Privacy en elektronische handel

van Esch, R.E.; Prins, J.E.J.

Published in:
Recht en elektronische handel

Publication date:
2002

16. Privacy en Elektronische Handel[1]

J.M.A. Berkvens, J.E.J. Prins[2]

16.1. INLEIDING

Elektronische handel en de verwerking van persoonsgegevens lijken onlosmakelijk met elkaar verbonden. Er is immers vrijwel geen e-commerce toepassing voorstelbaar waarbij geen persoonsgegevens worden verwerkt. De persoonsgegevens kunnen bewust worden vrijgegeven (er worden bijvoorbeeld NAW-gegevens verstrekt om een geplaatste bestelling af te handelen) of onbewust (in de vorm van bijvoorbeeld een IP-adres). Alhoewel het gebruik van persoonsgegevens bij Business-to-Consumer (B2C) intensiever is dan bij Business-to-Business (B2B) handel, worden bij de laatste vorm van elektronische handel veelal ook persoonsgegevens verwerkt. Gedacht kan worden aan betalingstrajecten en het uitwisselen van bedrijfsinformatie op het gebied van belastingen, sociale zekerheid en statistieken. In zijn algemeen kan worden gesteld dat gebruikers van telecommunicatienetwerken en dus gebruikers van e-commerce toepassingen een digitaal spoor achterlaten. Dit spoor stelt anderen in staat om grote hoeveelheden persoonsgegevens over de betreffende persoon te verzamelen.

Bij de discussie omtrent het succes van elektronische handel, duikt iedere keer het argument op dat er nog onvoldoende vertrouwen bestaat bij met name consumenten in dit alternatief voor de traditionele wijze van zakendoen. Veelal wordt dan betoogd dat elektronische handel nog niet tot volle wasdom is gekomen omdat het ontbreekt aan onder meer een adequate privacybescherming bij deze toepassing.[3]

Inmiddels is en wordt op nationaal en internationaal niveau via regulering getracht het niveau van privacybescherming op het Internet en meer specifiek elektronische handel op te schroeven. Zo heeft de OECD de aanbeveling betreffende *Guidelines for Consumer Protection in the Context of Electronic Commerce* vastgesteld.[4] Hierin wordt de lidstaten aanbevolen de nodige maatregelen te nemen om de bepalingen van de betreffende richtlijnen te implementeren. In par. VII van de richtlijnen is een bepaling opgenomen over de bescherming van persoonsgegevens. Deze bepaling luidt als volgt: 'Business-to-consumer electronic commerce should be conducted in accordance with the recognised privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980), and taking into account the OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998) to provide appropriate and effective protection for consumers'.

Ook op Europees niveau zijn maatregelen getroffen. Alhoewel de Richtlijn elektronische handel[5] niet van toepassing is op kwesties in verband met diensten van de informatiemaatschappij die onder de privacyrichtlijnen (Richtlijn 95/46/EG en Richtlijn 97/66/EG) vallen[6], hebben enkele bepalingen uit de Richtlijn elektronische handel wel degelijk een effect op de omgang met persoonsgegevens. Genoemd kan bijvoorbeeld worden de bepaling over de te verstrekken informatie alsmede de bepaling inzake commerciële communicatie (reclame). Op eenzelfde wijze is de Richtlijn Verkoop-op-afstand van

---

[1] Met dank aan Rob van Esch voor zijn bijdrage aan het opstellen van dit hoofdstuk.

[2] Jan Berkvens is adjunctdirecteur Directoraat juridische en fiscale zaken, Rabobank Nederland en hoogleraar aan de Katholieke Universiteit Nijmegen. Corien Prins is hoogleraar recht en informatisering bij het Centrum voor recht, bestuur en informatisering van de Katholieke Universiteit Brabant.

[3] Als andere factoren worden genoemd de weinig eenvoudige en veilige betaalmiddelen, het feit dat de afwikkeling van de transacties te wensen overlaat, en het gebrek aan transparantie waardoor de consument moeilijk zijn recht kan halen.

[4] *Recommendation of the OECD Council concerning guidelines for consumer protection in the context of electronic commerce*, Parijs: OECD 1999.

[5] 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, *PbEG* 2000 L 178/1.

[6] Artikel 1, lid 5, Richtlijn elektronische handel.

belang voor de omgang met persoonsgegevens.[7] Een richtlijn die wel concrete bepalingen voor de omgang met persoonsgegevens bevat is de Richtlijn Elektronische Handtekeningen.[8] Op deze bepalingen zal later in dit hoofdstuk nader worden ingegaan.

Behalve de wetgevingsmaatregelen, trachten diverse nationale en internationale organisaties en instellingen ook via zelfregulering tot een betere privacybescherming bij elektronische handel te komen. Bekend zijn de gedragscodes en de webkeurmerken. Ook deze instrumenten zullen in dit hoofdstuk nader aan de orde komen.

Tenslotte is er natuurlijk de toepasselijke Nederlandse wet- en regelgeving. Zo staan in hoofdstuk 11 van de Telecommunicatiewet specifieke regels inzake de omgang met persoonsgegevens. Daarnaast is er de algemene privacywet, de Wet bescherming persoonsgegevens, die sedert 1 september 2001 van kracht is. Alhoewel de diverse bepalingen van deze wet integraal van toepassing zijn op elektronische handel, roept de toepassing in concrete situaties soms toch weer nadere vragen op. We vangen dit hoofdstuk aan met een bespreking van een aantal van dergelijke vragen vanuit het perspectief van elektronische handel.

16.2. DE WBP EN ELEKTRONISCHE HANDEL

16.2.1 Persoonsgegeven

In art. 1 sub *a* Wbp treffen we de definitie van een persoonsgegeven aan: het gaat om elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Wat is de betekenis van deze definitie bij toepassingen van elektronische handel?

Bij elektronische handel kan gebruik worden gemaakt van diverse applicaties voor de uitwisseling van (persoons)gegevens, bij B2C zal met name de e-mail faciliteit populair zijn. Deze en andere applicaties worden door een scala aan dienstaanbieders aangeboden, waarbij wat betreft e-mail de aanbieder vaak een e-mail server heeft waarop zich de mailboxen van zijn (al dan niet betalende) abonnees bevinden. Hiernaast bestaat ook zogenaamde webmail. Dit is een e-mail dienst die vanuit iedere willekeurige plek op het Internet kan worden benaderd. Men hoeft dus geen toegang te krijgen via de eigen Internet dienstverlener, maar kan bijvoorbeeld ook via de Internettoegang van de werkplek zo'n dienst bereiken.

Een ieder die gebruik wil maken van e-mail heeft daartoe een e-mailadres nodig. Consumenten, dat wil zeggen privé gebruikers van e-mail, kunnen veelal zelf hun e-mailadres kiezen, hetgeen betekent dat ze ook een andere dan hun werkelijke naam kunnen gebruiken (pseudoniem). Dit betekent dat dit e-mailadres niet zonder meer herleidbaar zal zijn tot een geïdentificeerde of identificeerbare natuurlijke persoon. De concrete omstandigheden van het geval zullen bepalen of het e-mailadres kan worden aangemerkt als een persoonsgegeven in de zin van de Wbp. Maar ook indien het e-mailadres de naam van de houder bevat, is het niet altijd mogelijk dat de leverancier zonder onevenredige inspanning de identiteit van de afnemer kan achterhalen. Dat geldt bijvoorbeeld als hij de gegevens van de betreffende persoon niet in een databank beschikbaar heeft. Vooralsnog is er geen algemene elektronische internetadreslijst beschikbaar, waarin de ontvanger van een e-mail de identificerende gegevens van de afzender kan opzoeken. Wel bestaan adreslijsten, waar personen of bedrijven vrijwillig hun e-mailadres met identificerende gegevens kunnen registreren. Daarbij dient echter te worden opgemerkt dat de instellingen die dergelijke vrijwillige adreslijsten onderhouden, de juistheid van de aangeboden gegevens niet verifiëren. Het voorgaande betekent dat de leverancier zich soms veel moeite zal moeten getroosten om de afnemer te identificeren. De Wbp geeft geen indicatie over de mate van inspanning die men zich moet getroosten. In de Memorie van Toelichting wordt

---

[7] Richtlijn 97/7/EG, PbEG 1977 L 144/19. De richtlijn is omgezet naar Nederlands recht voornamelijk door aanpassing van enkele artikelen van Boek 7 BW. Wet van 21 december 2000, Stb, 617, 2000. Deze wet is op 1 februari 2001 in werking getreden.

[8] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *PbEG* 2000 L 13/12. Bij de Tweede Kamer werd in mei 2001 een wetsvoorstel ter implementatie van de richtlijn ingediend (TK 2000-2001, 27743, nrs. 1-3). Zie ook hoofdstuk 18 van dit boek.

opgemerkt dat er sprake is van onevenredige inspanning indien bijvoorbeeld identificatie van de persoon door de computer vele dagen in beslag zou nemen.[9] In dat geval zou men tot de conclusie kunnen komen dat de gegevens in het e-mailbericht geen persoonsgegevens zijn in de zin van de Wbp, tenzij het bericht zelf gegevens bevat aan de hand waarvan de persoon van de afnemer kan worden geïdentificeerd.[10] Bij een zakelijk e-mailadres zal veelal wel sprake zijn van een persoonsgegeven omdat in dit adres meestal de naam van de werknemer en de naam van het bedrijf of de organisatie is verwerkt.
Behalve via een e-mailadres kan de leverancier ook op andere wijze met persoonsgegevens van (potentiële) afnemers te maken krijgen. Indien een afnemer een website van een leverancier op internet bezoekt, zal de computer van de afnemer aan de website server zijn IP-adres kenbaar maken. Dit gegeven kan door de website server tezamen met de gegevens over de activiteiten van de afnemer (bijvoorbeeld diens specifieke zoekgedrag) worden opgeslagen. In principe zegt het IP-adres niets omtrent de persoon die website heeft bezocht. Zeker als de afnemer gebruik maakt van een dynamisch IP-adres zal niet snel sprake zijn van een persoonsgegeven. Toch zijn er ook situaties waarin het IP-adres wel aangemerkt wordt als persoonsgegeven in de zin van de Wbp. Dit is het geval indien namelijk via het IP-adres zonder onevenredige inspanningen de identiteit van de afnemer kan worden achterhaald. Dit is bijvoorbeeld het geval indien de afnemer met een vast IP-adres, zoals internetgebruikers met kabelaansluiting, zich bij het eerste bezoek aan de website moest aanmelden en daarbij identificerende gegevens heeft verstrekt. Aan de hand van deze gegevens kan in samenhang met het IP-adres bij een volgend bezoek de identiteit van de afnemer worden vastgesteld. In dit verband moet ook worden gewezen op de praktijk van het gebruik van een zogenaamd 'cookie', een klein tekstbestand dat op de harde schijf van de bezoeker wordt geplaatst. Bij hernieuwd bezoek aan de webpagina, gaat de informatie uit dit cookie mee. Deze informatie bevat meestal een uniek nummer dat de computer van de gebruiker identificeert. Het kan ook het password bevatten waarmee de gebruiker toegang krijgt tot die bepaalde webpagina. Door de informatie uit een cookie uit te lezen, kan de aanbieder vaststellen of het om een terugkerende bezoeker gaat. Daarmee verkrijgt hij op zich geen informatie waarmee de identiteit van de bezoeker kan worden vastgesteld. Daarvoor is aanvullende informatie nodig. Indien de aanbieder een contractuele relatie met de afnemer heeft kan deze aanvullende, identificerende informatie, beschikbaar komen via het koppelen van de gegevens in IP-adresbestanden met bestanden, waarin een combinatie van IP-adressen en identificerende gegevens zijn opgenomen. Indien een contractuele relatie ontbreekt kan de aanbieder aan identificerende gegevens komen door de bezoeker informatie te laten geven, bijvoorbeeld door het invullen van een enquête.

Bij elektronische handel wordt gebruik gemaakt van telecommunicatienetwerken. In dit licht is een belangrijke vraag in hoeverre de gegevens die nodig zijn voor het tot stand brengen van de elektronische communicatie, de zogenaamde verkeersgegevens, ook als persoonsgegevens kunnen worden gekwalificeerd. Met het oog op toepassingen van e-commerce via mobiele communicatienetwerken gaat deze vraag steeds meer spelen. Verkeersgegevens betreft namelijk gegevens als het oproepende telefoonnummer (aansluitnummer), het opgeroepen telefoonnummer, datum, duur, en tijdstip, oproeppoging, cel-ID in geval van GSM (locatiegegeven). Mede naar aanleiding van de komst van nieuwe faciliteiten zoals een specificatie van de telefoonrekening, marketinginstrumenten voor de verkoop van specifieke telecom- en Internetdiensten en het opsporen van fraude, worden dergelijke gegevens momenteel vaak opgeslagen en gedurende een bepaalde periode bewaard. Juist vanwege het feit dat de verkeersgegevens (die in eerste instantie slechts technische gegevens zijn) nu worden opgeslagen om voor bepaalde doeleinden te worden verwerkt, kunnen het in juridische zin ook persoonsgegevens zijn. Verwacht mag worden dat met de komst van de nieuwe Richtlijn privacy bij elektronische communicatie de mogelijkheden tot het bewaren van verkeersgegevens worden verruimd. Op voorwaarde dat daartoe toestemming is verkregen van de

[9] *Kamerstukken II* 1998/99, 25 892, nr. 13, p. 2.
[10] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 45-48. Vergelijk K. Koelman & L. Bygrave*, Privacy, Data Protection and Copyright. Their Interaction in the Context of Electronic Copyright Management Systems*, Amsterdam: Institute for Information Law 1998, p. 14. Anders M.E. Heinemann, 'Over IP-adressen en de WBP. Grenzen aan privacybescherming op Internet', *Privacy & Informatie* 1999-4, p. 149-150

gebruiker van de dienst, mogen in het geval van reclame voor elektronische communicatiediensten dan wel dat zogenaamde toegevoegdewaardediensten worden verleend de verkeersgegevens worden verwerkt (art. 6 lid 3).[11] Een zelfde regeling wordt getroffen voor locatiegegevens (art. 9 lid 1).

Cruciaal bij de vaststelling of verkeersgegevens ook als persoonsgegevens kunnen worden aangemerkt, is of het gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon zijn. De Memorie van Toelichting zegt hierover dat gegevens van een netwerkaanbieder over het gebruik van het netwerk via aansluitpunten teneinde het goed functioneren van het netwerk te waarborgen, geen persoonsgegevens zijn zolang elke reële mogelijkheid is uitgesloten dat die gegevens worden gebezigd om het gebruik van het netwerk door individuele personen in ogenschouw te nemen. Vervolgens wordt echter ook opgemerkt dat indien het daarentegen mogelijk is de gegevens te gebruiken om bij voorbeeld fraude mee op te sporen, deze gegevens aangemerkt moeten worden als persoonsgegevens. Daarbij is niet relevant of het de bedoeling is de gegevens voor dat doel te gebruiken. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt. Kijkend naar de voornoemde overwegingen voor telecommunicatieaanbieders en Internetdienstverleners, zoals aanbieders van e-commerce, om verkeersgegevens op te slaan, kan worden vastgesteld dat deze gegevens zijn aan te merken als persoonsgegevens onder de Wbp.

Ook aan het vereiste dat het moet gaan om gegevens betreffende een geïdentificeerde of identificeerbare persoon, zal veelal zijn voldaan. Immers, de verkeersgegevens kunnen veelal worden gecombineerd met andere (voor het in rekening brengen van abonnement- en gesprekskosten) beschikbare gegevens over naam-, adres-, en woonplaats. Dit is niet het geval bij pre-paid abonnementen voor mobiele telefonie. Immers, de aanbieder van deze diensten heeft geen naam-, adres- en woonplaatsgegevens nodig om de rekening te versturen. De met deze dienst gemoeide verkeersgegevens, waaronder het oproepende telefoonnummer en opgeroepen telefoonnummer, zullen daarom niet, of in ieder geval niet eenvoudig, in verband te brengen zijn met een geïdentificeerde of identificeerbare gebruiker. Zodra echter deze aanbieder nadere adresgegevens van de gebruiker vraagt (bijvoorbeeld om deze gebruiker te benaderen voor marketingdoeleinden) kan wel weer worden gesproken van persoonsgegevens in de zin van de Wbp.[12]

Van belang voor de vraag of bij elektronische handel gebruik wordt gemaakt van een persoonsgegeven is ook het eventueel gebruik van een digitale handtekening. Een dergelijke handtekening wordt met behulp van asymmetrische encryptie berekend over de hashwaarde van een elektronisch bericht. De afzender versleutelt de hashwaarde met behulp van zijn geheime private sleutel en een algoritme en de ontvanger ontcijfert de hashwaarde met behulp van de bijbehorende openbare publieke sleutel van de afzender en hetzelfde algoritme. Om de ontvanger enige mate van zekerheid te verschaffen omtrent de identiteit van de houder van de publieke sleutel, kan gebruik worden gemaakt van een elektronisch certificaat dat is uitgegeven door een Certificaataanbieder, ook vaak aangeduid met Trusted Third Party (TTP). In dat certificaat verklaart de CA dat de publieke sleutel toebehoort aan een bepaalde persoon of instelling. Het certificaat wordt digitaal ondertekend door de CA. Het certificaat bevat meestal direct identificerende gegevens van de houder van de publieke sleutel, zoals zijn naam.[13] Certificaten kunnen echter ook zonder deze gegevens worden uitgegeven: er bestaan niet alleen identiteitscertificaten, maar ook anonieme certificaten en pseudonieme certificaten. Alhoewel anonieme certificaten technisch mogelijk zijn, zal het (mede in het licht van de regeling inzake de aansprakelijkheid van certificatiedienstverleners) de voorkeur hebben dat het certificaat tot een bepaalde persoon is te herleiden. Dit betekent echter niet dat het uit te geven certificaat daarmee ook direct een identiteitscertificaat dient te zijn, kortom dat het de identiteitsgegevens van de certificaathouder vermeldt. Op grond van artikel 8 Richtlijn elektronische handtekeningen mogen de lidstaten niet verhinderen dat certificatiedienstverleners op het certificaat een pseudoniem vermelden

---

[11] Europese Richtlijn betreffende het verwerken van persoonsgegevens en het beschermen van privacy in de elektronische communicatiesector, COM (2000) 385, 12 juli 2000, *Pb*. C365 E, 19 december 2000. In januari 2002 werd de ontwerp-tekst zoals goedgekeurd door de ministerraad gepubliceerd.

[12] In dit verband kan ook worden gewezen op de discussie over het gebruik van persoonsgegevens door aanbieders van gratis Internetdiensten. Zie hierover: W. Diephuis, 'Hoe gratis is gratis Internet', Privacy & Informatie 2000/6, p. 258-265.

[13] Zie voor meer details, hoofdstuk 18 in dit boek.

in plaats van de werkelijke naam van de ondertekenaar. Ook in de situaties dat gebruik wordt gemaakt van een identificerend certificaat, zijn er zeker ook argumenten aan te voeren om te betwijfelen of de gegevens in het bericht, dat digitaal is ondertekend door de afzender, persoonsgegevens zijn in de zin van de Wbp. Hierbij speelt het probleem dat de ontvanger nimmer met zekerheid weet of de geheime private sleutel is gebruikt door de houder zelf of wellicht door een (onbevoegde) derde.
Desalniettemin ga wij ervan uit dat ondanks het ontbreken van zekerheid omtrent de identiteit van de gebruiker van de digitale handtekening, in de meeste gevallen sprake zal zijn van persoonsgegevens in de zin van de Wbp. Een uitzondering op dit beginsel kan zich bijvoorbeeld voordoen indien het certificaat door de TTP is geplaatst op een zwarte lijst van certificaten waarvan de private sleutel in handen is gekomen van een onbevoegde.
Uit het bovenstaande kan worden geconcludeerd dat bij het gebruik van de diverse technische toepassingen ter uitvoering van elektronische handel persoonsgegevens in de zin van de Wbp worden verzameld. Voor de personen die hun gegevens bewust dan wel onbewust bij aanbieders achterlaten ontstaat vervolgens het gevoel geen greep meer te hebben op het gebruik dat vervolgens van de gegevens wordt gemaakt. Om deze reden wordt er wel voor gepleit om gebruikers de mogelijkheid te bieden om anoniem of met behulp van een pseudoniem van het netwerk gebruik te maken. Technologieën die dit mogelijk maken, worden ook wel Privacy-enhancing technologies (PET's) genoemd.[14] Inmiddels is wordt ook op het instrument van de Privacy Enhancing Mediary[15] gewezen en zelfs gewerkt aan de ontwikkeling van een software agent die gebaseerd is op het PET-concept.[16]
Voor wat betreft elektronische handel kan een aantal concrete toepassingen van anonimisering worden genoemd. Allereerst is dat de mogelijkheid om met behulp van een zogenaamde remailer e-mailberichten anoniem te sturen naar de geadresseerde.[17] De afzender stuurt het bericht naar de instelling die de remailer exploiteert. Deze stuurt het betreffende bericht zonder de identificerende gegevens van de afzender naar de geadresseerde. In dergelijke gevallen is de afzender in beginsel niet identificeerbaar door de geadresseerde, tenzij zijn identiteit uit het bericht zelf kan worden afgeleid. Eenzelfde resultaat kan worden bereikt met een zogenaamde anonimiserende server met behulp waarvan anoniem gebruik kan worden gemaakt van internet bijvoorbeeld voor het bezoeken van websites of het verrichten van transacties. Ook kan worden genoemd de mogelijkheid van anonieme toegang tot internet. Dit kan bijvoorbeeld worden verwezenlijkt doordat een internetgebruiker een chipkaart koopt met een bepaald internettegoed, waardoor hij het recht verkrijgt om voor het bedrag van het tegoed zich toegang te verschaffen tot internet. Er zal dan in de meeste gevallen geen sprake zijn van persoonsgegevens in de zin van de Wbp.
Wat de anonieme betaling via internet van afgenomen goederen of diensten betreft, kan worden gedacht aan elektronisch geld als elektronische munten of elektronische bankbiljetten. Dit zijn bestanden uitgegeven door een bank of een andere uitgevende instelling[18] die een bepaalde waarde vertegenwoordigen.[19] De verkrijger krijgt tegen betaling van een uitgevende instelling een of meer bestanden met een zelfde waarde als het bedrag dat hij heeft afgedragen. Dit bestand zet hij op de

---

[14] Zie over anonimiteit en pseudoniemen in het algemeen J.E.J. Prins, "What's in a name. De juridische status van anonimiteit", *Privacy & Informatie*, no. 4 2000, pp 153-157.. Zie over PET: H. van Rossum e.a., *Privacy-enhancing Technologies. The path to anonymity. Volume I en II*, Rijswijk: Registratiekamer 1995. Het College Bescherming Persoonsgegevens geeft in de brochure 'Mag het een bitje minder zijn?' van april 2001 een overzicht van de stand van zaken in Nederland met betrekking tot PET. Zie: <www.cbpweb.nl>.
[15] H.J.M. Gardeniers, 'Privacy Enhancing Mediaries. Nieuwe mogelijkheden voor privacybescherming?', Privacy & Informatie, 2001/1, p. 17-19.
[16] Zie: <http://pet-pisa.openspace.nl/pisa_org/pisa/index.html>
[17] Diverse toepassingen worden ook genoemd in Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Recommendation 3/97. Anonymity on the Internet*, Europese Commissie, XV D/5022/97 final, 1997.
[18] Zie Richtlijn 2000/46/EG van het Europees Parlement en de Raad van 18 september 2000 betreffende de toegang tot, de uitoefening van en het bedrijfseconomisch toezicht op de werkzaamheden van instellingen voor elektronisch geld, *PbEG* 2000 L 275/39. Deze richtlijn bevat geen bepalingen die betrekking hebben op de verplichtingen van de instellingen voor elektronisch geld ten aanzien van de bescherming van persoonsgegevens.
[19] Meer in detail: R.E. van Esch, *Giraal betalingsverkeer/elektronisch betalingsverkeer*, Deventer: Kluwer 2001, p. 161.

harde schijf van zijn computer. Zodra hij een betaling moet verrichten op internet, zendt hij elektronische munten en bankbiljetten met een gelijke waarde als zijn geldschuld naar de schuldeiser. De elektronische munten en bankbiljetten zijn anoniem, zodat de schuldeiser zelf, die de munten en bankbiljetten ter voldoening van een geldverbintenis ontvangt, in principe de identiteit van zijn wederpartij niet kan afleiden uit de betaling. Hiermee wordt dezelfde situatie gecreëerd als in het geval dat iemand in een winkel anoniem een product betaalt met fysieke munten en bankbiljetten. Zo publiceerde het Canadese softwarebedrijf *Zero-Knowledge* begin 2000 een plan voor webbetalingen waarbij het onmogelijk is de identiteit van de betalende persoon te achterhalen. Gebruikers behoeven in dit geval bij betaling met digitaal geld op het Internet niet langer diverse persoonsgegevens aan te leveren, maar krijgen een certificaat waarop bijvoorbeeld hun leeftijd staat, vergezeld van een pseudoniem. Te denken valt ook aan toepassingen waarbij een gebruiker – bijvoorbeeld in een Internetcafé of een openbare bibliotheek - een bepaalde on-line tijd heeft gekocht en daarbij anoniem een e-mail adres heeft gekregen.
Natuurlijk is anonimiteit niet altijd een haalbare kaart. Zeker in de gevallen dat na een elektronische bestelling van fysieke goederen deze op een bepaalde plaats afgeleverd moeten worden zal de leverancier toch de naam en het adres van de koper dienen te kennen om de zaak bij de koper te kunnen afleveren. Toch zijn er ook faciliteiten waarbij dit probleem wordt opgelost. Eventuele fysieke goederen kunnen anoniem worden opgehaald bij een (variant van de) 7-11 shop, waarbij verificatie van de bevoegdheid tot afhalen plaatsvindt middels een code op de chipkaart waarmee de on-line betaling plaatsvond.[20] Men blijft anoniem, en krijgt de gekochte goederen mee als men de correcte chipkaart met bijbehorende code blijkt te bezitten.
Tenslotte moet worden opgemerkt dat de toepassingen van anonieme transacties in de praktijk zeker niet altijd volstrekt anoniem zijn. Vele van de momenteel in omloop zijnde technieken om anonimiteit te bewerkstelligen werken op basis van het principe dat de in beginsel anonieme berichten onder omstandigheden toch tot de betrokken persoon kunnen worden herleid. In feite is er dus geen sprake van echte anonimiteit. Voorbeelden hiervan zijn de chipknip en andere virtuele betaalmiddelen. Veelal is slechts sprake van pseudo-anonimiteit. De uitgever van virtuele betaalmiddelen bijvoorbeeld zal waarschijnlijk in zijn administratie vastleggen aan wie hij welke munten en bankbiljetten in welke hoeveelheid heeft uitgegeven, zodat hij bij fraude de zaak kan reconstrueren of bij een geschil met de klant omtrent de debitering van zijn rekening in verband met de uitgifte van de betreffende betaalmiddelen dit kan bewijzen. Indien de betreffende betaalmiddelen na overdracht door de oorspronkelijke verkrijger aan de schuldeiser door laatstbedoelde niet meer kunnen worden hergebruikt voor het vereffenen van geldschulden, zou de uitgever aan de hand van de hem beschikbare gegevens kunnen vaststellen welke transacties zijn klant met de betreffende betaalmiddelen heeft verricht.[21]

16.2.2. Verwerking
De Wet bescherming persoonsgegevens hanteert een ander aanknopingspunt dan de voormalige Wpr en geldt nu ten aanzien van *verwerkingen* van persoonsgegevens ongeacht of deze gegevens in een persoonsregistratie voorkomen. Daarbij is ook de voorwaarde dat het moet gaan om gegevens van meerdere personen (een voorwaarde van de Wpr) komen te vervallen. Met het aanknopingspunt van registratie lag onder de Wpr het accent op gebruiks- en verstrekkingshandelingen. Door het aanknopingspunt voor bescherming nu te verleggen naar de verwerking van persoonsgegevens, geldt de Wbp eveneens voor alle technische verwerkingshandelingen. De wet heeft daardoor een aanzienlijk groter bereik gekregen.

Voor ons hoofdstuk is nu relevant welke verwerkingshandelingen met betrekking tot elektronische handel onder het regime van de wet vallen. Allereerst is daarbij relevant dat het begrip verwerking een zeer ruime strekking heeft. Artikel 1 onder b Wbp definieert het begrip als volgt: “elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van

[20] In Japan kunnen bij dergelijke 7-11 shops reeds anoniem goederen worden opgehaald.
[21] Zie Prins, a.w. 2000. Zie ook de webpagina *www.privacy.org/pi/activities/mondex*, waarop wordt ingegaan op de anonimiteit van door Mondex uitgegeven digitale cash.

terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens". Aldus omvat het begrip iedere mogelijke technische verwerkingshandeling of gebruikshandeling met betrekking tot een persoonsgegeven. Dat betekent dat iedere handeling vanaf de verzameling en opslag tot de verwijdering en vernietiging van een persoonsgegeven als een verwerkingshandeling dient te worden opgevat[22]. Dus valt het surfen over Internet en het daarbij bezoeken van sites waarop persoonsgegevens te vinden zijn of het met een zoekmachine opsporen van een Amerikaans emailadres geldt als verwerking. Te denken valt ook aan de leverancier die gegevens bewaart omtrent de personen die bij zijn virtuele winkel een product of een dienst hebben afgenomen, en deze gegevens gebruikt voor direct marketing-doeleinden. Of de TTP die een bestand met gegevens omtrent personen waaraan een certificaat is uitgegeven, raadpleegbaar maakt voor derden, zoals leveranciers van producten of diensten. Of de internetprovider die ten behoeve van abonnees e-mails met persoonsgegevens, zoals elektronische orderbevestigingen, in de elektronische postbussen van de abonnees opslaat.

Bij de inventarisatie van verwerkingshandelingen moet men zich zeker niet laten leiden door de vraag of desbetreffende verwerkingshandeling relevant is voor de bescherming van iemands persoonlijke levenssfeer. De mogelijke relevantie van een verwerking in de context van de bescherming van de persoonlijke levenssfeer doet namelijk weinig ter zake. Ook technische verwerkingshandelingen betreffende persoonsgegevens die geen persoonsgerichte context hebben vallen binnen het bereik van de Wbp.[23] Wel is van belang dat degene die de verwerkingshandeling voor zijn rekening neemt enige feitelijke macht over de persoonsgegevens kan uitoefenen (niet relevant is of deze invloed daadwerkelijk wordt uitgeoefend). Van feitelijke macht zal daarom al snel sprake zijn.[24] Voor wat betreft de implicaties bij elektronische handel citeren we ter illustratie citeren uit de tekst van de Memorie van Toelichting bij art. 1 Wbp: 'Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, verwerkt daarmee geen persoonsgegevens. Wanneer echter bijvoorbeeld een Internet service provider de mogelijkheid heeft het verspreiden van onrechtmatige berichten tegen te gaan, is er wel sprake van mogelijke invloed en daarmee van gegevensverwerking en is daarom de wet volledig van toepassing'.

Het bovenstaande heeft alles te maken met de vraag of uitsluitend sprake is van een transmissie van persoonsgegevens. Blijkens de Memorie van Toelichting dient enkelvoudige transmissie van persoonsgegevens niet als een verwerking in de zin van de Wbp te worden aangemerkt. Dat wordt evenwel anders indien de doorvoerende instantie tijdens het transport enige praktische vorm van zeggenschap over de gegevens krijgt. Vanaf dat moment is er sprake van verantwoordelijkheid. Feitelijke macht kan overigens ook bestaan uit de mogelijkheid om verspreiding van de gegevens te voorkomen. Zo zal de access provider persoonsgegevens die door een abonnee worden verspreid, verwerken indien hij de mogelijkheid heeft om deze verspreiding te voorkomen. Denk bijvoorbeeld aan het geval dat de access provider zelf een bulletin board exploiteert, waarop door derden goederen en diensten te koop kunnen worden aangeboden, en hij controle uitoefent op de inhoud van de communicaties. Bij dit alles dient echter te worden aangetekend dat de Wbp access providers niet verplicht tot controle op de gegevens die zij doorzenden of voor de opslag waarvan zij capaciteit ter beschikking stellen.[25] Zolang een dergelijke controle ontbreekt, beperkt de verwerking van gegevens door de access provider zich tot de doorgifte of de routering van gegevens. Hij staat in dat opzicht op één lijn met een aanbieder van een telecommunicatiedienst.

We vermelden tenslotte dat menselijke tussenkomst bij de verwerking van persoonsgegevens geen vereiste is. Dit betekent bijvoorbeeld dat ook verwerkingen die volledig geautomatiseerd plaatsvinden onder het regime van de Wbp vallen. We wijzen hier op de (toekomst)situatie dat een

---

[22]De enkelvoudige transmissie van gegevens vormt blijkens p. 52 en p. 60 van de Memorie van Toelichting een uitzondering. Vergelijk ook art. 4 lid 2 Wbp inzake de doorvoer van persoonsgegevens.

[23]Zie *Kamerstukken II* 1997/98, 25892, nr. 3, p. 51.

[24] *Kamerstukken II* 1997/98, 25892, nr. 3, p. pp. 51-51.

[25] Vergelijk ook art. 15 van 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. Dit artikel bepaalt dat de lidstaten aan tussenpersonen, zoals access providers, geen algemene verplichting mogen opleggen om toezicht te houden op de informatie die zij doorgeven of opslaan.

intelligent agent wordt ingezet ten behoeve van de (voorbereiding van de) elektronische transactie. Het betreft in dit geval programmatuur die voor de gebruiker op diens verzoek bepaalde taken op het Internet kan uitvoeren. Zo kan de agent op het Internet zoeken naar informatie en sites, deze sorteren, e-mail afhandelen enzovoorts. Wanneer op termijn de techniek van dergelijke agents verder is verbeterd, kunnen ze over de voorwaarden van het downloaden van bijvoorbeeld gegevens uit een databank 'onderhandelen' met de intelligent agent die is geplaatst op de computer van een informatieleverancier. In dit geval wordt de verzending, ontvangst en verdere verwerking van persoonsgegevens zonder menselijke tussenkomst afgewikkeld. Desondanks zal er in dat geval sprake zijn van een verwerking in de zin van de Wbp.[26]

16.2.3 Rechtmatige verwerking

Voor de vraag of bepaalde persoonsgegevens wel rechtmatig ten behoeve van een concrete toepassing van e-commerce worden verzameld en vervolgens rechtmatig worden gebruikt, is het van groot belang te weten voor welke doeleinden dit precies gebeurt. De Wbp geeft daartoe een limitatieve opsomming van de gronden voor rechtmatige verwerking en vult de open normen aan met een aantal noodzakelijkheidscriteria waaraan moet worden voldaan. Bij de normering is de doelomschrijving opnieuw van belang. Allereerst betekent dit dat, conform de vereisten van art. 6 en 7 Wbp, de gegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Daarbij dienen de gegevens toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig te zijn. Concreet betekenen deze eisen dat verwerkers kritisch moeten kijken welke gegevens nu precies noodzakelijk zijn in het licht van hetgeen met de verwerking wordt beoogd. Via sites blijken bijvoorbeeld vaak gegevens omtrent gezinssamenstelling, geslacht en leeftijd te worden gevraagd, terwijl deze lang niet altijd nodig blijken te zijn voor het specifieke doel waarvoor ze worden verzameld. Ook dient vanuit deze normen ook de nodige aandacht te worden besteed aan het onderhoud van de gegevensbestanden: zijn de gegevens in deze bestanden bijvoorbeeld nog actueel?

Het voornoemde stelsel van materiële normen wordt vervolgens in art. 8 Wbp aangescherpt door te stellen dat verwerking slechts is toegestaan indien *noodzakelijk* in verband met de in datzelfde art. 8 Wbp genoemde belangen dan wel met ondubbelzinnige toestemming van de betrokkene.[27] Bij het verzamelen van gegevens wordt dus niet slechts gekeken naar rechtmatigheids- en zorgvuldigheidsvoorwaarden. Het betreft een zestal gronden en voor de verwerker betekent dit dat hij concreet dient te inventariseren welke grondslag aan de verwerking de rechtmatigheid daarvan toekent. Gaat het om een verwerking van persoonsgegevens in het kader van EC in de categorie bedrijven-consumenten, dan zal de basis voor de rechtmatige verwerking vaak kunnen worden gevonden in art. 8 sub *b* Wbp, dat de verwerking van persoonsgegevens toestaat indien dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst. Denk aan het geval dat een klant bij een Trusted Third Party (TTP) een certificaat voor digitale handtekeningen aanvraagt en de TTP naar aanleiding van deze aanvraag een certificaat opstelt met daarin vermeld persoonsgegevens van de aanvrager. Bij een uitwisseling van gegevens in de categorie bedrijven-overheden zal de grond voor de rechtmatige verwerking meestal kunnen worden gevonden in art. 8 sub *c* Wbp, dat een verwerking toestaat indien deze noodzakelijk is om een wettelijke verplichting na te komen waaraan het bedrijf onderworpen is.

We gaan in het onderstaande nader in op de grondslagen en randvoorwaarden daarbij die specifiek bij elektronische handel van belang zijn. Het betreft dan art. 8 sub *a* en sub *f* Wbp.

Toestemming (art. 8 sub *a* Wbp)

Voor veel toepassingen van elektronische handel zal artikel 8 sub a Wbp een zeer relevante grondslag zijn. Met name als (nog) geen contractuele relatie in zicht is, zal het verkrijgen van toestemming een

[26] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 51.

[27] De term 'noodzakelijk' is tijdens de parlementaire behandeling van de Wbp voorwerp van discussie geweest. Het ging daarbij om de vraag of de vertaling van de Engelse term 'necessary' door 'nodig' beter zou zijn geweest. Blijkens de uitleg in de Memorie van Toelichting dient het begrip 'noodzakelijk' in horizontale relaties minder strikt te worden uitgelegd dan in verticale relaties. Vgl. *Kamerstukken II* 1997/98, 25892, nr. 3, p. 88.

vereiste zijn. Blijkens art. 8 sub *a* Wbp is verwerking van persoonsgegevens namelijk geoorloofd, indien de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend. Voor het verlenen van toestemming geldt geen vormvereiste. Deze toestemming kan ook op elektronische wijze worden verstrekt. Wil de toestemming voldoen aan de eisen dan dient aan de volgende drie elementen te zijn voldaan: vrijheid van beslissen, duidelijke omschrijving van de reikwijdte van de toestemming en op basis van goede informatie.[28] In het geval ondubbelzinnige toestemming is vereist >moet iedere twijfel zijn uitgesloten= bij de verantwoordelijke omtrent de toestemming. Doorgaans betekent dat een zwaardere informatieplicht richting betrokkene. Ook kan er sprake zijn van een verificatieplicht. In de Memorie van Toelichting wordt het uit handen geven van een smart card of het in een interactieve omgeving herhaald aanklikken van een ja-knop aangemerkt als een omstandigheid die verdere verificatie overbodig maakt. Een aanbieder van e-commerce diensten kan dus aan de informatieplicht vorm geven door de website zodanig in te richten dat de afnemer eerst langs een pagina moet waarop informatie staat omtrent de wijze(n) waarop de leverancier de persoonsgegevens van de afnemer wil verwerken. De toestemming zou in dat geval kunnen worden verkregen door de bezoeker eerst aan het eind van deze informatiepagina op een akkoordknop te laten klikken, alvorens hem in de gelegenheid te stellen om andere pagina's van de website te bezoeken.

In het rapport 'Klant in het web' merkt het College Bescherming Persoonsgegevens (ten tijde van het verschijnen van het rapport, de Registratiekamer) op: "Er zijn providers die de potentiële abonnee bij de installatie van de software uitdrukkelijk wijzen op de van toepassing zijnde algemene voorwaarden. Hierbij kan deze de software pas installeren nadat hij door het aanklikken van een daartoe bestemde button verklaart kennis genomen te hebben met de getoonde algemene voorwaarden en akkoord gaat met de daarin opgenomen voorwaarden. Voor zover de voorwaarden hierbij voldoen aan de inhoudelijke vereisten van ondubbelzinnige toestemming, is verdedigbaar dat de abonnee met die handeling inderdaad toestemming voor de gegevensverwerking verleent." Ook in andere situaties kan de ondubbelzinnige toestemming voor een bepaalde verwerking van persoonsgegevens blijken uit gedragingen van de betrokkene. Zo zal bijvoorbeeld degene die via internet een betalingsopdracht verstrekt aan een bank, geacht kunnen worden toestemming te hebben gegeven voor het verwerken van de persoonsgegevens voor zover noodzakelijk om de opdracht uit te voeren. Een afzonderlijke toestemming is daarvoor niet nodig. Men mag echter niet te snel uit een gedraging afleiden dat er toestemming is verleend voor het verwerken van persoonsgegevens. Zo men wij dat uit het bezoeken van een website niet mag worden afgeleid dat de bezoeker heeft ingestemd met het vastleggen van gegevens omtrent de pagina's, die hij op de betreffende website heeft bezocht.[29]

Zoals we later in dit hoofdstuk zullen bespreken zijn de afgelopen jaren diverse initiatieven op de rails gezet om middels technische instrumenten vorm te geven aan privacybescherming. Een van deze toepassingen is de filter. Uitgangspunt hierbij is dat een eigenaar van een website in de meta-tags van zijn pagina zijn privacybeleid specificeert. De filterprogrammatuur van de bezoeker zou aan de hand van vooraf ingegeven criteria kunnen vaststellen of de bezoeker met de specificaties van het privacybeleid van de aanbieder van goederen of diensten kan instemmen.[30] Indien van dergelijke filterprogrammatuur gebruik wordt gemaakt en met behulp daarvan wordt besloten om bepaalde persoonsgegevens te verstrekken aan de aanbieder van goederen of diensten, zou men kunnen stellen dat de bezoeker van de website toestemming heeft gegeven tot de verwerking van de verstrekte persoonsgegevens overeenkomstig de specificaties die zijn opgenomen in de meta-tags van de webpagina.

Relevant is overigens in dit verband ook dat een eenmaal gegeven toestemming kan worden ingetrokken. De intrekking heeft geen terugwerkende kracht met betrekking tot verwerkingen in het verleden.[31] Eerder onder de Wpr of anderszins afgegeven toestemming hoeven bij de inwerkingtreding van de Wbp niet te worden vernieuwd.

---

[28] *Kamerstukken II* 1997/98, 25892, nr. 3, p. 65.
[29] Zo ook R.E. van Esch, 'Electronic Commerce', *Privacyregulering in theorie en praktijk*, 3e druk, Kluwer, Deventer 2002.
[30] T. Oudejans, 'Internet on line. Privacy off-site?', *Privacy & informatie* 1998-4, p. 156
[31] *Kamerstukken II* 1997/98, 25892, nr. 3, p. 67.

Tenslotte willen we hier wijzen op de positie van een TTP (CA). Behalve de Wbp, is voor deze dienstaanbieder namelijk ook de Europese Richtlijn elektronische handtekeningen van belang. Centraal staat wat betreft de verwerking van persoonsgegevens staat artikel 8 van deze Richtlijn[32], waaruit blijkt dat hier strengere eisen worden gesteld aan de verwerking van persoonsgegevens door certificatiedienstverleners, dan in de Wbp. De enige rechtmatige grondslag voor de verwerking is de uitdrukkelijke toestemming van de betrokkene. Daarbij mogen slechts die gegevens worden verzameld die een direct verband houden met de afgifte en het beheer van het certificaat. TTP's zullen ten behoeve van hun activiteiten alsmede het veiligstellen van hun aansprakelijkheidspositie diverse persoonsgegevens willen verzamelen. Zo zullen ze de identiteit van de persoon op wiens naam zij het certificaat uitgeven, willen controleren, waartoe zij een paspoort of een ander identiteitsbewijs van de aanvrager van het certificaat nodig hebben. De gegevens uit deze documenten zullen zij willen opslaan, teneinde achteraf te kunnen bewijzen dat zij voldoende zorgvuldig zijn geweest bij het identificeren van de houder van het certificaat. Voorts zullen zij in sommige gevallen de juistheid van de verstrekte persoonsgegevens willen controleren in externe bestanden. Denk aan het geval dat in het Verificatie en identificatiesysteem (VIS) wordt gecontroleerd of het betreffende identiteitsbewijs als gestolen of vermist is opgegeven. In al deze situaties kunnen de gegevens dus slechts met de uitdrukkelijke toestemming van de betrokken persoon zelf worden verkregen. Ook de verdere verwerking van de persoonsgegevens kan uitsluitend op basis van uitdrukkelijke toestemming van de betrokkene. Een uitzondering hierop vormen de wettelijke regels die opsporings- en inlichtingendiensten de mogelijkheid geven tot het aftappen van het berichtenverkeer naar en van de TTP alsmede het verlangen van medewerking bij ontsleuteling.

Gerechtvaardigd belang (artikel 8 sub f Wbp)

Een andere mogelijke grondslag voor de verwerking van persoonsgegevens bij elektronische handel kan zijn gelegen in art. 8 sub *f* Wbp: de is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. Beperkende factor is wel het belang of de fundamentele rechten en vrijheden van de betrokkene. Indien deze prevaleren boven het gerechtvaardigde belang van de verantwoordelijke, is verwerking van de persoonsgegevens niet rechtmatig. Bij deze afweging spelen het proportionaliteitsbeginsel en het subsidiariteitsbeginsel een rol. Als voorbeeld kan worden gewezen op de situatie waarin een access provider met behulp van de DNS-server registreert hoeveel malen bepaalde bestanden door zijn abonnees worden geraadpleegd of gedownload van internet. Indien een bestand veelvuldig wordt geraadpleegd of gedownload, zou hij om communicatiekosten te besparen kunnen besluiten om het betreffende bestand op zijn server te zetten (het zogenaamde cachen).[33] Een dergelijk belang rechtvaardigt echter nog niet dat de access provider ook gegevens gaat registreren over de individuele personen die het betreffende bestand hebben gedownload. Een registratie van het aantal bezoeken zonder persoonsgegevens is voldoende voor het verwezenlijken van het beoogde doel.
Overigens kan bij dit voorbeeld terzijde de vraag worden gesteld of de voornoemde access provider ook als verantwoordelijke voor de gegevensverwerking middels caching moet worden aangemerkt. Immers, diens feitelijke macht is vaak zeer beperkt. Verantwoordelijk is zoals eerder aangegeven degene die doel en middelen van gegevensverwerking bepaalt. De access provider bepaalt wellicht weliswaar doel en middelen van tijdelijke opslag van webpagina's, maar beoogt daarbij in eerste instantie geen verwerking van persoonsgegevens. De cache heeft geen zelfstandige betekenis, maar is slechts een hulpmiddel bij het organiseren van het transport. Ook een blik op de Europese Richtlijn elektronische handel leert dat de access provider slechts zeer beperkte invloed heeft op hetgeen wordt opgeslagen. Hij is bijvoorbeeld slechts verplicht bepaalde informatie te verwijderen indien daartoe gesommeerd door bevoegde autoriteiten. Artikel 15 van de Richtlijn verbiedt bovendien het actief monitoren van inhoudpagina's. De vraag doet zich dan ook voor hoe deze bepalingen zijn te rijmen met rechten en verplichtingen van verantwoordelijke onder Wbp.

---

[32] Na inwerkingtreding van de Wet elektronische handtekeningen, *Kamerstukken II* 2000/01, 27 743, zal deze bepaling zijn opgenomen in art. 11.5a lid 1 Telecommunicatiewet.

[33] Caching is dus de tijdelijke opslag van recent-opgevraagde informatie in het werkgeheugen of op de server (in een zogenoemde 'cache') om deze informatie bij een nieuw verzoek tot raadpleging sneller beschikbaar te hebben.

16.2.4 Verwerking onverenigbaar met doeleinden (artikel 9 Wbp)
Persoonsgegevens mogen krachtens art. 9 lid 1 Wbp niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Netwerken als internet bieden de mogelijkheid profielen op te stellen van gebruikers, bijvoorbeeld middels datamining. Zo zou bijvoorbeeld de access provider op redelijk eenvoudige wijze profielen kunnen maken van zijn abonnees op basis van de gebruiksgegevens. Hij kan bij het registreren van gegevens op abonneeniveau een gerechtvaardigd belang hebben. Bijvoorbeeld indien hij met deze gegevens zijn abonnees wil adviseren omtrent het modem of het (transport)medium dat zij gebruiken. Het is echter niet toegestaan om de beschikbare persoonsgegevens te gebruiken voor andere doeleinden, zoals het beschikbaar stellen van deze gegevens aan een leverancier van producten of diensten, die op grond daarvan de abonnee benadert met een aanbod tot afname van een goed of een dienst.[34]
Hetzelfde geldt bijvoorbeeld voor het handelsregister. Het is in strijd met de doeleinden van het handelsregister om de daarin opgenomen gegevens omtrent personen als bulkgegevens op een zodanige wijze te verstrekken dat anderen daaruit gemakkelijk overzichten bevattende rangschikkingen van gegevens naar individuele personen kunnen maken.[35] Daarbij kan bijvoorbeeld worden gedacht aan een overzicht van de commissariaten van een bepaald persoon. Het handelsregister is immers bedoeld om in een specifiek geval de gegevens omtrent een lid van een bestuurscollege of een procuratiehouder van een bepaalde rechtspersoon te kunnen raadplegen.[36] Een en ander betekent dat de gegevens uit het handelsregister in beginsel niet op zodanige wijze raadpleegbaar mogen worden gemaakt voor derden via internet dat deze de hiervoor bedoelde individuele overzichten kunnen maken. Zo ook art. 15 lid 3 Handelsregisterwet 1996, waarin tevens is vastgelegd aan welke instanties de Kamer van Koophandel bij wijze van uitzondering dergelijke overzichten mag verstrekken.
In dit kader moet ook worden gewezen op art. 8 lid 2 van de hiervoor reeds genoemde Europese richtlijn betreffende elektronische handtekeningen en het Nederlandse wetsvoorstel ter implementatie hiervan. Hierin is bepaald dat de lidstaten ervoor zorgdragen dat TTP's die certificaten voor digitale handtekening aan het publiek afgeven, slechts persoonsgegevens verzamelen welke voor de afgifte en het beheer van het certificaat vereist zijn. Voorts bepaalt dit artikel dat TTP's de betreffende persoonsgegevens niet zonder uitdrukkelijke toestemming van de betrokkene voor andere doeleinden mogen verzamelen of verwerken.[37]

16.2.5 Bijzondere gegevens
Behalve gewone persoonsgegevens, kent de wet ook nog een afzonderlijke categorie gegevens waarvoor strengere regels gelden. De naam van de categorie is ten opzichte van de Wpr gewijzigd van "gevoelige gegevens" in "bijzondere gegevens". Bij bijzondere gegevens conform artikel 16 ev. Wbp gaat het om gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging (dit laatste is nieuw t.o.v. de Wpr). Ook worden strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag als gevoelig aangemerkt.
Art. 16 Wbp verbiedt in beginsel de verwerking van de daarin vermelde bijzondere persoonsgegevens. Men kan zich in dit kader afvragen of een enkel bezoek aan een bepaalde website een gevoelig gegeven over de bezoeker kan opleveren. Zijn bijvoorbeeld gegevens omtrent een bezoek aan een Gay-site persoonsgegevens betreffende het seksuele leven van de betrokkene? Dit behoeft niet noodzakelijkerwijs zo te zijn. Mensen kunnen ook louter uit nieuwsgierigheid zo'n site bezoeken. Gegevens omtrent de verkoop van bepaalde producten die worden aangeboden op zo'n site, geven echter een sterkere indicatie over het seksuele leven van de koper en kunnen wel als gevoelige gegevens worden beschouwd.

---

[34] Vergelijk *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 92.
[35] *Kamerstukken II* 1998/99, 25 892, nr. 6, p. 31.
[36] Zoals de naam, de vertegenwoordigingsbevoegdheid en de handtekening.
[37] Na inwerkingtreding van de Wet elektronische handtekeningen, *Kamerstukken II* 2000/01, 27 743, zullen deze bepalingen zijn opgenomen in art. 11.5a Telecommunicatiewet.

Een ander voorbeeld waarin de verwerking van bijzondere gegevens aan de orde is betreft het plaatsen van een foto op het internet. In dit geval is immers uit de foto informatie over iemands ras af te leiden. Ook bij het leveren van goederen of diensten kunnen bijzondere gegevens, als bedoeld in art. 16 Wbp, worden verwerkt. We wijzen als voorbeeld op de situatie waarin een verzekeraar persoonsgegevens betreffende de gezondheid van de verzekerde verwerkt. Een dergelijke verwerking van bijzondere gegevens is blijkens art. 23 Wbp onder meer toegestaan, indien dit geschiedt met uitdrukkelijke toestemming van de betrokkene. Zonodig kan deze toestemming worden verkregen via internet. In dat geval zal de uitdrukkelijke toestemming pas aanwezig mogen worden geacht wanneer de betrokkene zijn toestemming voor de verwerking van gegevens in het kader van de verstrekking van een specifieke dienst, door middel van een aparte klik of een combinatie van klikken heeft bevestigd.[38]

16.2.6 De verantwoordelijke

Op grond van privacywetgeving is van belang vast te stellen wie als verantwoordelijke kan worden aangemerkt. De verantwoordelijke is immers degene die primair wordt aangesproken op naleving van de wettelijke bepalingen in verband met de bescherming van de persoonlijke levenssfeer. Bij elektronische handel kan een diversiteit van partijen betrokken zijn. Allereerst zijn dat de partijen die met elkaar een overeenkomst aangaan. Het gaat daarbij om het transactie-niveau: aanbod en aanvaarding. Daarnaast is sprake van een tweede niveau: het transportniveau van de intermediairen. Daarbij valt te denken aan intermediairen die een virtuele markt onderhouden. Maar ook internet providers: zowel access providers als service providers. Op de derde plaats is er het niveau van de financiële afhandeling waarbij veelal financiële instellingen betrokken zullen zijn met de beide contractspartijen als opdrachtgever respectievelijk begunstigde. Indien opdrachtgever en begunstigde bij verschillende banken bankieren of in verschillende landen zijn gevestigd worden nog andere partijen betrokken zoals correspondentbanken, bancaire transportnetten (bijvoorbeeld SWIFT) en clearing instituten. Indien bij de dienstverlening gebruik wordt gemaakt van certificaten worden nieuwe partijen aan het proces toegevoegd. Alle betrokken partijen houden zich uiteindelijk bezig met de verwerking van persoonsgegevens. De persoonsgegevens kunnen worden uitgesplitst naar categorieën. Er zijn gegevens die noodzakelijk zijn om het uitwisselingsproces te faciliteren. Het gaat daarbij om routeringsgegevens. Dat zijn bij voorbeeld internet adressen, telefoonnummers en bankrekeningnummers. Daarnaast is de inhoud van de berichten van belang. Daar kan sprake zijn van verschillen in niveau. Bij betaalopdrachten is sprake van opdrachtgegevens die ook voor de bank bestemd zijn. Maar veelal is tevens sprake van begeleidende informatie die namens de opdrachtgever door de bank wordt doorgegeven aan de begunstigde. Dat betekent dat ten aanzien van bepaalde gegevens de verwerkende instantie optreedt als doorgeefluik in andere gevallen sprake is van een actieve rol. Sommige processen hebben een black box karakter waarbij de verwerkende instantie geen invloed op de gegevens kan uitoefenen. In andere gevallen kan de verwerkende instantie feitelijke macht uitoefenen over de gegevens. Niet in alle gevallen waar het theoretisch mogelijk is, is het ook feitelijk toegestaan.

Zowel de Wbp als de privacyrichtlijn bevatten een op het eerste gezicht eenvoudige definitie van de figuur van de verantwoordelijke. Het is de persoon die als formeel juridisch verantwoordelijke doel en middelen van de verwerking vaststelt. Indien de verantwoordelijke bij de verwerking een derde inschakelt die in zijn opdracht conform zijn instructies werkzaamheden verricht wordt deze persoon aangeduid als verantwoordelijke. Indien de verantwoordelijke een bewerker inschakelt is hij verplicht de opdracht in schriftelijke vorm vast te leggen. Het probleem is echter dat de term verwerking een complex begrip is. Het begrip verwerking is gedefinieerd als *een verwerking of een geheel van samenhangende verwerkingen*. Dat betekent dat bij voorbeeld in het geval van de elektronische handel sprake kan zijn van een proces van samenhangende activiteiten waarbij naast bewerkers sprake kan zijn van meer dan één verantwoordelijke. Volgend de Memorie van Toelichting op de Wbp geldt bij een betaalopdracht dat de bank verantwoordelijke is ten aanzien van de afhandeling van de betaalopdracht.[39] Ten aanzien van het berichtenveld van een betaalopdracht geldt evenwel dat de

[38] *Kamerstukken II* 1998/99, 25892, nr. 6, p. 41.

[39] Vgl. Voor een uitgebreide behandeling Holvast, *Privacyregels voor EDI-berichten,* ITER-reeks nr. 24, Kluwer 2000.

opdrachtgever verantwoordelijk is voor de inhoud terwijl de bank verantwoordelijk is voor de ongewijzigde doorgifte. De Wbp onderscheid verschillende soorten verantwoordelijkheid.[40] Naast de enkelvoudige verantwoordelijkheid is er ook de gezamenlijke verantwoordelijkheid. Daarbij zijn enkele partijen gezamenlijk verantwoordelijke voor het geheel van een verwerking (hoofdelijk) of is iedere partij verantwoordelijk voor een deel van het proces. Een ander in de toelichting genoemd model gaat uit van enerzijds verantwoordelijkheid voor de juistheid en volledigheid van gegevens en anderzijds verantwoordelijkheid voor de integriteit van het verwerkingsproces als zodanig (het zogenaamde ziekenhuismodel.). Een andere variant is die van de groepsverantwoordelijkheid. Indien binnen een groep van rechtspersonen één rechtspersoon formeel juridisch verantwoordelijk is voor het gehele proces bestaat de mogelijkheid om onder bepaalde voorwaarden die rechtspersoon als verantwoordelijke aan te merken. Hierbij zij aangetekend dat indien opdrachten afkomstig zijn van particulieren de Wbp niet van toepassing is voor zover die personen als verantwoordelijke zouden worden aangemerkt. Die verantwoordelijkheid valt dan namelijk weg in de uitzondering van artikel 3 lid 2 Wbp.
Het moge duidelijk zijn dat de toepassing van privacyregels op elektronische handel tot een onoverzichtelijk beeld kan leiden. Deze onoverzichtelijkheid heeft in het verleden geleid tot discussies over het fenomeen van de geschaalde verantwoordelijkheid.[41] Met name de opkomst van de chipkaart gaf voeding aan deze discussie. Daarbij heeft men uiteindelijk besloten om af te zien van pogingen om tot begrijpelijke wetgeving te komen. In plaats daarvan werd het accent gelegd op het tot stand komen van vormen van zelfregulering waarbij alle bij een proces betrokken partijen werden verplicht om hun eigen verantwoordelijkheden te expliciteren. Deze verantwoordelijkheden dienden op elkaar aan te sluiten teneinde te voorkomen dat er voor met name consumenten gaten zouden vallen.

16.2.7. Informatieverstrekking aan de betrokkene

Op grond van artikel 33 en 34 Wbp moet de verantwoordelijke de betrokkene informeren omtrent zijn identiteit en de voorgenomen gegevensverwerking. Zulks tenzij de betrokkene reeds op de hoogte is. De informatieverstrekking kan langs elektronische weg plaats vinden. Indien sprake is van consumenten die via internet informatie uitwisselen met een leverancier kan de verplichte informatie via de website van die leverancier worden verstrekt.[42] Indien de leverancier structureel gegevens over de consument verzamelt zonder deze daarover te informeren is op grond van artikel 31 Wbp een voorafgaand onderzoek noodzakelijk. Dat is bij voorbeeld het geval als door middel van cookies buiten weten van de consument informatie over het computersysteem van de consument naar de leverancier worden verstuurd. Men denke bij voorbeeld aan electronic copyright management systems die informatie verzamelen over illegale kopieën van software of andere auteursrechtelijk beschermde werken. Het kan dan gaan om een verzamelactiviteit die op zich gerechtvaardigd kan worden onder artikel 8f Wbp maar om efficiencyredenen niet wordt publiek gemaakt. Indien informatie wordt verzameld die bestemd is om voor marketingdoeleinden te worden ingezet dient de leverancier op grond van artikel 41 Wbp de betrokkene te informeren over zijn recht van opt out.
Bij internet kan men zich nog afvragen in welke taal de verplichte informatie dient te worden verstrekt. Ons lijkt redelijk dat de verplichte informatie wordt verstrekt in dezelfde taal als die waarin de website is ingericht. Bij het inrichten van een website dient men er overigens op bedacht te zijn dat het beschikbaar stellen van informatie omtrent contactpersonen die bij de leverancier werkzaam zijn sprake kan zijn van verstrekking van persoonsgegevens in de betekenis van de Wbp. Indien de website gericht is op de markt van een land buiten de EER valt een dergelijke verstrekking onder de restricties van hoofdstuk 11 van de Wbp (zie hierover verderop in dit hoofdstuk).

---

[40]Zie Prins en Berkvens, *De wet bescherming persoonsgegevens*, hoofdstuk 5 in *Privacyregulering in theorie en praktijk* (ed. Prins en Berkvens), Kluwer 2000, 2e druk, p. 87.

[41]Vgl. Gardeniers, *Chipcards en privacy, regels voor een nieuw kaartspel*, Achtergrondstudies en verkenningen nr. 6, Registratiekamer, september 1995.

[42]Zie uitgebreid Artz en van Eijk, *Klant in het web, privacywaarborgen voor internettoegang*, Achtergrondstudies en verkenningen nr. 17, Registratiekamer, juni 2000.

16.2.8 Rechten van betrokkene

Een belangrijk uitgangspunt voor het realiseren van een voldoende transparante gegevensverwerking, is dat de persoon van wie gegevens worden verwerkt hiervan op de hoogte wordt gesteld. De Wbp geeft de betrokkene aldus het recht om over de verwerking van zijn persoonsgegevens te worden geïnformeerd. Vervolgens kan de betrokkene met enkele andere hem toegekende rechten (recht op inzage, recht op correctie en recht op verzet) bij de verantwoordelijke aandringen op een wijziging in diens verwerkingsbeleid. Uitgangspunt is dat de diverse rechten de betrokkene in staat moeten stellen na te gaan welke hem betreffende gegevens met welke herkomst worden verwerkt en ze zonodig te laten corrigeren of verwijderen. Met name in de grenzeloze en complexe structuur van het internet, en dus bij toepassingen van elektronische handel, is het van groot belang dat de rechten van betrokkenen adequaat worden vormgegeven. In veel situaties zullen de persoonsgegevens op een andere wijze worden verkregen dan rechtstreeks van de betrokkene. Als voorbeeld noemen we het verkrijgen door een internet provider van persoonsgegevens naar aanleiding van het beheer van een netwerk. In dit geval worden de gegevens veelal verkregen door eigen observatie bij het vastleggen van de clickstreams van de individuele abonnee. In deze en andere gevallen zal de verwerker de betrokkene dienen te informeren conform de voorwaarden van artikel 33 en 34 Wbp. Hiertoe biedt het internet overigens ook weer nieuwe instrumenten. We wijzen hier op de zogenaamde 'privacy-statement'. In een dergelijke verklaring kunnen providers en aanbieders van elektronische diensten hun klanten informeren over het beleid rondom het gebruik van persoonsgegevens. Veelal is de verklaring beschikbaar door deze aan te klikken via een speciale button op de site. Hiernaast werken diverse organisaties, belangenverenigingen, etc. aan modelbepalingen waaraan een keurmerk wordt gekoppeld. Een voorbeeld is het keurmerk van het Amerikaanse TRUSTe.[43] Bedrijven die zich conformeren aan de modelbepalingen mogen vervolgens het keurmerk op hun site vermelden.

Dat transparantie niet altijd direct een vanzelfsprekende zaak is, toont het voorbeeld van de zogenaamde finger-commando. Met dit commando kan een ieder die op het Internet actief is opvragen of een bepaalde gebruiker is ingelogd en zo ja, sinds welk tijdstip en zo nee, wanneer de gebruiker voor het laatst was ingelogd. In deze situatie heeft een provider geen actieve rol bij het verstrekken van de persoonsgegevens van diens abonnee aan derden. De persoonsgegevens komen hier door toedoen van de toegepaste technologie voor derden beschikbaar. Een klacht bij de Registratiekamer vormde de aanleiding voor discussie over de vraag of een internet provider verplicht is gebruikers de mogelijkheid te bieden om het e-mailadres en andere login-gegevens te blokkeren zodat derde gebruikers hiervan geen kennis kunnen nemen. Na overleg met de betreffende provider werd vastgesteld dat providers het aan de abonnees zelf moeten overlaten of deze het finger-commando aan of uit willen zetten en wel of niet wensen te worden opgenomen in de 'who is online page'. In ieder geval geldt voor wat betreft het systeem van de provider de standaard optie 'uit'.[44]

In art. 35 en artikel 36 Wbp zijn het inzage- en correctierecht uitgewerkt. Het verzoek tot inzake of correctie is vormloos, hetgeen betekent dat de betrokkene dit verzoek ook elektronisch (via e-mail) naar de verantwoordelijke kan sturen. Vreemd is dat de verantwoordelijke in beginsel schriftelijk dient te reageren. Waarom zou een aanbieder van e-commerce diensten niet door middel van een e-mail op een inzageverzoek kunnen reageren indien de consument zelf via e-mail het verzoek heeft gedaan? Van belang bij het inzageverzoek is dat art. 37 lid 2 Wbp vereist dat de verantwoordelijke de identiteit van de verzoeker vaststelt. Indien het verzoek elektronisch is verstuurd en ondertekend met behulp van een digitale handtekening, zal de verantwoordelijke aan deze verplichting kunnen voldoen door de digitale handtekening van de betrokkene te verifiëren.

We wijzen tenslotte nog op art. 38 Wbp waarin wordt bepaald dat de verantwoordelijke na een correctie van persoonsgegevens van deze correctie mededeling dient te doen aan derden aan wie de gegevens voorafgaand aan de correctie zijn verstrekt. Uitzondering geldt indien een dergelijke mededeling onmogelijk blijkt of een onevenredige inspanning kost. Deze laatste situatie kan zich bijvoorbeeld voordoen in het geval dat gegevens uit een e-mailadressenlijst op internet zijn gecorrigeerd. In dat geval kan in redelijkheid van de houder van het adressenbestand niet worden

---

[43] <http://www.truste.org>.

[44] Registratratiekamer, januari 1998, 97.K.0560

gevergd dat hij een ieder die het heeft geraadpleegd, van de correctie op de hoogte stelt. Hetzelfde geldt voor openbare registers die via publieke netwerken als internet kunnen worden geraadpleegd.[45]

16.3 GEGEVENSVERKEER MET LANDEN BUITEN DE EUROPESE UNIE

16.3.1 Algemeen

In hoofdstuk 11 van de Wbp wordt het gegevensverkeer *(doorgifte*) naar landen buiten de Europese Unie (lees: buiten de EER[46]) gereguleerd.[47] Ten opzichte van de Wpr[48] is sprake van een forse aanscherping van de regels. Onder de Wpr bestond de mogelijkheid voor de Minister om gegevensverkeer met het buitenland in bepaalde gevallen nader te reguleren. Van die mogelijkheid is nooit gebruik gemaakt. Onder de Wbp wordt een onderscheid gemaakt tussen gegevensverkeer binnen de Europese Unie en gegevensverkeer naar landen buiten de Europese Unie. In het eerste geval zijn er geen belemmeringen. Als hoofdregel geldt dan dat het recht van het land van de vestiging van een verantwoordelijke van toepassing is. Bij gegevensuitwisseling naar het buitenland geldt evenwel de hoofdregel van artikel 76 lid 1 Wbp. Gegevensexport is dan verboden indien in het ontvangende land geen passend niveau van privacybescherming bestaat. In artikel 76 lid 2[49] wordt vervolgens aangegeven hoe moet worden bepaald of het beschermingsniveau passend is.[50] Het gaat daarbij om open normen die in eerste instantie door de verantwoordelijke zelf moeten worden geïnterpreteerd.[51] De verantwoordelijke moet zich daarbij houden aan eventuele beslissingen van de nationale overheid omtrent het al dan niet passend zijn van het niveau van bescherming. Inmiddels is door de Commissie

---

[45] Vergelijk *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 162.

[46]Richtlijn 95/46 heeft een ruimer bereik dan alleen de landen die bij de Europese Unie behoren. Alle landen die zijn aangesloten bij de Europese Economische Ruimte (EER) vallen onder het bereik van de richtlijn. Het gaat daarbij naast de leden van de EU om Noorwegen, IJsland en het later tot de EER toegetreden Liechtenstein. De EER is een associatieverdrag gebaseerd op art. 310 van het EU-verdrag. Ongeveer 80 % van alle EU regels geldt voor de EER-landen die geen lid van de EU zijn. Waar hierna wordt gesproken over gegevensverkeer binnen de Europese Unie worden daarmee mede de andere drie EER leden aangeduid.

[47]Van der Klaauw-Koops en Prins, *Internationale privacy regulering*, in *Privacyregulering in Theorie en Praktijk* (red. Prins en Berkvens), Serie Recht en Praktijk 75 2e druk, Kluwer Deventer 2000. Zie ook derde druk 2002.

[48]Artikelen 47 t/m 49.

[49] *"Het passend karakter van het beschermingsniveau wordt beoordeeld gelet op de omstandigheden die op de doorgifte van gegevens of op een categorie gegevensdoorgiften van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde of de doeleinden en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectoriële rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd.*"

[50]DG XV D/5025/98 *Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens,* werkdocument *Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-Richtlijn betreffende gegevensbescherming,* goedgekeurd door de groep op 24 juli 1998.

[51]Deze opvatting correspondeert met p. 193 uit de MvT. Echter, in TK 27 043 nr. 1, *Toepassing van artikel 25 en 26 van Richtlijn 95/46/EG (gegevensverkeer tussen de EU en derde landen)* op p. 14 werd een ander standpunt ingenomen waarbij export zonder vergunning werd verboden. Die opvatting werd na forse discussie weer herroepen bij de slotbehandeling van de Wbp in de Eerste Kamer (Handelingen EK 34-1635 van 3 juli 2000). Zie uitvoerig Berkvens, *Wet bescherming persoonsgegevens en grensoverschrijdend persoonsgegevensverkeer*, BJB 2000/14, p. 138/139.

ten aanzien van een drietal landen, te weten Zwitserland[52], Hongarije[53] en Canada[54] beschikt dat hun wetgeving afdoende is. Ten aanzien van de Verenigde Staten is beschikt dat ondernemingen die voldoen aan de voorwaarden van de zogenaamde Safe Harbor beschikking eveneens een passend niveau van bescherming bieden[55]. Het gaat daarbij om ondernemingen die zich onderwerpen aan een set van regels die vergelijkbaar zijn met de inhoud van Richtlijn EG 95/46 en die onderworpen zijn aan het toezicht van de Federal Trade Commission of het Amerikaanse Ministerie van Vervoer. Organisaties als banken of verzekeraars vallen buiten dat toezicht en vallen dus buiten de mogelijkheden van Safe Harbor. Indien het ontvangende land onvoldoende bescherming biedt kan artikel 77 lid 1 soelaas bieden. In dit artikel wordt een aantal gronden genoemd die de export naar dergelijke landen toelaatbaar maken. Het gaat daarbij met name om export in verband met overeenkomsten of met toestemming van de betrokkene. Indien ook deze tweede mogelijkheid niet bruikbaar is dient de exporteur een vergunning aan te vragen bij het Ministerie van Justitie dat vervolgens verplicht is om het College Bescherming Persoonsgegevens om advies te vragen. Inmiddels is door het College een Position Paper op haar Website gepubliceerd waarin het stelsel wordt uitgelegd.[56] Tevens is een model vergunningsaanvrage gepubliceerd.[57] Verzoekers die voornemens zijn om door de Europese Commissie goedgekeurde modelclausules te gebruiken kunnen er op rekenen dat hun aanvraag zal worden gehonoreerd. Inmiddels zijn er 2 sets modelvoorwaarden, die de Commissie zelf heeft opgesteld, goedgekeurd.[58] Andere organisaties als ICC bereiden eveneens modelclausules voor. Als sluitstuk op de regeling geldt artikel 75 Wbp waarin overtreding van een exportverbod strafbaar wordt gesteld.
Ten aanzien van gegevensimport vanuit derde landen naar landen binnen de Europese Unie geldt op grond van artikel 4 van Richtlijn 95/56 (resp. Art. 4 Wbp) dat het recht van het importerende EU-land van toepassing is. Indien geen sprake is van import door een verantwoordelijke (maar bij voorbeeld door een bewerker) dient de exporterende partij een vertegenwoordiger in Nederland aan te wijzen. Die wordt vervolgens als een verantwoordelijke aangemerkt. Indien de activiteiten in Nederland beperkt blijven tot enkelvoudige doorvoer is de Wbp niet van toepassing.
De toepasselijkheid van de artikelen. 76 t/m 78 Wbp cumuleert met de overige bepalingen van de Wbp. Zo zal een exporterende Nederlandse verantwoordelijke dus eerst er voor moeten zorgen dat zijn

---

[52]COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304), OJ L215/1 of 25/08/2000.

[53]COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary, OJ L215/4 of 25/08/2000.

[54]Beschikking van de Commissie van 20 december 2001overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad,betreffende de gepastheid van de bescherming van persoonsgegevens geboden door de Canadese Personal Information Protection and Electronic Documents Act (kennisgeving geschied onder nummer C(2001)4539), *Pb* EG 2002, L 2/13-16.

[55]Beschikking 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, Pb EG 2001, L 215 e.v.

[56]Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act (WBP), Diana Alonso Blas.

[57]Application form for a permit as defined in Article 77.2 WBP (compulsory use).

[58]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), Pb EG 2001, L 181/19-31. Alsmede: 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, *Pb* EG 2001 L 6/52-6/62.

verwerking in overeenstemming is met het nationale regime en zal vervolgens ook nog eens aanvullend getoetst moeten worden aan de eisen van hoofdstuk 11.

16.3.2 Doorgifte

De geschetste regeling is van toepassing op iedere *doorgifte* van persoonsgegevens naar derde landen. De term *doorgifte* komt slechts in hoofdstuk 11 van de Wbp voor. Ook in de uitvoerige definitie van *verwerking* in art. 1 (b) van de Wbp wordt de term doorgifte niet gehanteerd. Het enige wat er op lijkt is de term *doorvoer* die in artikel 4 lid 2 wordt gehanteerd. De term *doorgifte* omvat een ruim aantal mogelijkheden. Daarbij is niet van belang of er sprake is van fysieke overdracht van gegevens voor technische verwerkingsdoeleinden (uitbesteding) of dat er sprake is van fysieke overdracht van gegevens in het kader van de overdracht van een gebruiksrecht aan de ontvangende partij. Bij iedere vorm van fysieke overdracht van persoonsgegevens vanuit Nederland naar een derdenland is er sprake van *doorgifte*.

De term *doorgifte* is evenmin afhankelijk van de status van de overdragende partij. Zowel de overdracht door een verantwoordelijke als de overdracht door een bewerker vormen een doorgifte als bedoeld in hoofdstuk 11 van de Wbp.

Blijkens de memorie van toelichting geldt artikel 76 ook indien sprake is van persoonsgegevensverkeer tussen concernonderdelen waarbij onderdelen van het concern buiten Europa gevestigd zijn. De verstrekking vanuit Nederland naar een buiten de Europese Unie gevestigd concernonderdeel valt dus gewoon onder artikel 76. Dit geldt ook indien de Nederlandse bron volledige zeggenschap heeft over de verwerkingen binnen de ontvangende organisatie van de buiten de Europese Unie gevestigde dochtermaatschappij.

Niet helemaal duidelijk is de positie van een transporteur. Vaak zal de overdracht van persoonsgegevens van een Nederlandse bron naar een buitenlandse ontvanger verlopen via de tussenkomst van een telecommunicatie dienstverlener. De vraag doet zich voor of artikel 76 zich eveneens richt tot een dergelijke verlener van transportdiensten. De memorie van toelichting op dit punt is niet geheel duidelijk. De Richtlijn geeft in considerans 47 slechts aan dat een transporteur van berichten niet als verantwoordelijke hoeft te worden aangemerkt en slechts verantwoordelijk is ten aanzien van de verwerking van de verkeersgegevens. Daarmee is niet uitgesloten dat de transporteur als bewerker moet worden aangemerkt. Ook de definitie van *verwerking* is niet erg duidelijk op dit punt. Er wordt slechts gesproken over *verstrekken door middel van doorzending*. Een redelijke toepassing van de wet brengt naar onze mening met zich mee dat zuivere transporthandelingen niet als zelfstandige verwerking in de zin van de Wbp worden aangemerkt. Dat betekent dat degene die gegevens *verstrekt via doorzending* zelf als verantwoordelijke respectievelijk bewerker moet worden aangemerkt ook indien de doorzendactiviteit is uitbesteed aan een telecommunicatie dienstverlener.

Blijkens de Memorie van Toelichting valt onder *doorgifte* ook *het ter beschikking stellen van gegevens met het oog op de bewerking ervan*. Men kan daarbij denken aan een gegevensverzameling die via Internet toegankelijk is voor derden buiten de Europese Unie. De vraag doet zich voor wanneer sprake is van doorgifte. Op het moment dat de gegevens voor raadpleging beschikbaar zijn of op het moment dat daadwerkelijk sprake is van raadpleging. De laatste optie lijkt meer voor de hand te liggen. Praktisch bezien maakt het antwoord vermoedelijk weinig uit omdat de beveiligingsplicht van art. 13 met zich mee brengt dat ongeautoriseerde bevragingen worden tegengegaan.

Indien door een buitenlandse partij cookies worden geplaatst in een Nederlandse computer kan dat leiden tot doorgifte van persoonsgegevens. Steeds wanneer de Nederlandse gebruiker contact neemt met de buitenlandse website zal de op zijn computer geplaatste cookie gegevens naar die buitenlandse website verzenden. Een dergelijke activiteit valt (althans volgens de "Groep" op p. 28 van haar Advies WP37 inzake Internet[59]) onder de term doorgifte:

This will be the case, for example, for a text file installed on the hard drive of a computer which will receive, store and send back information to a server situated in another country. Such text files, named cookies, are used to collect data for a third party. If the computer is situated in an EU country and the

[59] *ARTICLE 29 - DATA PROTECTION WORKING PARTY*, nr. 5063/00/EN/FINAL, WP 37, *Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection-Adopted* on 21st November 2000.

third party is located outside the EU, the latter shall apply the principles of the national legislation of that Member State to the collection of data via the means of the cookie. In such a case, according to article 4 2., the controller will also have to designate a representative in the territory of the Member State, without prejudice to legal actions which could be initiated against the controller himself.

Ten aanzien van het verzamelen van gegevens met als bestemming de export naar derdenlanden wordt in de Memorie van Toelichting opgemerkt dat dergelijke activiteiten geen onderdeel van de doorgifte uitmaken doch gewoon onder de algemene nationale regels vallen. Daarbij is uiteraard wel van belang dat het doel waarvoor de gegevens worden verzameld voldoet aan de algemene criteria van hoofdstuk 2 van de Wbp. Het verzamelen van gegevens met het oog op de export dient dus voor de verantwoordelijke een rechtmatig doel te vormen. Artikel 76 geldt slechts ten aanzien van de doorgifte van persoonsgegevens *die aan een verwerking worden onderworpen of die bestemd zijn om na hun doorgifte te worden verwerkt*.

Indien persoonsgegevens worden doorgegeven zonder dat er sprake is van een verwerkingsdoelstelling, geldt het bijzondere regime van hoofdstuk 11 Wbp niet. Men zou daarbij kunnen denken aan een doorgifte van de ene lidstaat naar de andere via het grondgebied van een derdenland. Ook zou men kunnen denken aan gegevens die in het verstrekkende land als *persoonsgegeven* worden aangemerkt maar die in het ontvangende land door het ontbreken van herleidingsmogelijkheden niet meer als *persoonsgegeven* gelden. De formulering van deze bepaling is wederom vatbaar voor discussie. Indien de persoonsgegevens via een derdenland worden doorgegeven naar een andere lidstaat kan sprake zijn van tijdelijke opslag op het grondgebied van het derdenland. Aangezien ook een dergelijke opslag een verwerkingshandeling is volgens de definitie van art. 1(b) Wbp, zou de regeling van art. 76 toch van toepassing kunnen zijn. Een redelijke toepassing van de wet brengt naar onze mening met zich mee dat de bepaling over doorvoer van artikel 4 lid 2 analoog wordt toegepast en dat *mere conduit*, ook als die gepaard gaat met tijdelijke opslag, steeds leidt tot niet toepassing van hoofdstuk 11 Wbp. Daarvoor pleit naar onze mening eveneens het gebruik van de term *bestemming* in artikel 76 lid 1 Wbp waaruit men zou kunnen afleiden dat naar de *eindbestemming* moet worden gekeken en niet naar de tussenliggende stappen.

16.4. GEGEVENSVERKEER EN DE TELECOMMUNICATIEWET

Zoals we in de Inleiding reeds kort aanstipten bevat niet alleen de Wbp relevante bepalingen voor de omgang met persoonsgegevens bij elektronische handel. Hoofdstuk 11 Telecommunicatiewet bevat de bepalingen zoals die op Europees niveau zijn neergelegd in Richtlijn 97/66/EG, de privacy-telecommunicatierichtlijn. Zoals hiervoor al werd opgemerkt, publiceerde de Europese Commissie zomer 2000 een richtlijnvoorstel tot aanpassing van deze eerdere richtlijn uit 1997.[60] Wij bespreken in dit hoofdstuk uitsluitend kort de privacybepalingen van de Tw.[61] Voor het overige verwijzen we naar het hiernavolgende hoofdstuk.

De Telecommunicatiewet is, waar het de regeling betreffende persoonsgegevens in hoofdstuk 11 betreft, een lex specialis ten opzichte van de Wbp. Aldus gaat een specifieke bepaling in de Tw voor op de algemene bepaling van de Wbp, die daarmee samenloopt. Belangrijk is tevens te vermelden dat enkele bepalingen uit hoofdstuk 11 Tw, waaronder de bepaling over verkeersgegevens, niet alleen van toepassing is op natuurlijke personen, maar eveneens op rechtspersonen.
Allereerst is de regeling rondom verkeersgegevens van belang. Hierover stelt artikel 11.5, eerste lid, Tw dat verkeersgegevens moeten worden verwijderd of geanonimiseerd bij beëindiging van de

[60] Dit is gebeurd in het kader van de herziening van het Europese telecommunicatierecht (de zgn. ONP-review). Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, COM(2000) 385 definitief. Beschikbaar via: http://www.ispo.cec.be/infosoc/telecompolicy/review99/. In november 2001 werd het Gemeenschappelijk Standpunt vastgesteld. Zie: Pb C 337, 30 november 2001.
[61] Overigens moet worden opgemerkt dat deze bepalingen uit de Richtlijn niet geheel correct in de Telecommunicatiewet zijn geïmplementeerd. Inmiddels is dat middels de wet tot wijziging van de Telecommunicatiewet rechtgezet (*Stb.* 2001, 559).

oproep. Vervolgens bepaalt artikel 11.5, tweede lid, Tw limitatief in welke gevallen een uitzondering bestaat op deze hoofdregel en verkeersgegevens dus ook ná de oproep mogen worden verwerkt. Daarmee is artikel 11.5 Tw dus een lex specialis ten opzichte van artikel 7 Wbp. Wat betreft de gevallen genoemd in artikel 11.5 lid 2 Tw moet alleereerst worden genoemd de mogelijkheid om verkeersgegevens te gebruiken voor het opstellen van nota's van eindgebruikers en voor verrekeningen tussen operators onderling (ingeval van interconnectie of bijzondere toegang). Tevens mogen deze gegevens worden gebruikt voor zover dat noodzakelijk is voor marktonderzoek en verkoopactiviteiten, voor berechting van geschillen, voor verkeersbeheer en voor het geven van inlichtingen aan klanten. In hoofdstuk 11 Tw worden nog diverse andere regels gesteld inzake de omgang met persoonsgegevens bij telecommunicatiediensten. Zo bepaalt artikel 6 van dit hoofdstuk dat in de telefoongids en in het door de abonnee-informatiedienst gebruikte abonneebestand slechts die persoonsgegevens mogen worden opgenomen die noodzakelijk zijn om een abonnee te kunnen identificeren, tenzij de abonnee er ondubbelzinnig mee heeft ingestemd dat er bijkomende persoonsgegevens worden opgenomen. Deze bepaling is te zien als een invulling van artikel 11 lid 1 Wbp dat voorschrijft dat persoonsgegevens slechts mogen worden verwerkt voor zover zij toereikend, ter zake dienend en niet bovenmatig zijn. Artikel 11.6 Tw kent verder de abonnee diverse rechten toe.

In artikel 11.9 TW wordt de nummeridentificatie geregeld. Een abonnee heeft op grond van artikel 11.9 lid 2 sub a het recht om te verhinderen (blokkeren) dat zijn oproepende nummer wordt doorgegeven aan de opgeroepen persoon. Deze bepaling regelt tevens het zogenaamde block blocking, namelijk dat de opgeroepen persoon eveneens kan blokkeren dat zijn nummer worden meegezonden. Een belangrijke vraag die zich bij deze bepaling voordoet is of het blokkeringsrecht ook van toepassing is op een IP-adres of Internettelefonie. Dit lijkt niet het geval te zijn, nu artikel 11.9 Tw en artikel 11.10 Tw uitsluitend van toepassing zijn op telefonische oproepen in het kader van telefoniediensten. Aldus biedt de regeling vooralsnog geen basis om anoniem surfen op Internet mogelijk te maken.

Tot slot moet er ten aanzien van de regeling in hoofdstuk 11 Tw op worden gewezen dat er genoeg aanleiding is voor verwarring wat betreft de terminologie. De regeling in de Tw hanteert namelijk andere begrippen dan de Wbp. Zo spreekt de Tw niet van "verantwoordelijke" maar van de "aanbieder van een openbare telecommunicatiedienst". Ook wordt niet gewerkt met de term "betrokkene", maar wordt gesproken van "abonnee" of "gebruiker".

16.5. ZELFREGULERINGSINITIATIEVEN INZAKE PRIVACY EN E-COMMERCE

Zoals bij diverse andere juridische deelgebieden die worden beinvloed door elektronische handel, spelen ook op het terrein van de privacybescherming zelfreguleringsinstrumenten een belangrijke rol. Alles wijst er op dat private sturingsinstrumenten een steeds belangrijker rol spelen bij het vormgeven van de toepasselijke normen, waarden en concrete gedragsregels op het Internet en meer specifiek bij elektronische handel. Niet alleen de techniek, maar ook de gedragscode, het certificaat en de individuele overeenkomst vormen de leidende instrumenten bij de regulering van maatschappelijke en economische verhoudingen.

Wat betreft technische instrumenten hebben we eerder in dit hoofdstuk al gewezen op de mogelijkheden van PET en anonimiseringsapplicaties. Hiernaast kunnen consumenten gebruik maken van een techniek als P3P. P3P staat voor het Platform for Privacy Preferences, een project opgezet door het World Wide Web Consortium (W3C), dat een set protocollen en afspraken omvat waarmee browsers of andere programma's automatisch over de afgifte van persoonsgegevens kunnen 'onderhandelen'.[62] Het systeem werkt op basis van privacywensen en privacyprofielen die gebruikers kunnen instellen. De artikel 29 Groep heeft in 1998 een advies uitgebracht over het P3P-initiatief. Alhoewel de eindconclusie was dat het initiatief steun verdiende, was er toch een aantal kritische kanttekeningen. Zo waarschuwde de Groep dat de installatie van P3P in de volgende generatie browsers, de in de EU gevestigde aanbieders niet in de waan moet brengen dat zij van sommige van hun wettelijke verplichtingen ontslagen kunnen worden. Ook geeft men aan dat een technisch platform

[62] <http://www.w3.org/P3P>

voor de bescherming van persoonsgegevens op zichzelf niet voldoende is voor adequate privacy op het Internet. Het moet ook worden toegepast binnen een kader van afdwingbare regels inzake gegevensbescherming, aldus de Groep. Tot slot stelde men dat P3P en OPS in de browsertechnologie moet worden toegepast met default-instellingen die in overeenstemming zijn met het belang van de gebruiker om aanspraak te kunnen maken op een hoog niveau van privacybescherming.[63]
Het World Wide Web Consortium heeft te kennen gegeven met deze kanttekeningen rekening te houden door daarop in te gaan in de FAQ (vragen en antwoorden). Daarin geeft zij bijv. aan dat P3P niet in plaats van maar naast wetgeving gebruikt moet worden en dat wet en technologie elkaar niet uitsluiten maar ondersteunen.[64] Alhoewel de P3P standaard al wel wordt gebruikt, is dat nog op kleine schaal. Bij het ontwikkelen van een dergelijke technische standaard ondervond men meer problemen dan oorspronkelijk verwacht. Overigens is het voor een adequaat gebruik van het initiatief wel noodzakelijk dat de Internetconsument een adequaat inzicht in het gebruik van deze techniek heeft. Default-instellingen zullen daarom zeker van belang zijn.
Naast de technische instrumenten zijn ook andere private reguleringsinstrumenten op het terrein van privacybescherming voorhanden. Allereerst kan worden gewezen op de gedragscode. Specifiek op het terrein van elektronische handel is met name de Model Gedragscode voor Elektronisch Zakendoen van het Electronic Commerce Platform Nederland (ECP.NL) bekend.[65] Op een internationaal nievau kan worden gewezen op de criteria opgesteld door TrustUK voor de accreditering van organisaties die via internet goederen of diensten aanbieden. Deze organisaties dienen een gedragscode te hanteren. In art. 6 van de accreditatiecriteria van TrustUK is aangegeven aan welke eisen met betrekking tot de bescherming van persoonsgegevens de gedragscode van een organisatie moet voldoen, wil deze worden geaccrediteerd door TrustUK.[66] Een vergelijkbaar Nederlands initiatief is *Webtrader* van de Nederlandse Consumentenbond. Een Nederlandse aanbieder van elektronische diensten die het webtrader-logo voert, zegt toe zich te houden aan de door de Consumentenbond geformuleerde voorwaarden voor elektronisch zakendoen. Belangrijk bij deze voorwaarden is de omgang met persoonsgegevens, de keuzevrijheid voor consumenten, de eenvoudige prijs-kwaliteit vergelijking en de transparantie van de transactievoorwaarden.[67] Per 1 januari 2002 is de Consumentenbond met dit initiatief gestopt.[68] Naast het voornoemde initiatief heeft de Consumentenbond ook Privacy-regels voor internetbedrijven gepubliceerd.[69]

Vergelijkbaar met het systeem van een gedragscode waaraan aanbieders zich conformeren en daarmee een keurmerk mogen voeren, is het initiatief van de het kwaliteitszegel voor privacyverklaringen (Privacy Policy of Privacy Statement). In een dergelijk document dat veelal via een huperlink op de hoofdpagina van de aanbieder beschikbaar is, geeft deze aan hoe hij omgaat met persoonsgegevens van de bezoeker van de website. Het gebruik van dergelijke verklaringen komt vanuit de Verenigde Staten, waar ze onder druk van consumentenorganisaties en de Federal Trade Commission zijn geïnitieerd. Deze constateerden dat heimelijk verzamelen van persoonsgegevens door eigenaars van websites een grote vlucht nam en hoopten met de verklaringen meer transparantie te bewerkstelligen. Privacy Policies kenmerken zich veelal door eenzelfde aanpak. Er wordt informatie gegevens over de verzameling van de gegevens, het gebruik dat er van wordt gemaakt, mogelijkheden tot wijziging en correctie, verstrekking aan derden, beveiliging, bescherming van kinderen en ook wel technische informatie over cookies en het gebruik daarvan. In ieder geval bij Amerikaanse aanbieders is veelal voorzien in een regeling voor geschillenbeslechting door de eigen organisatie of door een derde, zoals het bekende TRUSTe.
De non-profit organisatie TRUSTe heeft een belangrijke bijdrage geleverd aan het privacybesef in de Amerikaanse on-line wereld en aan het bevorderen van de ontwikkeling van Provicy Policies en vooral ook de naleving daarvan. De doelstelling van de organisatie is het ontwikkelen en bevorderen

---

[63] Artikel 29 Groep, Advies 1/98/WP 11, Platform for Privacy Preferences (P3P) en de Open Profiling Standard (OPS)
[64] Zie: <http://www.w3.org/P3P/p3pfaq.html>
[65] In oktober 2002 verscheen een nieuwe versie van deze Code. Beschikbaar via: <http://www.ecp.nl>
[66] TrustUK *Accreditation criteria*, te vinden op www.trustuk.org.uk
[67] <http://www.webtrader.nl>
[68] Een ander dergelijk initiatief, thuiswinkel waarborg <http://www.thuiswinkel.org>, blijft na 2001 wel bestaan.
[69] Zie: <http://www.consumentenbond.nl>

van gebruikersvertrouwen in het Internet een de bevordering van de ontwikkeling van het Internet. Er is een TRUSTe kwaliteitszegel ontwikkeld, waar bedrijven en organisaties voor kunnen opteren. Hun Privacy Policy moet dan aan bepaalde kwaliteitseisen voldoen, die door middel van externe privacy audits worden gecontroleerd.[70]
Om het gebruik van de Privacy Policy te stimuleren heeft de OECD een hulpmiddel ontwikkeld waarmee bedrijven en organisaties een Privacy Policy kunnen ontwerpen. Het is toepasselijk van de naam *Privacy Statement Generator* voorzien. Het is vooral een hulpmiddel om instanties 'op te voeden' en als eerste aanzet om de interne privacypraktijken te evalueren en het privacybeleid te ontwikkelen.[71] Sinds enige tijd doen ook in Nederland Privacy Policies en Privacy Statements opgang. De vraag doet zich voor wat de status is van dergelijke verklaringen. In Nederland hebben wij immers, anders dan in de Verenigde Staten, een wettelijk kader voor de on-line verwerking van persoonsgegevens. Een Privacy Statement (privacy-verklaring) kan uiteraard nooit de wettelijke verplichtingen buiten spel zetten. Wel kan het een belangrijk instrument zijn bij het vormgeven van de informatieplichten uit artikel 33 Wbp. Dat daarmee transparantie wordt bewerkstelligd inzake hetgeen daadwerkelijk met de persoonsgegevens wordt gedaan, blijkt niet het geval. In de studie van het College Bescherming Persoonsgegevens, getiteld "Klant in het web" wordt geconstateerd dat in de algemene voorwaarden soms andere doelstellingen worden geformuleerd dan in de opgestelde privacy-verklaring.[72] Aanbieders van e-commerce diensten zullen er dus goed op moeten letten of de opgestelde en gepubliceerde privacy-verklaring overeenstemt met hetgeen is bepaald in de algemene voorwaarden en de eventuele aanmelding bij het College. Ook dient het te worden afgestemd met andere uitingen zoals die in brochures of reclamefolders.
We wijzen hier nog op de bevindingen van Consumers International in een rapport uit januari 2001.[73] Uit dit vergelijkend onderzoek naar het privacybeleid van een groot aantal websites in de Verenigde Staten en Europa, bleek dat ondanks de strenge wetgeving in Europa de websites hier geen betere informatie geven dan in de VS en dat de consument ook niet meer keuze heeft met betrekking tot de verwerking van zijn persoonsgegevens.

Een laatste instrument van zelfregulering is de overeenkomst. Opvallend is de grote aandacht die er recentelijk is voor het contractuele instrument bij het vormgeven van privacybescherming. In de Europese privacyrichtlijn wordt de overeenkomst expliciet genoemd als een mogelijkheid om te voorzien in een adequaat beschermingsniveau bij grensoverschrijdend verkeer van persoonsgegevens. Inmiddels zijn door diverse internationale organisaties projecten gestart waarin gewerkt wordt aan model contracten. Een dergelijke contractuele bepaling komen we bijvoorbeeld tegen in de Model EDI-overeenkomst van de Europese Commissie[56] en de concept *Uniform Rules for Electronic Trade and Settlement* (URETS)[74] van de Internationale Kamer van Koophandel (ICC).[57] Beide bevatten bepalingen die aanbieders van e-commerce door verwijzing kunnen incorporeren in hun overeenkomst. Belangrijk voordeel van het Internet is dat het als het ware de optimale randvoorwaarden schept voor een contractuele afhandeling van rechten en plichten. Het is niet toevallig dat waar een koper in de fysieke wereld veelal nooit een (uitgewerkt) contract voor zijn neus krijgt, hij op het Internet wordt geconfronteerd met een diversiteit aan zogenaamde 'mouse-click' of 'click-through' overeenkomsten.[75]
De opmars van het contract valt te verklaren uit de kenmerken van het Internet: rechtstreekse relaties tussen aanbieders en gebruikers, eenvoud, interactiviteit en flexibiliteit. Bovendien lijkt het Internet de

[70] Zie voor meer informatie: <http://www.truste.org>
[71] Zie: <http://www.oecd.org>
[72] *Klant in het web, Privacywaarborgen voor Internettoegang*, Achtergrondstudies en verkenningen 17, juni 2000, paragraaf 6.3.2 te downloaden van: <http://www.registratiekamer.nl>
[73] Privacy@net, a comparative study of consumer privacy on the internet: <http://www.consumersinternational.org/news/pressreleases/privreport.pdf>
[74] Art. 2.4.3 van de URETS bepaalt dat iedere partij de regels voor de bescherming van persoonsgegevens zoals nader uitgewerkt in haar nationale wetgeving, zal naleven.
[75] Bij dergelijke overeenkomsten aanvaardt de gebruiker met een druk op de muisknop de voorwaarden dan wel klikt door de voorwaarden heen. Door de eenvoud waarmee informatie op het Internet kan worden geplaatst worden en vervolgens ook door gebruikers (moet) worden aanvaard, plaatsen informatie- en dienstenaanbieder op het Internet alles wat met rechten en plichten te maken heeft op hun site.

geografische afstand voorbij, hetgeen betekent dat partijen veel van de verschillen tussen de wereldwijde rechtsstelsel wensen te 'wegcontracteren'.[76] Daarbij is de grensoverschrijdende context in combinatie met de vooralsnog terughoudende opstelling van de overheid waar het de regulering van handelingen en relaties betreft een uitstekende voedingsbodem voor het experimenteren met contractuele afspraken tussen partijen. Dat de relaties op het Internet in toenemende mate door het contactenrecht worden beheerst, heeft ook zijn keerzijde. Op het terrein van de privacybescherming stellen we vast dat via het contract het gebruik van persoonsgegevens vogelvrij wordt verklaard. Via een clausule in de algemene voorwaarden van de meerderheid van de gratis Internetproviders doen gebruikers afstand van hun privacy en mogen de persoonsgegevens worden gebruikt voor marketingdoeleinden. Kortom, het gevaar bestaat dat fundamentele vrijheden zoals de *free flow of information* en privacy op de tocht komen te staan bij een te ongebreidelde opmars van het contract.

Uit het voorgaande blijkt wel dat inmiddels een scala aan zelfreguleringsinstrumenten is ontwikkeld om privacybescherming op het Web en meer specifiek ook bij elektronische handel verder te stimuleren en te ondersteunen. Behalve de voornoemde keurmerken, generators en modelcontracten wordt ook via andere wegen door de diverse internationale organisaties en belangenverenigingen getracht invloed uit te oefenen. Gewezen kan worden op de Raad van Europa die middels Aanbeveling R (99)5 richtlijnen heeft gepubliceerd voor de bescherming van personen met betrekking tot de verzameling en de verwerking van persoonsgegevens op informatiesnelwegen.[58] Deze aanbeveling bevat zowel richtlijnen voor de gebruikers van internet als voor de aanbieders van internetdiensten. De Raad van Europa roept aanbieders van diensten op om goede procedures en technologieën te gebruiken om persoonsgegevens van gebruikers te beschermen. Voorts verzoekt hij hen om gebruikers te informeren over de risico's verbonden aan het verstrekken van persoonsgegeven via internet, en de mogelijkheden om deze risico's te beperken. Daarnaast bevat de aanbeveling een aantal gedragsregels met betrekking tot de verwerking van persoonsgegevens door aanbieders van internetdiensten. Gewezen kan ook worden op het document *A Global Action Plan for Electronic Commerce*, van de Alliance for Global Business.[59] Hierin wordt door het bedrijfsleven een aantal beleidsbeginselen voor electronic commerce genoemd. Beleidsbeginsel 8 luidt als volgt: 'The protection of users, in particular with regard to privacy, confidentiality, anonymity, and control content should be pursued through policies driven by choice, individual empowerment, industry-led solutions. It will be in accordance with applicable laws.' Vervolgens wordt in beleidsbeginsel 9 het volgende bepaald: 'Business should make available to consumers and, where appropriate, business users the means to exercise choice with respect to privacy, confidentiality, content control and, under appropriate circumstances, anonymity.' Daarna worden in dit document de verschillende beleidsbeginselen nader uitgewerkt. In hoofdstuk 3 wordt ingegaan op de bescherming van persoonsgegevens. Daarin wordt aandacht besteed aan de acties en overwegingen van het internationale bedrijfsleven op dit terrein. Tevens wordt een overzicht gegeven van de acties die van de overheid worden verwacht, om de bescherming van persoonsgegevens in het kader van elektronische handel in het algemeen en internet in het bijzonder op zodanige wijze in regelgeving gestalte te geven dat zij geen belemmering vormt voor het (grensoverschrijdend) gebruik van elektronische handel.

[76] Dat wil zeggen dat partijen – gegeven het in principe in vele rechtsstelsels gehanteerde uitgangspunt van contractsvrijheid - in feite hun eigen regels kunnen stellen en daarmee de door de diverse nationale overheden gestelde regels ter zijde kunnen stellen. Dit geldt overigens niet voor de bepalingen van dwingend recht.