kinderen via internet wettelijk geregeld in de Children's Online Privacy Protection Act (COPPA, 21 april 2000). Deze wet schrijft voor dat website aanbieders in een privacy policy op de website moeten omschrijven wanneer en hoe men verifieerbare toestemming van de ouders verkrijgt en welke verplichtingen de website aanbieder heeft ter bescherming van de privacy van kinderen de beveiliging van hun persoonsgegevens. De COPPA is van toepassing op commercieel handelende website aanbieders en internet service providers die zich nadrukkelijk richten tot kinderen tot 13 jaar. Daarnaast is de COPPA van toepassing op website aanbieders die zich weliswaar niet uitsluitend richten op kinderen, maar die wel willens en wetens persoonsgegevens via kinderen op internet verzamelen.

De COPPA is, zoals gezegd, van toepassing op het verzamelen van persoonsgegevens van kinderen tot 13 jaar. Persoonsgegevens betekenen hier: individueel identificeerbare informatie met betrekking tot een kind, welke informatie online is verzameld. Dergelijke informatie kan bijvoorbeeld bestaan uit: de volledige naam, adres, e-mail adres, telefoonnummer of enige andere informatie waardoor het kind kan worden geïdentificeerd of gecontacteerd. De COPPA heeft ook betrekking op persoonsgegevens zoals hobby's, interesses en informatie die door middel van 'cookies' of andere 'tracking' technieken is verzameld.

Om te kunnen bepalen in hoeverre een website specifiek op kinderen is gericht, kunnen verschillende factoren worden gebruikt. Door de Amerikaanse Federal Trade Commission (FTC) zijn de volgende factoren bepalend daarvoor:

- Het onderwerp van de website;
- De inhoud in de vorm van beeld en geluid;
- De leeftijd van de modellen die op de website zijn afgebeeld;
- Het taalgebruik op de website;
- Of advertenties op de website is gericht op kinderen;
- Informatie die duidelijk is gericht op publiek van een bepaalde leeftijd;
- Het gebruik van animaties of andere toepassingen die op kinderen zijn gericht.

De FTC heeft een aantal praktische richtlijnen gepubliceerd voor website aanbieders en ouders, alsmede voor leraren, over hoe de privacy van kinderen op internet te beschermen.[116]

Privacy policy

De aanbieder van een website die is gericht op kinderen is verplicht een privacy policy of privacystatement op de homepage van de website of van de online aangeboden dienst te

116. Federal Trade Commission, *How to protect Kid's Privacy Online*, <http://www.ftc.gov/opa/1999/9902/petapp4.99.htm>, 12 February 1999.

plaatsen. Een privacy policy moet informatie bevatten over het privacybeleid van de website aanbieder. Die informatie moet worden weergegeven op iedere pagina waar persoonsgegevens van kinderen worden verzameld. Een aanbieder van een website die op een algemeen publiek is gericht, maar wel een aparte 'kinderhoek' heeft, moet een link opnemen op die kinderpagina.

Een link naar de privacy policy moet duidelijk en prominent aanwezig zijn. Met het oog daarop is het wenselijk dat de privacy policy voor kinderen in een groter lettertype of in een afwijkende kleur tegen een contrasterende achtergrond op de website wordt gepresenteerd. Een onopvallende link onderaan de internet pagina (zoals zo vaak voorkomt) wordt niet voldoende duidelijk en prominent geacht. Er wordt wel gepleit voor het plaatsen van een grote letter 'K' voor 'Kids' of 'Kinderen', bijvoorbeeld rechtsboven op de homepage.[117] Dat zou direct duidelijk maken dat deze homepage voldoet aan de eisen van de COPPA. Daarnaast wordt ook voorgesteld te streven naar samenwerking tussen website aanbieders, teneinde tot een zekere standaardisering te komen van privacy policies. Ouders kunnen dan sneller en gemakkelijker beoordelen in hoeverre deze website voldoet aan de COPPA. Tegelijkertijd maakt dit het ook gemakkelijker voor website aanbieders om een privacy policy te ontwikkelen die aan de COPPA voldoet.

Volgens de COPPA dient een privacy policy uit de volgende elementen te bestaan:

- De naam en contact informatie (adres, telefoonnummer, e-mail adres) van alle aanbieders die via deze internetpagina of elektronische dienst persoonsgegevens bij kinderen verzamelen of beheren;
- De soorten persoonsgegevens die bij kinderen worden verzameld en op welke wijze (rechtstreeks van het kind of door middel van 'cookies');
- Waarvoor de website aanbieder de persoonsgegevens gebruikt (voor marketing doeleinden of om prijswinnaars te informeren);
- Of de website aanbieder persoonsgegevens aan derden verstrekt en zo ja, wat voor categorie ontvangers dat zijn, de doeleinden waarvoor de gegevens worden gebruikt en of deze ontvangers vertrouwelijkheid en beveiliging van de gegevens hebben toegezegd;
- De mogelijkheid voor ouders om toestemming te verlenen met het verzamelen en gebruiken van de persoonsgegevens zonder tevens in te stemmen met de doorverstrekking van deze gegevens aan derden;
- Dat de website aanbieder niet meer persoonsgegevens bij kinderen verzamelt dan redelijkerwijs nodig is om te kunnen participeren in een bepaalde activiteit (bijvoorbeeld meedoen aan een prijsvraag of toegang verkrijgen tot een chatruimte);

117. Deze maatregel is voorgesteld door het Annenberg Public Policy Center, in het rapport *Privacy Policies on Children's Websites: Do They Play By the Rules?* 28 maart 2001.

- Dat de ouders recht op toegang hebben tot de persoonsgegevens van hun kinderen, alsmede recht op verwijdering daarvan en recht om verdere verzameling of gebruik van die gegevens te verbieden, inclusief de procedures die de ouders daartoe dienen te volgen.

Informatieplicht naar de ouders
De inhoud van de informatieplicht tegenover de ouders bestaat uit een schriftelijke mededeling of een mededeling via een e-mail bericht aan de ouders, dat de website aanbieder persoonsgegevens (en welke) wil verzamelen (of heeft verzameld) bij het kind via internet. De mededeling behelst voorts dat de aanbieder van de website de ondubbelzinnige toestemming nodig heeft van (één van) de ouders om de gegevens te mogen verzamelen, gebruiken en eventueel aan derden verstrekken.

Verifieerbare ouderlijke toestemming
De aanbieder van de website dient op grond van de COPPA voorts redelijke maatregelen te treffen waardoor zekerheid bestaat dat de ouder(s) op de hoogte is (zijn) van de gegevensverzameling teneinde vervolgens daarvoor toestemming te kunnen geven. Bij uitsluitend intern gebruik van de gegevens gelden minder strenge eisen dan bij doorverstrekking naar derden. Bij beperking tot intern gebruik kan worden volstaan met via e-mail verkregen toestemming. Maar wanneer het de bedoeling is dat de gegevens ook aan derden worden verstrekt, gelden strengere eisen:

- een door (één van) de ouders ondertekend formulier, dat per post of fax is ingestuurd;
- acceptatie en verificatie van een credit card nummer, in combinatie met een transactie;
- een speciale gratis telefoonlijn voor ouders waar deskundig personeel de ouders te woord kunnen staan; of
- een e-mail bericht voorzien van een digitale handtekening.

Uitzonderingen
Voor aanbieders van populaire online diensten bestaan enkele uitzonderingen op het vereiste van toestemming van de ouders. Wanneer met het oog op een populaire toepassing voor kinderen, zoals een prijsvraag, een elektronische nieuwsbrief, hulp bij huiswerk of elektronische ansichtkaartdiensten, bijvoorbeeld het e-mail adres van het kind wordt verzameld, is de ouderlijke toestemming niet nodig. Verder is de ouderlijke toestemming evenmin vereist:

- als een aanbieder het e-mail adres van (één van) de ouders verzamelt teneinde aan zijn informatieplicht te kunnen voldoen en om ouderlijke toestemming te kunnen vragen;
- als een aanbieder eenmalig een e-mail adres van een kind verzamelt teneinde aan een eenmalig verzoek van het kind te kunnen voldoen;

- als een aanbieder een e-mail adres verzamelt teneinde meer dan eens te kunnen communiceren op een specifiek verzoek, zoals het versturen van een nieuwsbrief. In dat geval dient de aanbieder wel de ouders te informeren dat er regelmatig met het kind gecommuniceerd zal worden. Daarbij dient de ouders de gelegenheid te worden geboden om de toezending te stoppen;
- als een aanbieder de naam of correspondentiegegevens van het kind verzamelt, teneinde de veiligheid van het kind op de site te kunnen garanderen. In dat geval dient de aanbieder de ouders te informeren en deze de gelegenheid bieden verder gebruik van de gegevens te verbieden;
- als een aanbieder de naam of correspondentiegegevens van het kind verzamelt, teneinde de beveiliging of aansprakelijkheid van de website te beschermen, of om te kunnen voldoen aan een justitieel bevel.

Nieuwe mededeling
Een nieuwe informatieplicht ontstaat als er wijzigingen zijn in het verzamelen, het gebruik en de verstrekking van de gegevens, wanneer ouders met een eerdere verzameling hebben ingestemd. Het geval kan zich voordoen als gegevens zijn verzameld van een kind in het kader van een prijsvraag, maar de aanbieder wil dat kind een nieuwe dienst aanbieden, bijvoorbeeld de toegang tot een chat-room.

Verificatie bij inzage
Ouders hebben in beginsel recht op inzage in de gegevens die bij hun kinderen zijn verzameld. Wanneer van dat recht gebruik wordt gemaakt, is de aanbieder van de website verplicht de identiteit van de ouders vast te stellen. Hij kan dat doen op (één van) de volgende wijzen:

- via een daartoe ondertekend formulier van de ouders worden verkregen per reguliere post of fax;
- via een geaccepteerd en geverifieerd credit card nummer;
- via een gratis telefoonlijn die wordt bezet door getraind personeel;
- een e-mail vergezeld van een digitale handtekening;
- een e-mail vergezeld van een PIN of wachtwoord, verkregen via één van bovenstaande andere verificatiemethoden.

Intrekking toestemming en verwijdering van de gegevens
Ouders mogen te allen tijde hun verleende toestemming voor het verzamelen en verder gebruiken van persoonsgegevens die bij hun kinderen zijn verkregen intrekken. Voorts kunnen zij opdracht geven tot het vernietigen van de bij hun kinderen verzamelde gegevens. Dit kan uiteraard wel tot gevolg hebben dat de dienst niet langer kan worden aangeboden aan het kind (zoals de toegang tot een chat-room).

Vergelijking met Nederland

Een vergelijking met de Nederlandse bescherming van persoonsgegevens van kinderen op internet dringt zich op.[118] De Wbp is op 1 september 2001 in werking getreden. Voor de toelaatbaarheid van het verzamelen en verwerken van persoonsgegevens is een aantal beginselen alles bepalend: er moet een welomschreven, gerechtvaardigde doelstelling zijn voor het verzamelen van de persoonsgegevens (artikel 7), er moet een rechtmatige grondslag voor de verwerking van de gegevens zijn (artikel 8) en voor de verdere verwerking of verspreiding van de verzamelde persoonsgegevens is het verenigbaar gebruik bepalend (artikel 9). Van deze beginselen is de rechtmatige grondslag van eminent belang voor zowel de rechtmatigheid van het doel als voor de verdere verwerking. De memorie van toelichting (blz. 79) bij de Wbp is in dezen volstrekt helder: indien gegevens in strijd met artikel 8 worden bewaard dan is niet voldaan aan het gerechtvaardigde doel en mogen de gegevens niet worden verzameld.

De enige grondslag waarop de verwerking kan worden gebaseerd is de ondubbelzinnige toestemming van de betrokkene.[119] Aangezien gegevens bij kinderen worden verzameld is artikel 5 van de Wbp relevant. In dat artikel wordt aangegeven dat indien de betrokkene minderjarig is en de leeftijd van zestien jaar nog niet heeft bereikt, in plaats van de betrokkene de toestemming van de wettelijke vertegenwoordiger nodig is.

De Wbp kent geen uitdrukkelijke verplichting tot het publiceren van een privacy policy op een webpagina. Maar op grond van de artikelen 33 en 34 bestaat er wel een informatieplicht voor de verantwoordelijke (de website aanbieder) jegens de betrokkene (het kind en diens ouders).[120] De verantwoordelijke is verplicht om, vóór het moment van verkrijging van de persoonsgegevens, de bezoeker van de website de identiteit van de verantwoordelijke, de doeleinden van de gegevensverwerking, alsmede nadere informatie mee te delen, voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen (i.c. via kinderen) of het gebruik dat er van wordt gemaakt, nodig is om tegenover de betrokkene (i.c. de kinderen en de ouders) een behoorlijke en zorgvuldige verwerking te waarborgen. Als het een commerciële website betreft, kan daarbij tevens de informatie worden verstrekt die verplicht is op grond van artikel 7:46c BW (Wet koop op afstand).

In dit voorbeeld luidt de conclusie voor ons land dat het verzamelen van persoonsgegevens bij kinderen niet toelaatbaar is zonder de ondubbelzinnige toestemming van (veelal) de ouders. In tegenstelling tot de Verenigde Staten geldt op grond van de Wbp in ons

118. Zie hierover: J. Holvast en J. Nouwt, Privacy van kinderen op internet is al bij wet geregeld, *Nederlands Juristen Blad*, 2002, afl. 22, p. 1063-1065.
119. Voor een nadere uitleg en argumentatie zij verwezen naar J. Holvast en J. Nouwt, Privacy van kinderen op internet is al bij wet geregeld, *Nederlands Juristen Blad*, 2002, afl. 22, p. 1063-1065.
120. Zie hierover ook: A. Holleman, Privacystatements op het internet, *Privacy & Informatie* 2003, nr. 6, p. 253-258.

land een leeftijdsgrens van zestien jaar, waarmee de regeling de facto en de jure in Nederland strenger is dan in de VS. Een uitdrukkelijke plicht tot het publiceren van een privacy policy op de webpagina bevat de Wbp niet. De informatieplicht van de Wbp brengt echter met zich mee dat het niet voldoende informeren van betrokkenen over de verwerking van persoonsgegevens via internet, leidt tot onrechtmatige verwerking van persoonsgegevens. Om hier invulling aan te geven, kan bijvoorbeeld aansluiting worden gezocht bij de inhoud van privacy policies volgens de COPPA.

5.9 Conclusie

In dit hoofdstuk werd het tweede deel van de derde onderzoeksvraag behandeld: "Welke zelfreguleringsinitiatieven voor gegevensbescherming kunnen we onderscheiden?" Daarbij werd nader ingegaan op het concept van zelfregulering en zijn diverse voorbeelden van zelfreguleringsinitiatieven ter bescherming van persoonsgegevens op internet beschreven.

Zelfregulering valt te overwegen in de volgende gevallen: wanneer het gedrag van 'professionals' moet worden gereguleerd, in situaties waarin individuele of groepsbelangen niet te zeer verschillen van het belang dat de desbetreffende wet beoogt te dienen en in omstandigheden waarin (volledige) overheidsregulering niet of slechts zeer moeizaam te controleren en te handhaven is. Met name op basis van de als laatste genoemde omstandigheden, lijkt zelfregulering voor de privacybescherming van de consument op internet een nuttig instrument.

De Stichting voor Economisch Onderzoek (SEO) publiceerde in 2003 een onderzoeksrapport waarin 22 verschillende zelfreguleringsinstrumenten worden onderscheiden. Deze kunnen in vijf clusters worden onderverdeeld: 1) techniekgerichte instrumenten, 2) gedragsgerichte instrumenten, 3) informerende instrumenten, 4) contractuele instrumenten en 5) geschilbeslechtende instrumenten. Als zesde cluster worden de publiekrechtelijke beroepsorganisaties genoemd. Dat cluster is een zeer vergaande vorm van zelfregulering die op de grens ligt tussen zelfregulering en overheidsregulering.

Op techniekgerichte instrumenten wordt in het volgende hoofdstuk ingegaan. In dit hoofdstuk zijn enkele voorbeelden uit de andere clusters beschreven. De gedragscode is een voorbeeld van een gedragsgericht instrument. Het privacykeurmerk is een voorbeeld van een informerend instrument. De modelcontracten van de International Chamber of Commerce en van de Europese Commissie in verband met de doorgifte van persoonsgegevens naar derde landen, zijn voorbeelden van contractuele instrumenten. Het *enforcement principle* in de Safe Harbor Principles is een voorbeeld van een geschilbeslechtend instrument.

Zelfregulering blijkt uitdrukkelijk op de beleidsagenda's van enkele internationale organisaties voor te komen. Dat geldt in elk geval voor de Europese Unie, de OESO en de VN, in het bijzonder de ITU. Zelfregulering heeft vooral de aandacht van deze organisaties vanuit het perspectief van het internet en de elektronische handel.

Uit het voorbeeld met betrekking tot het verzamelen van persoonsgegevens bij kinderen blijkt dat commercieel handelende website aanbieders en internet service providers zich onder andere richten tot de doelgroep van kinderen tot 13 jaar. Dit is uit marketingoogpunt kennelijk een interessante doelgroep voor bedrijven die hun producten en diensten aanbieden via internet. Tegelijkertijd is hier sprake van een redelijk naïeve doelgroep. Jonge kinderen kunnen niet altijd de gevolgen van hun handelen op internet overzien. Waar de volwassen consument bij het verrichten van een koop op afstand al extra consumentenbescherming geniet, is een dergelijke bescherming zeker op zijn plaats voor kinderen jonger dan 13 jaar. Het is daarom nodig en wenselijk zowel kinderen als ouders duidelijk worden geïnformeerd en dat ouders enige controle kunnen uitoefenen over het verzamelen van de persoonsgegevens van hun kinderen via internet.

De in dit hoofdstuk besproken voorbeelden van zelfregulering (gedragscodes, contractuele regelingen, Safe Harbor programma, privacykeurmerken en privacy policies) hebben nog niet geleid tot een sluitende en betrouwbare bescherming van de consumentenprivacy op internet. Daarom worden in het volgende hoofdstuk instrumenten besproken met behulp waarvan de consument door eigen handelen de bescherming van zijn privacy op internet kan bevorderen.

6 Zelfregulering via techniek

6.1 Inleiding

Hiervoor zijn al voorbeelden beschreven van zelfreguleringsinitiatieven op regelingniveau. Hier wordt ingegaan op technische mogelijkheden voor zelfregulering in de vorm van privacy zelfbescherming. In het onderzoeksrapport *Zelf doen?*[121] worden deze aangeduid als techniekgerichte instrumenten van zelfregulering. Dit hoofdstuk staat in het teken van de vierde onderzoeksvraag, die luidt:

"Welke bescherming kan de techniek zelf bieden?"

Volgens de Artikel 29 Werkgroep, vormt het doelbeginsel het uitgangspunt voor de zogenoemde privacybevorderende maatregelen.[122] Het begrip 'privacybevorderende *maatregelen*' is ruimer dan het begrip 'privacybevorderende *technieken*' of 'Privacy Enhancing Technologies' (PET). Privacybevorderende maatregelen omvatten zowel technische als organisatorische voorzieningen ter bescherming van de privacy.

Het begrip 'privacybevorderende maatregelen', zoals dat door de Artikel 29 Werkgroep wordt gehanteerd, is een begrip dat uiteenlopende methoden omvat ter verdediging van de persoonlijke privacy, met name door het terugdringen of onmogelijk maken van het verzamelen of verwerken van identificeerbare gegevens. Privacybevorderende maatregelen zijn gericht op het voorkomen van onrechtmatige vormen van verwerking door het bijvoorbeeld voor ongeautoriseerde personen technisch onmogelijk te maken om toegang te krijgen tot persoonsgegevens en zo eventuele vernietiging, wijziging of inzage ervan te verhinderen. Hieronder komen enkele voorbeelden van dergelijke maatregelen aan de orde.

6.2 Digitale pseudoniemen

De technieken die als privacybevorderende maatregel worden gebruikt zijn veelal gebaseerd op de toepassing van een zogenoemde identiteitsbeschermer. Een identiteits-

121. B. Baarsma e.a., *Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten*. Onderzoek in opdracht van het Ministerie van Economische Zaken. Amsterdam: Stichting voor Economisch Onderzoek, april 2003, SEO-rapport no. 664.
122. Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* WP 37, 21 november 2000, p. 88 e.v.

beschermer is te beschouwen als een onderdeel in een informatiesysteem dat het vrijgeven van de identiteit van een persoon bij de diverse processen binnen het informatiesysteem regelt. De taak ervan is er op gericht om bepaalde gebruikersdomeinen van het systeem die geen inzage behoeven te hebben van de ware identiteit af te schermen. Eén van de voornaamste functies van de identiteitsbeschermer is de echte naam van een gebruiker om te zetten in een pseudo-identiteit, dat wil zeggen een vervangende (digitale) identiteit die de gebruiker bij het werken met het systeem kan aannemen.

Een identiteitsbeschermer kan op verschillende manieren aan een informatiesysteem worden toegevoegd. Enkele voorbeelden zijn: encryptietechnieken met gebruikmaking van digitale handtekeningen, blinde handtekeningen, digitale pseudoniemen en vertrouwde derden.[123]

6.3 Anonymizers

Anonimiseringssoftware stelt internetgebruikers in staat om bij een bezoek aan een website anoniem te blijven. Daartoe moet de gebruiker eerst naar een andere website gaan waar de eigen identiteit onherkenbaar wordt gemaakt. Voorbeelden van dit soort websites zijn The Anonymizer[124], het Zero Knowledge System[125] en iPrivacy[126].

The Anonymizer functioneert als tussenstation dat bij sitebezoeken van gebruikers zijn/haar identiteit absoluut verborgen houdt voor privacyaantastende traceringsmethoden. Voorts houdt The Anonymizer internetprogramma's tegen die ingebed zijn in webpagina's (Java en JavaScript) en de computer van de gebruiker kunnen beschadigen dan wel gevoelige persoonlijke gegevens kunnen verzamelen.

The Anonymizer biedt diverse producten aan. *Private Surfing* is een pakket dat de internetgebruiker onzichtbaar houdt voor websites en on-line adverteerders, beschermt de persoonsgegevens van de gebruiker tegen spammers, maakt het mogelijk te internetten op het werk, zonder gemonitord te worden door de baas of door collega's, maakt het mogelijk geheel anoniem foto's, films en muziek te downloaden van internet en garandeert veilig winkelen op internet.

Het pakket *Total Net Shield* bestaat uit *Private Surfing*, maar uitgebreid met *secure tunneling*, waardoor al het verkeer van en naar de computer van de eindgebruiker versleuteld wordt. Daarnaast bestaat de uitbreiding onder meer uit de mogelijkheid om veilig en anoniem te e-mailen, aan nieuwsgroepen deel te nemen en anoniem en veilig te chatten.

123. Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* WP 37, 21 november 2000, p. 88.
124. Anonymizer, *Online Privacy and Security.* Op internet: <http://www.anonymizer.com>, laatst bezocht op 28 mei 2003.
125. Zero Knowledge, *Zero Knowlegde Systems*. Op internet: <http://www2.zeroknowledge.com/>, laatst bezocht op 28 mei 2003.
126. iPrivacy, *Welcome*. Op internet: <http://www.iprivacy.com/index.html>, laatst bezocht op 28 mei 2003.

Internetgebruikers moeten wel altijd verbinding zoeken met de Anonimyzer-website. Dat maakt deze dienst zeer kwetsbaar voor bewaking door derden. Bij het surfen, mailen en bestandsoverdracht functioneert de Anonymizer technisch gesproken als een proxy-server die de chattering van HTTP-browsers en het IP-adres van de surfer ontraceerbaar maakt.

Een bezwaar van het gebruik deze diensten is dat de internetgebruiker het bedrijf moet vertrouwen, terwijl dit bedrijf op de hoogte is van alles dat de gebruiker op het internet doet.

Het Zero Knowledge System biedt het softwarepakket *Freedom* aan. *Freedom* kent drie varianten: de *Security Bundle*, bestaande uit de onderdelen Anti-Virus, Firewall en Pop-Up Blocker, *Privacy Bundle*, bestaande uit de onderdelen Firewall, Pop-Up Blocker en Web Secure, en een *Custom Bundle*, waarvan de gebruiker zelf de samenstelling kan bepalen.

Bij deze opzet worden alle verbindingen met websites eerst versleuteld door middel van zware (minstens 128-bit) encryptie en vervolgens gestuurd naar de *Freedom* proxy-server. Vervolgens wordt door de proxy-server verbinding gemaakt met de website, terwijl het IP-adres beschermd wordt en de verbinding beschermd wordt tegen inbreuken op privacy en beveiliging. Ook hackers kunnen geen bestanden of scripts naar de computer van de internetgebruiker sturen. De websites die de gebruiker bezoekt, kunnen geen persoonlijke gegevens traceren of het surfgedrag monitoren.
Het systeem iPrivacy biedt consumenten en bedrijven de faciliteit om de online identiteit op brede schaal op internet te beschermen. iPrivacy biedt die identiteitsbescherming door middel van een proxy-server die de volgende drie soorten gegevens afschermt voor derden: persoonlijke informatie zoals naam, adres, telefoonnummer, credit cardnummer, on-line informatie, zoals e-mailadres en IP-adres, en informatie over het surfgedrag op internet, inclusief koopgedrag en cookies.

Het onder de naam iPrivacy aangeboden systeem maakt, zo stelt men, anonieme e-handel mogelijk, van surfen tot en met aanschaf en levering. Consumenten kunnen ermee browsen en internet afzoeken, er aankopen doen en deze ook laten afleveren zonder dat de identiteit van de ontvanger daarbij kenbaar wordt. Volgens de makers zouden zelfs zij de ware identiteit van de consumenten die hun diensten gebruiken niet kennen. Bij transacties beschikken alleen de klant zelf en de creditcardgebruiker over enige persoonlijke informatie aangaande de on line gedane aankoop.[127]

6.4 Cookie crunchers

Op internet zijn veelal gratis of als shareware programma's tegen cookies te vinden, die elke internetgebruiker op de computer kan installeren.[128] Voorbeelden daarvan zijn Cookie

127. Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* WP 37, 21 november 2000, p. 90-92.
128. Zie bijvoorbeeld < http://cookies.pagina.nl/>.

Washer, Cookie Master en Cookie Cruncher. Deze programma's tegen cookies kennen echter ook enkele nadelen. Zo moet de internetgebruiker zijn/haar cookiebestanden dagelijks geval voor geval doornemen omdat de cookies van aard kunnen verschillen. Bij shareware-programmatuur moet de internetgebruiker soms betalen om zich te beschermen. De wijze waarop men met de anti-cookie programmatuur moet omgaan is niet altijd erg gebruikersvriendelijk en voor een gemiddelde internetgebruiker soms niet eenvoudig te begrijpen.[129]

6.5 Proxy-servers

Een proxy-server is een computer die een soort tussenstation vormt tussen de gebruiker en het internet. Een proxy-server fungeert als webcache en levert daardoor een drastische verbetering op van de internetfunctionaliteit. Veel grote internetaanbieders en organisaties hebben een proxy-server geïnstalleerd. Het heeft tot gevolg dat elke pagina, elk beeld of logo dat van buiten de organisatie zelf door een gebruiker van de organisatie wordt binnengehaald, wordt opgeslagen in het cachegeheugen, waardoor die informatie voor andere gebruikers binnen die organisatie ogenblikkelijk en dus sneller beschikbaar is.

Bij gebruik van een proxy-server is het niet nodig dat elke individuele gebruiker binnen de organisatie een eigen IP-adres heeft. Proxy-servers geven in de regel ook geen IP adressen van de internetgebruikers aan websites door en ze kunnen met filters de chattering van browsers tegenhouden. Omdat proxy-servers met het HTTP-protocol werken, kunnen cookies die opgeslagen zijn in de HTTP-header gemakkelijk door de server worden verwijderd, veranderd of opgeslagen.[130]

6.6 P3P

Het Platform for Privacy Preferences Project (P3P) is een groeiende industriestandaard die het websites mogelijk maakt hun privacybeleid uit te drukken in een gestandaardiseerd formaat, dat automatisch wordt opgehaald en beoordeeld door 'user agents'. P3P heeft tot doel internetgebruikers te helpen informeren over het privacybeleid van websites door het lezen ervan te vereenvoudigen. Met P3P hoeft een gebruiker niet elke privacy policy te lezen op iedere website die hij bezoekt. Informatie over de gegevens die door een website worden verzameld worden automatisch meegedeeld aan de gebruiker. Verschillen tussen de privacypraktijk van een website en de voorkeuren van de gebruiker worden automatisch gesignaleerd.

129. Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* WP 37, 21 november 2000, p. 90.
130. Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* WP 37, 21 november 2000, p. 90.

In april 1998 heeft de Internationale Werkgroep voor Gegevensbescherming en Telecommunicatie een gemeenschappelijke verklaring uitgebracht over essentiële kenmerken van (o.a. P3P) privacybevorderende technologieën op het internet[131]. Dit document bevat een overzicht van een drietal essentiële voorwaarden waaraan ieder technisch platform voor privacybescherming op het internet moet voldoen teneinde het systematisch verzamelen van persoonsgegevens te voorkomen. De eerste voorwaarde luidt, dat technologie dient te worden toegepast binnen de grenzen van een regelgevend kader, omdat technologie op zichzelf genomen geen privacy op internet kan waarborgen. De tweede voorwaarde luidt, dat iedere gebruiker op internet te mogelijkheid moet hebben om anoniem op het internet te surfen. Dezelfde voorwaarde geldt voor de situatie dat men informatie uit het publieke domein wil opvragen. De derde voorwaarde luidt, dat vóórdat persoonsgegevens, met name die welke door een gebruiker zijn verschaft, door een websitebeheerder worden verwerkt, deze de weloverwogen toestemming van de betrokkene moet verwerven. Bovendien moet het technische platform in de toestemmingsprocedure enkele basisvoorwaarden ingebouwd hebben die niet kunnen worden overzien of uitgeschakeld.[132]

Twee maanden later, in juni 1998, gaf ook de Artikel 29 Werkgroep haar mening.[133] Hierin wordt onderstreept dat een technisch platform voor privacybescherming op zichzelf met betrekking tot privacy op het Web niet volstaat. Het moet, aldus de Werkgroep, werken binnen het juridische kader van verplichtende bepalingen voor gegevensbescherming die iedere persoon een niet onderhandelbaar minimum aan privacy bieden. Verder is in dit advies een aantal specifieke punten vermeld die de invoering van zo'n systeem binnen de Europese Unie met zich zou brengen.

De Artikel 29 Groep is van mening dat P3P binnen het kader van Richtlijn 95/46/EG naar verwachting een positieve rol kan spelen. Zo kan volgens de Artikel 29 Groep P3P bijdragen aan de standaardisatie van privacystatements. Op zichzelf leveren die weliswaar geen privacybescherming, maar de bredere toepassing ervan kan wel de transparantie van gegevensverwerking op internet sterk verbeteren en dat kan bijdragen aan een betere privacybescherming. Voorts kan P3P meer keuzemogelijkheden bieden op het gebied van privacyniveaus, met inbegrip van anonimiteit en pseudoniemgebruik. De artikel 29 Groep wijst echter ook op de beperkingen van P3P. Zo kan P3P de privacy van gebrui-

131. International Working Group on Data Protection in Telecommunications, *Common position on Essentials for privacy-enhancing technologies (e.g. P3P) on the World-WideWeb,* adopted at the 23rd Meeting in Hong Kong SAR, China, 15 april 1998. Op internet: <http://www.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm>, laatst bezocht op 28 mei 2003.
132. Zie Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming.* WP 37, 21 november 2000, p. 94.
133. Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Advies 1/98 Platform for Privacy Preferences (P3P) en de Open Profiling Standard (OPS*), goedgekeurd door de Groep op 16 juni 1998. WP 11, XV D/5032/98.

kers niet beschermen in landen waar de privacywetgeving onvoldoende is. P3P is immers niet in de positie om het overheidsbeleid te bepalen en kan evenmin de eigen specificaties verplicht aan de markt opleggen. Voorts kan P3P niet garanderen dat bedrijven een privacybeleid hanteren en heeft het in feite geen middelen om te waarborgen dat een site zich aan de eigen beweringen houdt. Sancties voor het geval men zich niet aan eigen intentieverklaringen houdt zijn alleen te realiseren door middel van wetgeving of via het lidmaatschap van een orgaan met zelfopgelegde eigen regelgeving.[134]

P3P voorziet in een technische maatregel die de internetconsument helpt bij het informeren over gehanteerde privacy policies voordat zij persoonlijke informatie afstaan. Het bevat geen voorziening die ook garandeert dat de betreffende website handelt overeenkomstig de gepubliceerde privacy policy. P3P is bedoeld ter aanvulling op centrale wetgeving en op zelfreguleringsinitiatieven die kunnen helpen bij de naleving van website policies. Hoewel P3P geen mechanismen bevat voor de verstrekking of beveiliging van persoonsgegevens, kan het wel worden ingebouwd in toepassingen die zijn ontwikkeld om verstrekking van persoonsgegevens mogelijk te maken.

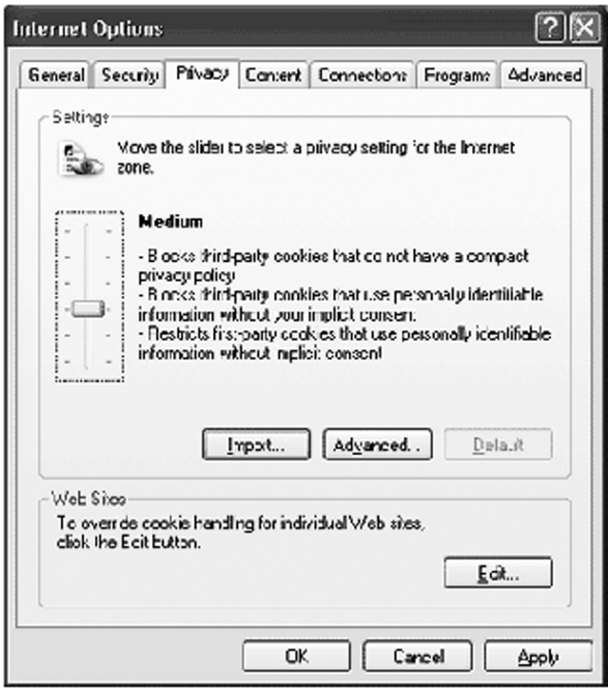
Een voorbeeld van een toepassing waarin P3P is ingebouwd, is Microsoft's Internet Explorer, versie 6 (IE6).[135] Volgens de uitleg die Microsoft zelf geeft, draagt IE6 bij aan de privacybescherming van de gebruiker doordat het de gebruiker meer controle biedt over de cookies en meer informatie verschaft over de privacy policy van een website. Een cookie is een klein tekstbestand dat wordt aangemaakt door een website op de PC van de internetgebruiker. Het zorgt ervoor dat de website automatisch over bepaalde informatie van de gebruiker beschikt, zoals instellingen van de browser, of naam, adres of telefoonnummer, zodra de gebruiker een volgende keer de website raadpleegt. Een website privacy policy informeert de websitebezoeker over de gegevens die door de site worden verzameld, hoe die gegevens worden gebruikt door die website en aan wie die gegevens worden verstrekt.

In IE6 is het mogelijk dat de gebruiker er van de eigen privacyvoorkeuren voor het al dan niet accepteren van cookies instelt. Wanneer men dan een website bezoekt bepaalt IE6 of die website wel P3P informatie verschaft. Van websites die deze informatie verschaffen, vergelijkt IE6 de privacyvoorkeuren van de gebruiker met de informatie over het privacybeleid van de website. Aldus beslist IE6 of cookies al dan niet worden geaccepteerd. Zo is het mogelijk om cookies te blokkeren die tot personen herleidbare gegevens verwerken zonder de toestemming van de betrokkene. Een P3P-conforme website moet een duidelijke omschrijving van de privacy policy bevatten. Dergelijke websites dienen ook de volgende beleidsinformatie te verschaffen:

134. Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming*, WP 37, 21 november 2000, p. 95.
135. Zie ook Microsoft, *Web Privacy*. Op internet: <http://www.microsoft.com/windows/ie/evaluation/overview/privacy.asp>. Gepubliceerd op 27 augustus 2001.

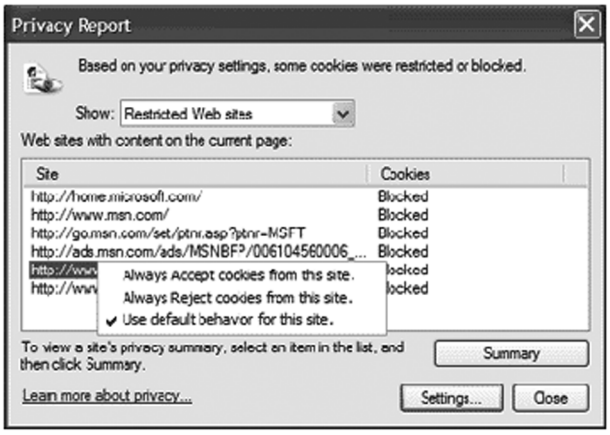
- De organisatie die de gegevens over de gebruiker verzamelt.
- De soort gegevens die worden verzameld.
- Het doel waarvoor de gegevens worden gebruikt.
- In hoeverre de gegevens worden verstrekt aan andere organisaties.
- In hoeverre de betrokkene toegang tot zijn gegevens heeft en invloed heeft op het gebruik van die gegevens door de organisatie.
- Hoe conflicten met de organisatie kunnen worden opgelost.
- Hoe de organisatie de verzamelde gegevens zal bewaren.
- Waar openbaar toegankelijke en gedetailleerde informatie over de privacy policy van de organisatie is te vinden.

Het volgende plaatje van de privacy-tab in IE6 geeft weer op welk niveau het blokkeren van cookies is ingesteld.



In deze privacy-tab kunnen de cookie privacy voorkeuren worden ingesteld, kan men toegang krijgen tot een lijst voor het behandelen van cookies per website en kan men toegang krijgen tot geavanceerde privacy opties. Ook is het mogelijk een bestand te importeren met standaard voorkeuren om te werken met P3P voor het behandelen van cookies.

Het volgende plaatje uit IE6 geeft een privacyrapport weer.



Door middel van dit privacyrapport is het mogelijk een lijst te bekijken van de bouwstenen van een website. Het is mogelijk om privacy samenvattingen van de websites te bekijken en vervolgens te selecteren hoe deze websites met de cookies van de gebruiker moeten omgaan. Het is ook mogelijk toegang te krijgen tot het privacyrapport van een website via de menu-optie View (beeld) en vervolgens op Privacy Report (Privacyrapport) of door te klikken op een privacy icoon op de website, indien aanwezig.

Op grond van artikel 5, derde lid, Richtlijn 2002/58/EG is de aanbieder van een website verplicht de bezoeker te informeren wanneer de website gebruik maakt van het plaatsen van cookies. Overwegingen (24) en (25) van de Richtlijn luiden als volgt:

> (24) Eindapparatuur van gebruikers van netwerken voor elektronische communicatie en in die apparatuur bewaarde informatie maken deel uit van de persoonlijke levenssfeer van de gebruikers die op grond van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden bescherming vereist. Zogeheten spionagesoftware, webtaps, verborgen identificatoren en andere soortgelijke programmatuur kunnen de terminal van de gebruiker zonder diens medeweten binnenkomen teneinde toegang tot informatie te krijgen, verborgen informatie op te slaan of de activiteiten van de gebruiker te traceren en kunnen ernstig inbreuk maken op de persoonlijke levenssfeer van die gebruikers. Het gebruik van die programmatuur dient alleen te worden toegestaan voor legitieme doeleinden met medeweten van de betrokken gebruikers.
>
> (25) Dergelijke programmatuur, bijvoorbeeld zogeheten cookies, kan evenwel een legitiem en nuttig hulpmiddel zijn om bijvoorbeeld de doeltreffendheid van het ontwerp van websites en van reclame te onderzoeken, en om de identiteit te bepalen van gebruikers die on-line- transacties verrichten.Wanneer dergelijke programmatuur, bijvoorbeeld cookies, voor een legitiem doel bestemd is, zoals het vergemakkelijken van de levering van diensten van de informatiemaatschappij, dient hun gebruik te worden toegestaan op voorwaarde dat gebruikers worden voorzien van duidelijke en nauwkeurige informatie, overeenkomstig Richtlijn 95/46/EG, over de doeleinden van cookies of soortgelijke programmatuur, welke verzekert dat de gebruiker zich ervan bewust is dat er informatie op de door hem gebruikte eindapparatuur wordt geplaatst. De gebruikers dienen de gelegenheid te hebben te weigeren dat een cookie of soortgelijke voorziening op hun eindapparatuur wordt opgesla-

gen. Dat is met name belangrijk in situaties waarin ook andere gebruikers toegang hebben tot de eindapparatuur en zo tot op die apparatuur opgeslagen gegevens die privacygevoelige informatie bevatten. De informatie en het recht van weigering kan voor het gebruik van de verschillende programmatuur bestemd om op de eindapparatuur van gebruikers te worden geïnstalleerd, éénmaal gedurende eenzelfde verbinding worden aangeboden en geldt dan ook voor het eventuele verdere gebruik van die programmatuur gedurende volgende verbindingen. De wijze waarop informatie wordt gegeven, een recht van weigering wordt aangeboden of toestemming wordt gevraagd dient zo gebruikersvriendelijk mogelijk te zijn. Aan toegang tot specifieke inhoud van een website kan nog altijd de voorwaarde worden verbonden dat een cookie of soortgelijke voorziening, indien gebruikt voor een legitiem doel, bewust wordt aanvaard.

Informatie over het gebruik van cookies op een website kan aan de bezoeker worden verstrekt door middel van een privacystatement op de webpagina. Daarin kan ook worden gewezen op de mogelijkheid om cookies te weigeren door middel van het instellen van de voorkeuren in de browser.

6.7 E-mail privacy

Twee systemen die door de Artikel 29 Werkgroep uitdrukkelijk worden genoemd als belangrijke technische maatregelen die de privacy kan bevorderen bij gebruik van e-mail. Dit systemen zijn e-mailfilters en anonieme e-mail.

E-mailfilters bestaan uit regels aan de hand waarvan het mailprogramma de inkomende e-mail van een gebruiker kan controleren om vervolgens alleen berichten door te laten waarvan hij/zij heeft aangegeven ze te willen ontvangen. Deze systemen worden vooral gebruikt tegen spamming. E-mailfilters worden geleverd als zelfstandige programmatuur door verschillende bedrijven. Daarnaast beschikken ook bestaande e-mailprogramma's, zoals Microsoft's Outlook, over de mogelijkheid om filterregels in te stellen.

Gebruikers van internet zijn door middel van anonieme e-mail in staat hun e-mailadres on line te gebruiken zonder hun identiteit prijs te geven. Dergelijke voorzieningen worden aangeboden op internet door zogenaamde "remailer"-bedrijven. Een remailer zorgt ervoor dat de identiteit van een gebruiker automatisch wordt verwijderd bij de aflevering van e-mailberichten. Antwoorden op deze anonieme e-mail komen terecht bij de remailer, die vervolgens de anonieme adressen vervangt door de werkelijke e-mailadressen en de berichten veilig aan de klant aflevert.

6.8 Infomediairs

Een informatie-intermediair of 'infomediair' is "een vertrouwde persoon of via het Web opererende organisatie die gespecialiseerd is in kennis- en informatiediensten voor, over en uit naam van een virtuele gemeenschap. De infomediair vergemakkelijkt en stimuleert intelligente communicatie en wisselwerkingen tussen de leden van de virtuele gemeenschap. Hij administreert en bevordert een besloten kennisbasis met onder meer inhoud en hyperlinks die voor de gemeenschap van specifiek belang is. Binnen het privacymandaat dat de virtuele gemeenschap hem heeft toegekend verzamelt, organiseert en

selecteert de infomediair informatie over de gemeenschap en haar leden met het doel de belangen ervan zo goed mogelijk te behartigen…".[136]

Een infomediair is te vergelijken met een organisatie als United Consumers.[137]United Consumers is een BV die als doel heeft commodities (zoals motorbrandstof, telecom en nutsvoorzieningen) goedkoper beschikbaar te maken voor de deelnemende consumenten. United Consumers is er op gericht om groepskortingen voor de individuele consument mogelijk te maken. Door te werken via internet bespaart zij veel kosten, die zij vervolgens als voordeel (korting) aan de klant doorgeven. Bovendien is zij zeer effectief in marketing om een grote groep te blijven. De persoonlijke gegevens van de deelnemers worden alleen gebruikt voor het uitkeren van de opgebouwde spaartegoeden én voor de noodzakelijke communicatie ten behoeve van de kortingsadministratie.

Een infomediair is te beschouwen als een soort 'personal assistant' die bemiddelt voor de consument bij aanbieders op internet. Het gebruik van een infomediair zou lagere transactiekosten en meer privacy voor de consument tot gevolg hebben.[138]

Door gegevens over transacties en het gedrag van de consument te bewaren, heeft deze infomediair de mogelijkheid om zeer gedetailleerde klantprofielen op te stellen, over de transactieactiviteit en de behoefte en voorkeuren van de klant. De infomediair kan in de hoedanigheid van informatiemakelaar deze waardevolle maar zeer gedetailleerde klantinformatie anoniem aanbieden aan aanbieders van producten en diensten op internet. Daarmee is tevens het privacyrisico van infomediairs aangegeven.

Persoonsgegevens krijgen op deze manier economische waarde voor de consument. Voor het bedrijfsleven hebben persoonsgegevens al veel langer economische waarde, wat zijn neerslag onder meer vindt in het gebruik van persoonsgegevens voor direct marketingdoeleinden, met spam als negatieve uitwas daarvan. Consumenten zouden hun privacy kunnen versterken door zich door middel van een infomediair te verenigen en van hun persoonsgegevens handelswaar te maken in de relatie met producenten en aanbieders op internet. De infomediair kan uit naam van de consument klantinformatie verhandelen aan bedrijven en tegelijkertijd hun persoonsgegevens tegen misbruik beschermen. Een infomediair kan in veel gevallen de bestelde goederen of diensten bij de

136. Groep Gegevensverwerking Artikel 29, *Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming.* WP 37, 21 november 2000, p. 93. Zie ook: Fourth Wave Group Inc., *Lexicon – Infomediary.* Op internet: <http://www.fourthwavegroup.com/fwg/lexicon/1635w.htm>, laatst bezocht op 6 juni 2003.

137. United Consumers. Op internet: <www.unitedconsumers.nl>, laatst bezocht op 18 september 2003.

138. H. Gardeniers, 'Privacy Enhancing Mediaries: Nieuwe mogelijkheden voor privacybescherming?' In: *Privacy & Informatie* 2001/1, p. 19., die daarin verwijst naar J. Hagel III en M. Singer, De Waarde van het Internet, groeiscenario's voor elektronisch zakendoen. In: *Business Contact*, 2000 (origineel: J. HAGEL III en M. SINGER, *Net Worth: the emerging role of the infomediary in the race for customer information*. Harvard Business School Press).

consument af (laten) leveren, zonder dat deze zijn/haar anonimiteit hoeft prijs te geven.[139]

De persoonsgegevens van de consument kunnen worden verhandeld, doordat de infomediair aan de verkoper een vergoeding vraagt, telkens wanneer de consument er mee instemt dat zijn identiteit en e-mailadres aan de verkoper kenbaar wordt gemaakt. De vergoeding kan bijvoorbeeld bestaan uit een uitbetaling of korting op de prijs van een besteld of te bestellen product. Daarnaast is het mogelijk een aparte vergoeding te vragen aan verkopers die toegang wensen tot het informatieprofiel van de consument. De hoogte van deze vergoeding zal afhangen van de mate waarin de consument wenst vast te houden aan de vertrouwelijkheid van zijn informatieprofiel. Het is mogelijk volledig anoniem te blijven, maar dan deelt men niet mee in de vergoedingen. Wie kan instemmen met de beperkingen die de infomediair hanteert en geen bezwaar heeft tegen selectieve verstrekking van zijn persoonsgegevens, kan daarmee inkomsten verwerven. De infomediair maakt de consument uiteindelijk minder afhankelijk van privacywetgeving en zelfregulering, doordat de consument zelf de regie over de eigen persoonsgegevens in handen neemt.[140]

6.9 Conclusie

De Artikel 29 Werkgroep komt in het rapport *Privacy on the internet*, tot een aantal conclusies. Deels kunnen we daar bij aansluiten, maar daarnaast vallen er nog enkele aanvullende conclusies te trekken als het gaat om het gebruik van privacybevorderende technieken.

De conclusies van de Werkgroep luiden als volgt:

- er dienen aanbevelingen te komen die moeten leiden tot browsers die in de meest privacybeschermende instelling voldoen aan de privacybepalingen;
- anonieme *proxy-servers* kunnen het IP-adres verbergen en zouden door elke *ISP* als gratis standaard service bij een internetaanbieding geboden kunnen worden;
- websites dienen geen toegang te weigeren aan gebruikers die geen *cookies* wensen te accepteren, tenzij die sessiecookies onmisbaar zijn voor de totstandbrenging van de link tussen een gebruiker en zijn/haar verschillende on-lineaankopen ten behoeve van de correcte facturering; (vgl. art. 5, lid 3, Richtlijn 2002/58/EG);
- toepassing van privacybevorderende technologieën dient te worden gestimuleerd, in het bijzonder de installatie ervan door *ISPs* of andere partijen;
- de indruk bestaat dat het publiek meer informatie zou moeten krijgen over de werking van privacybevorderende technologieën. De openbare sector dient de nodige

139. Vergelijk de werking van iPrivacy, zoals hiervoor beschreven.
140. Vgl. H. Gardeniers, 'Privacy Enhancing Mediaries: Nieuwe mogelijkheden voor privacybescherming?' In: *Privacy & Informatie* 2001/1, p. 18.

stappen te ondernemen om de toepassing van en voorlichting over deze technologieën te versterken, mede door ze ook zelf toe te passen en te promoten;
- de Groep zou een Europese norm voor privacykeurmerken kunnen ontwikkelen. Hierin dient de verplichting voor websites te worden vervat om periodieke audits te ondergaan.

Ter aanvulling op deze aanbevelingen van de Artikel 29 Groep, vallen uit dit hoofdstuk nog enkele aanvullende conclusies te trekken.

Bij het stimuleren van de toepassing van privacybevorderende technieken, kan ook worden gedacht aan de vrije keuzemogelijkheid die een consument zou moeten hebben om anoniem te blijven of onder een pseudoniem op internet te consumeren. Het voorbeeld van iPrivacy maakt duidelijk dat anonimiteit en e-commerce goed samen kunnen gaan.

Het gebruik van privacybevorderende technieken zou vooral gestimuleerd kunnen worden door de overheid. In Nederland is tijdens de parlementaire behandeling van de Wbp in de motie Nicolaï uitgesproken dat de overheid de ontwikkeling en toepassing van privacybevorderende maatregelen dient aan te moedigen. Binnen de openbare sector zou de overheid het initiatief dienen te nemen bij de verwerkingen van persoonsgegevens door de overheid en dit soort initiatieven te promoten. Promoten van privacybevorderende technieken is ook nodig voor de bewustwording van de consument. Zoals blijkt uit de in hoofdstuk 3 genoemde 'privacy surveys' van de Europese Unie, zijn veel Europese burgers nog onbekend met PET. En als men er al eens van heeft gehoord, weet men de techniek in de praktijk vaak niet toe te passen.

Daarnaast zou bevorderd moeten worden dat consumenten de handen ineen slaan en zich gaan organiseren, bijvoorbeeld in virtuele gemeenschappen, teneinde persoonsgegevens van consumenten de economische waardering te kunnen bieden die het verdient. Bij voorkeur met steun van consumentenorganisaties, zoals de Consumentenbond. Dat dergelijke virtuele gemeenschappen economisch interessant zijn voor consumenten, bewijst de organisatie United Consumers.

Tot nu toe werd het kostenaspect van de bescherming van privacy en persoonsgegevens vooral eenzijdig benaderd vanuit het standpunt van het bedrijfsleven. Het is nog onvoldoende erkend dat bescherming van privacy en persoonsgegevens ook een kostenfactor voor de betrokkenen (consumenten) betekent. Privacybewuste consumenten besteden immers hun geld en tijd ook aan middelen die hun privacy en persoonsgegevens op internet kunnen beschermen: volgens Amerikaans onderzoek per gezin zo'n $ 200 tot $ 300 per jaar.[141] Ook de vele ongevraagde commerciële e-mail berichten die

141. Robert Gellman, *Privacy, Consumers, and Costs. How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete,* maart 2002. Op internet: <http://www.epic.org/reports/dmfprivacy.html>.

door consumenten worden ontvangen, betekenen een flinke kostenpost aan de zijde van de consument ten bedrage van € 10 miljard per jaar.[142]

Daarnaast wordt vaak vergeten dat het niet voldoende beschermen van de privacy en persoonsgegevens van consumenten ook nadelige financiële consequenties voor het bedrijfsleven kan hebben, bijvoorbeeld omdat consumenten websites mijden die men op dit punt onvoldoende vertrouwt.

De inzet van infomediairs maakt het mogelijk om de economische waarde van persoonsgegevens beter tot zijn recht te laten komen.[143] Het biedt de consument de mogelijkheid de regie over zijn persoonsgegevens in eigen handen te nemen, in aanvulling op bestaande privacywetgeving en zelfreguleringsinitiatieven.

142. Serge Gauthronet, Etienne Drouard, *Unsolicited Commercial Communications and Data Protection*. Commission of the European Communities, January 2001 (Internal Market DG – Contract n° ETD/99/B5-3000/E/96).
143. Meer over commodificering van persoonsgegevens in hoofdstuk 8 van dit boek.

7 Conclusie: het zelfreguleringstekort

7.1 Inleiding

In de voorgaande twee hoofdstukken is uiteengezet welke zelfreguleringsinstrumenten ter bescherming van de informationele privacy op internet kunnen worden onderscheiden. In dit hoofdstuk wordt ingegaan op de vijfde onderzoeksvraag: "Wat kunnen zelfregulering en techniek betekenen voor de bescherming van persoonsgegevens op internet?"

In de kabinetsnota Wetgeving voor de Elektronische Snelweg (WES) van februari 1998, heeft de Nederlandse regering haar voorkeur uitgesproken voor zelfregulering van het internet boven overheidsregulering.[144] In het algemeen valt zelfregulering te overwegen wanneer het gedrag van 'professionals' moet worden gereguleerd, in situaties waarin individuele of groepsbelangen niet te zeer verschillen van het belang dat de desbetreffende wet beoogt te dienen en in omstandigheden waarin (volledige) overheidsregulering niet of slechts zeer moeizaam te controleren en te handhaven is. Met name op basis van de als laatste genoemde omstandigheden, lijkt zelfregulering voor de bescherming van de privacy op het wereldwijde internet een nuttig instrument.

Niet alleen de Nederlandse regering verwacht veel heil van zelfregulering. Dat geldt ook voor enkele internationale organisaties en voor de VS.[145] In dit hoofdstuk wordt geconcludeerd in hoeverre zelfregulering van privacy op internet tot nu toe voldoende effectief is gebleken.

7.2 Criteria voor zelfregulering

7.2.1 Criteria volgens Bennett en Raab

Colin Bennett en Charles Raab maken in hun analyse van zelfreguleringsinstrumenten ter bescherming van persoonsgegevens onderscheid in vier elkaar mogelijk overlappende soorten: *privacy commitments, privacy codes, privacy standards* en *privacy seals*.[146] *Privacy commitments* kunnen bijvoorbeeld bestaan uit een eenzijdige verklaring dat het bedrijf de

144. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2 (Nota Wetgeving voor de elektronische snelweg).
145. Zie § 5.4, resp. § 4.2 in dit boek.
146. Colin J. Bennett, Charles D. Raab, *The governance of privacy: policy instruments in global perspective*, Aldershot: Ashgate 2003, hoofdstuk 6: 'Self-Regulatory Instruments', p. 122.

privacy van de klant zal respecteren. Vaak zal zo'n verklaring vooral uit een oogpunt van public relations worden gedaan. Anders dan een *privacy commitment*, bevat een privacy gedragscode voorschriften voor personeelsleden, aangesloten leden of aangesloten organisaties. Nog verder gaat de *privacy standard*. Een standaard impliceert tevens een proces waarmee de naleving van een norm door een organisatie op objectieve wijze kan worden getoetst. Door middel van standaardisatie kan dus op onafhankelijke wijze worden vastgesteld dat een organisatie 'zegt wat het doet, en doet wat het zegt'. Een voorbeeld is de Code voor Informatiebeveiliging, die is gebaseerd op de Britse standaard BS7799. Een privacykeurmerk bestaat uit een algemeen erkend en duidelijk kenmerk of symbool dat wordt toegekend aan een organisatie die daartoe is gecertificeerd of geregistreerd.[147]

Uit hun analyse van vrijwillige zelfreguleringsinitiatieven op het gebied van privacybescherming leiden Bennett en Raab een viertal criteria af die de zelfregulering door bedrijven, organisaties of branches zou kunnen bevorderen.[148] Hierbij moet worden aangetekend dat Bennett en Raab deze criteria formuleren voor situaties waarin er geen algemene wetgeving ter bescherming van persoonsgegevens bestaat. De criteria zijn de volgende:

1. Grote behoefte aan grensoverschrijdend verkeer van persoonsgegevens;
Wanneer in een onderneming of organisatie een grote behoefte bestaat uit de grensoverschrijdende uitwisseling van persoonsgegevens, dan zal ook de behoefte en bereidheid om aan internationale privacy standaarden te voldoen groter zijn, alsook de motivatie voor zelfregulering. Bennett en Raab wijzen er in dit verband op dat de EU privacyrichtlijn 95/46/EG een drijvende kracht is achter de vorming van een internationale privacy standaard. Dit komt vooral tot uitdrukking in hoofdstuk IV dat een passend beschermingsniveau eist in een derde land waar persoonsgegevens naar toe worden doorgegeven. Mede met het oog daarop is het Safe Harbor Programma tot stand gekomen voor de gegevensuitwisseling tussen de EU en de Verenigde Staten als belangrijke handelspartner. De Safe Harbor lijst, maar ook de TRUSTe lijst tonen aan dat vooral wereldwijd opererende bedrijven bereid zijn zich te conformeren aan een dergelijke standaard.

2. Gebruik van privacybedreigende technologieën;
Naarmate een onderneming of organisatie gebruik maakt van nieuwe technologieën waarvan algemeen wordt aangenomen dat deze gevolgen hebben voor de privacy en bescherming van persoonsgegevens van consumenten, zal die organisatie eerder bereid zijn zich aan zelfregulering te conformeren. Daarmee kunnen die organisaties de angst voor aantasting van privacy bij hun consumenten verminderen of wegnemen. Hoewel

147. Zie over het keurmerk als zelfreguleringsinstrument ook § 5.7 van dit boek.
148. Colin J. Bennett, Charles D. Raab, *The governance of privacy: policy instruments in global perspective,* Aldershot: Ashgate 2003, hoofdstuk 6: 'Self-Regulatory Instruments', p. 133 e.v.

dat niet altijd terecht is – verstrekken van credit card gegevens kan via internet veiliger zijn dan in de off line wereld – kan het gebruik van nieuwe technologieën ertoe leiden dat organisaties op consumentenangst anticiperen en daardoor een hoger niveau van zelfregulering toepassen.

3. De mate waarin een organisatie slachtoffer is van negatieve publiciteit;
Een onderneming of organisatie die het slachtoffer is geworden van negatieve publiciteit is sterker gemotiveerd om via zelfregulering het vertrouwen van de consumenten te herwinnen. In de VS was Doubleclick Inc. het middelpunt van een privacyschandaal in 1999-2000, toen het probeerde geanonimiseerde clickstreams te koppelen aan een database van Abacus met tot personen herleidbare gegevens. Intel leed in 1998 onder negatieve publiciteit van de plannen rond de introductie van de Pentium III chip. Microsoft wordt onder meer door de Europese Commissie in de gaten gehouden en in het bijzonder door de Artikel 29 Data Protection Werkgroep.[149]

4. De mate waarin binnen een sector toezicht wordt uitgeoefend door een branche-organisatie.
De mate waarin een representatieve branche-organisatie die in staat is zelfregulering te ontwikkelen toezicht kan houden binnen een sector is mede bepalend voor de effectiviteit van zelfregulering. Zelfregulering voor een sector kan zogeheten 'vrijbuiters' weren uit de branche. Met name in Canada, Japan en Australië hebben enkele van de grote branche-organisaties in de diensten sector zelfregulering bevorderd. Hierdoor werd het de regeringen van die landen mogelijk gemaakt om consensus te bereiken over de beginselen voor gegevensbescherming. Vervolgens konden deze door zelfregulering tot stand gekomen beginselen tot wet worden verheven.

Deze voorwaarden zijn internationaal, technologisch en bedrijfsmatig van aard. Indien aan deze voorwaarden is voldaan kan worden aangenomen dat zelfregulering ter bescherming van persoonsgegevens ook effectief zal kunnen zijn.

Waar Bennett en Raab voorts terecht op wijzen is dat de grenzen tussen de sectoren aan het vervagen zijn. Dat geldt bijvoorbeeld voor het onderscheid tussen de publieke en private sector. Tegelijkertijd verkopen supermarkten tegenwoordig ook mobiele telefoons en doen zij ook in bancaire zaken. De vraag welke sectorale zelfregulering van toepassing is, is dan moeilijk te beantwoorden.

Voor het bepalen van de effectiviteit van zelfregulering zijn criteria te formuleren op basis van een analyse van beleidsdocumenten uit diverse landen, zoals Nederland (Nota

149. Zie hierover D. Alonso Blas, The pioneer work of the Article 29 Working Party in the field of on-line authentication: the Microsoft .NET Passport case. *Privacy & Informatie*, 2003, nr. 6, p. 263-266.

Wetgeving voor de elektronische snelweg, p. 181-182), Europa (White paper European Governance, 2001 p. 21), VS (Dept. Of Commerce, The Emerging Digital Economy, 1998; en FTC, Online Profiling), Australië (Task Force on Industry Self-Regulation, Checklist) en de ITU World Summit on the Information Society (Declaration 2003).[150] Deze criteria zullen in de volgende paragraaf worden uiteengezet.

7.2.2 Criteria volgens Holvast en Gardeniers

In hun eindrapport *Privacy, zelfregulering en internet*[151] (2001) formuleren Jan Holvast en Huib Gardeniers een uitgebreide set met voorwaarden en afwegingen voor zelfregulering van privacybescherming op internet. Deze voorwaarden en afwegingen zouden ter beoordeling van een specifieke vorm van zelfregulering kunnen worden toegepast. Zij hebben betrekking op de set zelfreguleringsafspraken – zoals een gedragscode of een aantal leidende beginselen – alsmede op het stelsel voor het vaststellen, de herziening en toepassing van deze afspraken. De *inhoudelijke afwegingen* zijn de volgende:

A 1. Is er een duidelijke set zelfreguleringsafspraken (zoals een gedragscode of een aantal leidende beginselen)?
A 2. Vindt er voldoende binding met de zelfreguleringafspraken plaats door alle partijen?
A 3. Zijn de regels voldoende kenbaar voor degenen die er een beroep op kunnen doen?
A 4. Zijn de doelgroepen die in het geding zijn, voldoende georganiseerd?
A 5. Is de groep die de regels opstelt voldoende representatief voor de groep of sector waarop de regels van toepassing zijn?
A 6. Is het een code die door één partij of meerdere partijen is opgezet? (een- of tweezijdig, bijvoorbeeld bedrijfsleven en consumentenorganisaties)
A 7. Vindt er een gelijkwaardige behartiging van de maatschappelijke belangen plaats en wordt er voldoende rekening gehouden met belangen van zwakkere partijen?
A 8. Zijn de afspraken in voldoende mate onpartijdig, is er bijvoorbeeld een standaard?
A 9. Is de handhaving van de afspraken in voldoende mate verzekerd? (wordt er ook daadwerkelijk uitvoering gegeven aan de regels, is er controle en toezicht op de naleving)
A 10. Geeft de zelfregulering voldoende rechtszekerheid?
A 11. Is de juridische reikwijdte van de regeling voldoende?
- territoriaal (is de omvang territoriaal voldoende?);
- functioneel (dekt het voldoende de gewenste activiteiten en gebeurtenissen af?).

150. Zie ook het hoofdstuk over zelfregulering, door B.-J. Koops, M. Lips, S. Nouwt, C. Prins en M. Schellekens, in het boek *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-liners*, (voorlopige titel) geschreven door diverse onderzoekers van het TILT – Tilburg Institute for Law, Technology, and Society (nog te verschijnen).
151. J. Holvast, H. Gardeniers, *Privacy, zelfregulering en internet,* eindrapport, mei 2001, p. 66 e.v.

A 12. Is de duur van de code in overeenstemming met het doel, en zijn de aanpassings-, en herzieningsprocedures voldoende flexibel?
A 13. Is de groep die de regels wil onderschrijven voldoende in omvang om effectief te kunnen zijn (en zijn er niet teveel free-riders)?

Daarnaast formuleren Holvast en Gardeniers een aantal afwegingen met betrekking tot de *zelfreguleringorganisatie*:

B 1. Is de zelfreguleringorganisatie een onafhankelijke organisatie met zelfstandige beslissingsbevoegdheden?
B 2. Is het toezicht op de naleving onafhankelijk van de onderneming(en) en/of organisaties die de afspraken hebben vastgesteld en/of deze kunnen herzien?
B 3. Is er een stelsel voor het vaststellen, de herziening en toepassing van deze afspraken?
B 4. Zijn het beslissingsproces en de toewijzingen transparant?
B 5. Beschikt de organisatie, waarvan de zelfregulering uitgaat of die daarbij partij is, over voldoende mogelijkheden en bezit deze voldoende gezag (moreel en/of praktisch) om de zelfregulering bij het betrokken deel van het bedrijfsleven te doen aanvaarden en naleven. Deze aanvaarding, dus de verbindendheid voor de betrokken ondernemingen, houdt tweeërlei in:
   a. de organisatiegraad moet voldoende hoog zijn, zodat er weinig outsiders zijn;
   b. binnen de betrokken organisatie moeten er voldoende mogelijkheden bestaan om ook tegenstemmende leden tot naleving van de zelfregulering te nopen, dat wil zeggen er moet een interne structuur zijn, die het mogelijk maakt om leden van organisaties te binden aan besluiten van een orgaan van de organisatie.[152]
B 6. Geschilprocedure/klachtenregeling. Is er een behoorlijke regeling van het klachtrecht en een geschillenregeling, waartoe zowel leden als consumenten toegang hebben?

Dit klachtrecht dient ook toe te komen aan consumentenorganisaties. Een dergelijke groepsactie of collectieve actie mag niet dienen ter verkrijging van nakoming, schadevergoeding of ontbinding, maar wel ter verkrijging van een door de rechtsprekende instantie uit te spreken verbod of gebod, mede wegens de preventieve en corrigerende werking. Concreet gaat het hierbij om maatstaven met betrekking tot de toegankelijkheid (o.a. van informatie, bij voorkeur laagdrempelig), beperkte procedure in relatie tot kosten en tijd, onafhankelijkheid met een eerlijke procesgang, efficiëntie en effectiviteit en een geschikte wijze van aflegging van verantwoording.

152. Het gaat hierbij o.a. om de vraag of de organisatie voldoende macht bezit om beslissingen af te dwingen en of er bij het bedrijf of binnen de bedrijfstak of beroepsgroep voldoende dwang aanwezig is tot normconformiteit.

In een schema geven Holvast en Gardeniers vervolgens aan wat volgens hen de relatieve waarde is van de afwegingen A en B. Daaruit blijkt welke onderdelen zij belangrijker vinden dan andere.

A1 Duidelijke set van zelfreguleringsafspraken	++
A2 Voldoende binding door alle partijen (die meedoen)	++
A3 Kenbaarheid	+++
A4 Organisatiegraad	+
A5 Representativiteit	+
A6 Code opgezet door één of meer partijen	++
A7 Afweging maatschappelijke belangen en/of zwakke partijen	+++
A8 Onpartijdige afspraken	+++
A9 Worden de regels daadwerkelijk nageleefd	+++
A10 Geven de regels rechtszekerheid	++
A11 Juridische reikwijdte voldoende	++
A12 Duur/flexibiliteit	+
A13 Positie free riders	+

B1 Onafhankelijke organisatie	+++
B2 Onafhankelijk toezicht	+++
B3 Stelsel van afspraken	++
B4 Transparante beslissingsproces	+
B5 Moreel gezag	++
B6 Geschillenprocedure	+++

Zoals gezegd kunnen deze afwegingen worden toegepast ter beoordeling van een specifieke vorm van zelfregulering ter bescherming van persoonsgegevens op internet. Maar in hoeverre sluiten deze afwegingen aan bij de meer algemeen te formuleren eisen die kunnen worden gesteld aan zelfregulering in het ICT-tijdperk. Daarover gaat de volgende paragraaf.

7.2.3 Algemene criteria volgens Koops e.a.

Onderstaande criteria zijn te beschouwen als criteria voor zelfregulering bij gebruik van ICT in het algemeen, dus niet in het bijzonder voor zelfregulering ter bescherming van persoonsgegevens.[153]

Eerlijkheid

Algemeen wordt aangenomen dat de regels die in zelfreguleringsinitiatieven zijn neergelegd, eerlijk moeten zijn. Eerlijkheid houdt in dit verband in dat in het bijzonder de sociale belangen van zwakkere partijen voldoende gewaarborgd moeten worden. Zij zijn in het algemeen niet of nauwelijks betrokken bij de totstandkoming van de initiatieven en lopen daardoor kans om nadeel te ondervinden van de macht van de grootindustrieën. Belangen die gerespecteerd moeten worden zijn met name: gelijkheid, nondiscriminatie en andere fundamentele rechten. Daarnaast moet ook eerlijke concurrentie gewaarborgd zijn. Wanneer sprake is van 'verdringing' moet worden voorkomen dat bepaalde groepen in de samenleving niet ten achter worden gesteld. Bij 'verdringing' is het onmogelijk als burger te functioneren zonder toegang te hebben tot de meest voorkomende elektronische infrastructuren en diensten, doordat de traditionele middelen hun betekenis verloren hebben.[154]

Gebrek aan eerlijkheid kan een belangrijke reden zijn voor overheidsregulering. Dit is het geval wanneer fundamentele rechten van burgers of consumenten in het geding zijn of wanneer bepaalde groepen burgers of consumenten gediscrimineerd dreigt te worden. De eerlijke behartiging van de belangen van burgers of consumenten kan dan niet aan de zelfregulerende instanties worden overgelaten.

Representativiteit

Een tweede criterium voor effectieve zelfregulering is dat het proces waarlangs het zelfreguleringsinitiatief tot stand komt voldoende representatief is. Daarmee wordt met name gedoeld op de representativiteit van degene die de regels opstelt voor de adressaten van de zelfregulering. De belanghebbenden zullen in het algemeen goed georganiseerd moeten zijn om uiteindelijk te kunnen bepalen waar hun wensen en grenzen liggen. Dit criterium hangt in die zin samen met het eerste criterium, dat de representativiteit wordt bevorderd door deelname van zwakkere belanghebbenden (burgers, consumenten) in het zelfreguleringsproces. Anders dan het eerste criterium gaat het bij de representativiteit

153. Deze algemene criteria zijn grotendeels gebaseerd op het hoofdstuk over zelfregulering, door B.-J. Koops, M. Lips, S. Nouwt, C. Prins en M. Schellekens, in het boek *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-liners*, (voorlopige titel) geschreven door diverse onderzoekers van het TILT – Tilburg Institute for Law, Technology, and Society (nog te verschijnen).

154. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 4 (Nota Wetgeving voor de elektronische snelweg).

echter vooral om dat de effectiviteit van zelfregulering afhangt van de mate waarin de regels door de achterban worden erkend.

Naleving

Zoals Bennett en Raab ook al aangeven, is de naleving van zelfregulering en de handhaving daarvan door middel van toezicht, een belangrijke voorwaarde voor de effectiviteit van ervan. Van belang hiervoor is de mate waarin en de instrumenten waarmee organisaties die onder de zelfregulering vallen aansprakelijk kunnen worden gehouden voor het niet naleven van de regels waarvan de consument mag verwachten dat zij die nakomen. Anders dan bij overheidsregulering valt een gedragscode niet automatisch onder een traditioneel handhavingsregime.

Wel bevatten sommige gedragscodes geschillenregelingen. Dat is bijvoorbeeld het geval in de Gedragscode Verwerking Persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus, de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen van de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars en de Gedragscode Gezondheidsonderzoek.

Een organisatie die een gedragscode niet naleeft, kan uiteindelijk worden geroyeerd als lid van de brancheorganisatie. Negatieve publiciteit kan ook een effectief middel zijn om een verantwoordelijke onder druk te zetten om de gedragscode na te leven.

Transparantie

Van even groot belang als de naleving, is de transparantie rondom zelfregulering: zowel wat betreft de regulering zelf als wat betreft de totstandkoming van de zelfregulering. Zelfregulering komt immers op een andere, minder inzichtelijke wijze tot stand dan de met democratische waarborgen omklede overheidsregulering. Consumenten spelen in het algemeen niet of nauwelijks een rol bij de totstandkoming van zelfregulering. Wanneer de regels vervolgens ook niet of nauwelijks bekend zijn bij de consument, kan die ook niet klagen als de regels niet worden nageleefd.

Transparantie is van belang voor de effectiviteit van zelfregulering omdat regels die niet kenbaar of onduidelijk zijn in het algemeen minder vertrouwd zullen worden door de consument. Dat heeft tot gevolg dat de organisaties ze in mindere mate zullen opvolgen. In dat opzicht heeft transparantie ook met naleving te maken omdat onwillige organisaties niet mee zullen werken aan de uitvoering van de zelfregulering als de regels en de procedures niet voldoende duidelijk zijn.

Rechtszekerheid

Het criterium van rechtszekerheid hangt in zekere zin samen met transparantie. Bij rechtszekerheid draait het om de vraag of de regels wel voldoende duidelijk zijn, ondubbelzinnig en consistent. Alleen dan kan de praktijk in voldoende mate op de regels vertrouwen. Overigens hoeft zelfregulering niet altijd de rechtszekerheid te bevorderen. In die gevallen is de rechtszekerheid meer gebaat bij overheidsregulering. Dat is met name

het geval als die overheidsregulering is gericht op domeinen waarbinnen gedetailleerd uitgewerkte regelgeving bestaat teneinde voor voldoende rechtszekerheid te kunnen zorgen. In andere domeinen kan het echter effectiever zijn om zelfregulering te ontwikkelen, omdat de regels sneller en gemakkelijker aangepast kunnen worden aan snel veranderende omstandigheden. Het hangt daarom af van het domein en van de daarbinnen betrokken actoren of zelfregulering beter is voor de rechtszekerheid dan overheidsregulering.

Contextafhankelijkheid

Van belang voor de effectiviteit van zelfregulering is voorts de context waarbinnen zelfregulering wordt ontwikkeld. Die context wordt mede bepaald door de branche (bankwezen, gezondheidszorg) en het domein of voorwerp van zelfregulering dat daar veelal mee zal samen hangen. Van belang zijn voorts de technologie die wordt toegepast (internet) en het nationale of internationale niveau waarop zelfregulering wordt ontwikkeld. Het hoeft niet altijd effectiever te zijn om zelfregulering op internationaal niveau te ontwikkelen. Dat hangt mede af van de branche, het voorwerp van zelfregulering en de techniek die wordt gebruikt. Het is immers op internationaal niveau niet altijd eenvoudiger om regulering tot stand te brengen dan op nationaal niveau.

De effectiviteit van zelfregulering hangt ook af van de politieke context. Zelfregulering lijkt beter geschikt en dus effectiever te zijn voor politiek neutrale onderwerpen, dan voor politiek beladen onderwerpen. Voor politiek neutrale onderwerpen kan zelfregulering zich bijvoorbeeld richten op het beantwoorden van vragen, zoals de voorwaarden waaraan een elektronische handtekening moet voldoen. Zelfregulering lijkt minder geschikt en effectief als er politieke standpunten in worden ingenomen, zoals over de vraag of 'spam' is toegestaan of niet. Belangrijke rechtspolitieke keuzes moeten vooral door de wetgever worden gemaakt en niet door private partijen.

Efficiëntie

In tegenstelling tot overheidsregulering wordt zelfregulering vaak gezien als een manier van regulering die eenvoudiger is, sneller en goedkoper. Zelfregulering is vaak ook flexibeler en daardoor sneller en gemakkelijker aan te passen aan veranderde omstandigheden. Dit geldt niet alleen voor het proces van regulering. Ook de kosten van naleving van zelfregulering kunnen lager uitvallen omdat men de regels eenvoudiger kan aanpassen aan de werkelijkheid van de branche. Wanneer de andere criteria niet doorslaggevend zijn voor zelfregulering, zouden redenen van efficiëntie er toe kunnen leiden om te kiezen voor zelfregulering.

Continuïteit

Een criterium dat eveneens van belang is voor de effectiviteit van zelfregulering is continuïteit. Daarmee wordt in het bijzonder gedoeld op de continuïteit van het zelfreguleringsinitiatief of van de organisatie die het zelfreguleringsinitiatief heeft opgezet. Er zijn

diverse privacykeurmerken die een voorbeeld zijn van een zelfreguleringsinitiatief. Van Web Trader (zie hierna) is inmiddels bekend dat de consumentenorganisaties in Engeland en Nederland zijn gestopt met het Web Trader keurmerk. Een voorbeeld van discontinuïteit van een organisatie van een zelfreguleringsinitiatief is het faillissement van DMSA. Na verloop van tijd is een zelfreguleringsinitiatief van DMSA (Antwoordnummer 666) opgevolgd door een nieuw initiatief: Infofilter van DDMA.

7.2.4 De algemene criteria toegepast op de bescherming van persoonsgegevens

Bovenstaande algemene criteria voor zelfregulering in het ICT-tijdperk lijken ook geschikt voor de beoordeling van de effectiviteit van zelfregulering ter bescherming van persoonsgegevens op internet. De inhoudelijke afwegingen van Holvast en Gardeniers zijn vrij eenvoudig te scharen onder de algemene criteria, zoals de volgende tabel illustreert.

Algemeen criterium	**Inhoudelijke afweging Holvast en Gardeniers**
1. Eerlijkheid	A7, A8
2. Representativiteit	A2, A4, A5, A13
3. Naleving	A9
4. Transparantie	A1, A3
5. Rechtszekerheid	A1, A8, A9, A10
6. Contextafhankelijkheid	A4, A5, A6, A7, A11, A13
7. Efficiëntie	A6, A12
8. Continuïteit	A11, A12, A13

7.3 Toepassing van de criteria voor zelfregulering op enkele zelfreguleringsinitiatieven

7.3.1 De ondergang van Web Trader

Met betrekking tot e-commerce zijn niet alleen privacykeurmerken, maar ook meer algemene keurmerken voor *dotcom*-websites ontwikkeld. Deze algemene keurmerken bevatten tevens criteria ter bescherming van persoonsgegevens. Een voorbeeld van zo'n algemeen keurmerk is Web Trader.

Web Trader is een keurmerk dat door consumentenorganisaties in verschillende landen is gehanteerd: België, Frankrijk, Italië, Nederland, Portugal, Spanje en het Verenigd Koninkrijk (zie § 5.7 in dit boek). Web Trader heeft vooral tot doel gehad het vertrouwen van de consument in elektronisch winkelen te bevorderen door via een onafhankelijke gedragscode rechtsbescherming aan de consument te bieden. Tegelijkertijd was de Web Trader code erop gericht om de totstandkoming van wetgeving voor elektronische

handel te bevorderen, de maatschappelijke discussie over consumentenbescherming op internet aan te wakkeren en het gedrag van de branche van internetwinkels te beïnvloeden.

Intussen zijn de consumentenorganisaties in het Verenigd Koninkrijk en Nederland gestopt met het Web Trader keurmerk. Volgens de Nederlandse Consumentenbond is gestopt met het toepassen van de Web Trader code wegens het succes van het behalen van de gestelde doelen.[155] Er bestaat intussen voldoende aandacht voor de consumentenproblematiek, er is nieuwe wetgeving en er bestaan nieuwe initiatieven van de Nederlandse Thuiswinkel Organisatie. De functie van Web Trader is, aldus de Consumentenbond, overgenomen door de Wet Kopen Op Afstand, de Wet Bescherming Persoonsgegevens, het keurmerk Thuiswinkel Waarborg (met algemene voorwaarden die in overleg met de Consumentenbond tot stand zijn gekomen) en de daarbij behorende onafhankelijke geschillencommissie (waarin de Consumentenbond zitting heeft). Sinds 1 januari 2002 is het keurmerk verdwenen.

Het is maar de vraag of de werkelijkheid van consumentenbescherming bij elektronisch winkelen inderdaad zo rooskleurig is als de Consumentenbond beweert. Amper vijf dagen na het persbericht waarin het einde van Web Trader werd aangekondigd, publiceerde dezelfde Consumentenbond de resultaten van een onderzoek, uitgevoerd door de wereldkoepel van consumentenorganisaties Consumers International, waaruit blijkt dat internetwinkels zich niet houden aan de nieuwe regels voor kopen op afstand. De Consumentenbond vraagt de minister van Economische Zaken dan ook om streng toe te zien op de naleving van deze wetgeving.

Waar de Nederlandse Consumentenbond met positieve argumenten het einde van Web Trader aankondigde, blijkt de reden van de Britse Consumers' Association om te stoppen met de *Which? Web Trader* gedragscode (W?WT) vooral een negatieve te zijn.[156] De Britse consumentenorganisatie stelt dat de gedragscode zijn invloed heeft gehad doordat het vertrouwen van consumenten in elektronische handel is toegenomen en de consumentenbescherming heeft bevorderd. De werkelijke reden waarom de Britse Consumers' Association is gestopt met W?WT is omdat het hanteren van de W?WT gedragscode jaarlijks een te grote financiële belasting voor de consumentenorganisatie betekende. Daarom heeft de Britse Consumers' Association besloten te stoppen met W?WT per 31 januari 2003. Het bevorderen van het consumentenvertrouwen in elektronische handel heeft de Consumers' Association nu overgelaten aan bedrijfsleven en overheid.

155. Consumentenbond, *Consumentenbond stopt met Web Trader,* persbericht, 5 september 2001.
156. Which?, *Consumers' Association to close UK code of practice scheme for online traders,* Which? Consumers' Association Press Releases 6 January 2003. Op Internet: < http://www.which.net/media/pr/jan03/general/webtrader.html>.

Kijkend vanuit de criteria voor zelfregulering naar de ondergang van Web Trader, kan het volgende worden geconcludeerd.

In de eerste plaats valt op dat het de Consumentenbonden zijn geweest die besloten om te stoppen met Web Trader. Dit is opvallend omdat de Consumentenbond niet de internetwinkels vertegenwoordigt, maar de wederpartij: de consumenten. Er kan dus niet gezegd worden dat de Consumentenbond voldoende *representatief* is voor de sector waar de zelfregulering op van toepassing is. De Web Trader code was met name gericht op het bevorderen van *transparantie* en *rechtszekerheid* bij de consument. Na de invoering van overheidsregulering op verschillende terreinen (koop op afstand, bescherming persoonsgegevens) vond de Consumentenbond deze doeleinden van zelfregulering niet langer van toepassing. Door met Web Trader te stoppen, maakte de Consumentenbond een einde aan de *continuïteit* van dit zelfreguleringsinitiatief.

De Britse Consumers' Association geeft een negatieve reden op voor deze discontinuïteit. De naleving van W?WT zou een te grote financiële belasting betekenen. Uit een oogpunt van *efficiëntie* is daarom besloten te stoppen met W?WT. Dit is opmerkelijk omdat in het algemeen wordt aangenomen dat zelfregulering juist efficiënter zou zijn dan overheidsregulering.

7.3.2 Gebrekkige naleving Safe Harbor programma

Uit een onderzoek van de Europese Commissie naar een andere vorm van zelfregulering, het Safe Harbor programma, dat is gesloten tussen de Europese Unie en het ministerie van Handel van de VS, blijkt dat ook dit zelfreguleringsinitiatief nog geen succes kan worden genoemd.[157] De volgende twee conclusies uit het onderzoek zijn op zijn minst opmerkelijk te noemen:

1. "Een groot aantal organisaties die hebben verklaard de veiligehavenbeginselen te onderschrijven (zelfcertificering) lijken, wat hun algemene verplichtingen of wat de inhoud van hun privacybeleid betreft, zich niet te houden aan de verwachte transparantie. Transparantie is in zelfreguleringssystemen van vitaal belang en het is dan ook noodzakelijk dat organisaties hun praktijken op dit gebied verbeteren, willen wij de geloofwaardigheid van de regeling in haar geheel niet aantasten."
2. "Geschillenafhandelingsmechanismen beschikken over een groot aantal sancties om naleving van de veiligehavenregels af te dwingen. Maar niet alle geschillenafhandelingsmechanismen hebben openlijk aangegeven dat zij erop toe zullen zien dat de vei-

157. *Werkdocument van de diensten van de commissie over de toepassing van Beschikking 520/2000/EG van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd,* Brussel: Commissie van de Europese Gemeenschappen, 13 februari 2002, SEC (2002) 196.

ligehavenregels worden nageleefd en niet alle mechanismen hebben een privacybeleid op zichzelf van toepassing dat in overeenstemming is met de beginselen, zoals door de veiligehavenregels wordt vereist. Rechtshandhaving is een sleutelelement in de veiligehavenregeling en het is daarom noodzakelijk dat veiligehavenorganisaties alleen een beroep doen op geschillenafhandelingsmechanismen die volledig aan de vereisten van de veilige haven voldoen."

Ondanks de aansluiting bij het Safe Harbor programma door bedrijven, die daarbij moeten verklaren dat zij de Safe Harbor Principles zullen naleven, blijkt dat veel organisaties desondanks het transparantiebeginsel niet voldoende naleven. Daarnaast blijkt dat de organisaties voor geschillenbeslechting niet allemaal garanderen dat de Safe Harbor Principles worden nageleefd en bovendien hanteren niet alle organisaties voor geschillenbeslechting zelf een privacybeleid dat voldoet aan de Safe Harbor Principles.

In navolging hierop, heeft de Artikel 29 Werkgroep op 2 juli 2002 autoriteiten, organisaties en verenigingen opgeroepen om informatie te verzamelen over de naleving van het Safe Harbor programma, in het bijzonder op de punten transparantie en handhaving:

- regelingen om de transparantie met betrekking tot de ondertekenende organisaties te vergroten, vooral indien een verklaring van toetreding tot de veilige haven niet vergezeld gaat van een passend privacybeleid;
- de mogelijkheid om te voorzien in extra controlemechanismen met betrekking tot de procedure om zich bij de overeenkomst aan te sluiten, de overeenstemming van het gedrag van veiligehavendeelnemers met hun privacybeleid en het eventuele verlies van de voordelen van de veilige haven;
- de te nemen initiatieven met het oog op een betere kennis van de voorwaarden voor toetreding tot de veilige haven, ook door middel van korte, gemakkelijk te begrijpen documenten en de eventuele integratie van het Safe Harbor Workbook;
- de te nemen maatregelen om geschillenafhandelingsmechanismen te verfijnen, de uniformiteit en de bekendheid van de relevante criteria te vergroten, de transparantie van het resultaat van deze geschillen te vergroten en de mechanismen voor de bekendmaking ervan te stroomlijnen;
- de moeilijkheden die kunnen ontstaan doordat dezelfde organisatie verschillende vormen van privacybeleid heeft aangemeld;
- de prioriteitscriteria en eventuele door de bevoegde Amerikaanse instanties genomen aanvullende initiatieven en de regelingen voor hernieuwde samenwerking tussen het Europese gegevensbeschermingspanel, instanties voor geschillenafhandeling en de Federal Trade Commission.

Wanneer deze conclusies van de Artikel 29 Groep worden getoetst aan de criteria voor zelfregulering, dan is vast te stellen dat de *transparantie* ontbreekt bij een groot aantal

organisaties die bij het Safe Harbor programma zijn aangesloten. Hoewel het transparantiecriterium voor zelfregulering met name betrekking heeft op de kenbaarheid van de regels bij organisaties en van de procedure van totstandkoming daarvan, is transparantie ook van belang voor de consument. Een organisatie die onvoldoende transparant is voor de consument, ondermijnt daarmee tevens het criterium van *rechtszekerheid*. De Artikel 29 Groep constateerde voorts dat er iets schort aan de *naleving* van de Safe Harbor regels, doordat de organisaties voor geschillenbeslechting de handhaving ervan niet garanderen. Het ontbreekt bij het Safe Harbor programma dus vooral aan de volgende criteria voor zelfregulering: *transparantie*, *rechtszekerheid* en *naleving*.

7.4 De VS gaan om

Ook in de VS wordt intussen steeds kritischer tegen zelfregulering aangekeken. Volgens de Amerikaanse Federal Trade Commission (FTC), mag van zelfregulering door het bedrijfsleven niet te veel worden verwacht. Zoals we al zagen in § 4.2, is de FTC van mening dat zelfreguleringsinitiatieven vanuit het bedrijfsleven op zichzelf niet tot voldoende privacybescherming op de elektronische markt kunnen leiden. Hoewel de FTC de rol van zelfregulering wel van belang acht, is men van mening dat het Amerikaanse Congres in aanvulling daarop wetgevingsinitiatieven dient te nemen. Uit vrijwel alle Amerikaanse privacy polls blijkt dat dit standpunt door de meerderheid van de ondervraagden wordt gedeeld.[158]

Het Amerikaanse pleidooi tegen zelfregulering en voor centrale overheidsregulering als het gaat om privacybescherming van consumenten, mag op zijn minst opmerkelijk worden genoemd. In de VS heeft men in het algemeen immers altijd een sterke voorkeur gehad voor zelfregulering van privacybescherming door de industrie boven overheidsregulering.

Centrale overheidsregulering zou nu, aldus de FTC, moeten resulteren in een minimum niveau van privacybescherming voor op consumenten gerichte commerciële websites. Dit minimum niveau zou moeten leiden tot een standaardpraktijk met betrekking tot het online verzamelen van persoonsgegevens en tot de oprichting van een organisatie die meer gedetailleerde standaarden moet kunnen bevorderen. Wanneer commerciële websites persoonsgegevens verzamelen, zouden zij in ieder geval dienen te voldoen aan de vier *fair information practice principles: Notice, Choice, Access* en *Security*.

Maar dan nog is het de vraag in hoeverre privacy statements op internet hun doel wel bereiken, te weten: de consument voldoende uitleg verschaffen over het beleid inzake de omgang met persoonsgegevens. Uit een Amerikaans onderzoek uit 2003 blijkt dat de meeste Amerikanen ondanks de aanwezigheid alom van privacystatements op websites niet begrijpen of en hoe Amerikaanse website aanbieders informatie over hen gebruiken.[159] De meeste van hen denken dat als een website een privacy statement heeft, de

158. Zie § 3.7.3 van dit boek.
159. J. Turow, *Americans and Online Privacy. The System is Broken,* A Report from the Annenberg Public Policy Center of the University of Pennsylvania, June 2003.

aanbieder hun persoonsgegevens niet zal uitwisselen met andere aanbieders of bedrijven. Bovendien weten de meeste Amerikanen niet hoe die aanbieders en bedrijven gebruik maken van hun persoonsgegevens, bijvoorbeeld door het opstellen van profielen. Bijna alle ondervraagde Amerikanen (95%) vinden wel dat zij het recht moeten hebben op kennisneming van hetgeen een website aanbieder aan informatie over hen heeft. De auteur van het rapport, Joseph Turow, doet drie specifieke aanbevelingen. Ten eerste zouden, op grond van de Amerikaanse federale wetgeving, alle websites verplicht moeten zijn om gebruik te maken van P3P, de industriestandaard voor privacybeleid van websites.[160] Ten tweede zou de Amerikaanse federale wetgeving alle website aanbieders moeten verplichten om de consumenten online toegang te verschaffen tot de over hen verwerkte persoonsgegevens. De consument zou moeten worden geïnformeerd over welke persoonsgegevens over hem zijn verzameld, of en hoe die persoonsgegevens zijn gekoppeld met andere gegevens, welke andere organisaties hun persoonsgegevens hebben ontvangen en waarvoor zijn persoonsgegevens in de toekomst nog meer worden gebruikt. De derde aanbeveling van Turow luidt, dat de overheid auditors zou moeten opdragen om steekproefsgewijs de naleving van beide wettelijke voorschriften (verplicht P3P gebruik en informatieplicht) in de praktijk te controleren. Dit op kosten van de onderzochte organisaties, terwijl overtreding van beide verplichtingen zou moeten leiden tot een veroordeling wegens oneerlijke mededinging door de Federal Trade Commission.

7.5 Het tekort van de techniek

In hoofdstuk 6 is ingegaan op de mogelijkheden van zelfregulering door middel van de techniek. Daarin zijn technologische zelfreguleringsinstrumenten besproken, zoals digitale pseudoniemen, anonymizers, cookie-crunchers, proxy-servers, en P3P. Daaruit kan worden geconcludeerd dat er in elk geval instrumenten zijn waarmee de consument zijn persoonsgegevens op internet zelf zou kunnen beschermen. 'Zou kunnen', want waar het aan ontbreekt is dat veel consumenten het bestaan van dergelijke instrumenten niet kennen. Uit het onderzoek van de Europese Commissie naar de mening van de EU burger over gegevensbescherming volgt dat 59% van de ondervraagde Nederlandse burgers nog nooit gehoord heeft van technieken om de eigen persoonsgegevens te beschermen.[161] Voor de 15 EU lidstaten waarbinnen dit onderzoek is uitgevoerd, ligt het gemiddelde op 72%. De Nederlandse burger steekt er daarbij dus in positieve zin bovenuit. Van de ondervraagde Nederlandse burgers zegt 26% er wel van gehoord te hebben, maar heeft ze nooit gebruikt. Van de ondervraagde Nederlandse burgers heeft 12% wel gehoord van

160. Zie ook § 6.6 in dit boek.
161. The European Opinion Research Group EEIG, Data Protection. Special Eurobarometer 196 – Wave 60.0. December 2003. Op internet: EUROPA, Internal Market, Data Protection, Information collected for the preparation of the report, <http://www.europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf>.

privacybeschermende technologieën en deze ook gebruikt. Samen met Zweden (14%) en Denemarken (13%) valt Nederland hiermee in positieve zin op.

Aan degenen die er wel van hadden gehoord, maar deze technieken nog nooit hadden gebruikt is vervolgens gevraagd naar het waarom. De ondervraagde *Nederlandse* burgers antwoordden daarop als volgt:

- weet niet hoe ik het moet installeren op mijn computer (33%);
- weet niet hoe ze te gebruiken (31%);
- niet overtuigd van de effectieve werking ervan (21%);
- maak me geen zorgen over mijn privacy op internet (23%);
- te duur (6%);
- andere redenen (15%).

De gemiddelde percentages van de 15 onderzochte *EU lidstaten* wijzen uit dat 21% niet weet hoe de instrumenten op de computer moeten worden geïnstalleerd, 30% weet niet hoe deze technieken te gebruiken, 18% is niet overtuigd van de effectiviteit, 20% maakt zich geen zorgen over de privacy op internet, 6% vindt ze te duur en 16% geeft andere redenen op.

Deze cijfers komen overeen met de resultaten van een workshop over Privacy Enhancing Technologies, die de Europese Commissie op 4 juli 2003 organiseerde.[162] De workshop werd bijgewoond door experts uit de academische wereld, het bedrijfsleven, overheden, consultancy, consumentenorganisaties, toezichthouders en de Europese Commissie. Met betrekking tot het gebruik van PET door consumenten concludeerden de experts dat veel consumenten niet bekend zijn met het concept van PET. In het algemeen willen consumenten, aldus de experts, goedkope en eenvoudige bescherming van hun privacy en persoonsgegevens. Zij willen zelf geen tijd en geld investeren in het toepassen van beschermende instrumenten. De consument wenst geïntegreerde instrumenten die geen ingewikkelde wijzigingen van de computerinstellingen vergen en ook geen andere gecompliceerde technische stappen vereisen.

Er valt derhalve te concluderen dat de privacytechnologieën momenteel nog tekort schieten. Een van de algemene conclusies van de workshop van de Europese Commissie op 4 juli 2003 is dan ook dat er behoefte is aan bewustzijnbevordering van PET bij consumenten, bedrijfsleven en overheden. Daarbij ziet men een belangrijke rol weggelegd voor met name de toezichthoudende autoriteiten en de consumentenorganisaties.

162. De resultaten daarvan zijn te vinden in: *Main outcomes of the technical workshop on Privacy-Enhancing Technologies*, 4 July 2003. Op internet: <http://www.europa.eu.int/comm/internal_market/privacy/docs/lawreport/pet/200304-pet-outcome_en.pdf>.

7.6 Conclusie

In dit hoofdstuk stond de vijfde onderzoeksvraag centraal: "Wat kunnen zelfregulering en techniek betekenen voor de bescherming van persoonsgegevens op internet?" Met het oog op het beoordelen van de effectiviteit van zelfregulering is eerst ingegaan op de criteria die zelfregulering zouden kunnen bevorderen, zoals door Bennett en Raab geformuleerd. Vervolgens is een aantal voorwaarden en afwegingen voor zelfregulering besproken, zoals beschreven door Holvast en Gardeniers in 2001. Bennett en Raab en Holvast en Gardeniers hebben hun criteria en voorwaarden geformuleerd met betrekking tot de bescherming van privacy en persoonsgegevens. Daarnaast zijn, op basis van het werk van Koops e.a., criteria geïnventariseerd voor effectieve zelfregulering bij het gebruik van ICT in het algemeen. Vervolgens zijn deze toegepast op enkele van de beschreven zelfreguleringsinitiatieven. Daaruit kan worden geconcludeerd dat sprake is van een zelfreguleringstekort. Zelfregulering ter bescherming van privacy en persoonsgegevens op internet lijkt niet langer het 'ei van Columbus'. Zo is bijvoorbeeld gewezen op de ondergang van WebTrader in Nederland en in het Verenigd Koninkrijk. In het Verenigd Koninkrijk is met Web Trader gestopt omdat het niet efficiënt zou zijn. Dat is opmerkelijk, omdat zelfregulering juist efficiënter zou moeten zijn dan overheidsregulering.[163]

Het Safe Harbor programma, dat ook als zelfreguleringsinstrument kan worden beschouwd, is ook geen succes, zo blijkt uit een onderzoek van de Europese Commissie. Van de Amerikaanse bedrijven die zich hebben aangesloten bij het Safe Harbor programma, blijken verschillende zich niet te houden aan de vereisten met betrekking tot transparantie en geschillenbeslechting. Bij het Safe Harbor programma lijkt het vooral aan de volgende criteria voor zelfregulering te ontbreken: *transparantie*, *rechtszekerheid* en *naleving*.

Het zelfreguleringstekort is ook af te leiden uit het feit dat de Verenigde Staten op dit terrein 'om' lijken te gaan. Zo stelt de FTC zich, op basis van een eigen onderzoek, op het standpunt dat zelfreguleringsinitiatieven vanuit het bedrijfsleven op zichzelf niet tot voldoende privacybescherming op de elektronische markt kunnen leiden. Aanbieders van goederen en diensten op internet blijken zich namelijk niet te houden aan de door hen zelf vastgestelde beleidsregels (privacystatements) voor de omgang met persoonsgegevens van consumenten. Hoewel de FTC de rol van zelfregulering wel van belang acht, is men van mening dat het Amerikaanse Congres in aanvulling daarop wetgevingsinitiatieven dient te nemen. Uit vrijwel alle Amerikaanse privacy polls blijkt dat dit standpunt door de meerderheid van de ondervraagden wordt gedeeld. Dit Amerikaanse pleidooi voor centrale overheidsregulering als het gaat om privacybescherming van consumenten, is op zijn minst opmerkelijk. In de VS is men er in het algemeen immers altijd van over-

163. Zie bijvoorbeeld B. Baarsma e.a., *Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten*, Onderzoek in opdracht van het Ministerie van Economische Zaken, Amsterdam: Stichting voor Economisch Onderzoek, april 2003. SEO-rapport no. 664, p. 19.

tuigd geweest dat zelfregulering van privacybescherming door de industrie te prefereren valt boven overheidsregulering.

Het zelfreguleringstekort betreft niet alleen gedragsgerichte, informerende, contractuele en geschilbeslechtende instrumenten. Ook wat betreft de techniekgerichte instrumenten valt een zelfreguleringstekort te signaleren. Uit de privacy surveys van de EU en uit een workshop georganiseerd door de Europese Commissie, kan worden geconcludeerd dat er behoefte is aan bewustzijn bevordering van privacy bevorderende technieken (PET) bij consumenten, bedrijfsleven en overheden. Als men al weet van het bestaan van PET, weet men vaak niet hoe deze technieken toe te passen. Dit beeld wordt bevestigd in een rapport van de Amerikaanse FTC.[164]

Zelfregulering van privacy op internet laat te wensen over. Er is sprake van een zelfreguleringstekort. Echt effectief is zelfregulering van privacy op internet nog niet. Het lijkt voorlopig vooral een handig PR-instrument te zijn. Of, om bij de constatering van Joel Reidenberg aan te sluiten:[165]

> "E-commerce proponents are strong advocates of the self-regulatory philosophy. But the history of industry self-regulation and technological privacy demonstrate that these mechanisms have not and will not provide effective protection for citizens without the support of legal rights. The non-regulatory solutions may have been promoted with the best intentions of industry and government policymakers, but the conditions of market failure are too strong. In the end, self-regulation and technical tools have proven to be more public relations than meaningful information privacy for citizens."

Voorlopig kan slechts worden geconcludeerd dat privacybescherming via zelfregulering alleen onvoldoende waarborgen biedt ter bescherming van de privacy van de internetconsument. Met name transparantie, rechtszekerheid en naleving zijn punten van zorg bij zelfregulering, zo blijkt in de praktijk. Zelfregulering kan weliswaar een rol van betekenis spelen, maar dan in combinatie met andere sturingsmechanismen. Met betrekking tot de bescherming van de privacy van de internetconsument, valt dan vooral te denken aan aanvulling in de vorm van centrale overheidsregulering en de toepassing van door de consument zelf te treffen technische maatregelen. Aangezien ook de inzet van technische maatregelen door de consument vooralsnog tekort schiet, blijft er daarom een belangrijke rol voor overheidsregulering over.

De uiteindelijke conclusie van dit onderzoek luidt dan ook dat overheidsregulering van belang blijft ter bescherming van de privacy en persoonsgegevens van consumenten op

164. Federal Trade Commission, *Staff Workshop Report: Technologies for Protecting Personal Information,* gepubliceerd naar aanleiding van workshops in mei en juni 2003. Op Internet: <http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf>.
165. Joel R. Reidenberg, E-commerce and Trans-Atlantic Privacy, *Houston Law Review,* 2001 (38), p. 726.

internet. In de VS, het zelfreguleringsland bij uitstek, is dat door de burgers en de FTC bevestigd. Zelfregulering door middel van gedragscodes, keurmerken e.d. kan in aanvulling daarop ook een rol van betekenis spelen, maar daarbij moet rekening worden gehouden met het in dit onderzoek gesignaleerde zelfreguleringstekort. Technieken ter bevordering van privacy en de bescherming van persoonsgegevens zijn er al volop. Uit onderzoek blijkt echter dat deze slechts voor een kleine groep technologisch ingewijden bruikbaar zijn. Voor de wetgever, het bedrijfsleven en de consument valt er nog voldoende te klussen om de privacy op internet te beschermen.

8 Nabeschouwing: aandachtspunten voor de toekomst

8.1 Inleiding

Maatschappelijke, economische, juridische en informatietechnologische ontwikkelingen staan niet stil. Het lijkt dan ook nuttig om in deze nabeschouwing te wijzen op enkele aandachtspunten die op de korte of langere termijn van invloed kunnen zijn op de vraag in hoeverre zelfregulering ter bescherming van persoonsgegevens effectief zal kunnen zijn. Met het oog daarop wordt hieronder achtereenvolgens ingegaan op ontwikkelingen in verband met persoonlijkheidsprofilering, personalisatie en de commodificering van persoonsgegevens. De vraag die deze ontwikkelingen oproepen luidt, in hoeverre die bescherming zich nog wel zou dienen te concentreren op het beschermen van persoonsgegevens.

8.2 Persoonlijkheidsprofilering

Heeft de aandacht voor de bescherming van persoonsgegevens zijn langste tijd gehad en zal binnenkort de aandacht vanuit privacyoogpunt vooral bestaan voor het profileren van personen? Wordt momenteel te veel het accent gelegd op de rechtmatigheid van het enkele feit dat persoonsgegevens worden verzameld c.q. verwerkt en moet de aandacht zich meer richten op de vraag hoe persoonsgegevens worden verwerkt, in welke context en met welk doel? Er lijkt in elk geval al sprake te zijn van een 'omslag in het omgaan met gegevens en persoonsgegevens'.[166] Niet iedereen is er echter van overtuigd dat bijvoorbeeld een fenomeen als *data mining* nieuwe vragen en risico's met zich mee brengt.[167] Zolang er echter een Wet bescherming persoonsgegevens (Wbp) bestaat, zal het verwerken van persoonsgegevens uiteraard aan deze wettelijke voorschriften moeten voldoen. Het belang hiervan lijkt echter af te nemen wanneer aangenomen wordt dat de Wbp niet zozeer beoogt om verwerkingen van persoonsgegevens te voorkomen, maar om die verwerkingen te reguleren of

166. E. Schreuders, *Data mining, de toetsing van beslisregels & privacy, Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen,* Den Haag: Sdu Uitgevers 2001. Nationaal Programma Informatietechnologie en Recht, nr. 48, p. 12.
167. Zie J.E.J. Prins, Acht gesprekken over privacy en aanpalende belangen. In: H. Franken e.a. (red.), Zeven essays over informatietechnologie en recht, Den Haag: Sdu Uitgevers 2003, Nationaal Programma Informatietechnologie en Recht, nr. 63, p. 63.

zelfs te legitimeren. Mede met het oog op nieuwe technologische ontwikkelingen zou het wel eens belangrijk kunnen zijn dat de aandacht wordt verlegd.

Een voorbeeld van zo'n technologische ontwikkeling is *ubiquitous computing*: de alomtegenwoordige computer. Door de huidige alomtegenwoordige informatie- en communicatietechnologieën ontstaat een maatschappelijke omgeving waarin consumenten en burgers zich gecontroleerd weten door talloze ICT-toepassingen die in staat zijn ons gedrag te monitoren. Naast mogelijkheden tot monitoring beschikken *ubiquitous* computers ook over zoekmogelijkheden om de grote hoeveelheid opgeslagen informatie terug te kunnen vinden.[168]

In onze omgeving worden aldus op vele, ons vaak onbekende, manieren verschillende persoonsgegevens over ons verzameld, bijvoorbeeld via sensoren, micro-apparatuur, software agents, die vervolgens worden opgeslagen in databanken of *datawarehouses*. Mede als gevolg daarvan dreigt ons hele sociale leven als consument en burger transparant te worden. De verzamelde persoonsgegevens zullen in toenemende mate worden gebruikt om ons als consument (bijvoorbeeld met het oog op direct marketing) en als burger (bijvoorbeeld met het oog op pro-actieve dienstverlening) te typeren aan de hand van persoonlijkheidsprofielen. Het ziet er dan dus naar uit dat mogelijk weinig meer valt te ondernemen om te voorkomen dat onze persoonsgegevens worden verzameld. Tegelijkertijd kan dan echter de behoefte wel toenemen aan informatie en controle over de totstandkoming en de toepassing van persoonlijkheidsprofielen.

Een aantal studies gaat nader in op het gebruik van persoonlijkheidsprofielen en de bescherming van persoonsgegevens.

Schreuders wijst er in zijn dissertatie op dat bij toepassing van data mining (of Knowledge Discovery in Databases: KDD) niet zozeer de bescherming van persoonsgegevens, maar de met behulp van geautomatiseerde middelen opgestelde beslisregels het juridisch aangrijpingspunt vormen om de rechtmatigheid ervan te kunnen toetsen. Volgens Schreuders zijn de materiële normen van de Wbp maar ten dele toereikend.[169] Persoonsgegevens worden weliswaar gebruikt om beslisregels te maken (door Schreuders gelijkgesteld aan 'profielen'), maar zo'n beslisregel valt als zodanig niet onder de definitie van 'persoonsgegeven'. Het toepassen van een beslisregel in een concrete situatie, waarin een commerciële of publiekrechtelijke beslissing wordt genomen met betrekking tot een individu, is daarentegen weer wel als een verwerking van persoonsgegevens te beschou-

168. Marc Langheinrich, *Privacy Invasions in Ubiquitous Computing*, Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, Ubicomp 2002 Conference, Göteborg, Sweden, October 2002. Meer publicaties van Marc Langheinrich over privacy en *ubiquitous computing* op: <http://www.inf.ethz.ch/personal/langhein/talks/archive.html>.

169. E. Schreuders, *Data mining, de toetsing van beslisregels & privacy, Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen,* Den Haag: Sdu Uitgevers 2001, Nationaal Programma Informatietechnologie en Recht, nr. 48, p. 74.

wen. De behandeling van een individu in het maatschappelijk verkeer lijkt belangrijker te worden dan de toepassing van de Wbp. Het gaat dan ook uiteindelijk om de vraag of personen behoorlijk en zorgvuldig, oftewel 'fatsoenlijk' worden behandeld.[170]

'Fatsoen' is ook voor Custers het belangrijkste criterium voor data mining en groepsprofilering.[171] Custers signaleert dat het verzamelen van persoonsgegevens de afgelopen jaren sterk is toegenomen en dat op steeds grotere schaal wordt getracht om uit die gegevens kennis af te leiden. Door middel van data mining komen aldus groepsprofielen tot stand. Onze samenleving lijkt niet meer denkbaar zonder groepsprofielen. Custers richt zich in zijn onderzoek op het gebruik van groepsprofielen in de epidemiologie, de studie van de distributie en determinanten van ziektefrequenties bij mensen.

Custers onderscheidt drie typen morele problemen: schendingen van morele beginselen, morele conflicten en andere problemen die zich voordoen als onduidelijk is welke morele beginselen van toepassing zijn. Morele beginselen zijn bijvoorbeeld: 'geen schade aanrichten' en 'goed doen'. Andere morele beginselen die spelen in relaties tussen groepen en de samenleving en die door groepsprofielen onder druk komen te staan zijn rechtvaardigheid en solidariteit. In relaties tussen individuen en groepen kunnen groepsprofielen leiden tot problemen met betrekking tot autonomie, individualiteit en oprechtheid. Daarnaast zijn relevante beginselen bijvoorbeeld voor de arts het vertrouwen van patiënten en de betrouwbaarheid en toereikendheid van informatie. De onderzoeker heeft vooral behoefte aan vrijheid van onderzoek, en met name toegang tot de nodige gegevens. Zorgverzekeraars hebben behoefte aan winst om hun continuïteit te kunnen waarborgen. Door middel van data mining en groepsprofielen zijn zij in staat risico's vast te stellen. Risicoselectie leidt uiteindelijk weer tot een beoordeling met maatschappelijke gevolgen, bijvoorbeeld tot uitdrukking komend in insluiting of uitsluiting of in de hoogte van de te betalen premie. Daarmee lijken waarden als solidariteit, rechtvaardigheid en respect voor autonomie belangrijker te worden dan de bescherming van persoonsgegevens.

Holvast wijst er op dat het gebruik van data mining door de overheid kleiner is dan door het bedrijfsleven.[172] Volgens minister Van Boxtel gebruikt de overheid bij pro-actieve

170. E. Schreuders, *Data mining, de toetsing van beslisregels & privacy, Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen*, Den Haag: Sdu Uitgevers 2001. Nationaal Programma Informatietechnologie en Recht, nr. 48, p. 13.
171. B. Custers, *The Power of Knowledge, Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology,* Dissertatie UvT, Nijmegen: Wolf Legal Publishers (WLP) 2004., p. 258.
172. J. Holvast, *Het gebruik van persoonlijkheidsprofielen in de publieke sector,* Den Haag: Sdu Uitgevers 2001, Nationaal Programma Informatietechnologie en Recht, nr. 42, p. 114. Zie over het gebruik van data mining bij politie en justitie ook R. Sietsma, J. Verbeek, J. van den Herik, *Datamining en opsporing,* Den Haag: Sdu Uitgevers 2001, Nationaal Programma Informatietechnologie en Recht, nr. 55.

dienstverlening niet de techniek van data mining maar worden specifieke gegevens uit bestanden van verschillende overheidsorganisaties aan elkaar gekoppeld. De pro-actieve dienstverlening bestaat momenteel met name uit de oproep voor de hielprik bij pasgeborenen, het onderwijs, de dienstplicht, kwijtschelding voor gemeentelijke belastingen en de attenderingsservice dat het paspoort of rijbewijs dreigt te verlopen. Daarbij wordt nog geen gebruik gemaakt van data mining of datawarehousing.

Niettemin verwacht Holvast dat dit in de nabije toekomst zal veranderen. De overheid zal op nog grotere schaal persoonsgegevens verzamelen en verder verwerken, waaronder koppelen door middel van integratie van bestanden. Als gevolg daarvan ontstaat een datawarehouse met een enorme hoeveelheid persoonsgegevens.

Holvast voorziet twee mogelijke vormen van gebruik van zo'n datawarehouse. In de eerste plaats zullen persoonlijkheidsprofielen worden gemaakt op basis van een geformuleerde mogelijk veelzijdige en algemene vraagstelling, zoals: wie komen er in aanmerking voor huursubsidie en hebben daar zelf niet om gevraagd? In de tweede plaats zullen persoonlijke beslissingen worden genomen, bijvoorbeeld op basis van een aanvraag voor een uitkering of kwijtschelding. Daarbij kan tevens worden bekeken voor welke andere voorzieningen de aanvrager nog meer in aanmerking komt. Holvast duidt deze twee vormen aan met indirecte en directe pro-actieve dienstverlening. In het bedrijfsleven wordt de tweede vorm ook wel aangeduid met één-op-één communicatie of personalisatie.[173]

8.3 Personalisatie

Zowel binnen de private als de publieke sector zijn ontwikkelingen gaande die zijn gericht op het aanbieden van diensten op individuele maat aan consumenten en burgers. Door nieuwe toepassingen van ICT kunnen tegelijkertijd en wereldwijd grote groepen klanten worden benaderd met een aanbod van diensten die op de individuele wensen en behoeften zijn aangepast. Een organisatie die actief is op het terrein van de elektronische handel of de elektronische overheid maakt aldus gebruik een bepaalde strategie die men ook wel 'personalisatie' noemt.[174] Personalisatie als strategie is dan te omschrijven als de organisatorische doeleinden die zijn gericht op de optimalisering van de online dienstverleningsrelatie met de individuele klant op basis van gebruikersinformatie.[175]

Momenteel wordt personalisatie vooral toegepast bij dienstverlening via internet en wordt dan aangeduid als online-personalisatie of web-personalisatie. Maar met online personalisatie wordt ook gedoeld op situaties waarbij gebruik wordt gemaakt van andere

173. J. Holvast, *Het gebruik van persoonlijkheidsprofielen in de publieke sector,* Den Haag: Sdu Uitgevers 2001, Nationaal Programma Informatietechnologie en Recht, nr. 42, p. 115.
174. Zie bijvoorbeeld A.M.B. Lips, S. van der Hof, J.E.J. Prins, A.A.P. Schudelaro, *Issues of Online Personalisation in Commercial and Public Service Delivery,* Tilburg: June 2004.
175. S. van der Hof, M. Lips, C. Prins, Personalisatie in private en publieke dienstverlening, *JAVI – Juridische aspecten van internet*, augustus 2004, p. 137.

technieken dan internet om dienstverlening op maat aan te bieden aan de consument of burger. Daarbij kan men bijvoorbeeld denken aan intelligente gebouwen (ook wel 'domotica' genoemd[176]), mobiele Location-Based Services, RFID-tags, chipkaarten en biometrische toepassingen.

Op het internet zijn diverse voorbeelden te vinden van gepersonaliseerde dienstverlening.[177] Op de commerciële website van MyYahoo![178] kunnen consumenten vrijwillig en gratis gebruik maken van persoonlijke informatie-, communicatie- en transactiediensten. De inhoud van de webpagina kan aan de persoonlijke wensen van de consument worden aangepast. Op de pagina kan de consument zelf hyperlinks, aandelenportefeuilles, een persoonlijke agenda en dergelijke bijhouden. Om deze vorm van personalisatie aan te kunnen bieden zijn persoonsgegevens zoals naam, adres, geboortedatum e.d. nodig die in een speciale gebruikersdatabank worden opgeslagen. Deze gegevens worden door de consument zelf aangeleverd op het moment van registratie als gebruiker van MyYahoo! Voor sommige diensten, zoals hypotheken, leningen en verzekeringen, zijn financiële gegevens nodig. Gedragsinformatie van de consument, zoals de gebruikte internet browser, het IP-adres van de gebruiker, informatie over cookies en de geraadpleegde pagina, wordt automatisch verzameld en opgeslagen in logbestanden. Bij elk bezoek aan MyYahoo! wordt het IP-adres verzonden. Aan de hand daarvan kan worden bepaald in welke regio de gebruiker zich bevindt, zodat MyYahoo! en gelieerde ondernemingen gerichte reclameboodschappen kunnen versturen. Yahoo!'s privacyverklaring bevat een lijst van derden (reclamebedrijven) die toegang hebben tot de cookiebestanden van de consument.

Andere voorbeelden van online personalisatie in de commerciële sector zijn bijvoorbeeld eBay, Rabobank en Microsofts Windows Media Rights Manager.

Een voorbeeld van een gepersonaliseerde online dienst in de publieke sector is MyVirginia: het overheidsportaal op internet van de Amerikaanse staat Virginia.[179] Burgers en bedrijven hebben daar toegang tot gepersonaliseerde publieke diensten. Via opties als 'Find My Community' kunnen burgers bijvoorbeeld hun postcode invoeren om websites te zoeken met informatie over hun wijk of buurt. Tevens kan langs deze weg een jacht- of visvergunning worden verkregen, een uittreksel uit het geboorteregister en toegang tot kinderbijslaggegevens. Ook is het mogelijk boetes te betalen, het rijbewijs te verlengen en de orgaandonorstatus te wijzigen. Burgers kunnen de persoonlijke pagina zo instellen dat zij

176. Zie bijvoorbeeld ook Stichting Smart Homes, Smart Homes. Op Internet: <www.smart-homes.nl>.
177. Zie voor een overzicht en analyse: A.M.B. Lips, S. van der Hof, J.E.J. Prins, A.A.P. Schudelaro, *Issues of Online Personalisation in Commercial and Public Service Delivery*, Tilburg: June 2004, hoofdstuk 5.
178. <my.yahoo.com>. S. van der Hof, M. Lips, C. Prins, Personalisatie in private en publieke dienstverlening, *JAVI – Juridische aspecten van internet*, augustus 2004, p. 137.
179. <www.viriginia.gov>. Zie S. van der Hof, M. Lips, C. Prins, Personalisatie in private en publieke dienstverlening. *JAVI – Juridische aspecten van internet*, augustus 2004, p. 138.

automatisch worden geïnformeerd over openbare vergaderingen van de overheid, de gang van een wetsvoorstel, persberichten, en dergelijke. In de toekomst zal men proactief bericht kunnen ontvangen van de overheid dat het rijbewijs moet worden verlengd.[180]

Alleen als dat noodzakelijk is voor de dienstverlening aan de burger en het wettelijk is toegestaan, worden persoonsgegevens verzameld. Welke persoonsgegevens dat zijn hangt af van de dienst die wordt verleend. Daarnaast worden IP-adres, soort browser, datum en tijd van het bezoek vastgelegd van alle bezoekers van de portaalsite. Deze gegevens worden alleen gebruikt voor statistische doeleinden.

Andere voorbeelden van online personalisatie in de publieke sector zijn het geautomatiseerde toegangscontrolesysteem op Schiphol, de elektronische identiteitskaart voor burgers in Finland (FINEID), de Buddy Alert[181] en Leefstijl TV[182] dat persoonlijke gezondheidsadviezen verstrekt (vooralsnog aan inwoners van Kenniswijk te Eindhoven).

In zowel de commerciële als in de publieke sector worden bij online personalisatie methoden en technieken gebruikt om gebruikersinformatie te selecteren, te filteren en te classificeren met het oog op de informatierelatie tussen de consument en bedrijf of burger en overheid. De kern van de online personalisatie voorbeelden van MyYahoo en MyVirginia bestaat uit het verzamelen, beheren en gebruiken van gebruikersinformatie. Deze gebruikersinformatie kan uit de volgende drie categorieën bestaan:[183]

- door de gebruiker zelf verstrekte informatie (bijvoorbeeld door een webformulier in te vullen);
- indirect met de gebruiker geassocieerde informatie (bijvoorbeeld door vergelijkbare interesses of behoeften te identificeren); en
- gedragsinformatie die via gebruikers 'logins', 'cookies', of 'server logs' wordt vastgelegd.

Het verwerken van deze gebruikersinformatie leidt tot zekere privacyrisico's, althans risico's voor de bescherming van persoonsgegevens. Deze risico's zijn bijvoorbeeld de volgende:

- de gevraagde persoonsgegevens zijn niet noodzakelijk voor de levering van of de toegang tot de te verlenen dienst;
- het is onvoldoende duidelijk (transparant) voor de consument of burger dat gebruikersinformatie wordt verzameld (bijvoorbeeld via spyware, cookies, web bugs, e.d.);

180. Zie in dit verband ook: J. Holvast, *Het gebruik van persoonlijkheidsprofielen in de publieke sector*, Den Haag: Sdu Uitgevers 2001. ITER reeks nr. 42.
181. Via GSM (spraak of SMS) ontvangt men een bericht of een andere geregistreerde gebruiker in de buurt is (binnen een straal van 50 km).
182. <www.leefstijltv.nl>.
183. Zie S. van der Hof, M. Lips, C. Prins, Personalisatie in private en publieke dienstverlening, *JAVI – Juridische aspecten van internet*, augustus 2004, p. 139.

- de persoonsgegevens worden voor andere doeleinden gebruikt dan waarvoor zij oorspronkelijk zijn verzameld en opgeslagen;
- de gebruiker heeft zelf geen of onvoldoende toegang (bijvoorbeeld via de website) tot de eigen persoonsgegevens.

Wellicht is niet altijd nodig om gegevens te verwerken die herleidbaar zijn tot individuen. Idealiter zou telkens opnieuw moeten worden beoordeeld in hoeverre iemands identiteit bekend moet zijn om de beoogde gepersonaliseerde dienst te kunnen verlenen. Een uniek nummer of ander pseudoniem zou wellicht kunnen volstaan. In sommige gevallen kan men voor verschillende diensten andere nummers of pseudoniemen hebben, die dan uiteraard niet onderling uitwisselbaar mogen zijn.

Online personalisatie en de implicaties hiervan voor de bescherming van persoonsgegevens verdienen nader onderzoek, nu deze nieuwe vorm van elektronische handel en dienstverlening nog in de kinderschoenen staat.[184] De aandacht zou zich daarbij tevens dienen uit te strekken over de in- en uitsluiting van individuen bij gepersonaliseerde dienstverlening, het waarborgen van transparantie en de kwaliteit van personaliseringsprocessen, de kwaliteit en betrouwbaarheid van gepersonaliseerde informatie, de invloed en controle van betrokken partijen op het personalisatieproces, de rechtmatigheid van strategieën om het vertrouwen en de loyaliteit van consumenten en burgers te winnen, alsmede de beveiliging van de informatie.

8.4 Commodificering van persoonsgegevens

In aansluiting op deze constateringen, wordt in deze paragraaf gewezen op een ontwikkeling die de discussie over de bescherming van persoonsgegevens via zelfregulering in een nieuw daglicht zou kunnen plaatsen en dat hier wordt aangeduid met: de commodificering van persoonsgegevens.

Mede door het gebruik van infomediairs[185] krijgen persoonsgegevens van internetconsumenten economische waarde. Deze – volgens sommigen revolutionaire – ontwikkeling wordt wel aangeduid als de commodificering van persoonsgegevens.[186] Met de commodificering van persoonsgegevens wordt de economische verhandelbaarheid van persoonsgegevens bedoeld.[187] Om de stap naar commodificering van persoonsgegevens te kunnen

184. Zie S. van der Hof, M. Lips, C. Prins, Personalisatie in private en publieke dienstverlening, *JAVI – Juridische aspecten van internet*, augustus 2004, p. 141.
185. Zie § 6.8 in dit boek.
186. N. Netanel, N. Elkin-Koren, Introduction: The Commodification of Information, in: N. Elkin-Koren, N.W. Netanel (eds.), *The Commodification of Information,* The Hague – London – New York: Kluwer Law International, 2002, p. viii.
187. Dat persoonsgegevens economisch verhandelbaar zijn is op zichzelf geen nieuws. Gewezen zij op de levendige handel in adressenbestanden en de activiteiten van handelsinformatiebureaus.

maken, is het eerder in dit boek gemaakte onderscheid tussen bescherming van privacy en bescherming van persoonsgegevens relevant.[188]

In hoofdstuk 2 werd het onderscheid dat gemaakt kan worden tussen privacy en bescherming van persoonsgegevens aan de orde gesteld. Het staat niet ter discussie dat de bescherming van persoonsgegevens deel uitmaakt van het bredere concept van privacybescherming. Dat onderdeel van privacybescherming wordt 'informationele privacy' genoemd. Bescherming van persoonsgegevens heeft daardoor het karakter van een grondrecht. Het recht op privacy – of privé-leven of persoonlijke levenssfeer – is immers als fundamenteel recht opgenomen in de nationale en internationale catalogi van grondrechten. In het in 2004 ondertekende Handvest van de Grondrechten van de Europese Unie is het recht op bescherming van persoonsgegevens als afzonderlijk grondrecht opgenomen. De bescherming van persoonsgegevens moet aldus worden beschouwd als een grondrecht.

Behalve als grondrecht, is het recht op bescherming van persoonsgegevens ook te zien als een vermogensrecht.[189] Inmiddels is het een vrij algemeen aanvaarde opvatting dat eigendom op gedematerialiseerde goederen mogelijk is. In dat verband wordt wel gewezen naar artikel 1 van het eerste Protocol bij het EVRM[190]:

> "Iedere natuurlijke of rechtspersoon heeft het recht op het ongestoord genot van zijn eigendom. Aan niemand zal zijn eigendom worden ontnomen behalve in het algemeen belang en onder de voorwaarden voorzien in de wet en in de algemene beginselen van internationaal recht.
>
> De voorgaande bepalingen tasten echter op geen enkele wijze het recht aan, dat een Staat heeft om die wetten toe te passen, die hij noodzakelijk oordeelt om het gebruik van eigendom te reguleren in overeenstemming met het algemeen belang of om de betaling van belastingen of andere heffingen of boeten te verzekeren."

Het recht op bescherming van persoonsgegevens is op te splitsen in een persoonsrecht en een gebruiksrecht met betrekking tot persoonsgegevens. Het maakt verschil of het recht op bescherming van persoonsgegevens wordt beschouwd als een grondrecht of als een eigendomsrecht. Door dit recht te beschouwen als grondrecht staat het in feite los van de economische verhandelbaarheid van het recht, terwijl de eigendomsrechtelijke variant wel degelijk een zekere marktwaarde kan hebben.[191]

---

188. M.J. Radin, Incomplete Commodification in the Computerized World. In: N. Elkin-Koren, N.W. Netanel (eds.), *The Commodification of Information*. The Hague – London – New York: Kluwer Law International, 2002, p. 16-20.
189. Zie ook C. Cuijpers, *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn*. Dissertatie Tilburg. Wolf Legal Publishers 2004, p. 146 e.v.
190. Protocol bij het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Protocol van 20 maart 1952, *Trb.* 1952, 80. Herziene vertaling *Trb.* 1990, 157, gewijzigd 11 mei 1994, *Trb.* 1994, 165.
191. M.J. Radin, Incomplete Commodification in the Computerized World, in: N. Elkin-Koren, N.W. Netanel (eds.), *The Commodification of Information*, The Hague – London – New York: Kluwer Law International, 2002, p. 17.

Het gebruiksrecht op persoonsgegevens kan op grond van artikel 3:6 BW als een vermogensrecht worden gezien:

> "Rechten die hetzij afzonderlijk hetzij tezamen met een ander recht, overdraagbaar zijn, of er toe strekken de rechthebbende stoffelijk voordeel te verschaffen, ofwel verkregen zijn in ruil voor verstrekt of in het vooruitzicht gesteld stoffelijk voordeel, zijn aan te merken als vermogensrechten."

Het eigendomsrecht op persoonsgegevens staat daarmee op één lijn met bijvoorbeeld het eigendomsrecht op fysieke goederen. De bescherming van eigendom is echter anders van karakter dan de bescherming van een grondrecht. In het bijzonder is de bescherming van vermogensrechten eerder een economische bescherming, die gemakkelijker op geld waardeerbaar is. De bescherming van persoonsgegevens berust dan op het eigendomsrecht en op contractsvrijheid. Daarbij kan worden opgemerkt dat de contractsvrijheid het mogelijk lijkt te maken dat individuele consumenten (betrokkenen) zelf contractueel afspraken kunnen maken met bedrijven over het verzamelen, gebruiken, verstrekken en verdere verwerking van hun persoonsgegevens. De Europese regels ter bescherming van persoonsgegevens lijken aan die contractsvrijheid niet in de weg te staan.[192]

Deze benadering strookt, zo lijkt het, meer met de Amerikaanse benadering van privacy en bescherming van persoonsgegevens, dan met de Europese. In Europa wordt de bescherming van persoonsgegevens door de EU en door de Raad van Europa meer als een onvervreemdbaar en onverhandelbaar grondrecht beschouwd. Naast artikel 8 EVRM is het genoemde artikel II-68 van het Handvest van de Grondrechten van de Europese Unie daar een duidelijk voorbeeld van, in het bijzonder in relatie tot de preambule bij het Handvest. Een geheel andere opvatting is bijvoorbeeld te vinden in de VS, waar het bedrijfsleven in het algemeen redeneert dat het eigenaar is van de persoonsgegevens die het zelf heeft verzameld.

Het verschil in benadering is bijvoorbeeld van belang bij het gebruik van gegevens over iemands consumptiepatroon. Dergelijke informatie zal in Europa de bescherming van een grondrecht genieten. Van even groot belang in de Nederlandse rechtsorde is echter de contractvrijheid. Op basis daarvan is het mogelijk om bij contract af te wijken van hetgeen de nationale wetgeving ter bescherming van persoonsgegevens bepaalt. Een individuele consument zou dus afstand kunnen doen van zijn grondrecht en een ander (bijvoorbeeld een marketingbedrijf) het recht kunnen verlenen om zijn persoonsgegevens te gebruiken – al dan niet tegen betaling in geld of in natura.

192. C. Cuijpers, *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn*. Dissertatie UvT, Wolf Legal Publishers 2004, p. 164 e.v. Zie ook J.E.J. Prins, The Propertization of Personal Data and Identities, in: *Electronic Journal of Comparative Law*, vol. 8.3 (October 2004), <http://www.ejcl.org>.

Mede dankzij de 'globalisering' van de elektronische handel op internet, zullen relaties tussen producenten en consumenten vaker contractueel van aard zijn. Een overeenkomst over de koop van een product kan daarnaast tevens afspraken bevatten over het gebruik van persoonsgegevens. Niettemin zal niet altijd geheel duidelijk zijn of een dergelijke overeenkomst rechtmatig tot stand is gekomen. Komt er bijvoorbeeld een rechtsgeldige overeenkomst tot stand wanneer een website op een interne pagina stelt dat wie deze pagina bezoekt afstand doet van zijn privacyrechten? Of wanneer de consument in een pop-up scherm een knop moet aanklikken met de tekst "Ik accepteer deze voorwaarden", alvorens toegang te krijgen tot de website? Of wanneer de producent op de website € 2,00 korting op een bestelling aanbiedt in ruil voor afstand van de privacyrechten van de consument? In een grondrechtelijke benadering van het recht op bescherming van persoonsgegevens lijkt een dergelijke overeenkomst niet denkbaar. In een vermogensrechtelijke benadering van het recht op bescherming van persoonsgegevens kan dit echter anders liggen.

In het licht van het geconstateerde zelfreguleringstekort en de technologische ontwikkelingen rondom infomediairs verdient de benadering van commodificering van persoonsgegevens in de nabije toekomst zeker aandacht. In het verlengde van het in dit onderzoek mede gehanteerde onderscheid tussen privacy en de bescherming van persoonsgegevens, lijkt een splitsing tussen het grondrechtelijke aspect en de vermogensrechtelijke kant van deze rechten eveneens een nader onderzoek waard.[193] Op de achtergrond spelen daarbij de verschillende benaderingen op dit terrein in Europa en in de VS een rol, mede gelet op de handelsbetrekkingen die tussen beide bestaan.[194]

Of de commodificering van persoonsgegevens ook tot een betere bescherming van persoonsgegevens en privacy zal leiden, valt echter nog te bezien. Het is immers niet zeker dat het hebben van een eigendomsrecht op persoonsgegevens ook zal leiden tot een beperking van het verwerken van persoonsgegevens.

8.5 Conclusie

Persoonsgegevens zullen te allen tijde worden verwerkt, op legale of op illegale wijze. Wat even zo belangrijk lijkt als de mogelijkheid om te kunnen beschikken over de eigen persoonsgegevens, is transparantie: de mogelijkheid om te weten wie persoonsgegevens verzamelt, wie ze analyseert, aan wie ze worden verstrekt, et cetera. Hoewel dit van ouds-

193. Vgl. Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity. Work in progress, over eigendom op informatie in het kader van het ITeR onderzoek *Commodification of information, 'code' as law, and shifts in the public/private domain*. Dit document is geschreven ten bate van de workshop die op 1 en 2 juli 2004 in Amsterdam heeft plaatsgevonden en georganiseerd werd door IViR en het CRBI in samenwerking met ITeR. Op Internet: <http://rechten.uvt.nl/prins/upload/108200495825814235210.pdf>.

194. Illustratief voor de spanning die tussen de EU en de VS bestaat met betrekking tot de bescherming van persoonsgegevens in relatie tot handelsbetrekkingen, is bijvoorbeeld de discussie rond de Passenger Name Records.

her al een bestaand privacybeginsel is, staat het in een nieuw daglicht door de alomtegenwoordigheid van computers (*ubiquitous computing*), het gebruik van persoonlijkheidsprofielen, de initiatieven tot personalisatie en de waarneembare tendens tot commodificering van persoonsgegevens. Er wordt dan ook wel voor gepleit om de privacydiscussie in de toekomst te concentreren op de bescherming van identiteiten in plaats van persoonsgegevens.[195]

195. J.E.J. Prins, The Propertization of Personal Data and Identities, in: *Electronic Journal of Comparative Law*, vol. 8.3 (October 2004), <http://www.ejcl.org>.

Samenvatting

Dit onderzoek richt zich op de privacybescherming van consumenten die diensten of goederen kopen via internet en op de bescherming van hun persoonsgegevens. Privacybescherming wordt als een succesfactor voor de nieuwe economie gezien. Een consument zal minder snel een bestelling plaatsten via internet wanneer niet voldoende vertrouwen bestaat dat banken, credit card maatschappijen, winkeliers, overheden, etc. zorgvuldig met diens persoonsgegevens zullen omspringen. Hier ligt een belangrijke privacy-uitdaging. Bij privacybescherming gaat het immers niet zozeer om het beschermen van privacy als zodanig, maar privacybescherming is vooral een middel ter waarborging van individuele vrijheid voor burgers en (financiële) veiligheid voor consumenten. Een belangrijke vraag die ten grondslag ligt aan dit onderzoek is of er een evenwicht bestaat tussen overheidsregulering, zelfregulering door de industrie en de individuele verantwoordelijkheden van de consument. Alle drie komen ze in dit rapport aan de orde.

In hoofdstuk 2 is de eerste onderzoeksvraag behandeld: "Waaruit bestaat het verschil tussen privacybescherming en de bescherming van persoonsgegevens?" Daarin is uiteengezet dat er een fundamenteel onderscheid bestaat tussen de bescherming van privacy en de bescherming van persoonsgegevens. Dit verschil is benoemd als 'het privacygat'.

De meer fundamentele bescherming van privacy kan door consumenten op internet verschillend worden ervaren. Consumenten kunnen de volgende waarden achter privacy hanteren: zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering, ongestoord leven, eigenwaarde, vrij blijven van manipulatie, integriteit en autonomie.

De bescherming van persoonsgegevens is (slechts) een element van het meer algemene begrip 'privacy', ook wel aangeduid met 'informationele privacy'. De wettelijke regels ter bescherming van persoonsgegevens beogen in feite niet alleen de privacy te beschermen, maar stellen de grenzen vast tot waar – onder welke voorwaarden – persoonsgegevens mogen worden verwerkt.

In hoofdstuk 3 is de tweede onderzoeksvraag aan de orde gesteld: Hoe denkt de burger of consument over diens privacy op internet? Eerst zijn enkele praktijken beschreven van een aantal commerciële organisaties die via internet persoonsgegevens verzamelen. In het bijzonder is daarbij gekeken naar de praktijken van IBM, General Motors Corporation, The Procter & Gamble Company, Amazon.com en Microsoft. Hoewel in de VS van oudsher een voorkeur bestaat voor zelfregulering van privacybescherming in plaats van

centrale overheidsregulering, blijkt uit diverse Amerikaanse privacy surveys dat de publieke opinie hieromtrent momenteel een belangrijke verschuiving doormaakt. Amerikaanse burgers blijken steeds vaker een voorkeur te hebben voor wetgeving boven zelfregulering. Uit deze surveys blijkt voorts dat de Amerikaanse burger als consument op internet de volgende waarden achter de bescherming van persoonsgegevens belangrijk vindt: controle over het verzamelen en verstrekken van persoonsgegevens; aansprakelijkheid en beveiliging; anonimiteit op internet; geen 'web tracking'; vertrouwen in bedrijfsleven en overheid; privacy-zelfbescherming; openheid rond bestaande 'tracking' methoden; informatie; privacy ook na 11 september 2001.

Een aantal Nederlandse surveys uit 1988 en 1993 laat zien dat Nederlandse burgers graag zeggenschap uitoefenen over de eigen persoonsgegevens. Uit een onderzoek uit 1999 blijkt dat een meerderheid van de ondervraagde burgers (47%) van mening is dat de informatietechnologie een bedreiging vormt voor de privacy en dat dit in veel gevallen zou moeten zijn te voorkomen.

Europese privacy surveys laten zien dat een meerderheid van de Europese burgers (gemiddeld 67%) vreest voor aantasting van de privacy wanneer zij persoonsgegevens achter laten op internet. Hierbij moet wel worden opgemerkt dat de opvattingen van de burgers sterk kunnen verschillen van de ene tot de andere lidstaat.

In hoofdstuk 4 is ingegaan op het eerste deel van de derde onderzoeksvraag naar de bestaande overheidsregulering ter bescherming van persoonsgegevens. Allereerst zijn de algemene privacybeginselen besproken, die ten grondslag liggen aan de hedendaagse wet- en regelgeving met betrekking tot privacy en persoonsgegevensbescherming. De oude uit 1980 stammende 'Europese' privacybeginselen, neergelegd in het Verdrag van Straatsburg van de Raad van Europa, zijn in 1995 nog eens bevestigd in de EU privacyrichtlijn 95/46/EG, die recentelijk in de huidige privacywetgeving van de EU-lidstaten is geïmplementeerd. In de VS is rond dezelfde tijd een aantal vergelijkbare *fair information practice principles* geformuleerd. Voorts is de Amerikaanse industrie opgeroepen om deze beginselen door middel van zelfregulering te implementeren. Uit onderzoek van de FTC blijkt echter dat in 2000 slechts een minderheid de *fair information practice principles* ook daadwerkelijk toepast bij het verzamelen van persoonsgegevens via internet. Eveneens een minderheid heeft zich aangesloten bij zogeheten privacyprogramma's als TRUSTe. Hoewel de rol van zelfregulering van belang blijft, aldus de FTC, is zij tevens van mening dat het Amerikaanse Congres in aanvulling daarop wetgevingsinitiatieven dient te nemen. Dergelijke initiatieven zouden moeten leiden tot een minimum niveau van privacybescherming voor consumenten op internet.

Voorts is aandacht besteed aan Europese regelgeving die van toepassing is op de bescherming van de consumentenprivacy op internet. Het Europese juridische kader bestaat met name uit het nieuwe Europese Handvest van de Grondrechten van de Europese Unie en de EU-richtlijnen 95/46/EG (algemene privacyrichtlijn), 97/7/EG (richt-

lijn verkoop op afstand), 2000/31/EG (richtlijn inzake elektronische handel) en 2002/58/EG (richtlijn privacy en elektronische communicatie).

In hoofdstuk 5 is gezocht naar een antwoord op het tweede deel van de derde onderzoeksvraag: "Welke zelfreguleringsinitiatieven voor gegevensbescherming kunnen we onderscheiden?"

In de kabinetsnota Wetgeving voor de Elektronische Snelweg (WES) van februari 1998, heeft de Nederlandse regering haar voorkeur uitgesproken voor zelfregulering van het internet boven overheidsregulering. Zelfregulering valt te overwegen wanneer het gedrag van 'professionals' moet worden gereguleerd, in situaties waarin individuele of groepsbelangen niet te zeer verschillen van het belang dat de desbetreffende wet beoogt te dienen en in omstandigheden waarin (volledige) overheidsregulering niet of slechts zeer moeizaam te controleren en te handhaven is. Met name op basis van de als laatste genoemde omstandigheden, lijkt zelfregulering voor de bescherming van de privacy op het wereldwijde internet een nuttig instrument.

Vervolgens is een overzicht gegeven van zelfreguleringsinitiatieven: gedragscodes, contractuele regelingen, de Safe Harbor Agreement en keurmerken. Tevens is een voorbeeld uitgewerkt over privacy policies op grond van de Amerikaanse wet COPPA ter bescherming van persoonsgegevens van kinderen op internet. Uit deze beschrijving is gebleken dat al deze initiatieven niet hebben geleid tot een sluitende en betrouwbare bescherming van consumentenprivacy op internet.

In hoofdstuk 6 is ingegaan op de techniekgerichte instrumenten voor zelfregulering die de consument ter beschikking staan ten behoeve van privacy zelfbescherming. Dit hoofdstuk behandelde de vierde onderzoeksvraag, die luidt: "Welke bescherming biedt de techniek?"

In dat hoofdstuk is aandacht besteed aan al bestaande, maar ook nieuwe privacy bevorderende technieken en maatregelen.

Identiteitsbeschermers kunnen worden ingezet om digitale pseudoniemen te creëren. Door gebruikmaking van anonimiseringssoftware kan een consument een website anoniem bezoeken. Door een 'cookie cruncher' te installeren op de computer, kunnen cookies worden bestreden. Herkenning van het IP-adres is te voorkomen door gebruik te maken van een proxy-server. Door middel van P3P, toe te passen door de website-aanbieder, kan het privacybeleid aan de consument bekend worden gemaakt. Bij gebruik van e-mail kunnen e-mailfilters worden ingezet of kan men gebruik maken van remailers, waardoor de identiteit van de houder van een e-mailadres onbekend kan blijven. Tot slot kan een infomediair worden ingezet: een *personal assistant* die ervoor kan zorgen dat een consument alleen zaken doet met aanbieders van websites die op een zorgvuldige manier met persoonsgegevens om gaan, of die een financiële vergoeding geven voor het gebruiken van die persoonsgegevens.

De verwachtingen van dergelijke techniekgerichte instrumenten mogen nog niet al te hoog worden ingeschat. Uit de *privacy surveys* van de EU blijkt dat PET onder de burgers van de EU nog niet zo bekend is. Van alle EU burgers heeft gemiddeld 72% nog nooit gehoord van privacy bevorderende technieken. Slechts een kleine groep EU burgers (gemiddeld 6%) heeft wel gehoord van privacybeschermende technieken en heeft die vervolgens ook wel eens gebruikt. Degenen die er wel van hadden gehoord, maar deze technieken nog nooit hadden gebruikt gaven als redenen op dat men niet weet hoe deze technieken te gebruiken of hoe deze op de computer te installeren. Voorts blijkt dat de onderzochte bedrijven in de EU lidstaten nog maar weinig ervaring hebben met het toepassen van privacy enhancing technologies (PET). Volgens het onderzoek zou slechts eenderde (32%) van de ondervraagden PET toepassen. Nederlandse bedrijven scoren daarbij het hoogst: 47%. Bijna eenderde van de ondervraagden in de bedrijven (28%) heeft nog nooit gehoord van PET.

In hoofdstuk 7 stond de vijfde onderzoeksvraag centraal: "Wat kunnen zelfregulering en techniek betekenen voor de bescherming van persoonsgegevens op internet?" Met het oog op het beoordelen van de effectiviteit van zelfregulering is eerst ingegaan op de criteria die zelfregulering zouden kunnen bevorderen, zoals door Bennett en Raab geformuleerd. Vervolgens is een aantal voorwaarden en afwegingen voor zelfregulering besproken, zoals beschreven door Holvast en Gardeniers in 2001. Bennett en Raab en Holvast en Gardeniers hebben hun criteria en voorwaarden geformuleerd met betrekking tot de bescherming van privacy en persoonsgegevens. Daarnaast zijn criteria geïnventariseerd voor effectieve zelfregulering bij ICT in het algemeen. Vervolgens zijn deze toegepast op enkele van de beschreven zelfreguleringsinitiatieven. Daaruit kan worden geconcludeerd dat sprake is van een zelfreguleringstekort. Zelfregulering ter bescherming van privacy en persoonsgegevens op internet lijkt niet langer het 'ei van Columbus'. Zo is bijvoorbeeld gewezen op de ondergang van WebTrader in Nederland en in het Verenigd Koninkrijk. In het Verenigd Koninkrijk is met Web Trader gestopt omdat het niet efficiënt zou zijn. Dat is opmerkelijk, omdat zelfregulering juist efficiënter zou moeten zijn dan overheidsregulering.

Het Safe Harbor programma, dat ook als zelfreguleringsinstrument kan worden beschouwd, is ook geen succes, zo blijkt uit een onderzoek van de Europese Commissie. Van de Amerikaanse bedrijven die zich hebben aangesloten bij het Safe Harbor programma, blijken verschillende zich niet te houden aan de vereisten met betrekking tot transparantie en geschillenbeslechting. Bij het Safe Harbor programma lijkt het vooral aan de volgende criteria voor zelfregulering te ontbreken: *transparantie*, *rechtszekerheid* en *naleving*.

Het zelfreguleringstekort is ook af te leiden uit het feit dat de Verenigde Staten op dit terrein 'om' lijken te gaan. Zo stelt de FTC zich, op basis van een eigen onderzoek, op het standpunt dat zelfreguleringsinitiatieven vanuit het bedrijfsleven op zichzelf niet tot voldoende privacybescherming op de elektronische markt kunnen leiden. Hoewel de

FTC de rol van zelfregulering wel van belang acht, is men van mening dat het Amerikaanse Congres in aanvulling daarop wetgevingsinitiatieven dient te nemen. Uit vrijwel alle Amerikaanse privacy polls blijkt dat dit standpunt door de meerderheid van de ondervraagden wordt gedeeld.

Het zelfreguleringstekort betreft niet alleen gedragsgerichte, informerende, contractuele en geschilbeslechtende instrumenten. Ook wat betreft de techniekgerichte instrumenten valt een zelfreguleringstekort te signaleren. Uit de privacy surveys van de EU en uit een workshop georganiseerd door de Europese Commissie, kan worden geconcludeerd dat er behoefte is aan bewustzijn bevordering van privacy bevorderende technieken (PET) bij consumenten, bedrijfsleven en overheden. Als men al weet van het bestaan van PET, weet men vaak niet hoe deze technieken toe te passen.

Tot slot is in een nabeschouwing in hoofdstuk 8 vooruit gekeken naar de toekomst van de bescherming van privacy en persoonsgegevens. Daarbij is in het bijzonder ingegaan op de ontwikkelingen op het gebied van persoonlijkheidsprofilering, personalisatie en de commodificering van persoonsgegevens.

Persoonlijkheidsprofielen komen tot stand via analyse van grote hoeveelheden gegevens. Die gegevens kunnen persoonsgegevens zijn die zijn onmerkbaar voor de consument kunnen worden verzameld via *ubiquitous computing* en opgeslagen in datawarehouses. Daardoor is het mogelijk om pro-actief diensten op maat aan burgers aan te bieden en om één-op-één-communicatie toe te passen. Dergelijke toepassingen noemt men ook wel 'personalisatie'.

Online personalisatie en de implicaties hiervan voor de bescherming van persoonsgegevens verdienen nader onderzoek. De aandacht zou zich daarbij moeten richten op de in- en uitsluiting van individuen bij gepersonaliseerde dienstverlening, het waarborgen van transparantie en de kwaliteit van personaliseringsprocessen, de kwaliteit en betrouwbaarheid van gepersonaliseerde informatie, de invloed en controle van betrokken partijen op het personalisatieproces, de rechtmatigheid van strategieën om het vertrouwen en de loyaliteit van consumenten en burgers te winnen, en de beveiliging van de informatie.

Persoonsgegevens lijken in toenemende mate economische waarde te krijgen. De verhandelbaarheid van persoonsgegevens duidt men aan met de term 'commodificering'. Dit is eveneens uit een oogpunt van privacybescherming een interessante ontwikkeling die nader privacyonderzoek verdient, omdat daarbij het onderscheid zichtbaar wordt tussen de grondrechtelijke bescherming van privacy enerzijds en de vermogensrechtelijke benadering van persoonsgegevens anderzijds.

Summary

This book concerns the protection of information privacy of consumers when they purchase services or goods on the Internet. Data protection is often looked upon as a factor for the success of the new economy. If consumers cannot trust retailers, banks, credit card companies or others to process their personal data carefully, then they will hesitate to place orders through the Internet. Creating trust is an important challenge for information privacy. Privacy or data protection are not issues as such, but a means to guarantee freedom for the citizen and financial security for consumers. One of the important questions this book deals with is whether there is a balance between government regulations, industry self-regulations, and individual accountabilities for consumers.

The first question in this research is dealt with in Chapter 2 and is: "What is the difference between privacy protection and data protection?" A fundamental difference between the protection of privacy and the protection of personal data seems to exist. This difference is called 'the privacy gap'. Consumers can experience privacy protection on the Internet in different ways. In general, consumers consider the following privacy values to be important:[196]

- Independence
- Freedom of movement
- Equality
- Freedom from stigmatization
- Undisturbed life
- Self-esteem
- Freedom from manipulation
- Integrity
- Autonomy

196. G.C.J. Smink, A.M. Hamstra en H.M.L. van Dijk, *Privacybeleving van burgers in de informatiemaatschappij*, (Werkdocument 68 Rathenau Insituut), 1999, Den Haag, Rathenau Instituut.

These values were investigated in 1999 by the Rathenau Institute, which is a research institute in the Netherlands. Data protection is just one of the elements of privacy protection. Data protection is often called 'information privacy'. It is important to note that the legal framework for data protection not only protects information privacy, but also determines the boundaries as to when, and under what conditions, personal data can be processed.

In Chapter 3, we deal with the second question concerning this research: "What do citizens and consumers think of their privacy on the Internet?" First, several practices are described concerning the processing of personal data on the Internet by commercial organisations. Several businesses collect and use personal data from their potential customers. Insight into these data processing activities were presented at the hearings before the American House of Representatives in 2001.[197] At these hearings, representatives from IBM, General Motors Corporation, Proctor and Gamble and Amazon.com explained to the subcommittee how they carried out their data processing activities. These activities for example, involved the collection of IP-addresses which can often be traced to identifiable individuals. These addresses must be treated as personal data therefore, data protection legislation is applicable however, some consumers may not always experience this as an invasion of their privacy.

Second, an analysis is given of several privacy surveys being held in the Netherlands, Europe, and the United States. The American surveys show that public opinion in the US is changing. Nowadays, American citizens prefer government regulations instead of self-regulations. This is remarkable because formerly self-regulation is preferred in the US. It can also be concluded from these American surveys what American consumers consider to be important values behind data protection. These are: [198]

- Control of both initial collection of data and data sharing;
- Accountability and security;
- Comprehensive legislation, not self-regulation;
- Anonymity;
- No Web Tracking, especially when personal information is linked to the profile;
- Individuals do not trust companies to administer personal data and fear both private-sector and government abuses of privacy;
- Individuals want privacy self-defence;

197. How do businesses use customer information: Is the customer's privacy protected? Hearing before the subcommittee on commerce, trade, and consumer protection of the Committee on Energy and Commerce, US House of Representatives. One hundred seventh congress. First session. July 26, 2001. Serial No. 107–49.
198. EPIC, *Public Opinion and Privacy Page.* On the Internet: <http://www.epic.org/privacy/survey/default.html>. Last updated: June 25, 2003.

- Awareness of prevalent tracking methods;
- Notice;
- Data protection is important after September 11, 2001.

Privacy surveys carried out in the Netherlands from 1988 to 1993 show that Dutch citizens like to control their own personal data. The conclusion of a survey carried out in 1999 was that the majority of the people interviewed believed that information technologies were a threat to privacy and should be prevented.

European privacy surveys show that the majority of EU-citizens (average 67%) fear that their privacy will be invaded if their personal data is exposed on the Internet. However, it should be noted that EU-citizens' opinions differ strongly from one member state to another.

Chapter 4 deals with the first part of the third question in this research: "What government regulations exist to protect personal data?" In this chapter, the legal framework for the protection of personal data is described. Both in Europe and in the United States, data protection is based on general data protection principles. The Council of Europe and the Organisation for Economic Co-operation and Development (OECD) presented their data protection principles in 1980/1981. Shortly after the publication of the OECD Guidelines[199], the Council of Europe presented Convention no. 108[200], containing the same eight data protection principles. These data protection principles have been confirmed and elaborated in the European Data Protection Directive 95/46/EC, which has recently been implemented into the national data protection legislation of the member states of the European Union.

At the same time, a comparable set of data protection principles was formulated in de United States: the *fair information practice principles*. The principles are:

1. Notice
2. Choice
3. Access
4. Security
5. Enforcement.

The American industries were called upon to implement these principles by means of self-regulation.

199. Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris 1981.
200. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, January 28, 1981. ETS No. 108.

Several reports of the Federal Trade Commission (FTC)[201] show however, that a lot of website providers collect personal data from their customers, but a minority of them have implemented the *fair information practice principles*. The FTC is now of the opinion that online data protection is a challenge for government policies: "it is time for government to act to protect consumers' privacy on the Internet." The FTC recommends that Congress enact legislation to ensure adequate protection of consumer privacy online. In doing so, however, the FTC recognizes that industry self-regulation, as well as consumer and business education, should still play important roles in any legislative framework.

The proposed legislation from Congress should guarantee a basic level of data protection for all visitors of consumer-oriented commercial websites. All consumer-oriented commercial websites should comply with the four widely accepted *fair information practice principles*: Notice, Choice, Access, and Security.

The European legal framework for the protection of the personal data of visitors of consumer-oriented commercial websites is based on the protection of human rights as formulated in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) Article 8 has been elaborated in the Council of Europe Convention no. 108 to protect personal data with regard to the automated processing. The general data protection principles have been adopted and elaborated in the EU Data Protection Directive 95/46/EC. For the protection of privacy with regard to electronic communications, EU Directive 97/66/EC has recently been replaced by Directive 2002/58/EC. With regard to the openness principle, the relevance of the information requirements for consumer-oriented commercial websites has been stressed and formulated in the EU Directives Distance Selling 97/7/EC, and the E-commerce Directive 2000/31/EC.

Chapter 5 deals with the second part of the third question in this research, which is: "What kind of self-regulation initiatives for data protection are there?" This chapter also pays attention to the self-regulation policies of international organisations.

In the policy document *Legislation for the Electronic Highways* (February 1998), the Dutch cabinet stated that it preferred self-regulation for the Internet to government regulation. In general, self-regulation can be considered when the behaviour of professionals should be regulated. Self-regulation can also be considered in situations where individual or group interests slightly differ from the interest for which a specific act is intended. Finally, self-regulation can be considered in circumstances where there are no

201. For example: Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*. May 2000. On the Internet: <http://www.ftc.gov/privacy/index.html>.

government regulations or where they are very difficult to control and maintain. In the case of the latter, self-regulation would seem to be a useful instrument to protect information privacy on the Internet.

In its report published in 2003, the SEO Amsterdam Economic (a Dutch independent research institute), distinguished twenty-two different self-regulation instruments. These instruments are divided into five different clusters: technology-oriented instruments, behaviour-oriented instruments, information-oriented instruments, contractual instruments, and dispute resolution instruments. Chapter 5 describes the codes of conduct such as, (behaviour-oriented instrument), seal programs (information oriented instrument), and contractual arrangements (contractual instruments).

In Chapter 6 we discuss technology-oriented self-regulation instruments. This chapter deals with the fourth question in this research: "How can technology protect information privacy?" This chapter also deals with the existing and future privacy enhancing technologies and measures (PET). Some of these are: identity protectors which can be applied to create digital pseudonyms; anonymization software, which will allow a consumer to visit a website anonymously; the installation of cookie-crunchers on a personal computer which will allow cookies to be deleted; the recognition of IP-addresses can be prevented by making use of a proxy-server; by using a P3P, to be applied by a website provider, the privacy policy of a website can be electronically displayed to a consumer; the use of an e-mail filter or a consumer can use the service of an anonymous remailer to protect their identity. Finally, an infomediary can be used. This is a kind of personal assistant, who ascertains that a consumer only deals with website providers who process personal data in a lawful and careful way, or who offer financial compensation for the use of personal data.

Expectations of such privacy enhancing technologies should not be overestimated. From the privacy surveys in the European Union, it appears that an average of 72% of all EU-citizens have never heard of PET. Only a small number of EU-citizens (an average of 6%) have heard of PET and actually use them. Those who have heard of PET, but have never used them do not know how to use them or how to install them on their computer.

Furthermore, many companies in the European Union have little experience with applying PET. According to the privacy survey, only 32% of the people interviewed apply PET. Dutch companies score the highest: 47%. Almost one-third (28%) of the interviewed companies have never heard of PET.

Chapter 7 deals with the fifth question in this research: "What can self-regulation and technology mean for the protection of information privacy on the Internet?" First, to assess the effectiveness of self-regulation, the criteria to promote self-regulation, as

formulated by Bennett and Raab, are presented. Next, conditions and considerations for self-regulation are discussed, as described by Holvast and Gardeniers. These criteria, conditions, and considerations were formulated by these authors to protect information privacy. Furthermore, an inventory has been made of criteria for effective self-regulation of information and communications technologies in general, formulated by Koops and others.[202] These general criteria are applied to some of the self-regulation initiatives described in Chapter 5. It can be concluded that self-regulation is deficient. Self-regulation is no longer the right approach for the protection of information privacy on the Internet. This chapter has, for example, indicated the decline of WebTrader in the Netherlands and in the UK. It appeared that WebTrader has been abolished in the UK because it was not efficient enough. That is remarkable because self-regulation is normally considered to be more efficient than government regulation.

The Safe Harbor Program, which also can be considered as a self-regulatory instrument, cannot be considered as successful either. This was concluded in a study by the European Commission. Several American companies which adhered to the Safe Harbor Program did not comply with the principles of openness and enforcement. The deficiencies of the Safe Harbor Program lie especially in its lack of openness, legal certainty, and compliance.

The deficiency of self-regulation is also illustrated by the fact that the US seems to be shifting from self-regulation to government regulation. Based on its own research, the Federal Trade Commission (FTC) concludes that online privacy cannot be sufficiently protected by industry self-regulation initiatives. Online providers of services and goods appear not to comply with the privacy statements, drafted by them, concerning the processing of personal data from consumers. Although the FTC is aware of the importance of self-regulation, the FTC is of the opinion that the American Congress should also take initiatives for government regulations. From nearly all privacy polls made in the US, it appears that this opinion is shared by a majority of those interviewed.

The deficiency of self-regulation not only concerns behaviour-oriented instruments, information-oriented instruments, contractual instruments, and dispute resolution instruments. Self-regulation also seems deficient with regard to technology-oriented instruments. From the EU privacy surveys, and from a workshop organized by the European Commission, it can be concluded that there is a need to promote consumers, indu-

202. See the chapter about self-regulation as the starting point, by B.-J. Koops, M. Lips, S. Nouwt, C. Prins en M. Schellekens, in the book *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-liners*, (preliminary title) written by researchers from TILT – Tilburg Institute for Law, Technology, and Society (to be published).

stry, and government with the awareness of privacy enhancing technologies. A large amount of consumers and industries have never heard of PET and others do not know how to use it.

Finally, as an afterthought Chapter 8 discusses the future of privacy and data protection. Special attention is paid to developments concerning data mining and profiling, personalization, and the commodification of personal data.
Profiling persons and groups is realized by analyzing large amounts of data. These data may be personal data, collected, for example, imperceptibly for consumers by *ubiquitous computing*, and stored in data warehouses. This makes it possible to offer services to citizens in a pro-active way, and to apply one-to-one communication.

Online personalization and its implications for the protection of information privacy, deserves further research. Attention should be paid to the policies of inclusion and exclusion of individuals in personalized services. Also, attention should be paid to the guarantees for transparency, and the quality of personalization processes, the quality and reliability of personalized information, the influence and control on the personalization process by the parties involved, the lawfulness of strategies to gain trust and loyalty from consumers and citizens, and to data security.

Personal data seem to be of increasing economic value. The marketability of personal data is also specified as commodification. The commodification of personal data is an interesting development from an information privacy perspective, which also deserves further research. The commodification of personal data visualizes, for example, the difference between the human rights perspective of privacy on the one hand, and the property law perspective of personal data on the other.

Literatuur

Alonso Blas, D., The pioneer work of the Article 29 Working Party in the field of on-line authentication: the Microsoft .NET Passport case, *Privacy & Informatie*, 2003, nr. 6, p. 263-266.

Article 29 – Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers,* Adopted 3 June 2003, WP 74.

Baarsma, B. e.a., *Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten,* Onderzoek in opdracht van het Ministerie van Economische Zaken. Amsterdam: Stichting voor Economisch Onderzoek, april 2003. SEO-rapport no. 664.

Bennett, Colin J.; Raab, Charles D., *The governance of privacy: policy instruments in global perspective,* Aldershot: Ashgate 2003.

Blok, P.H, De splitsing van privacy. Advies over het grondrecht op privacy in het digitale tijdperk*, Ars Aequi,* 6(50), p. 435-439.

CEN-ISSS, *Data Privacy Workshop*, op internet: <http://www.cenorm.be/isss/Workshop/DPP/default.htm>.

Centrum voor Privacyonderzoek, *Geen totale geheimhouding, maar selectieve openbaarmaking,* Amsterdam, 1993.

Commissie Grondrechten in het digitale tijdperk, *Rapport Commissie "Grondrechten in het digitale tijdperk",* Den Haag, Mei 2000.

Commissie van de Europese Gemeenschappen, *Europese Governance. Een witboek,* Brussel 25.7.2001. COM (2001) 428 definitief.

Commissie van de Europese Gemeenschappen, *Werkdocument van de diensten van de commissie over de toepassing van Beschikking 520/2000/EG van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betref-*

fende de gepastheid van de bescherming geboden door de veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, Brussel, 13 februari 2002, SEC (2002) 196.

Commissie van de Europese Gemeenschappen, *eEurope 2005: Een informatiemaatschappij voor iedereen,* Brussel, 28.05.2002. COM (2002) 263 definitief.

Council of Europe, *Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data,* European Treaty Series No. 108.

Crouwers-Verbrugge, B.J., B.M.A. van Eck & E. Schreuders (red.), *Persoonsgegevens beschermd; Uitspraken van de Registratiekamer*, Den Haag: SDU 1997.

Cuijpers, C., *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn*, Dissertatie UvT, Wolf Legal Publishers 2004.

Custers, B., *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Dissertatie UvT, Nijmegen: Wolf Legal Publishers (WLP) 2004.

Eck, B.M.A. van, U. van de Pol & C.G. Zandee, *Persoonsgegevens beschermd. Van WPR naar WBP; Uitspraken van de Registratiekamer,* Den Haag: SDU 1997.
(2e herziene druk).

Eijlander, P., P.C. Gilhuis, & J.A.F. Peters (red.), *Overheid en zelfregulering. Alibi voor vrijblijvendheid of prikkel tot actie?* Zwolle: W.E.J. Tjeenk Willink, 1993.

Eijlander, P., & W. Voermans, *Wetgevingsleer,* Deventer: W.E.J. Tjeenk Willink, 1999.

Elkin-Koren, N., N.W. Netanel (eds.), *The Commodification of Information*, The Hague – London – New York: Kluwer Law International, 2002.

Esch, R.E. van, *'Elektronische handel'*, H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer*, Deventer: Kluwer 2001 (vierde druk).

Esch, R.E. van, *'Recente ontwikkelingen in het vermogensrecht op het terrein van de elektronische handel'*, *WPNR: Weekblad voor Privaatrecht, Notariaat en Registratie*, 28 april 2001, jrg. 132, nr. 6443.

European Opinion Research Group EEIG, *Data Protection,* Special Eurobarometer 196 – Wave 60.0. December 2003.

Federal Trade Commission, *How to protect Kid's Privacy Online*, <http://www.ftc.gov/opa/1999/9902/petapp4.99.htm>. February 1999.

Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress*, May 2000.

Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues,* February 2002.

Federal Trade Commission, *Staff Workshop Report: Technologies for Protecting Personal Information,* gepubliceerd naar aanleiding van workshops in mei en juni 2003.

FEDMA, *FEDMA Code On E-Commerce & Interactive Marketing*, 6 september 2000.

Gardeniers, H., Privacy Enhancing Mediaries: Nieuwe mogelijkheden voor privacybescherming?, *Privacy & Informatie* 2001/1.

Gauthronet, Serge, & Etienne Drouard, *Unsolicited Commercial Communications and Data Protection*, Commission of the European Communities, January 2001 (Internal Market DG – Contract n° ETD/99/B5-3000/E/96).

Gellman, Robert, *Privacy, Consumers, and Costs. How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete,* Maart 2002.

Groep Gegevensverwerking Artikel 29, *Werkdocument Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming,* goedgekeurd op 21 november 2000. WP 37.

Groep Gegevensbescherming Artikel 29, *Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU,* goedgekeurd op 30 mei 2002. WP 56.

Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Platform for Privacy Preferences (P3P) en de Open Profiling Standard (OPS*), Advies 1/98. WP 11, 16 juni 1998.

Hagel III, J. & M. Singer, *De Waarde van het Internet, groeiscenario's voor elektronisch zakendoen, Business Contact*, 2000 (origineel: J. HAGEL III en M. SINGER, *Net Worth:*

the emerging role of the infomediary in the race for customer information, Harvard Business School Press).

Harris-Equifax Consumer Privacy Survey 1991, Georgia, USA.

Hof, S. van der, M. Lips, C. Prins, Personalisatie in private en publieke dienstverlening, *JAVI – Juridische aspecten van internet*, augustus 2004.

Holleman, A., Privacystatements op het internet, *Privacy & Informatie* 2003, nr. 6, p. 253-258.

Holvast, Jan, Henny van Dijk en Gerrit Jan Schep, *Privacy Doorgelicht,* Den Haag: SWOKA, 1989.

Holvast, J., H. Gardeniers, *Privacy, zelfregulering en internet*, Eindrapport. Mei 2001.

Holvast, J., en J. Nouwt, Privacy van kinderen op internet is al bij wet geregeld, *Nederlands Juristen Blad*, 2002, afl. 22, p. 1063-1065.

Holvast, J., *Het gebruik van persoonlijkheidsprofielen in de publieke sector*, Den Haag: Sdu Uitgevers 2001.Nationaal Programma Informatietechnologie en Recht, nr. 42.

How do businesses use customer information: Is the customer's privacy protected? Hearing before the subcommittee on commerce, trade, and consumer protection of the committee on energy and commerce, House of Representatives, One hundred seventh congress, First session, Serial No. 107-49, July 26, 2001.

ICX, *The ICX Privacy Code of Conduct*, July 2000.

International Chamber of Commerce, *Model clauses for use in contracts involving transborder data flows*, 23 september 1998.

Johnson, J.L., Privacy and the Judgements of others, *The Journal of Value Inquiry*, 1989.

International Working Group on Data Protection in Telecommunications, *Common position on Essentials for privacy-enhancing technologies (e.g. P3P) on the WorldWideWeb,* Adopted at the 23rd Meeting in Hong Kong SAR, China, 15 april 1998.

IPSE, *Data Protection and Privacy. The Initiative for Privacy Standardization in Europe*.

Johnson, J.L., Privacy and the Judgements of others, *The Journal of Value Inquiry*, 1989.

Koopmans, T., Privacy and the dilemma's of human rights' protection, P. Ippel, e.a. *Privacy disputed*, Den Haag: SDU 1995.

Koops, Bert-Jaap, Corien Prins, Maurice Schellekens, Serge Gijrath, & Eric Schreuders, *Overheden over internationalisering en ICT-recht,* Den Haag: Sdu Uitgevers 2000. Nationaal Programma Informatietechnologie en Recht, nr. 39.

Koops, B.-J., M. Lips, S. Nouwt, C. Prins en M. Schellekens, hoofdstuk over zelfregulering in het boek *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-liners*, (voorlopige titel), geschreven door diverse onderzoekers van het TILT – Tilburg Institute for Law, Technology, and Society (nog te verschijnen).

Langheinrich, Marc, *Privacy Invasions in Ubiquitous Computing*. Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, Ubicomp 2002 Conference, Göteborg, Sweden, October 2002.

Lerouge, Jean-François, Internet Effective Rules: The Role of Self-Regulation, *The EDI Law Review*. The Hague, Vol. 8, nr. 4, 2001, p. 197-207.

Lips, A.M.B., S. van der Hof, J.E.J. Prins, A.A.P. Schudelaro, *Issues of Online Personalisation in Commercial and Public Service Delivery,* Tilburg, June 2004.

Nederlands Normalisatie Instituut, *Nederlandse Norm Medische Informatica – Informatiebeveiliging in de zorg – Algemeen,* NEN 7510: 2004 nl (1 april 2004).

NLIP – Brancheverenigingen van Nederlandse Internet Providers, *Gedragscode 2.0*.

Nota Wetgeving voor de Elektronische Snelweg. *Kamerstukken II*, 1997/98, 25 880, nr. 2.

Nouwt, J., Kid's Privacy on the Internet. Collecting Children's Personal Data on the Internet and the Protection of Privacy, *Multimedia und Recht*, 11/2002, p. 703-709.

Nouwt, J., Kinderen, internet en privacy, *Privacy & Informatie* 2003, nr. 2, p. 59-65.

OECD Working Party on Information Security and Privacy, Privacy Online: Policy And Practical Guidance, DSTI/ICCP/REG(2002)3/FINAL, 21 January 2003.

OECD Working Party on Information Security and Privacy, Report On Compliance With, And Enforcement Of, Privacy Protection Online, DSTI/ICCP/REG(2002)5/FINAL, 12 February 2003.

Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris 1981.

Prins, J.E.J., Acht gesprekken over privacy en aanpalende belangen, in: H. Franken e.a. (red.), *Zeven essays over informatietechnologie en recht,* Den Haag: Sdu Uitgevers 2003.

Prins, J.E.J., The Propertization of Personal Data and Identities, in: *Electronic Journal of Comparative Law*, vol. 8.3 (October 2004), <http://www.ejcl.org>.

Prins, Corien, Property and Privacy: European Perspectives and the Commodification of our Identity, Work in progress, over eigendom op informatie in het kader van het ITeR onderzoek *Commodification of information, 'code' as law, and shifts in the public/private domain,* Bijdrage aan workshop 1-2 juli 2004.

Reidenberg, J.R., E-commerce and Trans-Atlantic Privacy, *Houston Law Review* 38:2001, p. 717-749.

Schreuders, E., *Data mining, de toetsing van beslisregels & privacy, Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen,* Den Haag: Sdu Uitgevers 2001. Nationaal Programma Informatietechnologie en Recht, nr. 48.

Sietsma, R., J. Verbeek, J. van den Herik, *Datamining en opsporing,* Den Haag: Sdu Uitgevers 2001. Nationaal Programma Informatietechnologie en Recht, nr. 55.

Smink, G.C.J., A.M. Hamstra en H.M.L. van Dijk, *Privacybeleving van burgers in de informatiemaatschappij,* Den Haag: Rathenau Instituut, 1999, Werkdocument 68.

Terryn, E., Gedragscodes en labels in de elektronische handel, *Computerrecht* 2003/5, p. 283-294.

Turow, Joseph, *Americans and Online Privacy: The System is Broken*, A Report from the Annenberg Public Policy Center of the University of Pennsylvania, June 2003.

Turow, Joseph, *Privacy Policies on Children's Websites: Do They Play By the Rules?,* Annenberg Public Policy Center, University of Pennsylvania, 28 maart 2001.

Ukrow, J., *Self-regulation in the media sector and European Community Law,* Saarbrücken 1999.

Vedder, A.H., Privacy en woorden die tekort schieten, in: J. Nouwt, W. Voermans (red), *Privacy in het informatietijdperk*, Den Haag: SDU 1996.

Warren, S.D. & L.D. Brandeis, The right to privacy, *Harvard Law Review*, 1980, no.5.

Westin, A.F., *Privacy and Freedom*, New York, 1967.

World Summit on the Information Society, *Declaration of Principles*,
Document WSIS-03/GENEVA/DOC/4-E (12 December 2003).

Over de auteur

Mr. dr. Sjaak Nouwt is universitair docent bij het Tilburg Institute for Law, Technology, and Society (TILT) van de Universiteit van Tilburg (UvT). Hij verricht onderzoek en verzorgt onderwijs op het terrein van recht en ICT, in het bijzonder over de bescherming van privacy en persoonsgegevens. In het verlengde daarvan besteedt hij in zijn onderzoek ook aandacht aan de bescherming en beveiliging van bedrijfsgegevens en persoonsgegevens, evenals aan vraagstukken rond zelfregulering. Hij heeft zich gespecialiseerd in privacy binnen de gezondheidszorg. Van 2003 tot 2004 nam hij deel aan het door de artsenorganisatie KNMG gecoördineerde Implementatieprogramma WGBO. In 2003 was hij tevens projectleider van een RechtenOnline project, ter stimulering van het gebruik van ICT in het juridisch onderwijs. In 2004 en 2005 leidt hij een project ter ontwikkeling van e-learningprogramma's voor juridische informatievaardigheden. Hij is voorts coördinator van een internationaal netwerkvormend privacyonderzoek *PrivacyNetwork*.

Sjaak Nouwt heeft diverse publicaties in de vorm van boeken, tijdschriftartikelen en bijdragen aan boeken en losbladige uitgaven op zijn naam staan. Hij is o.a. redactielid van het tijdschrift *Privacy & Informatie* en eindredacteur van het *Journaal Privacy Gezondheidszorg*. Daarnaast is hij hoofdredacteur van de *Internet Law Library* of *Juridische Internet Bibliotheek*.

Sjaak Nouwt studeerde Nederlands Recht in Tilburg en is sindsdien werkzaam aan de UvT. Hij promoveerde aldaar in mei 1995 op het proefschrift getiteld *Zorg voor privacy.*

In de publicatiereeks van het Nationaal Programma voor Informatietechnologie en Recht zijn verschenen:

- ITeR nr. 1: J.E.J. Prins e.a., *In het licht van de Wet persoonsregistraties: zon, maan of ster? Verslag van een sociaal-wetenschappelijke evaluatie van de WPR,* Alphen aan den Rijn: Samsom BedrijfsInformatie 1995. [ISBN 90-14-05403-3]
- ITeR nr. 2: Jan Holvast, *Persoonsgegevens of niet: dat is de vraag*. Wim van de Donk e.a., *De WPR als zon, maan of ster*. Dirk Visser, *Auteursrechtvergoedingen in Europa en de VS*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1996. [ISBN 90-14-05427-0]
- ITeR nr. 3: Anne-Marie Kemna & Astrid Tuinder, met medewerking van Hans Franken & Dries Neisingh, *Regulering van encryptie*. Theo de Roos, Gerard Schuijt & Louisa Wissink, met medewerking van Peter Mostert & Lynn van der Velden, *Smaad, laster, discriminatie en porno op het Internet*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1996. [ISBN 90-14-05455-6]
- ITeR nr. 4: Wouter Hins, *De eeuwigdurende telecom-licentie*. Steven de Leeuw, met medewerking van Thijs Drupsteen, *Graafrechten voor telecommunicatievoorzieningen*. Maartje Verberne, Nico van Eijk & Egbert Dommering, *Veilen van frequenties voor Personal Communications Services*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1996. [ISBN 90-14-05469-6]
- ITeR nr. 5: Simone van der Hof, *Overheidsinformatie in de etalage. Belangen rondom de toegang tot overheidsinformatie*. Jitske de Jong, Marcel Rietdijk & Yvette Pluijmers, *Vastgoed persoonlijk benaderd. Bescherming van persoonsgegevens binnen vastgoedregistraties*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05559-5]
- ITeR nr. 6: Annemarie Beunen, *Digitale manipulatie van beeldmateriaal: grenzen aan de grenzeloosheid*. Mars van Leent, *Overheidstoezicht op bemiddelingsorganisaties in het auteursrecht*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05567-6]
- ITeR nr. 7: Simone van der Hof, met medewerking van Andreas Mitrakas, *De juridische status van de digitale handtekening*. Sylvia Huydecoper & Rob van Esch, *Geschriften en handtekeningen: een achterhaald concept?* Erik Schut en Elke Wiersema, met medewerking van Dries Neisingh, Anne-Marie Kemna & Peter Enneking, *Betrouwbaarheid van elektronische berichten in het betalingsverkeer.* ITeR workshop-verslag 17 december 1996, *De digitale handtekening. Juridische en organisatorische aspecten*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05568-4]
- ITeR nr. 8: Robert van Kralingen, Corien Prins & Jan Grijpink, met medewerking van Jan van Arkel & Franke van der Klaauw-Koops, *Het lichaam als sleutel. Juridische beschouwingen over biometrie*. Miriam Lips & Paul Frissen, *Wiring government. Integrated public service delivery through ICT.* Heleen de Vlaam, Hans de Bruijn & Ernst ten Heuvelhof, *Interconnection disputes. Sweden, Great Britain and the United States*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05569-2]

- ITeR nr. 9: Ingrid van den Berg, Hielke Hijmans & Aernout Schmidt (red.), *Regulering van het Internet*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05570-6]
- ITeR nr. 10: Dirk Visser, *Naar een multimedia-bestendig auteursrecht*. Kamiel Koelman, *Multimedialicenties. Enkele juridische en praktische knelpunten*. Jacqueline Seignette, *Exploitatie en clearance van intellectuele eigendomsrechten in een digitale omgeving*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1998. [ISBN 90-14-05775-X]
- ITeR nr. 11: Anne-Wil Duthler, *Met recht een TTP! Een onderzoek naar juridische modellen voor een Trusted Third Party*, Deventer: Kluwer 1998. [ISBN 90-14-05776-8]
- ITeR nr. 12: Kees Stuurman & Hugo Wijnands, *Electronic commerce. Een privaatrechtelijk kader voor multilaterale EDI*. Yao-Hua Tan, Andreas Mitrakas & Walter Thoen, *A formal analysis of Incoterms for electronic commerce*. Pascal Kolkman & Robert van Kralingen, *Verschuivend vertrouwen. Methoden voor het waarborgen van betrouwbaarheid in het elektronisch rechtsverkeer*, Deventer: Kluwer 1998. [ISBN 90-14-05777-6]
- ITeR nr. 13: Maurice Schellekens, *Strafbare feiten op de elektronische snelweg*. Rik Kaspersen, André Hofman & Joop Verbeek, *Vertrouwelijkheid van e-mail*. Joop Verbeek, Cyril van der Net & Jaap Tempelman, *Netwerkzoeking in theorie en praktijk*, Deventer: Kluwer 1999. [ISBN 90-14-05778-4]
- ITeR nr. 14: Mireille van Eechoud & Jan Kabel, *Prijsbepaling voor elektronische overheidsinformatie*, Deventer: Kluwer 1998. [ISBN 90-26-83357-1]
- ITeR nr. 15: *Telecommunicatienummers en domeinnamen*. Egbert Dommering, *Het adres in cyberspace heeft geen plaats. Over adressen, telefoonnummers en domeinnamen*. Ted Clarkson e.a., *Mechanismen voor de verdeling van telecommunicatienummers*. Nico van Eijk, *Toekenning van servicenummers met alfanumerieke betekenis*. Ido Hurkmans, *Regulering van informatienummers*. Babiche Westerbrink, *De merken- en handelsnaamrechtelijke aspecten van het Domain Name System*, Deventer: Kluwer 1999. [ISBN 90-268-3426-8]
- ITeR nr. 16: Hielke Hijmans & Annemique de Kroon (red.), *Wetgeving voor de elektronische snelweg: nadere beschouwingen*, Deventer: Kluwer 1999. [ISBN 90-268-3486-1]
- ITeR nr. 17: Evert Neppelenbroek, Kees Stuurman & Hugo Wijnands, *Aansprakelijkheid voor schade aan apparatuur door mobiele telefoons*. Mark van Twist, Hans de Bruijn & Ernst ten Heuvelhof, *Verhandelbaarheid van vergunningen in de telecomsector*. Miriam Lips, Paul Frissen & Corien Prins, *Regulatory review through new media in Sweden, the UK, and the USA: convergence or divergence of regulation?* Willem Grosheide & Claire de Schepper, *De juridische status van telefoonnummers. Opmerkingen over de plaats van het regio-telefoonnummer in het Nederlandse vermogensrecht*, Deventer: Kluwer 1999. [ISBN 90-268-3475-6]
- ITeR nr. 18: Bernd van der Meulen e.a., *Vertrouwelijk gegeven. Juridische beschouwingen over de verstrekking van bedrijfsgegevens aan de overheid en het beheer daarvan door de overheid*, Deventer: Kluwer 1999. [ISBN 90-268-3474-8]
- ITeR nr. 19: Joop Verbeek e.a., *Politie en Intranet. Normering van netwerkkoppeling en grensoverschrijdend gebruik van multimediale databases op een internationaal politieel Intranet*, Deventer: Kluwer 1999. [ISBN 90-268-3476-4]

- ITeR nr. 20: Sylvia Huydecoper, *Aansprakelijkheid, intermediairs en Electronic Data Interchange*. Merijn Seelt, *Aansprakelijkheid van de softwareleverancier voor de Millenniumbug*, Deventer: Kluwer 1999. [ISBN 90-268-3538-8]
- ITeR nr. 21: Rik Kaspersen e.a., *Contracten van Internetproviders: een adequate basis voor zelfregulering?*, Deventer: Kluwer 1999. [ISBN 90-268-3553-1]
- ITeR nr. 22: H. Franken e.a., *ICT en straftoemeting: de conferentie van 23 april 1998*. A.H.J. Schmidt, *ICT en rechtvaardige strafoplegging bij zeden- en opiumzaken*, Deventer: Kluwer 1999. [ISBN 90-268-3564-7]
- ITeR nr. 23: Tomas Oudejans, *Electronic Highway of Electronic Subway? Verborgen merkinformatie op het Internet in Amerikaans perspectief*, Deventer: Kluwer 1999. [ISBN 90-268-3551-5]
- ITeR nr. 24: *Toepassing van privacyregels op elektronische berichten*. Sjaak Nouwt, *Privacyregels voor Internetberichten*. Jan Holvast, *Privacyregels voor EDI-berichten*, Deventer: Kluwer 1999. [ISBN 90-268-3598-1]
- ITeR nr. 25: Laurens Mommers, *Knowing the law. Legal information systems as a source of knowledge*, Deventer: Kluwer 1999. [ISBN 90-268-3596-5]
- ITeR nr. 26: Lodewijk Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie*, Deventer: Kluwer 1999. [ISBN 90-268-3601-5]
- ITeR nr. 27: Maartje Louise Verberne, *Verdeling van het spectrum*, Deventer: Kluwer 2000. [ISBN 90-268-3600-7]
- ITeR nr. 28: J.E.J. Prins e.a., *De universiteitsbibliotheek in het databankenrecht. Een juridisch perspectief op de vraag naar de noodzaak en wenselijkheid van een bibliotheek als informatieproducent*, Deventer: Kluwer 2000. [ISBN 90-268-3645-7]
- ITeR nr. 29: Judica I. Krikke, *Het bibliotheekprivilege in de digitale omgeving*, Deventer: Kluwer 2000. [ISBN 90-268-3644-9]
- ITeR nr. 30: Leonie Siemerink, *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het Internet*, Deventer: Kluwer 2000. [ISBN 90-268-3629-5]
- ITeR nr. 31: Bert-Jaap Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000. [ISBN 90-268-3655-4]
- ITeR nr. 32: Babette Aalberts & Simone van der Hof, *Digital Signature Blindness. Analysis of legislative approaches toward electronic authentication*, Deventer: Kluwer 2000. [ISBN 90-268-3656-2]
- ITeR nr. 33: H.S.M. Kruijer, *De exoneratieclausules in de algemene voorwaarden van de Federatie van Nederlandse ondernemingen in de Informatietechnologie (FENIT)*, Deventer: Kluwer 2000. [ISBN 90-268-3640-6]
- ITeR nr. 34: Luuk Matthijssen, *Jurisprudentiedatabanken. Een internationaal vergelijkende studie naar de publicatie van rechterlijke uitspraken met behulp van informatietechnologie*, Deventer: Kluwer 2000. [ISBN 90-268-3658-9]
- ITeR nr. 35: Joop Verbeek, Theo de Roos & Jaap van den Herik, *Interceptie van vertrouwelijke communicatie. De institutionele kansen en bedreigingen van het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9259-9]

- ITeR nr. 36: A.R. Lodder, A. Oskamp & M.J.A. Duker, *Informatietechnologische ondersteuning binnen het strafprocesrecht*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9263-7]
- ITeR nr. 37: D.W.F. Verkade, D.J.G. Visser & L.D. Bruining, *Ruimere octrooiëring van computerprogramma's: technicality of revolutie?*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9267-X]
- ITeR nr. 38: Pascal Kolkman, Robert van Kralingen & Sjaak Nouwt, *Privacy in bits en bytes. Privacyaspecten van electronic monitoring in netwerkomgevingen*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9268-8]
- ITeR nr. 39: Bert-Jaap Koops e.a., met medewerking van Tomas Oudejans, *Overheden over internationalisering en ICT-recht. De standpunten van Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-5409-270-X]
- ITeR nr. 40: Mirjam Lips, Simone van der Hof & Kees Schalken, *Multiformity in information provision in a new media age. Challenged responsibilities for governments in Europe*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-5409-271-8]
- ITeR nr. 41: Tina van der Linden-Smith, *Een duidelijk geval: geautomatiseerde afhandeling*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-5409-278-5]
- ITeR nr. 42: Jan Holvast, *Het gebruik van persoonlijkheidsprofielen in de publieke sector*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09260-4]
- ITeR nr. 43: Arno R. Lodder, Anja Oskamp & Aernout H.J. Schmidt (eds.), *IT support of the Judiciary in Europe*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09284-1]
- ITeR nr. 44: Clara Sander, *Consumentenbescherming bij transacties op afstand*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09285-X]
- ITeR nr. 45: Bert-Jaap Koops & Anton Vedder, met bijdragen van Jos Mensink & Stephan Raaijmakers, *Opsporing versus privacy: de beleving van burgers*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09343-0]
- ITeR nr. 46: Nirmala Sitompoel e.a., *(Zelf)regulering van nummers en domeinnamen*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09348-1]
- ITeR nr. 47: Tom van Dijk, *Elektronische aanbesteding*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09349-X]
- ITeR nr. 48: Eric Schreuders, *Data mining, de toetsing van beslisregels & privacy. Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09350-3]
- ITeR nr. 49: Christiaan Alberdingk Thijm, *Privacy vs. auteursrecht in een digitale omgeving*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09451-8]
- ITeR nr. 50: Hans de Bruijn e.a., *Samenloop bij toezicht*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09461-5]
- ITeR nr. 51: Corrette Ploem, *Wetenschapsbeoefening en belemmerende privacywetgeving: de wetgever in balans?*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09471-2]
- ITeR nr. 52: Edward Peeman, *Electronic Commerce en de Europese omzetbelasting*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09472-0]

- ITeR nr. 53: Justin Broeders e.a., *Vergunningen op Internet: meer dan gokken op een handhaafbaar stelsel*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09501-8]
- ITeR nr. 54: Babette Aalberts, *Beelddatabanken: stilstaand beeld in beweging?*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09502-6]
- ITeR nr. 55: Ruben Sietsma, Joop Verbeek & Jaap van den Herik, *Datamining en opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: strafprocesrecht versus recht op privacy*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09503-4]
- ITeR nr. 56: Georges van den Eshof e.a., *Opsporing van verborgen informatie. Technische mogelijkheden en juridische beperkingen*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09504-2]
- ITeR nr. 57: Kamiel Koelman, *Auteursrecht en technische voorzieningen. Juridische en rechtseconomische aspecten van de bescherming van technische voorzieningen*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-12-09505-0]
- ITeR nr. 58: Alexander Tsoutsanis, *Domeinnaamgeschillen: inbreuk, onrechtmatige daad of kwade trouw? Stand van zaken-onderzoek voor een geschillenregeling in het .nl-domein*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-12-09506-9]
- ITeR nr. 59: Jelle Arts, *Toegang tot publiek gefinancierde data*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-5409-373-0]
- ITeR nr. 60: Hein Dries, Serge Gijrath & Paul Knol, *Openbaarheid van netwerken en diensten in de Telecommunicatiewet*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-5409-374-9]
- ITeR nr. 61: Kristianne Horrevorts & Rob van Esch, *De rol van zelfregulering bij de juridische erkenning van elektronische documenten en elektronische handtekeningen*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-335-8]
- ITeR nr. 62: Marjolijn van Gool & Rob van Esch, *Betalingen via Internet en faillissement*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-382-X]
- ITeR nr. 63: Hans Franken e.a., *Zeven essays over informatietechnologie en recht*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-391-9]
- ITeR nr. 64: Bart Schermer, *Opsporing vs. privacy in peer-to-peer netwerken*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-390-0]
- ITeR nr. 65: Harry Bouwman e.a., *Interconnectie: het vaste telefoonnet, het mobiele net en internet*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-393-4]
- ITeR nr. 66: Anne-Wil Duthler, *Digitale identiteit en pseudonieme digitale certificaten*, Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-395-1]
- ITeR nr. 67: Sophie van Loon, *Databankenrecht en mededinging, ontwikkelingen vanaf 1996 en evaluatie*, Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-407-9]
- ITeR nr. 68: Arno R. Lodder e.a., *Spam, spammer, …, analyse van het recht en de techniek rond elektronische ongevraagde commerciële communicatie, in het bijzonder via email*, Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-425-7]
- ITeR nr. 69: Joop Verbeek, *Politie en de Nieuwe Internationale Informatiemarkt, Grensregionale politiële gegevensuitwisseling en digitale expertise*, Den Haag, Sdu Uitgevers 2004. [ISBN 90 5409 424 9]

- ITeR nr. 70: Bert-Jaap Koops, Hanneke van Schooten en Merel Prinsen, *Recht naar binnen kijken: een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag, Sdu Uitgevers 2004. [ISBN 90 5409 430 3]
- ITeR nr. 71: Colette Cuijpers, *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn,* Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-435-4]
- ITeR nr. 72: Marga Groothuis, *Beschikken en digitaliseren. Over normering van de elektronische overheid*, Den Haag, Sdu Uitgevers 2004. [ISBN 90 5409 448 6]
- ITeR nr. 73: Sjaak Nouwt, *Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet*, Den Haag, Sdu Uitgevers 2005. [ISBN 90-1210-913-2]