Handhaving van intellectuele eigendomsrechten

van Eechoud, M.M.M.; van Daalen, O.

Publication date
2002

Published in
ICT regulering anno 2002. Reis om de wereld in acht landen en zestien onderwerpen.

ICT-regulering anno 2002

Reis om de wereld in acht landen en zestien onderwerpen

Bert-Jaap Koops
Ot van Daalen
Marcel Dellebeke
Mireille van Eechoud
Bastiaan Garnier
Simone van der Hof
Eric Kemmeren
Chris Nicoll
Gert-Jan van Norden
Sjaak Nouwt
Corien Prins
Maurice Schellekens
Ton Schudelaro
Arno Smits
Berend de Vries

Centrum voor Recht, Bestuur en Informatisering
Katholieke Universiteit Brabant
juni 2002

Inhoudsopgave

Samenvatting

Dit rapport geeft een overzicht van de stand van zaken rond ICT-regulering in acht landen, voorzover deze – in ruime zin – van belang is voor elektronische handel. Het doel is de internationale positie van Nederland op dit gebied in kaart te brengen. De nadruk ligt daarbij op recente ontwikkelingen.[1]
Het rapport is geschreven in opdracht van het Ministerie van Economische Zaken ten behoeve van de *Internationale ICT-toets 2002*. Omwille van de vergelijkbaarheid met de *Internationale ICT-toets 2000* is de indeling van dit rapport gebaseerd op die welke daarin is gehanteerd.

1. Totaalbeeld

ICT-regulering beslaat een breed terrein. De zestien onderwerpen die voor dit rapport zijn onderzocht, hangen alle – direct of indirect – samen met elektronische handel, maar zijn van uiteenlopende aard. Ook de onderzochte landen, hoewel alle geïndustrialiseerd, zijn divers: er bestaan grote verschillen tussen Europa en de VS, zowel in cultuur als in beleidsopvattingen, en ook binnen de EU bestaat diversiteit aan rechtsstelsels (*common law* en *civil law*), culturele opvattingen en reguleringstradities. Japan verschilt op tal van punten van zowel de VS als van Europa. De diversiteit aan onderwerpen, maar vooral ook de diversiteit aan landen en rechtsstelsels, maken het moeilijk om uitspraken te doen over ICT-regulering in algemene zin. Het maken van vergelijkingen is slechts mogelijk als onderzoeksresultaten in verband worden gebracht met de verschillende rechtsstelsels – iets waarvoor in dit onderzoek geen ruimte was. Om deze redenen dient dit totaalbeeld te worden beschouwd als een indicatie van de belangrijkste bevindingen van het onderzoek, waarbij bevindingen tentatief met elkaar in verband worden gebracht.

1.1. Algemeen

internationale afstemming
Een belangrijk deel van ICT-regulering wordt internationaal voorbereid of aangestuurd. Dit betreft bijvoorbeeld onderwerpen met een sterke financieel-economische inslag, zoals auteursrecht en fiscale aspecten van e-handel, en onderwerpen waarbij het scheppen van rechtszekerheid voorop staat als noodzakelijke voorwaarde voor het ontstaan van grensoverschrijdende e-handel, zoals de juridische status van elektronische contracten en handtekeningen. Ook op andere, cultureel gevoeliger, punten vindt echter in belangrijke mate internationale afstemming plaats in verband met rechtshandhaving, zoals de bestrijding van computercriminaliteit en de export van cryptografie.
Over de brede linie blijkt echter op wereldwijde schaal slechts weinig overeenstemming te bereiken. Voor veel onderwerpen lopen de meningen en tradities te zeer uiteen, zodat overeenstemming slechts in kleiner verband valt te bereiken, bijvoorbeeld binnen de Europese Unie. In de EU zijn voor onderwerpen als privacy en spam, die in de VS volledig aan zelfregulering worden toevertrouwd, geharmoniseerde regelingen vastgesteld. Vrijwel alle onderwerpen uit deze studie worden in de EU op gemeenschapsniveau aangepakt; zelfs voor onderwerpen die niet tot de bevoegdheid van de EG behoren (zoals strafrecht) komen steeds meer gemeenschappelijke regelingen.
Dat neemt niet weg dat ook op EU-niveau harmonisatie in de praktijk niet overal wordt bereikt. Richtlijnen bevatten noodzakelijkerwijs herhaaldelijk compromissen die op nationaal niveau verschillend worden uitgelegd; soms ook wordt regeling bewust overgelaten aan de lidstaten. De implementatie van richtlijnen blijkt dan ook herhaaldelijk verschillend uit te pakken. Hoewel dit deels veroorzaakt zal worden door de verschillen in rechtsstelsels, ontstaat soms de indruk dat lidstaten – bewust of onbewust – kiezen voor materieel verschillende implementatie. De strafrechtelijke aansprakelijkheid van ISP's, het toezicht op niet-gekwalificeerde

[1] Zie Landwell 2000 en Internationale ICT-toets 2000 voor een overzicht van de stand van zaken rond ICT-regulering in 2000.

certificatieaanbieders en de inwisselplicht voor e-betaalsystemen zijn daar voorbeelden van. In grote lijnen wordt de regeling van de onderscheiden onderwerpen dan wel geharmoniseerd, maar op bepaalde details lijkt harmonisatie achterwege te blijven.
De internationale initiatieven zoals hier geschetst beogen grotendeels om nationale reguleringen op elkaar af te stemmen. Harmonisatie of approximatie van regulering maakt immers grensoverschrijdend handelsverkeer eenvoudiger. Een aspect dat echter minder voortvarend blijkt te kunnen worden aangepakt is het afstemmen van visies op rechtsmacht. Op strafrechtelijk niveau is de vraag wanneer een staat rechtsmacht kan uitoefenen (bijvoorbeeld als via het Internet 'elders' wordt opgespoord) niet beantwoord bij het Cybercrime-verdrag. Ook op civielrechtelijk niveau lijken de visies over de reikwijdte van rechtsmacht uiteen te lopen; binnen de Haagse Conferentie bleek over jurisdictie in relatie tot het Internet vooralsnog geen overeenstemming te bereiken.

zelf-, co- en overheidsregulering
Hoewel de meeste landen uit dit onderzoek een duidelijke voorkeur zeggen te hebben voor zelfregulering (Frankrijk is een uitzondering), valt op dat bij bijna alle onderwerpen overheidsregulering de boventoon voert. In de EU verschijnen grote hoeveelheden richtlijnen, maar ook in de VS en Canada bestaat op veel terreinen wetgeving. Deze wetgeving lijkt niet in eerste instantie het gevolg van een inzicht dat zelfregulering op de desbetreffende onderwerpen tekortschiet, maar eerder van een behoefte aan het scheppen van rechtszekerheid of het nationaal of federaal willen harmoniseren van regelgeving. Daardoor lijkt de bij wetgevers veelgehoorde voorkeur voor zelfregulering eerder een illusie dan een daadwerkelijke praktijk.
Soms wordt zelfregulering ingekaderd in overheidsregulering. Deze benadering wordt vaak aangeduid met de term 'co-regulering'. Het duidelijkste voorbeeld hiervan is de vorm van toezicht op Trusted Third Parties die Nederland en het Verenigd Koninkrijk hebben gekozen. In vergelijking met de situatie van twee jaar geleden, lijken er echter niet veel meer gevallen van co-regulering te zijn ontstaan, wanneer men co-regulering opvat als een vorm van regulering waarbij naleving kan worden afgedwongen.[2] Een andere vorm van co-regulering is het betrekken door overheden van 'de markt' bij het nader vormgeven of invullen van regelgeving; deze vorm lijkt wel vaker voor te komen. Bij het inrichten van de 'elektronische overheid', bijvoorbeeld in het faciliteren van elektronische communicatie met de overheid, blijkt een duidelijke rol te worden toebedeeld aan marktpartijen.

Ondanks de vrijwel alomtegenwoordige regelgevingsijver, blijft er tussen de onderzochte landen wel een verschil bestaan in de mate van zelfregulering die wordt toegestaan. Vooral in de VS worden enkele onderwerpen voor een belangrijk deel aan zelfregulering overgelaten die de EU heeft gereguleerd. Het gaat om onderwerpen als privacy en ongevraagde e-reclame (spam), waarbij de balans tussen vrije markt en rechtsbescherming in de VS grotendeels doorslaat naar het eerste en in de EU naar het tweede. Daar staat tegenover dat de VS op enkele andere punten (elektronisch contracteren door *agents* en de procedure om mogelijk onrechtmatig materiaal van het Internet te verwijderen) een bredere regeling kent dan de EU, wellicht omdat de praktijk hier in de VS een roep om rechtszekerheid kent die in de EU nog weinig wordt gehoord.
Overigens zijn ook binnen de EU duidelijke verschillen zichtbaar in de mate van zelfregulering: Frankrijk en in mindere mate Duitsland tenderen meer naar een primaire voorkeur voor overheidsregulering, terwijl het VK en Nederland (zeggen) een voorkeur (te) hebben voor zelfregulering. Bij de onderwerpen waarbij zelfregulering een rol kan spelen, heeft de VK in de praktijk wellicht nog iets meer een 'light touch'-benadering dan Nederland, bijvoorbeeld door het ongereguleerd laten van ongevraagde e-reclame.

Slechts op enkele punten lijken verschuivingen zichtbaar sinds twee jaar geleden. In de VS staat de onverkorte voorkeur voor zelfregulering bij privacy ter discussie, en in de EU is recentelijk het grotendeels overlaten aan de markt van spamregulering (via een opt-outsysteem) losgelaten ten behoeve van consumentenbescherming (via een verplicht opt-insysteem).

[2] Zoals gehanteerd in Landwell 2000, p. 8; dit rapport concludeerde reeds dat TTP's het onderwerp was waarbij co-regulering het dichtst benaderd werd.

De verschuivingen op deze twee onderwerpen lijken zich vooral te laten verklaren door het inzicht in de (non-)effectiviteit van zelfregulering. Op het gebied van spam hebben de opt-outsystemen nauwelijks effect gehad om dit fenomeen te beteugelen. Ook de Safe Harbor Principles (die voor bedrijven in de VS een EU-rechtbestendige haven voor persoonsgegevens moeten creëren) lijken in de praktijk (nog) niet echt te werken. Er zijn evenwel geen aanwijzingen dat dergelijke bevindingen hebben geleid tot een veranderd inzicht in de algemene rol van zelfregulering.

Een ander aspect dat naar voren komt in het onderzoek is de rol die overheden spelen bij de actieve voorlichting aan burgers over ICT-regulering. Voor de effectiviteit van regulering die beoogt consumenten of burgers te beschermen is het van belang dat deze kennis en inzicht hebben in hun rechten en plichten. Op enkele terreinen blijken sommige overheden dan ook voorlichtingscampagnes te (willen gaan) voeren. Men ziet dit met name op het gebied van veilig Internetgebruik (Nederland, Canada, Duitsland, VS), elektronische handtekeningen (Canada, Japan) en privacy (Duitsland, Frankrijk, Nederland). Het gaat echter om enkele onderwerpen, die elk bovendien in lang niet alle landen worden opgepakt; over het algemeen lijken overheden zich niet actief in te spannen om via het Internet mensen bewust te maken van (de rechten en plichten van) ICT-regulering. De taak van voorlichting wordt voor een deel overgenomen door private instanties, zoals burgerrechtenorganisaties en brancheverenigingen. In het algemeen lijkt het erop dat overheden vooralsnog de publicatiemogelijkheden van nieuwe media niet aangrijpen om een actief voorlichtingsbeleid over de complexe ICT-regulering te voeren.

1.2. Positie van de diverse landen

Het globale beeld dat rijst uit het onderzoek is dat de stand van zaken in de vijf onderzochte EU-lidstaten over het algemeen onderling niet wezenlijk verschilt. ICT-regulering in de VS wijkt op diverse punten af van de situatie in Europa, terwijl Canada nu eens dichter bij de VS en dan weer dichter bij Europa staat. Japan kent voor een deel vergelijkbare regulering, maar voor een ander deel ook niet.

Meer in detail blijken binnen de EU wel verschillen te bestaan, niet alleen in de mate van zelf- of co-regulering (zie boven) maar ook in de aanpak van ICT-regulering. Nederland was het eerste land van de vijf onderzochte landen met een overkoepelende analyse van en visie op ICT-regulering (met de Nota WES uit 1998 en de nota IRIM uit 2000); meer recent heeft het VK iets soortgelijks, zij het minder uitgebreid, gedaan (de *E-Policy Principles* en de coördinatie door de e-Minister en e-Envoy), terwijl Frankrijk met het *Projet de loi sur la société de l'information* uit 2001 een poging heeft gedaan tot een meer overkoepelende regulering (die vooralsnog is gestrand door de verkiezingen). Nederland lijkt daarom meer dan de andere landen te hebben nagedacht over een integrale visie op ICT-regulering, hetgeen ook geldt in vergelijking met de VS, Canada en Japan. Daar staat tegenover dat de concrete regulering in Nederland vaak later tot stand komt dan in andere EU-lidstaten. Nederland loopt achter bij de implementatie van veel ICT-gerelateerde richtlijnen ten opzichte van de andere onderzochte landen (bescherming persoonsgegevens, elektronische handel, elektronische handtekeningen, elektronisch geld, auteursrecht in de informatiemaatschappij). Andere lidstaten (zoals het VK bij de e-handelrichtlijn) kiezen juist bewust voor snelle implementatie om tijdig rechtszekerheid te bieden en daarmee een aantrekkelijk klimaat voor nieuwe e-handelaars te scheppen.

Waar Nederland in de EU opvalt door een integrale visie en vaak trage wetgeving, valt verder vooral het VK op als de lidstaat waar een klimaat met een 'light regulatory touch' heerst; dit blijkt bijvoorbeeld uit het besluit de wettelijke bepalingen over toezicht op cryptografiedienstaanbieders vooralsnog niet van kracht te laten worden wegens het bestaan van een adequate zelfregulering. De lichte toets geldt evenwel met name voor direct e-handelgerelateerde regulering; op het punt van strafrechtelijke handhaving en terrorismebestrijding lijkt het VK juist repressiever dan de andere lidstaten (met uitzondering van Frankrijk).

De positie van de VS verschilt in twee opzichten van die van de EU, die mede samenhangen met het verschil in inzicht van beiden in de mogelijkheden van zelfregulering, maar ook in rechtsstelsels. Enerzijds laat de VS regulering op sommige terreinen (zoals privacy en spam) grotendeels over aan de markt, waar de EU rechtsbescherming laat prevaleren ten faveure van

overheidsregulering; soms ook, zoals bij elektronische handtekeningen, kiest de VS voor een globale kaderregeling, waar de EU ten behoeve van rechtszekerheid ook een meer gedetailleerde regeling heeft. Anderzijds kent de VS op andere terreinen, vaak samenhangend met een behoefte bij het bedrijfsleven aan rechtszekerheid, juist een meer uitgewerkte of bredere regulering dan de EU; het reguleringskader voor elektronische contracten en e-betaalsystemen zijn daar voorbeelden van. Tevens lijkt de VS (vermoedelijk omdat de technologische ontwikkeling daar iets voorloopt op die in de EU) aandacht te hebben voor nieuwe ICT-ontwikkelingen (zoals *agents*) die in de EU-regulering nog niet zijn doorgedrongen; ook de aandacht voor nieuwe bedreigingen (zoals identiteitsfraude, de privacy van kinderen op het Internet en het toezicht op aftappen van Internetverkeer) lijkt in de VS groter dan in de EU. Al deze verschillen nemen overigens niet weg dat op bepaalde terreinen de aanpak van de VS en van de EU wel overeenkomt, terwijl er ook wel wederzijdse pogingen worden ondernomen om dichter bij elkaar te komen.
De positie van Canada weerspiegelt de traditionele verbondenheid van dit land met zowel de VS als Europa. Op sommige terreinen overheerst de marktwerking en is de ICT-regulering vergelijkbaar met die in de VS (zoals e-handtekeningen en spam); op andere terreinen is evenwel de rechtsbescherming belangrijker en lijkt de regulering meer op die in de EU (zoals privacy).
De positie van Japan lijkt over het algemeen volgend te zijn. Op enkele terreinen voert Japan wetgeving door in navolging van internationale afspraken (zoals bij auteursrecht, cryptografie) of in verband met internationale ontwikkelingen (zoals aansprakelijkheid van Internetaanbieders, computercriminaliteit). Bepaalde onderwerpen, zoals regulering van elektronische overeenkomsten, e-betalen en cryptografie, lijken in Japan geen grote rol te spelen, en in het onderzoek zijn geen opvallende Japanse initiatieven of innovatieve standpunten op het gebied van ICT-regulering aangetroffen. De situatie van Japan is overigens vergelijkbaar met die van Zweden, waar evenmin opvallende initiatieven zijn aangetroffen. Hieraan kunnen evenwel geen scherpe conclusies worden verbonden, aangezien het onderzoek voor deze landen beperkt was tot vertaald materiaal.
Concluderend kan men stellen dat de positie van Nederland op ICT-reguleringsgebied internationaal gezien grotendeels vergelijkbaar is met die van de andere EU-lidstaten en op diverse vlakken afwijkt – soms meer, soms minder – van die van de VS. Nederland valt internationaal vooral op door het nadenken over een integrale visie en een vaak wat trage wetgeving. Enkele nieuwe onderwerpen (zoals *agents*, identiteitsfraude, privacy van kinderen op het Internet en toezicht op Internettaps) staan in andere landen wel maar in Nederland nog nauwelijks op de agenda.

2. Toerusten wet- en regelgeving

2.1. Elektronische contracten

De Europese richtlijn Elektronische handel vereist dat elektronische overeenkomsten – enkele uitzondering daargelaten – door de lidstaten van de Europese Unie uitdrukkelijk worden erkend. De meeste lidstaten hebben momenteel wetten (Duitsland, Frankrijk) of wetsvoorstellen (Nederland) ter implementatie van dit gedeelte van de richtlijn, waarin dit vereiste is opgenomen; voor enkele landen, zoals Zweden, kan expliciete implementatie achterwege blijven vanwege het bewijsstelsel.
Ook in de VS en Canada bestaat (model)wetgeving voor de staten waarin elektronische overeenkomsten uitdrukkelijk als rechtsgeldige vorm van contracteren worden erkend. Daarbij kunnen er evenwel uitzonderingen worden gemaakt.

Een duidelijk verschil tussen beide continenten is de aandacht voor geheel nieuwe vormen van e-contracteren – namelijk het gebruik van *electronic agents*. Deze worden juridisch erkend in Noord-Amerika: de Verenigde Staten en Canada zijn in dit opzicht duidelijk verder. De Verenigde Staten springt er voorts uit met de UCITA; deze modelwet bevat een volledige materieelrechtelijke regeling van transacties met betrekking tot informatieproducten. De Europese richtlijn E-handel bevat weliswaar ook enkele bepalingen van materieel recht, maar deze zijn betrekkelijk summier vergeleken bij de UCITA.

Conclusie: elektronische contracten kunnen inmiddels overal rechtsgeldig worden afgesloten. De VS en Canada zijn evenwel, met een volledige materieelrechtelijke regeling en aandacht voor *agents*, verder dan Europa in het algemeen regelen van elektronische contracten.

2.2. Aansprakelijkheid van Internetaanbieders

In Europa wordt de regeling van aansprakelijkheid van Internetaanbieders geharmoniseerd door de richtlijn inzake elektronische handel. Hierdoor worden toegangs-, *caching*- en *hosting*aanbieders onder bepaalde voorwaarden gevrijwaard van aansprakelijkheid. De meeste van de onderzochte implementaties (Duitsland, Nederland, Verenigd Koninkrijk en Zweden) nemen bepalingen in hun wetgeving op die tekstueel overeenstemmen met of dicht aanliggen tegen de regeling in de richtlijn; Frankrijk heeft bij de implementatie een duidelijke vertaalslag naar het Franse recht gemaakt.
In een aantal van de onderzochte implementaties, wordt voor de strafrechtelijke aansprakelijkheid een andere benadering gekozen dan voor de civiele aansprakelijkheid. Deze implementaties zijn ook aanzienlijk minder homogeen. Zo staat in de Zweedse regeling het opzet van de Internetaanbieder centraal en in Nederland het 'bevel van de officier van justitie'. Frankrijk heeft de bestaande strafrechtelijke vrijstelling met betrekking tot *hosting*activiteiten geschrapt. De Duitse implementatie geldt zonder onderscheid voor zowel het strafrecht als het civiele recht. Van echte harmonisatie op het gebied van het strafrecht kan derhalve niet gesproken worden.
Ook in de niet-Europese landen worden aparte regels voor de aansprakelijkheid van ISP's opgesteld. Een opvallend verschil tussen de Europese en de Amerikaanse benadering van de aansprakelijkheid van Internetaanbieders is dat Europa gekozen heeft voor een integrale, algemene regeling die voor alle soorten onrechtmatige informatie en activiteiten geldt. De VS en Canada kennen daarentegen meer een ad hoc-benadering, waarbij verschillende regelingen naast elkaar bestaan, die ieder slechts op bepaalde onrechtmatigheden zien. Daar staat tegenover dat de VS, in tegenstelling tot de EU, met de *notice-and-take-down*-regeling wel een wettelijke procedure heeft geschapen voor het (al dan niet) verwijderen van mogelijk inbreukmakend materiaal van het Internet, hetgeen de rechtszekerheid voor alle partijen ten goede lijkt te komen.
De benadering van de Japanse regeling lijkt meer op de Europese dan op de Amerikaanse aanpak.

Conclusie: Nederland volgt met de meeste EU-lidstaten de Europese richtlijn E-handel op het gebied van aansprakelijkheid van Internetaanbieders. De civiele aansprakelijkheid wordt daardoor geharmoniseerd, de strafrechtelijke echter niet. De Europese landen en Japan hebben een bredere regeling dan de VS en Canada, die slechts voor bepaalde soorten onrechtmatige handelingen de aansprakelijkheid regelen, maar Europa kent niet zoals de VS een wettelijke procedure voor verwijdering van mogelijk onrechtmatig materiaal.

2.3. Elektronische overheid

De elektronische overheid is sterk in opkomst. In alle landen zijn vele initiatieven op dit vlak, waaronder het stimuleren en regelen van elektronische communicatie met de overheid; alleen in Japan lijkt dit onderwerp pas sinds kort een rol te spelen. In Nederland worden diverse plannen uitgewerkt die meer omvatten dan uitsluitend het automatiseren van traditionele processen, maar waarin ICT wordt ingezet om tot een vernieuwing van het functioneren van de overheid te komen (zoals authentieke registraties, eenmalige gegevensverstrekking). Nederland kent nog geen concrete wetgeving voor elektronische afhandeling van rechtspraak, zoals dit bijvoorbeeld op statelijk niveau in de VS wel het geval is. Specifiek op het terrein van B2G is er in diverse landen aandacht voor e-voorzieningen om de administratieve lasten voor het bedrijfsleven terug te dringen, 24/7-bereikbaarheid, op maat gesneden informatie, en de betrouwbaarheid van de elektronische communicatie.
In diverse landen worden de ontwikkelingen rondom de elektronische overheid niet langer in een isolement bezien, maar heeft men aandacht voor de interactie tussen elektronische handel en

elektronische overheid. Eerdere ervaringen bij (de regulering van) elektronische handel kunnen worden benut voor het vormgeven van de elektronische overheid; in het VK wordt van beleidsmakers zelfs gevraagd hieraan expliciet aandacht te besteden. Verder wordt ook op het terrein van de elektronische overheid steeds meer over de landsgrenzen heen gekeken en waar mogelijk samengewerkt. Ook op Europees niveau wordt hier expliciet de aandacht voor gevraagd. Tot slot is van belang dat de beleidsplannen voor de elektronische overheid onderstrepen dat ook de private sector hierbij een actieve rol moet spelen en concreet bij de initiatieven moet worden betrokken. Met name binnen de uitwerking van het Europese *eEurope*-initiatief is dit naar voren gebracht.

Conclusie: alle landen zijn druk bezig de elektronische communicatie met de overheid vorm te geven, mede gericht op het verbeteren van de communicatie van bedrijven met de overheid. Hierbij is er aandacht voor de ervaring van e-handelregulering, internationale samenwerking en medewerking door de private sector. Nederland bevindt zich op dit gebied zeker niet in de achterhoede, maar behoort ook niet tot de internationale koplopers.

3. Bieden van rechtszekerheid

3.1. Privacy op het Internet

De beleidsinitiatieven op privacygebied in de EU-lidstaten worden nog steeds gedomineerd door de implementatie van de Richtlijn bescherming persoonsgegevens. Nederland heeft deze zeer laat geïmplementeerd, maar ook Frankrijk en Duitsland zijn door de EU aangesproken op verlate implementatie. Wat de inhoud betreft heeft de Nederlandse wetgever gekozen voor een genuanceerdere benadering, waarin de precisering van de richtlijnnormen in de Wbp slechts deels in het wetsvoorstel heeft plaatsgevonden. Nederland lijkt hierin niet fundamenteel af te wijken van andere EU-lidstaten. Opvallend is dat Zweden het plaatsen van persoonsgegevens op het Internet beschouwt als het verstrekken van persoonsgegevens naar derde landen (buiten de EU), omdat die gegevens vandaaruit toegankelijk zijn. Canada heeft minder vergaande federale wetgeving op het gebied van privacy (beperkt tot commerciële situaties), maar kent volgens de EU wel een passend beschermingsniveau. In Japan wordt de sectorale privacywetgeving als te gebrekkig ervaren; een voorstel voor een nieuwe privacywet beoogt betere bescherming van persoonsgegevens te bewerkstelligen, maar de bescherming zal in diverse situaties beperkt zijn. Zelfregulering van privacy op Internet staat nog steeds in de belangstelling. Niettemin zijn er signalen dat overheidsregulering en zelfregulering op dit terrein naar elkaar toe groeien. In de VS, waar zelfregulering van privacybescherming min of meer het uitgangspunt is, heeft dat onder andere geleid tot een aanbeveling van de FTC uit 2000 voor overheidsregulering van privacy en een wetsvoorstel voor de *Hollings Online Personal Privacy Act* in april 2002. Tegelijkertijd heeft de EU gesignaleerd dat de naleving van zelfregulering in de VS door middel van de Safe Harbor Principles nog tekortkomingen vertoont, die vooralsnog als kinderziektes worden beschouwd. De VS is overigens met overheidsregulering van privacy van kinderen op Internet verder dan de Europese landen, waar nog nauwelijks aandacht voor de bijzondere kwetsbaarheid van de privacy van jonge Internetgebruikers.
Diverse organisaties doen aan publieksvoorlichting over privacy op Internet; zo geven de privacytoezichthouders in Duitsland en Frankrijk voorlichting aan burgers over privacybescherming op Internet.

Conclusie: in de EU-landen is de Europese richtlijn bescherming persoonsgegevens in de meeste landen geïmplementeerd. In de VS staat zelfregulering bij privacy nog steeds voorop, maar lijkt enige overheidsregulering ook in zicht te komen. De Safe Harbor Principles die de verschillende benadering tussen EU en VS moeten overbruggen, kennen nog tekortkomingen in de naleving.

3.2. Handhaving IE-rechten

De handhaving van intellectuele-eigendomsrechten op het Internet wordt primair internationaal aangestuurd (TRIPs, WIPO-verdragen). Op Europees niveau gebeurt dit met name door implementatie van de Auteursrechtrichtlijn van 22 mei 2001. Duitsland loopt voorop in de implementatie hiervan; Nederland heeft hierover echter een uitgebreide maatschappelijke consultatie gehouden.
Op internationaal niveau zijn er de nodige initiatieven om producenten van informatiediensten (auteurs, uitvoerend kunstenaars, databankproducenten, omroeporganisaties) adequaat te beschermen in de digitale omgeving, maar het blijkt niet eenvoudig om op wereldwijde schaal overeenstemming te bereiken over de noodzaak en de precieze invulling van die bescherming.
Op nationaal niveau is dan ook te zien dat de toepassing van nieuwe en bestaande regels van intellectueel eigendom in de digitale omgeving geen sinecure is. Met name de ervaringen in de VS tonen aan dat het behouden van een goede balans tussen de belangen van producenten en gebruikers een uitdaging is, evenals het duiden van het economisch belang van nieuwe distributievormen in verband met de bepaling van redelijke gebruiksvergoedingen.

De ontwikkeling van een Europees eenheidsoctrooi vordert maar langzaam. Voor de ICT-sector is het vraagstuk van bescherming van computergerelateerde uitvindingen (programmatuur) en bedrijfsmethodes zeer relevant. Of en onder welke voorwaarden dergelijke bescherming een bijdrage levert aan innovatie en gezonde concurrentie is echter omstreden, hetgeen naar verwachting de aanname van de door de Europese Commissie voorgestelde Richtlijn inzake softwareoctrooien niet zal bespoedigen. In Japan is een softwareoctrooi wel mogelijk, evenals in de VS. In dat laatste land zijn ook bedrijfsmethoden octrooieerbaar; er gaan daar echter stemmen op om de ruime octrooieerbaarheid van bedrijfsmethoden in te perken.

Conclusie: de handhaving van IE-rechten op het Internet wordt primair internationaal aangestuurd, maar blijkt in de nationale uitwerking niet eenvoudig toepasbaar op nieuwe ontwikkelingen. In de EU bestaan minder mogelijkheden dan in de VS en Japan een octrooi op programmatuur te verkrijgen.

3.3. Computercriminaliteit

De laatste twee jaar hebben individuele staten weinig activiteiten ondernomen op het gebied van wetgeving van computercriminaliteit, met name omdat alle aandacht was gericht op de ontwikkeling van het Cybercrime-verdrag van de Raad van Europa, dat eind 2001 tot stand kwam. Waar handhaving van computercriminaliteitswetgeving tot nu toe voor een belangrijk deel een nationale aangelegenheid was van individuele landen, ligt er met het Cybercrime-verdrag de mogelijkheid om grensoverschrijdende computercriminaliteit aan te pakken. De approximatie van materiële bepalingen (waardoor aan het vereiste van dubbele strafbaarheid meestal zal worden voldaan) en de rechtshulpbepalingen, alsmede de oprichting van een 24/7-netwerk, betekenen een belangrijke stap voorwaarts in de handhaving van computercriminaliteitswetgeving op een internationaal niveau.
De zegeningen van het Cybercrime-verdrag moeten echter ook niet worden overschat. Voor uitingsdelicten is bijvoorbeeld geen overeenstemming bereikt, met uitzondering van kinderporno. De belangrijkste beperking is misschien dat op het vlak van rechtsmacht nauwelijks vooruitgang is geboekt: staten houden onverkort vast aan nationale soevereiniteit, voor positieve rechtsmachtconflicten (die zich bij computercriminaliteit snel voordoen) wordt geen structurele oplossing geboden, en de interpretatie van de situaties waarin een staat rechtsmacht kan opeisen kan behoorlijk uiteenlopen.
Op nationaal niveau lijken Canada en de VS op sommige vlakken verder te zijn dan de Europese landen, met name bij de specifieke strafbaarstelling van nieuwe fenomenen als identiteitsfraude en het online aanbieden van illegale diensten.

Naast de wetgevingsinitiatieven speelt ook zelfregulering een rol bij de bestrijding van computercriminaliteit, met name via meldpunten voor schadelijke of illegale inhoud. Nederland was hierin een van de voorlopers. De laatste jaren zijn in alle onderzochte landen, met uitzondering van Canada, meldpunten opgezet of uitgebreid. Japan, de VS en Zweden beperken

zich hierbij tot kinderporno en uitbuiting van kinderen via het Internet; de overige landen, waaronder Nederland, kennen meldpunten voor ook andere vormen van illegale inhoud. Overigens zijn de meldpunten niet in alle landen het resultaat van zuivere zelfregulering: in Frankrijk en de VS worden de meldpunten nadrukkelijk door de overheid ondersteund.
Tot slot verdient aandacht dat in diverse landen, waaronder Nederland, Canada, Duitsland en de VS, de overheid actief Internetpagina's onderhoudt ter voorlichting en waarschuwing aan het publiek, teneinde veilig gebruik van het Internet te stimuleren.

Conclusie: voor de bestrijding van computercriminaliteit is met het Cybercrime-verdrag uit 2001 een internationale inhaalslag gemaakt; Nederland heeft daardoor zijn pioniersrol in wetgeving achter zich gelaten, maar is wel zeer actief geweest bij de totstandkoming van dit verdrag. De zelfregulering van computercriminaliteitsbestrijding via meldpunten neemt nog steeds toe; Nederland blijft hierbij tot de koplopers behoren.

3.4. Terrorismebestrijding

De aanslagen op de VS van 11 september 2001 hebben tot een grote stroom aan beleids- en reguleringsinitiatieven geleid. Met uitzondering van Nederland en Zweden hebben alle onderzochte landen één of meer wetten aangenomen als directe reactie op de aanslagen. Nederland heeft daarentegen wel een grootschalig actieplan terrorismebestrijding gelanceerd, vol oude en nieuwe voorstellen, dat qua inhoud vergelijkbaar is met veel van de anti-terrorismewetten in de overige landen. Materieel betekent dit dat alleen Japan en Zweden zich relatief rustig hebben gehouden in de nasleep van 11 september, met slechts beperkte nationale wetsinitiatieven; zij leggen meer de nadruk op internationale samenwerking. De overige landen, waaronder Nederland, hebben ingrijpende wijzigingen voorgesteld of doorgevoerd naar aanleiding van 11 september. Vooral de VS, het VK en Canada voeren hierin de boventoon. Overigens is niet alle wetgeving even nieuw. Diverse bepalingen waren al eerder voorgesteld maar zijn door 11 september versneld aangenomen; bij andere eerder voorgestelde maatregelen heeft 11 september extra gewicht in de schaal gelegd – mogelijk zouden deze maatregelen anders niet zijn aangenomen.
De voorgestelde of doorgevoerde maatregelen die relevant zijn voor ICT-regulering betreffen vooral vergroting van de informatie-uitwisseling tussen veiligheidsdiensten en politie (bijvoorbeeld in de EU, Duitsland en Nederland), versterking van identificatiemogelijkheden (bijvoorbeeld in Duitsland, Nederland en het VK), het uitbreiden van DNA-databanken (Canada en de VS) en beveiliging van netwerken en infrastructuren (bijvoorbeeld in EU, Nederland en de VS). Daarnaast valt vooral op dat bevoegdheden voor het onderzoek van telecommunicatie worden uitgebreid: de telecomtap mag vaker worden toegepast (Canada en de VS) of wordt versneld verbeterd (Nederland), verkeersgegevens kunnen sneller worden overhandigd (de VS) of moeten verplicht worden bewaard (Frankrijk, het VK en mogelijk Nederland).
Alles overziend zijn de maatregelen en bevoegdhedenuitbreiding niet dusdanig ingrijpend dat er een verkillend effect op de elektronische handel mag worden verwacht, maar duidelijk is wel dat het bestaande grensvlak tussen veiligheid en persoonlijke vrijheden in de meeste landen is verschoven en dat er meer inbreuk op de burgerlijke vrijheden mogelijk is dan voorheen.

Conclusie: met uitzondering van Japan en Zweden hebben alle landen naar aanleiding van de aanslagen van 11 september 2001 ingrijpende wijzigingen in wetgeving voorgesteld of doorgevoerd voor terrorismebestrijding. Deze betreffen onder andere meer informatie-uitwisseling, beveiliging van netwerken en uitbreiding van bevoegdheden voor onderzoek van telecommunicatie.

4. Fiscale regimes

4.1. Directe- en verbruiksbelastingen

Op het terrein van de directe belastingen en e-handel zet de OESO de toon. Die rol is na 2000 alleen maar toegenomen. De opvattingen van de OESO lijken in het algemeen te stroken met de

Nederlandse opvattingen. Dit geldt ook voor Canada, Japan en Zweden. Dit kan niet met zoveel woorden worden gezegd voor Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten. De verschillen in belastingheffing kunnen tot concurrentieverstoringen leiden. De meest uitgesproken van de OESO afwijkende positie wordt door het Verenigd Koninkrijk ingenomen met het standpunt dat een enkele server (in OESO-termen: *stand-alone server*) geen vaste inrichting kan vormt. Hierdoor kan het Verenigd Koninkrijk een aantrekkelijker land voor de plaatsing van een enkele server zijn dan Nederland, omdat deze in het Verenigd Koninkrijk geen aanknopingspunt voor belastingheffing kan vormen, terwijl dit in Nederland wel het geval is. Aan de andere kant kan Nederland door het verschil in winsttoerekening aan een enkele server weer aantrekkelijker zijn dan, bijvoorbeeld, Duitsland.

Op het gebied van de verbruiksbelastingen (BTW) is de speelruimte van Nederland erg beperkt. Nederland is gebonden aan de beslissingen die op Europees niveau worden genomen. Dit geldt ook voor de overige EU-lidstaten. De nieuwe richtlijn inzake BTW en e-handel raakt enkel aan consumententransacties (B2C, naar verluidt ongeveer 10% van de markt). Het belang van de richtlijn moet dan ook niet overschat worden. De positie van Canada verschilt niet wezenlijk van de positie binnen de EU na implementatie van de nieuwe richtlijn. De positie van Japan is vooralsnog niet duidelijk maar neigt tot belastingheffing in het land van consumptie. Dit strookt met de uitgangspunten van de EU en derhalve ook van Nederland. De nieuwe Europese richtlijn heeft wel tot gevolg dat er met name vanuit de Verenigde Staten druk op de EU wordt uitgeoefend om de richtlijn te wijzigen, omdat Amerikaanse ondernemers een concurrentievoordeel gaan verliezen. Door implementatie van de richtlijn wordt de concurrentiepositie van de in de EU gevestigde aanbieders van elektronisch geleverde diensten, en derhalve ook van in Nederland gevestigde aanbieders, ten opzichte van de Amerikaanse aanbieders versterkt doordat meer een gelijkmatig speelveld wordt gecreëerd.

Conclusie: voor de directe verbruiksbelastingen zet de OESO de toon, maar sommige landen wijken hiervan af; met name het VK hanteert een ander standpunt door een enkele netwerkcomputer niet als vaste inrichting aan te merken. Voor de verbruiksbelastingen neemt een nieuwe Europese richtlijn een concurrentienadeel ten opzichte van de VS weg.

4.2. Fiscale stimulering van ICT-toepassingen

Wat betreft de fiscale stimulering van ICT-toepassingen voert Nederland een actief beleid (hoewel zeer recente ontwikkelingen een zekere mate van afbouw lijken te indiceren). Dat kan niet worden gezegd van Canada, Duitsland, Frankrijk en de Verenigde Staten. Daarentegen kennen Japan, het Verenigd Koninkrijk en Zweden op dit terrein wel fiscale stimuleringsmaatregelen. De fiscale stimuleringsmaatregelen in Zweden zijn ten opzichte van Nederland zeer beperkt te noemen. De fiscale maatregelen in Japan en Verenigd Koninkrijk zijn daarentegen aanzienlijk omvangrijker dan in Zweden. De afschrijvingen en belastingkortingen kunnen concurreren met de Nederlandse regelingen. Opgemerkt zij dat sommige Japanse maatregelen slechts een zeer beperkte looptijd hebben. Met name de recente uitbreidingen van de fiscale stimuleringmaatregelen in het Verenigd Koninkrijk versterken de positie van dit land. Deze versterking past in de ambitie van het VK om het beste land voor elektronische handel te zijn. Voor de positie van Nederland ten opzichte van de andere landen geldt dat met name de ontwikkelingen in het Verenigd Koninkrijk in de gaten dienen te worden gehouden.

Conclusie: op het gebied van fiscale stimulering van ICT-toepassingen voert het VK in toenemende mate een actief beleid, terwijl in Nederland een zekere mate van afbouw is te bespeuren. Nederland is echter actiever dan Japan en zeker dan Zweden. De overige landen voeren geen actief stimuleringsbeleid.

5. Vergroten vertrouwen

5.1. Elektronische handtekeningen

Alle onderzochte landen hebben inmiddels wetgeving op het gebied van elektronische handtekeningen afgekondigd. Inhoudelijk kan de wetgeving verschillen, in het bijzonder ten aanzien van de vereisten die aan de e-handtekeningtechniek worden gesteld. In Japan is deze strenger en voornamelijk gericht op de techniek van digitale handtekeningen (gebaseerd op cryptografie). De Verenigde Staten en Canada hebben een open en functionele benadering gekozen, op grond waarvan in beginsel (maar afhankelijk van de omstandigheden waarin de e-handtekening wordt gebruikt) iedere techniek voor e-ondertekenen kan worden toegepast. Een tussenvorm is de Europese benadering in de Richtlijn elektronische handtekeningen; deze combineert de open benadering voor e-handtekening in algemene zin (geen discriminatie) met een striktere benadering voor gekwalificeerde e-handtekeningen (bewijskracht). Onder deze laatste valt voornamelijk de op cryptografie gebaseerde techniek. Nederland volgt tamelijk letterlijk de bepalingen van voornoemde richtlijn (overigens met een te late implementatie), maar heeft omwille van de technologieonafhankelijkheid tevens een open bepaling toegevoegd. Ondanks de harmonisatie die met de Europese richtlijn wordt beoogd, blijven er binnen de Europese Unie nochtans verschillen op het gebied van de regulering van elektronische handtekeningen bestaan, bijvoorbeeld in het toezicht op uitgevers van niet-gekwalificeerde certificaten.

Conclusie: in de EU is de regulering van elektronische handtekeningen grotendeels geharmoniseerd, met evenwel nationale verschillen in de implementatie. Europa hanteert deels dezelfde, open benadering als de VS en Canada, maar kent daarnaast extra bescherming toe aan bepaalde technieken voor elektronisch ondertekenen.

5.2. Elektronisch betalen en financiële diensten

Op het gebied van elektronisch betalen is momenteel in Europa de belangrijkste ontwikkeling de implementatie van de Richtlijn instellingen voor elektronisch geld. De richtlijn kent een constructiefout in het voorkomen van geïnflateerde systemen voor elektronisch geld (een instelling die onder de richtlijn valt mag niet meer waarde aan e-geld uitgeven dan zij aan gewoon geld krijgt, maar een instelling die dat laatste doet valt per definitie niet onder de richtlijn); deze fout moet door de lidstaten rechtgezet worden. Duitsland, het Verenigd Koninkrijk en Zweden doen dit op een vergelijkbare manier, maar Nederland lijkt uit de pas te lopen door een afwijkende implementatie van de richtlijn. Terwijl de richtlijn beoogt om geïnflateerde systemen te voorkomen (een instelling mag niet meer (maar wel minder) waarde aan e-geld uitgeven dan zij in ruil hiervoor aan contanten of giraal geld ontvangt), kiest Nederland in het wetsvoorstel voor een consumentenbeschermende richting (een instelling mag niet minder (maar wel meer) waarde aan e-geld uitgeven dan zij in ruil hiervoor aan contanten of giraal geld ontvangt).
De Verenigde Staten hebben bij de regulering van elektronisch geld een andere aanpak gekozen dan de Europese Unie. In plaats van elektronisch geld als een aparte categorie van betaalsystemen te behandelen, is een aanpak gekozen waarbij elektronisch geld op dezelfde wijze behandeld wordt als andere alternatieve betaalmethoden. Dit leidt ertoe dat een groter gebied van betaalsystemen door de Amerikaanse wetgeving wordt geharmoniseerd. Bovendien lijken de Verenigde Staten zich meer te concentreren op transacties dan op het type instelling dat met deze transacties gemoeid is.
Op het gebied van financiële diensten is vooral van belang het Europese voorstel voor een Richtlijn verkoop op afstand van financiële diensten. Deze richtlijn beoogt consumentenbescherming bij verkoop op afstand van dergelijke diensten te regelen (vergelijkbaar met de Richtlijn verkoop op afstand voor verkoop van producten).

Conclusie: Nederland hanteert een afwijkende implementatie van de Richtlijn instellingen voor elektronisch geld. In Europa ligt de nadruk vooral op regulering van instellingen, in de VS op regulering van transacties. Voor financiële diensten die op

afstand worden aangeboden beoogt een voorstel voor een Europese richtlijn consumentenbescherming te bieden.

5.3. Trusted Third Parties

'Trusted Third Parties' is een verouderde term als men de internationale initiatieven en reguleringen op een rij zet. In het buitenland wordt deze term niet (meer) gebruikt; men spreekt hoofdzakelijk van cryptografische dienstaanbieders of van certificatiedienstaanbieders (CSP's).
De terminologie hangt samen met een onderscheid in soorten dienstaanbieders: er zijn dienstaanbieders die vertrouwelijkheidsdiensten faciliteren (waarbij het depot van cryptosleutels een mogelijkheid is) en dienstaanbieders die authenticiteit en integriteit faciliteren (de CSP's). Over andersoortige TTP-diensten dan deze twee is niets aangetroffen.
Nederland staat samen met Frankrijk en het VK alleen in het geïntegreerd willen aanpakken van beide soorten aanbieders; de overige landen beperken zich tot certificatieaanbieders (CSP's). Frankrijk stelt hierbij liberalisering voor van de beperkingen die van oudsher in de wetgeving bestaan, maar blijft verder gaan in regulering dan Nederland en het VK, die geconditioneerde zelfregulering voorstaan. Deze laatste aanpak lijkt ook in Canada te bestaan voor CSP's.
Voor certificatieaanbieders loopt de regulering uiteen. De EU-lidstaten hebben deze geënt op de Richtlijn elektronische handtekeningen; Nederland loopt hierbij achter met de implementatie. Voor gekwalificeerde CSP's zijn de eisen redelijk geüniformeerd conform de richtlijn; voor niet-gekwalificeerde CSP's loopt de regeling van accreditatie, certificatie en toezicht echter uiteen (waar de richtlijn ook ruimte voor biedt).
Buiten de EU heeft Japan een uitgebreide regeling voor accreditatie van CSP's, maar Canada en de VS kennen geen specifieke regulering van certificatieaanbieders, mede omdat hun elektronischehandtekeningwetgeving niet is geënt op cryptografische handtekeningen.
Diverse landen zijn bezig een *Public Key Infrastructure* op te zetten voor communicatie binnen of met de overheid. De VS en Canada lopen hiermee voorop, direct gevolgd door Nederland. De aanpak van Nederland verschilt van daarbij van die van de VS en Canada: Nederland ontwerpt een centrale, hiërarchische infrastructuur die opgehangen is aan één basiscertificaat; de VS en Canada kiezen voor een systeem van kruiscertificering door autonome overheids-certificatieaanbieders, waarbij in de VS een centrale instantie als facilitator optreedt.
Tot slot is vermeldenswaard dat Canada en Japan de noodzaak benadrukken van voorlichting aan het publiek om hen bewust te maken van elektronische handtekeningen en certificatieaanbieders; Japan heeft dit zelfs bij de wet aan de overheid opgedragen.

Conclusie: een wettelijke regulering van instanties voor vertrouwelijkheidsdiensten komt alleen voor in Frankrijk. De regeling van toezicht op certificatiedienstaanbieders loopt uiteen in de EU, behalve bij het verplichte toezicht op aanbieders van gekwalificeerde certificaten. Nederland volgt direct achter de VS en Canada bij het opzetten van een *Public Key Infrastructure* voor de overheid, met een meer hiërarchische benadering dan de VS.

5.4. Cryptografie

De export van cryptografie wordt voor het overgrote deel internationaal aangestuurd via het Wassenaar Akkoord. Vrijwel alle landen, waaronder Nederland, hebben de afspraken uit dit akkoord in nationale wetgeving geïmplementeerd. De laatste jaren zijn de nationale regelingen steeds meer naar elkaar toe gegroeid en versoepeld en is de maatschappelijke weerstand ertegen verstomd, waaruit men zou kunnen afleiden dat exportbeperkingen op cryptografie geen wezenlijk obstakel meer lijken te vormen voor internationale elektronische handel.
De binnenlandse regulering van cryptografie is, in tegenstelling tot de exportbeperkingen, vooral een nationale aangelegenheid. Internationale afstemming kon men op dit punt niet bereiken. Ook hier lijken de regelingen echter naar elkaar toe te groeien. Waar in de jaren negentig diverse overheden (Frankrijk, VS en VK) overhelden naar het inbouwen in cryptosystemen van een achterdeur voor overheidstoegang (hetgeen niet succesvol bleek), beperken de meeste landen zich nu tot een wettelijke ontsleutelplicht. Nederland was het eerste land dat een dergelijke ontsleutelplicht invoerde, zij het op beperkte schaal; Frankrijk en het VK hebben een verdergaande ontsleutelplicht. Daarnaast leggen diverse landen (Duitsland, Frankrijk en de VS)

de nadruk op het versterken van de technische kraakcapaciteit van de overheid; Nederland heeft daartoe vooralsnog geen stappen ondernomen.
Het geworstel van veel landen met binnenlandse cryptoregulering heeft lange tijd rechtsonzekerheid opgeleverd over de toelaatbaarheid van cryptogebruik. Nu de landen zich beperkt hebben tot een ontsleutelplicht, lijkt er geen belemmering meer voor cryptografiegebruik ter beveiliging van elektronische handel. Daarbij dient wel aangetekend te worden dat na bepaalde gebeurtenissen, zoals de terroristische aanslagen op de VS, de roep om verdergaande regulering wel weer wordt gehoord.

Conclusie: de internationaal aangestuurde exportbeperkingen op cryptografie in de diverse landen zijn de laatste jaren naar elkaar toe gegroeid en versoepeld. Op het vlak van binnenlandse regulering van cryptografie is de wereldwijde tendens van overheden zich te beperken tot een wettelijke ontsleutelplicht. Daarmee lijkt de rechtsonzekerheid over de toelaatbaarheid van cryptografie grotendeels verdwenen.

5.5. Commerciële communicatie en spam

Op het gebied van commerciële communicatie en spam is globaal bezien in de meeste landen op dit moment een *opt-out*systeem van kracht (e-reclame mag, tenzij de consument bezwaar heeft gemaakt), hetzij krachtens een wettelijke regeling, hetzij ingevolge zelfregulering. In Zweden lijkt momenteel een *opt-in*systeem voor e-mail te bestaan (e-reclame mag, mits de consument toestemming heeft gegeven). (In de EU kennen overigens vier lidstaten die niet in dit onderzoek zijn betrokken een opt-insysteem). Opvallend is dat in Duitsland en Frankrijk er door de regeringen (nog) geen concrete stappen zijn genomen ter regulering van spam (ongevraagde commerciële e-berichten). Nederland loopt, in vergelijking met de meeste andere landen, in de pas; er geldt op dit moment een opt-outregime, waarbij enkele garanties in wetgeving zijn vastgelegd.
De algemene Europese richting inzake spam is op dit moment nog de opt-outbenadering (spam mag, tenzij de consument bezwaar heeft gemaakt). Deze benadering gaat veranderen in een opt-inbenadering (spam mag, mits de consument toestemming heeft gegeven), zodra de Richtlijn privacy in de elektronischecommunicatiesector van kracht zal worden. De lidstaten van de EU zullen deze hoofdregel over ongeveer twee jaar in hun nationale regelgevingen moeten hebben implementeren, waarna de opt-inbenadering de hoofdregel zal zijn in de EU-landen. Deze hoofdregel kent overigens wel een nuance; zo mag een bedrijf haar bestaande klanten wel met e-mailberichten benaderen.
De bestaande opt-outregeling wordt in de praktijk veelal gerealiseerd via zelfregulering door brancheorganisaties voor *direct marketing*, mede ter voorkoming van overheidsregulering. Daarbij lijkt overigens weinig werk te zijn gemaakt van consumentenvoorlichting om betrokkenen te wijzen op de mogelijkheden van opt-out. Met de recente Europese omslag naar opt-in lijkt deze zelfreguleringsbenadering niet te hebben gewerkt.
In de VS en Canada bestaat op federaal niveau geen regulering van spam. Bijna de helft van de VS-staten kent wel regulering, die over het algemeen tendeert naar (een milde vorm van) opt-out. De belangen van de direct-marketingbedrijfstak wegen over het algemeen zwaarder in Noord-Amerika dan in Europa.

Conclusie: de meeste Europese landen kennen momenteel een (soms wettelijk gewaarborgde) opt-outregeling voor spam. Met de recente Europese richtlijn privacy in de elektronischecommunicatiesector zal in Europa een opt-insysteem van kracht worden. In de VS en Canada bestaat veel minder oog voor de consument en prevaleert momenteel zelfregulering met een lichte opt-outtint.

5.6. Gedragscodes en keurmerken voor webhandel

In de onderzochte landen worden gedragscodes en keurmerken belangrijk geacht voor het vergroten van het vertrouwen in elektronische handel, wellicht met uitzondering van Japan en Zweden. Zelfregulering wordt aldus in de meeste landen een belangrijke rol toegedicht bij het adequaat reguleren van e-handel.

Gedragscodes kunnen – vaak in afwachting van overheidsregulering – een rol spelen bij het scheppen van rechtszekerheid voor consumenten. Naarmate er meer overheidsregulering komt, functioneren gedragscodes vooral ook als vertaalslag van complexe regelgeving naar de praktijk van de webhandel. Nederland heeft op het gebied van gedragscodes een voortrekkersrol gespeeld met de Model Gedragscode van ECP.nl.
Voor de zichtbaarheid van de naleving van op overheids- of zelfregulering gebaseerde minimumnormen spelen keurmerken een belangrijke rol. Met name in Canada en de VS zijn er keurmerken ontstaan als product van pure zelfregulering. In Europa worden keurmerken evenwel over het algemeen meer ondersteund door de overheid, via financiering (door de Europese Commissie van het Webtrader-netwerk), het vaststellen van kwaliteitseisen waaraan keurmerken moeten voldoen of certificatie van keurmerken (Duitsland, Frankrijk, VK) en het aanbevelen van bepaalde keurmerken die als betrouwbaar worden gezien (Duitsland).
Op het gebied van keurmerken lijkt in Nederland evenwel een stap terug te zijn gedaan door het stopzetten van Webtrader door de Consumentenbond in januari 2002. Dit kan verwarring wekken bij consumenten, nu buitenlandse organisaties nog steeds verwijzen naar de Nederlandse Webtrader als internationaal afgestemd keurmerk; de onderlinge afstemming tussen de Webtraderpartijen lijkt dan ook niet groot. Bovendien groeit het aantal keurmerken de laatste tijd explosief, mede omdat elke subsector een eigen keurmerk lijkt te ontwikkelen; hierdoor vermindert de bekendheid en daarmee de zeggingskracht van keurmerken voor consumenten. In het buitenland is ook al geconstateerd dat de opkomst van diverse pseudo-keurmerken vertroebelend werkt. De effectiviteit van keurmerken lijkt vooralsnog dan ook niet groot.

Conclusie: in de meeste landen zijn voornamelijk via zelfregulering gedragscodes en keurmerken voor elektronische handel ontstaan; in Europa worden deze meer ondersteund door de overheid dan in Canada en de VS. Er vindt een sterke groei aan keurmerken (en mogelijk ook pseudokeurmerken) op het Internet plaats, die de consumentenbescherming, zeker ook in Nederland, niet ten goede komt.

5.7. Online geschillenbeslechting (ODR)

De mogelijkheid om geschillen online te kunnen beslechten (ODR) staat sinds enkele jaren in de belangstelling. Aanbieders van alternatieve geschillenbeslechting (ADR), zoals arbitrage-instellingen, beginnen voorzichtig om in een dergelijke mogelijkheid te voorzien. De Europese richtlijn elektronische handel bepaalt dat er geen wettelijke belemmeringen mogen zijn voor alternatieve geschillenbeslechting of het gebruik van ICT daarbij.
Online geschillenbeslechting verkeert nog duidelijk in de pioniersfase. Er worden wel initiatieven ondernomen, maar het lijkt er toch op dat aanbieders nog tastenderwijs hun weg aan het zoeken zijn. Ook de personen die een geschil hebben moeten hun weg naar ODR nog vinden. Het belang van informatievoorziening over ODR wordt dan ook van meerdere zijden onderstreept. Het belang van adequate procedurele waarborgen bij ODR wordt ook benadrukt.
Nederland heeft met ODR.nl, dat is opgezet onder de vleugels van ECP.nl en tot doel heeft de online afhandeling van klachten, een eerste stap gezet. Het VK en de VS zijn echter verder met initiatieven op het vlak van online geschillenbeslechting, waarbij bepaalde reguliere rechterlijke procedures online worden afgehandeld.
Bij domeinnaamgeschillen wordt evenwel al wel op behoorlijke schaal gebruik gemaakt van (gedeeltelijke) online geschillenbeslechting. Naast de internationale *Uniform Dispute Resolution Policy* (UDRP) van de ICANN, zijn voor vele nationale domeinnamen al procedures van kracht of wordt daaraan gewerkt. Van de onderzochte landen zijn de VS en het VK hierin het verst, gevolgd door Canada en Nederland.

Conclusie: online geschillenbeslechting verkeert in de pioniersfase. Er zijn diverse initiatieven, waarbij Nederland zeker niet achterloopt. Het VK en de VS zijn evenwel duidelijk verder, met initiatieven voor online beslechting van reguliere rechtszaken. Dat geldt ook voor beslechting van domeinnaamgeschillen, waar online beslechting al op een behoorlijke schaal plaatsvindt.

5.8. Rechtsmacht en toepasselijk recht bij privaatrechtelijke geschillen

De vaststelling van de rechtsmacht en het toepasselijk recht roepen in relatie tot de internationale e-handel vragen op. De tegenstelling tussen het belang van rechtszekerheid voor de aanbieder en belang bij bescherming van de consument lijkt in internationaal verband, in elk geval voorlopig, niet te kunnen worden aangepakt. Tekenend is dat er binnen grootschalig internationaal verband (zoals de OESO en de Haagse Conferentie) geen vooruitgang wordt geboekt. Naar verwachting zullen de onderhandelingen binnen de Haagse conferentie niet tot een snelle afronding komen. De kans is zelfs groot dat de conferentie slechts beperkt resultaat oplevert, waarbij aan de elektronische handel gerelateerde oplossingen geheel worden vermeden. In kleiner verband (zoals in de EU) gekozen richtingen, zoals rechtsmacht in het land van de consument onder de EEX-Vo, kunnen in breder – internationaal – verband niet altijd op instemming rekenen. Ipr-problemen spelen bij onrechtmatigedaadsituaties in versterkte mate een rol. Dit vraagstuk is tot nu toe onderbelicht gebleven en op internationaal niveau uiterst lastig aan te pakken, vanwege het bestaan van grote culturele verschillen en daarmee gemoeide uiteenlopende belangen. Ook zullen – anders dan bij overeenkomsten – over het algemeen vooraf geen afspraken zijn gemaakt in de vorm van een forum- en rechtskeuze.

Bij gebrek aan juridische initiatieven, zullen bedrijven en consumenten voorlopig genoegen moeten nemen met technische en organisatorische maatregelen. Partijen kunnen over en weer informatie uitwisselen omtrent woon- of vestigingsplaats en de inhoud van het toepasselijk recht, zodat zij tenminste een geïnformeerde keuze kunnen maken voor grensoverschrijdend contracteren. Ook kan het online aanbod uitdrukkelijk worden beperkt tot niet-consumenten of consumenten in bepaalde landen om het rechtsmachtrisico en het conflictenrechtelijke risico bij online consumentenovereenkomsten te beperken. In het geval van onrechtmatige daad zullen partijen naar verwachting echter weinig baat hebben bij technische en organisatorische oplossingen.

Conclusie: de regeling van rechtsmacht en toepasselijk recht in relatie tot grensoverschrijdende e-handel roept vragen op. In internationaal verband wordt er weinig vooruitgang geboekt om de nationale regelingen op elkaar af te stemmen. In contractuele relaties kunnen organisatorische en technische maatregelen mogelijk een deel van de pijn verzachten.

1. Inleiding

De regulering van informatie- en communicatietechnologie (ICT) maakt een geleidelijke ontwikkeling door. Waar in de jaren zeventig en tachtig op enkele specifieke terreinen waar nieuwe technologische ontwikkelingen zich voordeden de regulering zich beperkte tot een kleinschalige, sectorale en techniekgerichte aanpak, kwam in de jaren negentig geleidelijk meer aandacht voor een breder perspectief op ICT-regulering. Deze richtte zich met name op het Internet. De aanpak bleef echter grotendeels aangestuurd door de verschillende technische ontwikkelingen, en minder door een visie op de ontwikkeling van de informatiemaatschappij. Eind jaren negentig werd voor het eerst gepoogd om wel een integrale visie op ICT-regulering te formuleren. De Nederlandse regering gaf in de nota *Wetgeving voor de elektronische snelweg* van februari 1998[3] een beschrijving en analyse van ICT-ontwikkelingen en de uitdagingen die deze aan het recht stelden. Daarbij werd een toetsingskader geformuleerd voor ICT-regulering. Aangezien deze nota grotendeels gericht was op de Nederlandse situatie en de internationale dimensie als problematisch werd ervaren, vroeg het kabinet twee jaar later specifiek aandacht voor de internationaliserings- en rechtsmachtvraagstukken die een toenemende rol spelen bij ICT-regulering. Dit resulteerde in vuistregels die de Nederlandse inzet in internationale fora moeten leiden.[4]

Slechts weinig landen kennen (vooralsnog) een dergelijke integrerende aanpak van ICT-regulering. Een rechtsvergelijkende studie uit 2000[5] constateerde dat de VS, het VK en Duitsland geen overkoepelend beleid kenden; slechts Frankrijk had een poging gedaan in het consultatiedocument *Une société d'information pour tous*,[6] dat een opmaat was voor een breed wetsvoorstel dat vele aspecten van ICT beoogde te reguleren. Dit *Projet de loi sur la société de l'information* werd op 13 juni 2001 ingediend,[7] maar is in het parlementaire jaar niet aangenomen en door de verkiezingen van juni 2002 komen te vervallen.[8] Gezien de uitslag van de verkiezingen is het de vraag of het wetsvoorstel in de huidige vorm terugkeert. Bepaalde elementen uit het wetsvoorstel zijn overigens wel elders geïmplementeerd, maar een geïntegreerde benadering van ICT-regulering is vooralsnog in Frankrijk dus ook niet aan de orde.

Inmiddels heeft het Verenigd Koninkrijk wel principes geformuleerd voor ICT-regulering, de *E-Policy Principles*.[9] Deze acht uitgangspunten, geformuleerd door de e-Envoy (die is aangesteld 'to lead the drive to get the UK online'),[10] gaan uit van een 'light touch regulatory regime'. Ze zijn bestemd voor alle beleidsmakers die voorstellen doen met een mogelijk effect op de elektronische handel. De uitgangspunten komen voor een aanzienlijk deel overeen met de genoemde vuistregels van het Nederlandse kabinet.

Vooralsnog zijn Nederland en het VK evenwel de enige ons bekende landen met een aanpak van ICT-regulering die mede is gebaseerd op algemene uitgangspunten voor ICT-regulering. In het onderzoek dat ten grondslag ligt aan dit rapport zijn in de diverse landen verder geen verdere overkoepelende visies of strategieën op dit gebied aangetroffen. Dat hoeft overigens niet te maken te hebben met een gebrek aan visie. ICT-regulering bestrijkt naar haar aard een breed en divers terrein met complexe en weerbarstige onderwerpen. In de praktijk zijn algemene uitgangspunten dan ook niet altijd eenvoudig hanteerbaar.[11] Het is dus goed denkbaar dat landen zich concentreren op het aanpakken van specifieke problemen in plaats van algemene uitgangspunten te formuleren.

---

[3] TK 1997-1998, 25 880, nrs. 1-2, 12 februari 1998.
[4] TK 1999-2000, 25 880, nr. 10, 18 mei 2000.
[5] Koops e.a. 2000, p. 113.
[6] <http://www.finances.gouv.fr/societe_information/sommaire.htm>.
[7] Zie <http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi.htm>.
[8] "Ce projet de loi est devenu caduc à la fin de la onzième législature". Zie <http://www.assemblee-nationale.fr/dossiers/societe_information.asp>.
[9] <http://www.e-envoy.gov.uk/publications/guidelines/eprinciples/index.htm>.
[10] <http://www.e-envoy.gov.uk/news/bios/apinder.htm>.
[11] Zoals geconcludeerd werd in Koops e.a. 2000, p. 118.

Daarom is het interessant te kijken naar de praktijk van ICT-regulering: hoe worden al die verschillende en weerbarstige onderwerpen aangepakt door de diverse landen? En zegt dat iets over ICT-regulering in het algemeen? Met andere woorden, in welk stadium van ontwikkeling verkeert ICT-regulering anno 2002?

Doel, uitvoering en opzet

Dit rapport werd geschreven in opdracht van het Ministerie van Economische Zaken ten behoeve van de *Internationale ICT-toets 2002*.[12] Het beoogt een overzicht te geven van de stand van zaken rond ICT-regulering in acht landen, in het bijzonder in relatie tot elektronische handel. Het heeft als doel de internationale positie van Nederland op dit gebied te analyseren. Hoe verhoudt Nederlandse ICT-regulering zich tot de ontwikkelingen elders – speelt Nederland een voortrekkersrol of volgt het internationale ontwikkelingen? Vanwege het vraagstuk van positionering tussen andere landen, ligt het accent in dit onderzoek op nationale reguleringsinitiatieven. Veel ICT-beleid en -regelgeving wordt op internationaal niveau voorbereid of uitgewerkt; wij schetsen bij elk onderwerp eerst deze internationale dimensie, om de context aan te geven waarbinnen het nationale discours zich afspeelt, maar beperken ons vervolgens voornamelijk tot het nationale beleid en de regelgeving in de diverse landen.
De nadruk ligt in dit rapport op recente ontwikkelingen. In 2000 is door Landwell een soortgelijke momentopname gemaakt ten behoeve van de *Internationale ICT-toets 2000*.[13] Wij bouwen voort op de bevindingen uit dat rapport, waarbij we soms de belangrijkste bevindingen van voor 2000 aanstippen, maar ons grotendeels beperken tot de ontwikkelingen sinds 2000.

Dit onderzoek beslaat een breed terrein. Het omvat vele landen en onderwerpen en heeft daarom een schetsmatig karakter. De nadruk ligt op het signaleren van reguleringsinitiatieven, niet op het analyseren of diepgaand vergelijken ervan. Wij hebben allerminst de pretentie volledig te zijn; een beperking in de weergave was noodzakelijk niet alleen vanwege het brede terrein en de beperkte onderzoekstijd, maar op sommige punten ook vanwege een gebrek aan beschikbaarheid van Engels-, Frans- of Duitstalig materiaal.
De keuzes die ten grondslag liggen aan het onderzoek zijn gemaakt na overleg met de opdrachtgever. De landen zijn uitgekozen vanwege hun vermoede belangrijke rol op het vlak van ICT-regulering: de belangrijkste geïndustrialiseerde landen (VS, Canada, VK, Duitsland, Frankrijk en Japan) en een vertegenwoordiger van Scandinavië (dat traditioneel voorop loopt op ICT-gebied) (Zweden). De onderwerpen zijn gekozen vanwege hun (potentiële) relevantie voor de elektronische handel in brede zin. Dit betekent dat niet alleen onderwerpen die nauw samenhangen met e-handel (zoals contracten, handtekeningen, reclame, belastingen en aansprakelijkheid) aan bod komen, maar ook onderwerpen die een weerslag kunnen hebben op de (on)mogelijkheden van e-handel, zoals criminaliteitsbestrijding en elektronische communicatie met de overheid.
Het onderzoek is uitgevoerd door middel van literatuuronderzoek, vooral via het Internet[14] en tijdschriften op het gebied van ICT-regulering. Dit is aangevuld met informatie van contacten in de diverse landen, die waar nodig – afhankelijk van het onderwerp en het reeds voorhanden materiaal – nadere informatie hebben geleverd.

Het onderzoek is uitgevoerd door het Centrum voor Recht, Bestuur en Informatisering (CRBI) van de Katholieke Universiteit Brabant onder leiding van Bert-Jaap Koops. Hierbij is een bijdrage geleverd door het Fiscaal Instituut Tilburg (Eric Kemmeren en Gert-Jan van Norden, hoofdstuk

---

[12] In de nota *De Digitale Delta* (TK 1998-1999, 26 643, nr. 1) van juni 1999 kondigde het kabinet aan om tweejaarlijks een beeld te geven van de relatieve positie van Nederland op ICT-gebied in de wereld. Deze *Internationale ICT-toets* kent vijf pijlers: de (tele)communicatie-infrastructuur, kennis en innovatie, toegang en vaardigheden, regelgeving en ICT in de publieke sector. Het onderhavige rapport is de basis voor de pijler regelgeving in de integrale rapportage.
[13] Landwell 2000 respectievelijk Internationale ICT-toets 2000.
[14] We hebben ervan afgezien om bij elk individuele verwijzing te vermelden op welke datum de pagina ingezien is. De in dit rapport weergegeven Internetadressen verwijzen naar de inhoud die aldaar begin juni 2002 weergegeven was.

4) en het Instituut voor Informatierecht van de Universiteit van Amsterdam (Ot van Daalen en Mireille van Eechoud, m.m.v. Reinier Bakels, paragraaf 3.2). Alle overige onderzoekers zijn werkzaam bij het CRBI.

Het onderzoek is afgesloten op 1 juni 2002. De rapportage is afgerond op 28 juni 2002.

Omwille van de vergelijkbaarheid met de *Internationale ICT-toets 2000* is de indeling van dit rapport gebaseerd op de indeling en rubricering die daarin zijn gehanteerd. Vanwege de ontwikkelingen in het vakgebied zijn de indeling en rubricering wellicht aan herziening toe; de onderzoekers geven in overweging bij de volgende *Internationale ICT-toets* deze te heroverwegen.
De opzet van dit rapport volgt dus de indeling van de *Internationale ICT-toets 2000*, waarbij enkele onderwerpen zijn toegevoegd. Hoofdstuk 2 behandelt de initiatieven die wet- en regelgeving beogen toe te rusten op de informatiemaatschappij en e-handel. De nadruk ligt hier op de mogelijkheden van elektronische communicatie (e-contracteren, verplichtingen van Internetaanbieders, communicatie met de overheid). Hoofdstuk 3 gaat nader in op wet- en regelgeving ter rechtsbescherming (privacy, IE-rechten, computercriminaliteit en terrorismebestrijding). Hoofdstuk 4 behandelt fiscale aspecten van e-handel (directe en verbruiksbelastingen, stimuleringsmaatregelen). Hoofdstuk 5 geeft een overzicht van de belangrijkste initiatieven die het vertrouwen in e-handel beïnvloeden (elektronische handtekeningen, e-betaalmethoden, Trusted Third Parties, cryptografie(beperkingen), e-reclame, gedragscodes en online geschillenbeslechting). Hoofdstuk 6 biedt ten slotte enige conclusies, die met name ingaan op het algemene beeld van ICT-regulering en de positie van Nederland daarbinnen.

2. Toerusten wet- en regelgeving

2.1. Elektronische contracten

Voor elektronische handel is het van belang dat zoveel mogelijk kan worden gecommuniceerd via elektronische middelen en dat niet hoeft te worden teruggegrepen op papieren communicatie- en opslagmiddelen. Het kunnen afsluiten van overeenkomsten via elektronische weg is daarom een basisvoorwaarde voor een goede ontwikkeling van e-handel. De rechtswaarborgen waarmee overeenkomsten zijn omkleed, zijn evenwel van oudsher gebaseerd op papieren communicatie. De vraag is daarom relevant in hoeverre het recht toelaat dat elektronisch wordt overeengekomen, en welke rechtsgevolgen een dergelijke vorm van overeenkomen heeft voor de partijen. De hoofdvraag is of een elektronische overeenkomst rechtsgeldig is en een vergelijkbare juridische status heeft als een papieren overeenkomst. Daarnaast spelen vragen een rol rond de totstandkoming van e-overeenkomsten en de wederzijdse verplichtingen van partijen daarbij.

2.1.1. Internationaal

In 1996 heeft de UNCITRAL de *Model Law on Electronic Commerce* aangenomen. Deze modelwet bevat onder meer bepalingen met betrekking tot elektronisch contracteren. Deze betreffen onderwerpen als de totstandkoming van elektronische overeenkomsten, tijd en plaats van verzending en ontvangst van elektronische berichten, het gebruik van elektronische ontvangstbevestigingen en *incorporation by reference*. Tevens zijn in het kader van de UNCITRAL in 2001 voorbereidende werkzaamheden voor een verdrag betreffende e-contracteren begonnen.[15] Dit verdrag zal het Weens Koopverdrag 1980 kunnen complementeren voor wat betreft enkele pregnante kwesties rond elektronisch contracteren.

In de Europese Unie zijn relevante bepalingen voor elektronisch contracteren opgenomen in richtlijn 2000/31/EG betreffende de elektronische handel.[16] Op grond van deze richtlijn dienen lidstaten ervoor te zorgen dat een elektronische overeenkomst in hun nationale wetgeving in beginsel rechtsgeldig is. Enkele uitzonderingen, waaronder overeenkomsten met betrekking tot onroerend goed en testamenten, zijn echter toegestaan. Naast deze procedurele bepaling bevat de richtlijn tevens bepalingen van materieel recht, waaronder het vereiste van een bevestiging van ontvangst van een elektronische bestelling. Deze wordt geacht te zijn ontvangen door de klant, wanneer deze toegang heeft tot het bericht. De richtlijn geeft voorts aan dat online aanbieders contractuele voorwaarden op transparante wijze kenbaar moeten maken. Ook moeten zij duidelijkheid scheppen omtrent onder meer de stappen die tot een elektronisch contract leiden en de wijze van corrigeren van fouten vóór afsluiting van de elektronische overeenkomst.

2.1.2. Nederland

Op dit moment wordt in Nederland richtlijn 2000/31/EG geïmplementeerd, inclusief de bepalingen met betrekking tot elektronisch contracteren.[17] In het wetsvoorstel is voorzien in een uitdrukkelijke erkenning van de rechtsgeldigheid van elektronische overeenkomsten (voorgesteld art. 6:227a BW). Ook worden de overige bepalingen (onder meer transparantie van informatie, wijze van bestellen, correctiemogelijkheden) geïmplementeerd.

2.1.3. Canada

In september 1999 hebben de *Uniform Law Conference of Canada* en het Ministerie van Justitie de *Uniform Electronic Commerce Act* (UECA) aangenomen. Deze modelwel, die staten kunnen overnemen in hun wetgeving, is gebaseerd op de UNCITRAL-*Model Law on Electronic Commerce*

---

[15] Voluit: *Preliminary Draft Convention on [international] contracts concluded or evidenced by data messages*, UNCITRAL, Annex 1, zie <http://www.uncitral.org>.
[16] Richtlijn 2000/31/EG, *PbEG* 2000, L 178/1.
[17] TK 2001-2002, 28 197, nrs. 1-3.

(zie par. 2.1.1) en in grote lijnen vergelijkbaar met de Amerikaanse *Uniform Electronic Transactions Act* (zie par. 2.1.8). De wet behandelt onder meer de vereisten voor het rechtsgeldig afsluiten van een elektronische overeenkomst. Daarbij wordt eveneens het contracteren met behulp van *electronic agents* behandeld.

2.1.4. Duitsland

In Duitsland is richtlijn 2000/31/EG door middel van verschillende wetten geïmplementeerd. Het in 2001 in werking getreden *Gesetz zur Anpassung von Formvorschriften im Privatrecht und anderer Vorschriften an den Modernen Geschäftsverkehr* heeft in het privaatrecht voorkomende vormvoorschriften aan de eisen van het elektronische rechtsverkeer aangepast. Ten eerste kan het getekende geschrift worden vervangen door de nieuw ingevoerde elektronische vorm die is voorzien van een gekwalificeerde e-handtekening (§ 126 a BGB). Ten tweede is tevens de *Textform* in het Duitse privaatrecht geïntroduceerd (§ 126b BGB).[18] Dit is een duurzame weergave van een leesbare elektronische verklaring, die voorzien is van de naam van de verklarende en afgesloten is hetzij door nabootsing van de handtekening van de verklarende hetzij op andere wijze. Voor deze vorm is derhalve geen gekwalificeerde e-handtekening vereist. In het procesrecht kan in plaats van een geschrift eveneens de elektronische vorm worden gebruikt onder voorwaarde dat het e-document geschikt is voor verwerking door het gerecht. Voorts wordt in het bewijsrecht voorzien in een verlichting van de bewijslast ten aanzien van de elektronische vorm. Tenzij ernstige twijfel bestaat over de overeenstemming van de in elektronische vorm afgegeven verklaring met de wil van de verklarende, wordt aangenomen deze verklaring authentiek is (*Anscheinsbeweis*).
De overige bepalingen met betrekking tot elektronisch contracteren uit de richtlijn zijn geïmplementeerd door middel van de in januari 2002 in werking getreden Wet betreffende de modernisering van het verbintenissenrecht.[19]

2.1.5. Frankrijk

De implementatie van richtlijn 2000/31/EG betreffende elektronische handel heeft vormgekregen in het *Projet de loi sur la société de l'information* van juni 2001. Op grond van dit wetsvoorstel wordt de geldigheid van elektronische overeenkomsten onder de *Code Civil* uitdrukkelijk erkend. Vanuit het oogpunt van consumentenbescherming zijn enkele nadere bepalingen opgenomen, bijvoorbeeld over transparantie van het online bestelproces, het dubbelklikvereiste voor het afsluiten van *business-to-consumer*-transacties, archivering en het voor de consument toegankelijk maken van overeenkomsten die een bepaalde waarde overschrijden. Het wetsvoorstel is evenwel vervallen door de verkiezingen van 2002, zodat deze bepalingen vooralsnog niet zijn geïmplementeerd.

De bewijskracht van e-documenten is met de inwerkingtreding met de wet nr. 2000-230 van 13 maart 2000 betreffende het gebruik van elektronische handtekeningen en elektronische documenten als bewijs[20] geregeld in § 1316 *Code Civil*. Hierin wordt bepaald dat e-documenten dezelfde bewijskracht hebben als geschriften, indien de degene van wie het document afkomstig is kan worden geïdentificeerd en het document tot stand is gekomen en wordt bewaard onder voorwaarden die de integriteit ervan konden waarborgen.

Terzijde zij nog opgemerkt dat Frankrijk recentelijk ook aandacht heeft besteed aan andere vormen van gelijkschakeling van traditionele en elektronische middelen. Op 3 mei 2002 werd een decreet bekrachtigd (No. 2002-803) dat ondernemingen toestaat om onder de Nieuwe economische reguleringswet (No. 2001-420) ICT te gebruiken om de participatie in aandeelhoudersvergaderingen te vergroten.[21] Op basis hiervan mogen ondernemingen bijvoorbeeld het Internet gebruiken om jaarverslagen aan aandeelhouders te zenden, maar ook om *proxy voting* te faciliteren. Bedrijven die algemene of bijzondere aandeelhoudersvergaderingen

[18] Zie tevens par. 5.1.4.
[19] *Gesetz zur Modernisierung des Schuldrechts, BGBl* 29 november 2001, Teil I, p. 3138.
[20] Zie tevens par. 5.1.5.
[21] Beschikbaar op <http://www.legifrance.gouv.fr>.

willen openstellen voor elektronisch stemmen, dienen daartoe speciale webpagina's in te richten.[22]

2.1.6. Japan

Voorzover bekend bestaan er in Japan geen wetgevingsinitiatieven op het gebied van elektronische overeenkomsten.

2.1.7. Verenigd Koninkrijk

Onder § 8 van de *Electronic Communications Act 2000* zijn ministers onder bepaalde voorwaarden bevoegd om vormvereisten aan te passen ten behoeve van het rechtsgeldig elektronisch contracteren. In dat verband is inmiddels op diverse terreinen, waaronder overeenkomsten met betrekking tot onroerend goed, regelgeving aangenomen. Richtlijn 2000/31/EG wordt geïmplementeerd in de *Electronic Commerce (E.C. Directive) Regulations 2002*, die nog niet zijn aangenomen.
De status van een online aanbod is niet geheel duidelijk, maar mogelijk wordt het beschouwd als een *offerendum ad invitio*. Ook is onduidelijk op welk moment de aanvaarding van een aanbod in de online context plaatsvindt: wanneer de verklaring is ontvangen (zoals bij *instantaneous communication*) of wanneer de verklaring is verstuurd (zoals bij een verklaring die per post wordt overgebracht)?[23]

2.1.8. Verenigde Staten

Federaal
De *Electronic Signatures in Global and National Commerce Act* (E-sign) verklaart dat e-contracten – ook die waar *electronic agents* zijn ingezet en enkele uitzonderingen daargelaten – geen juridische geldigheid mogen worden ontzegd vanwege hun elektronische karakter. Indien voor een overeenkomst een geschriftvereiste bestaat, kan daaraan worden voldaan door ervoor te zorgen dat het e-document op een later tijdstip raadpleegbaar is. Voor wat betreft *business-to-consumer*-contracten is in beginsel vereist dat de consument instemt met elektronisch getekende contracten en het ontvangen van e-bestanden via het Internet. E-sign is beperkt tot interstatelijke en internationale transacties en is alleen toepasselijk buiten gevallen die worden bestreken door de *Uniform Commercial Code* (UCC).

Statelijk
De *National Conference of Commissioners on Uniform State Laws* heeft in de *Uniform Electronic Transactions Act* (UETA) en de *Uniform Computer Information Transactions Act* (UCITA) bepalingen met betrekking tot e-handtekeningen opgenomen. Daarbij is de functionele benadering zoals gepropageerd door de UNCITRAL-*Model Law on Electronic Commerce* gevolgd. Beide modelwetten zijn of worden momenteel in verschillende staten geïmplementeerd. In de UETA wordt het elektronisch contracteren uitdrukkelijk erkend. Daarnaast regelt de UCITA *computer information transactions* ofwel transacties met betrekking tot digitale informatie (*soft products*), zoals de *Uniform Commercial Code* overeenkomsten betreffende zaken regelt. In beide modelwetten wordt tevens ingegaan op geautomatiseerde transacties, denk aan overeenkomsten afgesloten door *electronic agents*.

2.1.9. Zweden

Richtlijn 2000/31/EG betreffende elektronische handel is op 6 juni 2002 geïmplementeerd in de *Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster* van 6 juni 2002 (Wet op de elektronische handel en andere diensten van de informatiemaatschappij).[24] Deze wet bevat eisen voor elektronische bestellingen, onder andere met betrekking tot informatievoorziening en de totstandkoming van een overeenkomst, die dicht aanliggen tegen de Europese richtlijn.

---

[22] Zie *World Internet Law Report* juni 2002, p. 7-8.
[23] Baker & McKenzie 2001, p. 193.
[24] Beschikbaar via <http://.194.52.125.3>.

Het Zweedse recht kent slechts een gering aantal vormvereisten (bijvoorbeeld bij overeenkomsten over onroerend goed) die in de weg kunnen staan aan e-contracteren. Een elektronische verklaring heeft echter niet dezelfde status als een geschrift en is derhalve niet voldoende wanneer er een geschriftvereiste bestaat.[25]

2.1.10. Samenvatting

Met de implementatie van richtlijn 2000/31/EG betreffende elektronische handel moeten elektronische overeenkomsten – enkele uitzondering daargelaten – door de lidstaten van de Europese Unie uitdrukkelijk worden erkend. Ook in Noord-Amerika bestaat (model)wetgeving waarin elektronische overeenkomsten uitdrukkelijk als rechtsgeldige vorm van contracteren worden erkend. In beide gevallen kunnen er nochtans uitzonderingen worden gemaakt. In Japan zijn geen initiatieven op dit gebied bekend.
Een duidelijk verschil tussen de EU en Noord-Amerika is de aandacht voor geheel nieuwe vormen van e-contracteren – namelijk het gebruik van *electronic agents* – en juridische erkenning ervan in Noord-Amerika. De Verenigde Staten en Canada zijn in dit opzicht duidelijk verder. De Verenigde Staten springen er voorts uit met de UCITA. Deze modelwet bevat een volledige materieelrechtelijke regeling van transacties met betrekking tot informatieproducten. Richtlijn 2000/31/EG betreffende elektronische handel bevat weliswaar ook enkele bepalingen van materieel recht, maar deze zijn betrekkelijk summier vergeleken bij UCITA.

[25] Zie Baker & McKenzie 2001, p. 176.

2.2. Aansprakelijkheid van Internetaanbieders

Internetaanbieders spelen een belangrijke rol bij elektronische handel. Zij faciliteren de toegang tot het netwerk, het transport en toegevoegdewaardediensten, alsmede het aanbieden van inhoud op het wereldwijde web. Zij houden zich bezig met het transporteren, toegang verlenen tot of aanbieden van gegevens, waaronder mogelijk ook gegevens die inbreuk maken op rechten van anderen of zelfs strafbaar zijn (zoals auteursrechtelijk beschermd materiaal, onrechtmatig verwerkte persoonsgegevens of kinderpornografie). De vraag rijst in welke mate Internetaanbieders aansprakelijk gehouden kunnen worden voor dergelijk materiaal. Een volledige aansprakelijkheid zou al snel kunnen leiden tot beperking in het aanbod van Internetdiensten, maar een volledige uitsluiting van aansprakelijkheid zou een effectieve rechtshandhaving ernstig kunnen belemmeren aangezien de Internetaanbieder vaak de toegangspoort is tot het achterhalen van de oorspronkelijke bron. Voor de elektronische handel is daarom de vraag relevant in hoeverre Internetaanbieders aansprakelijk gehouden kunnen worden voor de gegevensuitwisseling of het gegevensaanbod dat zij faciliteren. Deze vraag staat in deze paragraaf centraal.[26] De aansprakelijkheid van certificatiedienstaanbieders (CSP's) wordt behandeld in par. 5.3.

2.2.1. Internationaal

De Europese richtlijn inzake elektronische handel[27] kent een tamelijk gedetailleerde regeling over de aansprakelijkheid van Internetaanbieders (ISP's), waarbij onderscheid wordt gemaakt tussen verschillende diensten die ISP's aanbieden: 'mere conduit' (art. 12), 'caching' (art. 13) en 'hosting' (art. 14). De lidstaten moesten deze richtlijn voor 17 januari 2002 implementeren (art. 22 Richtlijn). De (voorgestelde) implementaties worden hierna genoemd. De beschrijving ervan blijft uiteraard beperkt tot bijzonderheden die specifiek zijn voor de desbetreffende lidstaat.

2.2.2. Nederland

In afwachting van de implementatie van de richtlijn inzake elektronische handel in het Nederlandse recht, is het vonnis van de Haagse rechtbank in Scientology/XS4ALL en anderen richtinggevend voor de ISP-aansprakelijkheid in Nederland.[28] Volgens dit vonnis handelt een Internetaanbieder die ervan in kennis wordt gesteld dat een gebruiker van zijn diensten op diens thuispagina auteursrechtinbreuk pleegt of anderszins onrechtmatig handelt, terwijl aan de juistheid van die kennisgeving in redelijkheid niet valt te twijfelen, zelf onrechtmatig indien hij alsdan niet ingrijpt.
Een wetsvoorstel tot regeling van de strafrechtelijke aansprakelijkheid van tussenpersonen (waaronder Internetaanbieders) is ingetrokken, omdat de regeling niet verenigbaar werd geacht met de – toen in voorbereiding zijnde – regeling in de richtlijn inzake elektronische handel.[29]
Ter implementatie van de richtlijn inzake elektronische handel heeft de Nederlandse regering in januari 2002 het voorstel voor een Aanpassingswet richtlijn inzake elektronische handel aan het parlement aangeboden.[30] Voor civielrechtelijke verhoudingen maakt de aanpassingswet (in navolging van de richtlijn) onderscheid tussen verschillende soorten aanbiederactiviteiten: de doorgifte (ook wel: *mere conduit*), het geautomatiseerd tussentijds en tijdelijk opslaan (denk aan *proxy-caching*) en de opslag van gegevens op verzoek (ook wel: *hosting*), al komen de termen 'mere conduit', 'caching' en 'hosting' zelf niet meer terug in de voorgestelde wetsbepaling.[31] In het Wetboek van Strafrecht wordt een niet-vervolgingsgrond opgenomen te behoeve van de 'tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van

---

[26] Zie Sieber 2002, p. 245-266, voor een internationaal overzicht van regelingen van aansprakelijkheid van Internetaanbieders.
[27] Richtlijn 2000/31/EG, *PbEG* 2000, L 178/1.
[28] Rb.'s-Gravenhage 9 juni 1999, *Informatierecht/AMI* 1999, p. 110-115.
[29] TK 1999-2000, 26 671, nr. 5 (Computercriminaliteit II).
[30] TK 2001-2002, 28 197, nrs.1-2.
[31] Zie het voorgestelde art. 6: 196c BW.

gegevens die van een ander afkomstig zijn'.[32] De tussenpersoon wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.

2.2.3. Canada

Artikel 13 lid 3 van de *Human Rights Act* uit 1985 voorziet in uitsluiting van aansprakelijkheid van netwerkaanbieders. Het is onduidelijk of deze bepaling ook van toepassing kan worden geacht op toegangsaanbieders. De regulering van aansprakelijkheid van Internetaanbieders wordt voor het overige overgelaten aan de provincies. Alleen Quebec kent op dit vlak specifieke wetgeving. De *Act to provide a legal framework for information technology* van 2001[33] kent een algemene aansprakelijkheidsuitsluiting voor Internetaanbieders, gekoppeld aan een *notice and take-down*-mechanisme.

De verplichtingen van Internetaanbieders bij de bestrijding van kinderporno zijn wel federaal geregeld. In maart 2001 heeft de federale regering van Canada een omvattend wetsvoorstel tot wijziging van het Wetboek van Strafrecht ingediend, waarmee onder andere kinderpornografie via het Internet bestreden moet worden (zie par. 3.3.3).[34] Internetaanbieders worden verplicht op bevel van een rechter een elektronische kopie van het materiaal aan de rechtbank ter beschikking te stellen, de opslag en beschikbaarstelling van het materiaal te beëindigen en informatie te verschaffen over de identiteit en de verblijfplaats van de inhoudsaanbieder.

2.2.4. Duitsland

De Europese richtlijn inzake elektronische handel voorziet zoals gezegd in een regeling over de aansprakelijkheid van Internetaanbieders (art. 12-15). Omdat in Duitsland telecommunicatie tot de bevoegdheid van de bond behoort en omroep tot de bevoegdheid van de bondsstaten, wordt de richtlijn 'dubbel' geïmplementeerd. Op het niveau van de bond wordt de richtlijn geïmplementeerd in het *Elektronischer Geschaftsverkehrgesetz* dat in december 2001 in werking is getreden.[35] Deze wet brengt wijziging in het *Teledienstegesetz*, dat reeds een eigen Duitse regeling over de (niet-)aansprakelijkheid van Internetaanbieders bevatte. Op het niveau van de bondsstaten wordt het geïmplementeerd in het Duits staatsverdrag tot wijziging van het Duitse staatsverdrag betreffende de mediadiensten (*Mediendiensteänderungsstaatsvertrag*).[36] Een ontwerp voor dit verdrag is aan de Europese Commissie genotificeerd.

2.2.5. Frankrijk

De Franse regering heeft op 13 juni 2001 een wetsvoorstel voor de implementatie van de e-handelrichtlijn (*Projet de loi sur la société de l'information*[37]) geïntroduceerd,[38] waarin onder andere de Wet op de communicatievrijheid (*Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*) wordt aangepast. Deze wet kende al een eigen Franse regeling over de aansprakelijkheid van Internetaanbieders. Volgens de 'oude' regeling zijn Intenetaanbieders slechts civielrechtelijk of strafrechtelijk aansprakelijk, indien zij niet prompt de toegang tot inhoud blokkeren zodra een gerechtelijke autoriteit hen bevolen heeft zulks te doen. Aangezien

---

[32] Zie het voorgestelde art. 54a Sr.
[33] S.Q. 2001 c.32, <http://www.assnat.qc.ca/archives-36leg1se/eng/Publications/Projets-loi/publics/00-a161.htm>.
[34] <http://www.parl.gc.ca/PDF/37/1/parlbus/chambus/house/bills/government/C-15_1.pdf>. Zie met name de wijzigingen in de artikelen 161, 163, 164 en 172 van het Canadese Wetboek van Strafrecht.
[35] Zie het *Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr* (*Elektronischer Geschäftsverkehr-Gesetz*, EGG) van 14 december 2001, *Bundesgesetzblatt* 2001, 20 december 2001, p. 3721-3728, zie <http://www.iid.de/iukdg/EGG/index.html> en <http://217.160.60.235/BGBL/bgbl1f/b101070f.pdf>.
[36] De concepttekst van het verdrag is beschikbaar op <http://europa.eu.int/comm/enterprise/tris/webdata/2001240NL.doc>.
[37] Zie <http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/prepa/pli.htm>.
[38] Zie <http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi.htm>.

het wetsvoorstel is vervallen door de verkiezingen van 2002, blijft voorlopig de oude regeling bestaan.

2.2.6 Japan

Japan onderhoudt een dialoog met de VS over onderwerpen van gemeenschappelijke zorg in de grenzeloze Internetwereld. Een van de onderwerpen die daar aan de orde komen is het wegen van de belangen en beschermen van de rechten van Internetaanbieders en rechthebbenden door de totstandbrenging van duidelijke regels over ISP-aansprakelijkheid.[39]
Op 22 november 2001 is een nieuwe wet over aanbiederaansprakelijkheid goedgekeurd en afgekondigd.[40] De wet is in mei 2002 in werking getreden. Zij regelt de wettelijke aansprakelijkheid van Internetaanbieders en webstekbeheerders voor de overdracht van materiaal dat inbreuk maakt op rechten van derden. Voor de bepaling van de aansprakelijkheid is van belang of de aanbieder technisch in staat is de overdracht van materiaal te voorkomen en de wetenschap draagt dan wel redelijkerwijze kan hebben van het inbreukmakend karakter van het materiaal. Op verzoek van de gelaedeerde verstrekt de aanbieder informatie over de verzender van het materiaal indien dit nodig is om een rechtsvordering te kunnen instellen of voor een andere legitieme reden.

In april 2002 heeft een *industry panel* richtlijnen afgekondigd over de verwijdering van informatie van weblocaties ter voorkoming van privacy- of auteursrechtinbreuken.[41]

2.2.7. Verenigd Koninkrijk

Het Verenigd Koninkrijk is een uitgebreide publieke consultatie gestart over de implementatie van de richtlijn inzake elektronische handel, waarbij zowel het Department of Trade and Industry[42] als HM Treasury[43] is betrokken. Een datum voor een officieel wetsvoorstel was begin juni 2002 niet bekend. Implementatie wordt verwacht in de zomer van 2002.[44] Het conceptvoorstel – de *Electronic Commerce (EC Directive) Regulatons 2002*[45] – voorziet in een regeling over de aansprakelijkheid die tekstueel dicht aanligt tegen de regeling in de richtlijn.

2.2.8. Verenigde Staten

De VS kent al langere tijd enkele sectorale wetten over de aansprakelijkheid van Internetaanbieders, zoals de *Communications Decency Act* van 1996 (die voor dit gedeelte niet ongrondwettig is verklaard) en de *Digital Millennium Copyright Act* uit 1998, die een specifieke regeling van een *notice-and-take-down regime* bevat.[46]
Een aantal grote Amerikaanse Internetaanbieders heeft in januari 2002 US ISPA opgericht, een vereniging die de belangen van Amerikaanse ISP's behartigt.[47] US ISPA wil nauwe banden onderhouden met rechtshandhavende instanties en tegelijkertijd de privacy van abonnees en de integriteit van netwerken garanderen.[48]
In december 2001 is de *Cybersecurity Enhancement Bill of 2001* (HR 3482) aan het congres aangeboden.[49] De voorgestelde wet slecht een aantal barrières die de samenwerking tussen Internetaanbieders en rechtshandhavende instanties bemoeilijken.

---

[39] 'Economic Minister Michalak's Remarks before the Council for Regulatory Reform', <http://www8.cao.go.jp/kisei/giji/010/1-2.html>.
[40] <http://www.freshfields.com/practice/ipit/publications/newsletters/ip-update/2855.pdf>.
[41] Zie <http://www.qlinks.net/quicklinks/liabil.htm>.
[42] Zie <http://www.dti.gov.uk/cii/ecommerce/europeanpolicy/ecommerce_directive.shtml>.
[43] Zie <http://www.hm-treasury.gov.uk/consultations_and_legislation/financial_services_and_markets_act/ecommerce/fsma_ecommerce_index.cfm>.
[44] Zie <http://www.euractiv.com/cgi-bin/cgint.exe/?1100=1&204&OIDN=1502808>.
[45] Zie <http://www.dti.gov.uk/cii/docs/regulations.pdf>.
[46] Zie hierover Landwell 2000, p. 49-50, en Sieber 2002, p. 252-259.
[47] Zie <http://www.usispa.org>.
[48] Zie <http://www.usispa.org/pressreleases.html>.
[49] Zie <http://www.usispa.org/pdf/HR3482.pdf>.

2.2.9. Zweden

Zweden heeft de richtlijn inzake elektronische handel geïmplementeerd in de *Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster* van 6 juni 2002 (Wet op de elektronische handel en andere diensten van de informatiemaatschappij).[50] De wet kent een drietal bepalingen (artikelen 16-18) die tekstueel dicht aanliggen tegen de bepalingen over *mere conduit*, *caching* en *hosting* in de richtlijn.[51] Voor strafrechtelijke verhoudingen wordt bepaald dat een dienstverlener die informatie ten behoeve van derden opslaat of transporteert, slechts voor een misdrijf in verband met de inhoud van informatie veroordeeld kan worden als het opzettelijk is begaan (artikel 19).
Zweden kende overigens al een regeling voor de aansprakelijkheid van *Bulletin Board System*-houders, waarvan werd aangenomen dat zij ook op Internetaanbieders van toepassing is.[52]

2.2.10. Samenvatting

In Europa vindt een harmonisatieslag plaats onder invloed van de richtlijn inzake elektronische handel. De meeste van de onderzochte implementaties (Duitsland, Nederland, Verenigd Koninkrijk en Zweden) nemen bepalingen in hun wetgeving op die tekstueel overeenstemmen met of dicht aanliggen tegen de regeling in de richtlijn (of hebben wetsvoorstellen van die strekking geformuleerd). Frankrijk heeft bij de implementatie een duidelijke vertaalslag naar het Franse recht gemaakt. De Franse aansprakelijkheidsregels staan verspreid over drie wetten (de Wet op de communicatievrijheid, het Wetboek van intellectuele eigendom en het Wetboek van post en telecommunicatie). Daarbij is niet steeds duidelijk of de Franse termen (bijv. 'opérateur de télécommunications' en 'offrir un accès') wel steeds de Europese concepten (bijvoorbeeld *caching (provider)* respectievelijk *mere conduit*) dekken.
In een aantal van de onderzochte implementaties wordt voor de strafrechtelijke aansprakelijkheid een van de civiele aansprakelijkheid afwijkende benadering gekozen. De implementaties met betrekking tot de strafrechtelijke aansprakelijkheid zijn ook aanzienlijk minder homogeen. Zo staat in de Zweedse regeling het opzet van de Internetaanbieder centraal en in Nederland het 'bevel van de officier van justitie'. Frankrijk heeft de bestaande strafrechtelijke vrijstelling met betrekking tot *hosting*activiteiten geschrapt. De Duitse implementatie van de aansprakelijkheidsbepalingen heeft – zonder onderscheid – zowel gelding voor het strafrecht als voor het civiele recht. Van echte harmonisatie op het gebied van het strafrecht kan derhalve niet gesproken worden.
Ook in de buiten-Europese landen worden aparte regels voor de aansprakelijkheid van Internetaanbieders opgesteld. Een opvallend verschil tussen de Europese en de Amerikaanse benadering van de aansprakelijkheid van Internetaanbieders is dat Europa gekozen heeft voor een integrale, algemene regeling die voor alle soorten onrechtmatige informatie en activiteiten geldt. De VS kent daarentegen meer een ad hoc-benadering met verschillende regelingen die ieder slechts op bepaalde onrechtmatigheden zien, naast elkaar bestaan. Zo heeft de *Digital Millennium Copyright Act* een notice-and-take-down regime gevestigd met betrekking tot auteursrechtinbreuken. De *Communications Decency Act* bevat een vrijstelling van aansprakelijkheid met betrekking tot smaad en laster. Daar staat tegenover dat de VS, in tegenstelling tot de EU, met de *notice-and-take-down*-regeling wel een wettelijke procedure heeft geschapen voor het (al dan niet) verwijderen van mogelijk inbreukmakend materiaal van het Internet, hetgeen de rechtszekerheid voor alle partijen ten goede lijkt te komen.
Canada kent op federaal niveau geen algemene regeling van aansprakelijkheid van Internetaanbieders, maar beperkt zich tot een regeling voor kinderpornografie. De benadering van de Japanse regeling lijkt daarentegen meer op de Europese dan op de Amerikaanse aanpak.

---

[50] Beschikbaar via <http://.194.52.125.3>.
[51] Vgl. <http://europa.eu.int/comm/enterprise/tris/webdata/200275NL.doc>.
[52] Zie <http://dsv.su.se/jpalme/society/swedish-bbs-act.html> en Sieber 2002, p. 248.

2.3. Elektronische overheid

De ontwikkelingen op het terrein van de elektronische handel en de elektronische overheid staan zeker niet los van elkaar. Het is om deze reden van belang in deze rapportage ook stil te staan bij de ontwikkelingen rondom de elektronische overheid. Daarbij zullen niet alle ontwikkelingen inzake de e-overheid aan bod komen, maar zal vanuit een algemene inventarisatie een toespitsing plaatsvinden op de relatie *business-to-government* (B2G). Immers, de ICT-ontwikkelingen binnen het bedrijfsleven worden deels ook beïnvloed door de mate en de wijze waarop het bedrijfsleven gebruik kan maken van ICT in de informatierelaties met de overheid. Ontwikkelingen in met name de Verenigde Staten laten zien dat er aldaar steeds meer aandacht is voor de mogelijkheden die online communicatie biedt om in de *government-to-business*-relatie (G2B) administratieve lasten te reduceren, via de éénloketgedachte efficiënt met de overheid te kunnen communiceren alsmede bedrijven meer inzicht te bieden in toepasselijke wettelijke regelingen.
Hiernaast zal in het onderstaande stil worden gestaan bij de interferentie tussen ontwikkelingen op het terrein van elektronische handel enerzijds en de elektronische overheid anderzijds. De recente aandacht voor deze interferentie blijkt allereerst uit de constatering dat diverse problemen waar in het recente verleden vanuit het thema elektronische handel aandacht voor werd gevraagd, nu ook naar voren blijken te treden bij de (verdere) ontwikkeling van elektronische dienstverlening door de overheid. Het gevolg is dat steeds meer beleidsdocumenten over de elektronische overheid wijzen op de lessen die mogelijk zijn te trekken uit eerdere ervaringen rondom regulering van elektronische handel. Zo wordt er in een recent beleidsdocument van de Amerikaanse president Bush op gewezen dat bij de verdere ontwikkeling van e-overheidsdiensten veel meer bekeken moet worden in hoeverre lering kan worden getrokken uit eerdere ervaringen op het terrein van de elektronische handel en in welke mate het mogelijk is: 'to apply the tools of E-Business to create E-Government'.[53] De interferentie van e-handel en e-overheid blijkt ook uit het feit dat het succes dan wel het falen van de inzet van bepaalde toepassingen binnen beide domeinen sterk afhankelijk van elkaar lijkt te zijn. Een illustratief voorbeeld in deze is de toepassing en het uiteindelijke succes van de digitale handtekening.

2.3.1. Internationaal

Op internationaal niveau zijn voor wat betreft het onderwerp elektronische overheid de ontwikkelingen in Europees verband relevant en dan specifiek binnen het zogenaamde *eEurope*-initiatief, dat in maart 2000 tijdens de zogenaamde 'dot-com'-top in Lissabon door de regeringsleiders werd gepresenteerd.[54] In juni 2001 organiseerde het Zweedse voorzitterschap van de Europese Unie onder de vlag van dit *eEurope*-initiatief een conferentie onder de titel "eGovernment in the service of European citizens and enterprises. What is required at the European level?" De belangrijkste doelstelling van de bijeenkomst was te komen tot een beter inzicht in de mogelijkheden van e-overheidsdiensten op Europees niveau. Zowel burgers als bedrijven zouden meer moeten kunnen profiteren van elektronische informatievoorziening door en communicatie met de Europese instellingen. De diverse vertegenwoordigers van de lidstaten stelden in Zweden vast dat hun nationale overheden weliswaar allemaal in meer of mindere mate vorm geven aan het concept elektronische overheid, maar dat deze dienstverlening vooralsnog beperkt blijft tot de eigen onderdanen. Ook blijken de ontplooide activiteiten in sterke mate te worden beïnvloed door de nationale administratieve en culturele tradities, waardoor ieder land in feite een geheel eigen visie op de 'elektronische overheid' heeft. Echter, zo stelden de deelnemers vast, "Within the single market citizens and enterprises in other Member States are also potential customers of these e-government services. Examples include on-line public procurement, company registration, change of residence, etc. The challenge for Europe's public administrations, therefore, is to ensure that e-government services are open to other Member

[53] 'New E-Government Strategy is Roadmap to Better Service. 24 New Initiatives Help Millions Who Access the Government Online' <http://www.whitehouse.gov/omb/pubpress/2002-11.html>.
[54] Beschikbaar via <http://europe.eu.int/comm/information_society/eeurope/>.

States' citizens and enterprises, to ensure the respect of single market principles".[55] In de slotverklaring werden de volgende punten geformuleerd:

- Er moet een gemeenschappelijke visie komen op de wijze waarop e-overheidsdiensten worden ontwikkeld en geïmplementeerd. Hierbij dient het uitgangspunt te zijn dat de verantwoordelijkheid voor de implementatie op decentraal niveau ligt, met wel een duidelijk beeld over de rol van de lidstaten, de Europese Commissie en andere betrokken instellingen.
- De te formuleren visie dient duidelijk te maken op welke wijze overheidsorganisaties zeker stellen dat burgers en bedrijven voldoende vertrouwen hebben in de elektronische vorm van communiceren met de overheid.
- De visie moet eveneens aandacht schenken aan de maatregelen die worden genomen om een grotere mate van transparantie in en betrokkenheid van burgers bij het regelgevend proces van de EU en de nationale overheden te bewerkstelligen.
- Overheidsinstellingen zijn niet alleen verantwoordelijk voor het vormgeven van een elektronische overheid. Ook de private sector moet hier nadrukkelijk bij worden betrokken.
- De introductie van een e-overheid is niet uitsluitend een zaak van technische oplossingen. De meerderheid van de maatregelen ligt op het terrein van de organisatorische processen.
- Er is geen uniek concept van een e-overheid. Het verdient aanbeveling dat de betrokken overheidsorganisaties voor de nieuwe diensten meerdere varianten en instrumenten ontwikkelen en inzetten (bijv. PCs, kiosks, digitale televisie, GSM, sms, WAP).

Een recent gepubliceerde ijkdoelstudie uitgevoerd onder de vlag van het *eEurope*-initiatief laat zien dat in de diverse lidstaten van de Europese Unie de nodige initiatieven in gang zijn gezet voor elektronische overheidsdiensten.[56]
Met name wat betreft de initiatieven op het terrein van B2G is van belang te vermelden dat de Europese Commissie in het voorjaar van 2002 aankondigde een beveiligde communicatieinfrastructuur op te gaan zetten waar ook bedrijven in hun relatie met de diverse Europese overheidsdiensten gebruik van moeten gaan maken. De doelstelling van de infrastructuur is om te komen tot 'a platform for new pan-European eGovernment services to citizens and enterprises by improving co-operation between European public services at all levels of government.'[57]

2.3.2. Nederland

In Nederland is de afgelopen jaren een groot aantal beleidsdocumenten, plannen en ambities gepubliceerd om de overheid van een digitale identiteit te voorzien. De start werd gegeven met de presentatie, eind 1998, door minister Van Boxtel van het *Actieprogramma Elektronische overheid*.[58] Sinds die tijd heeft een groot aantal vervolgnota's en projecten het licht gezien.[59] Uit het jaar 2000 kunnen de notitie *De Digitale Delta: e-Europe voorbij*[60] en de voortgangsrapportage *De elektronische Overheid aan het begin van de 21e eeuw* worden genoemd.[61] Voorjaar 2001 concludeerde een onderzoek naar 165 overheidsdiensten in 22 landen dat Nederland het goed doet met de digitale overheid.[62] De kopgroep werd gevormd door Canada, Singapore en de Verenigde Staten. In de loop van 2001 verscheen een groot aantal rapporten met verdere plannen (Commissie-Snellen, Commissie-Wallage, Commissie-Scheltema, Commissie-Docters van Leeuwen) alsmede een rapportage vanuit het kabinet over de voortgang van de in de Digitale Delta genoemde

---

[55] <http://europa.eu.int/ISPO/ida/>.
[56] eEurope-Benchmarkingverslag, COM(2002) 62def, februari 2002, beschikbaar via <http://europa.eu.int/eurlex/nl/com/cnc/2002/com2002_0062n101.pdf>.
[57] *Computer Law & Security Report* mei/juni 2002, p. 227-228. Meer informatie over het plan is te vinden via <http://europa.eu.int/ISPO/ida/>.
[58] Actieprogramma Elektronische Overheid, TK 1998-1999, 26 387, beschikbaar via <http://www.minbzk.nl/e-overheid>. Zie ook de eerste rapportage van 23 december 1999, TK 1999-2000, 26 387, nr. 4.
[59] Zie hierover de diverse documenten onder kamerstuknummer 26 387.
[60] TK 2000-2001, 26 643, nr. 14.
[61] TK 2000-2001, 26 387, nr. 9.
[62] Onderzoek Accenture, *Webwereld* 9 april 2001.

initiatieven.[63] Het rapport van de Commissie-Scheltema resulteerde in concrete voorstellen tot aanpassing van wetgeving (de Algemene wet bestuursrecht) aan het elektronisch overheidsbesluit. Het wetsvoorstel daartoe werd eind 2001 naar de Raad van State gezonden.
Van belang om te noemen met betrekking tot de relatie B2G, zijn de initiatieven inzake authentieke registraties, eenmalige gegevensverstrekking en een *public key infrastructure* (PKI-overheid). Juist wat dit laatste initiatief betreft, lijkt inmiddels ook duidelijk te worden dat het samen optrekken van overheid en bedrijfsleven noodzakelijk is voor een succesvolle introductie en gebruik van digitale handtekeningen. Een belangrijke overweging hierbij lijkt ook de hoge eisen die ten aanzien van de geavanceerde handtekening in de Europese Richtlijn elektronische handtekeningen zijn gesteld.

2.3.3. Canada

Op 1 april 2002 trad in Canada de *Communications Policy of the Government of Canada* in werking.[64] Doelstelling ervan "is to ensure that communications across the Government of Canada are well co-ordinated, effectively managed and responsive to the diverse information needs of the public." Het gebruik van ICT speelt een belangrijke rol bij het realiseren van deze doelstelling, waarbij "access to information and privacy rights, as well as language rights, must be honoured at all times."[65] Waar de nieuwe *Communications Policy* slechts zijdelings op de rol van ICT wijst, presenteert het uit 1999 daterende *Strategic Directions for Information Management and Information Technology. Enabling 21st Century Service to Canadians* diverse e-overheidspecifieke doelstellingen.[66] Opvallend is de grote aandacht voor de ontwikkeling van een *public key infrastructure* (PKI). Deze zal niet alleen een rol moeten spelen bij het bevorderen van vertrouwen in en veiligheid van de elektronische communicatie met de overheid, maar ook wezenlijk zijn voor de bescherming van persoonsgegevens en de acceptatie van *privacy-enhancing technologies* (PET).[67] De regering van Canada wijst expliciet op het belang te komen tot een internationale afstemming in dezen "to promote PKI implementation and interoperability."[68] (Zie ook par. 5.3.3.) Om het succes van PKI en de digitale handtekening te onderstrepen gebruikten twee Canadese en twee Britse ministers de faciliteit bij het ondertekenen van een samenwerkingsovereenkomst tussen de twee landen op het terrein van e-handel en e-overheid.[69] Bij deze gelegenheid gaven de regeringsvertegenwoordigers aan dat de twee landen grote waarde hechten aan de verdere ontwikkeling van elektronische overheidsdiensten. De beide landen willen op dit terrein informatie, *best practices* en ervaringen uitwisselen om zo samen effectiever en efficiënter om te gaan met nieuwe vormen van elektronische dienstverlening.

2.3.4. Duitsland

In Duitsland kwam de regering op 18 september 2000 met de nota *BundOnline 2005*,[70] waarin het een scala aan plannen ontvouwt om de komende jaren enkele honderden overheidsdiensten van een elektronische variant te voorzien. Veel aandacht is er in het rapport voor de wijze waarop ten behoeve van de gewenste betrouwbaarheid van de nieuwe online diensten gewerkt moet worden met 'anwenderfreundlichen, aber den rechtlichen Rahmenbedingungen genügenden Signatursystemen'.[71]

---

[63] TK 2001-2002, 26 643, nr. 32.
[64] Beschikbaar via <http://www.tbs-sct.gc.ca/pubs_pol/sipubs/comm/comm1_e.html>. Deze vervangt de uit 1988 daterende *Government Communications Policy*.
[65] Policy Statement no. 7.
[66] Zie ook eerder: *Blueprint for Renewing Government Services Using Information Technology*, <http://www.ifla.org/documents/infopol/canada/tb-bp.txt>.
[67] Treasury Board of Canada, *Strategic Directions for Information Management and Information Technology. Enabling 21st Century Service to Canadians*, 1999, <www.tbs-sct.gc.ca>; <www.cio-dpi.gc.ca/home_e.html>, p. 14.
[68] Treasury Board of Canada, *Strategic Directions for Information Management and Information Technology. Enabling 21st Century Service to Canadians*, 1999, <www.tbs-sct.gc.ca>; <www.cio-dpi.gc.ca/home_e.html>, p. 14.
[69] <http://e-com.ic.gc.ca/english/inter/72d4.html>.
[70] <http://www.staat-modern.de/infos/daten/egovernment.pdf>.
[71] <http://www.staat-modern.de/infos/daten/egovernment.pdf>, p. 7.

Ruim een jaar na het verschijnen van de nota, op 11 december 2001, presenteerde de Minister van Binnenlandse Zaken het concrete implementatieplan om welgeteld 376 overheidsdiensten die geschikt zijn voor een Internetapplicatie, daarvan ook daadwerkelijk te voorzien. Inmiddels wordt ook hard gewerkt aan een adequate juridische basis voor de initiatieven. Op 16 juli 2001 verscheen het *Entwurf eines Dritten Gesetzes zur Aenderung verwaltungsverfahrensrechtlicher Vorschriften*.[72] Het betreft een aanpassing van de bestuursrechtelijke wetgeving om aldus de rechtsgeldigheid van de elektronische afhandeling van overheidsbesluiten te garanderen. Uitgangspunt van de aanpassing is dat een overheidsdienst niet kan worden gedwongen een elektronisch overheidsbesluit af te geven. Overheidsbesluiten kunnen online worden afgegeven op voorwaarde dat de desbetreffende overheidsorganisatie heeft aangegeven dat deze weg openstaat.[73]
Behalve op federaal niveau, worden binnen de individuele deelstaten ook vele plannen voor elektronische dienstverlening door (lokale) overheden ontvouwd. Zo wordt in de plannen van de deelstaat Nordrhein-Westfalen veel aandacht gegeven aan de brede uitgifte van een elektronische 'Signaturkarte' waarmee burgers zich in hun relatie met de overheid kunnen identificeren en waar ook een betaalfunctie aan gekoppeld kan worden voor betalingen aan overheidsdiensten.[74]

2.3.5. Frankrijk

De Franse regering heeft, in verhouding tot diverse andere landen waaronder Nederland, tot voor kort weinig aandacht gehad voor ontwikkelingen binnen het thema elektronische overheid. In het langverwachte wetsvoorstel *Projet de loi sur la société de l'information* van 13 juni 2001 werd voor het eerst aandacht besteed aan onderwerpen als toegang van burgers tot elektronische informatie, vrijheid bij online communicatie en de verdere ontwikkeling van digitale infrastructuur.[75] Aangezien het wetsvoorstel echter is vervallen door de verkiezingen van 2002, worden deze bepalingen vooralsnog niet geïmplementeerd.

Op 26 februari 2002 verscheen het zogenaamde Truche-rapport getiteld *Administration Électronique et Protection des Données Personnelles*.[76] In het rapport wordt een poging gedaan te komen tot een belangenafweging tussen enerzijds de verdere ontwikkeling van een elektronische overheid en de daarbij behorende dienstverlening en anderzijds de bescherming van de persoonlijke levenssfeer van burgers. In het rapport wijst de Franse overheid de introductie van een uniform en uniek nationaal identiteitskenmerk voor alle elektronische communicatie met de overheid van de hand. Verder presenteert het rapport meerdere scenario's waarin de ontwikkeling van een 'e-administration' gecombineerd kan worden met privacybescherming. Hierbij wordt een soortgelijk voorstel als de in Nederland door de Commissie-Snellen voorgestelde digitale kluis gepresenteerd. In het Franse voorstel moeten burgers de mogelijkheid krijgen deze kluis te openen dan wel gesloten te houden bij hun communicatie met de overheid. Via de pagina <www.foruminternet.org> kan over de voorstellen van de Franse regering worden meegediscussieerd.

2.3.6. Japan

Uit de schaarse beleidsdocumenten waarin de regering van Japan aandacht besteedt aan de ontwikkeling van een elektronische overheid, blijkt dat anno 2002 de eerste voorzichtige stappen op dit terrein worden gezet. In het *e-Japan 2002 Program-Basic Guidelines Concerning the IT Priority Policies in FY2002* wordt aangegeven dat de aandacht met name zal uitgaan naar de ontwikkeling van een goede beveiligingsinstrumenten voor de elektronische overheidsdiensten, waarbij in het belang van de te ontwikkelen en evalueren beveiligingsprocedures ook maatregelen zullen

---

[72] Beschikbaar op <http://www.im.nrw.de>.
[73] Een uitgebreide bespreking en analyse van deze en andere ontwikkelingen in het buitenland is te vinden in de ITeR-studie Prins 2002.
[74] *E-Government in der Landesverwaltung Nordrhein-Westfalen. Sachstandsbericht*, Ministerie van Binnenlandse Zaken, juni 2001, p. 11-12, <http://www.im.nrw.de/inn/doks/itkonz.pdf>.
[75] <http://www.lsi.industrie.gouv.fr>.
[76] Truche 2002, beschikbaar op <www.fonction-publique.gouv.fr/communications/rapports/rapports_index.htm>.

worden genomen als 'ethical hacking'. Genoemd worden verder proefprojecten als elektronisch stemmen, het elektronisch indienen van aanvragen voor bepaalde voorzieningen, elektronische faciliteiten voor het binnenkantoor van de overheid en elektronische betaalsystemen.[77] Ten slotte dient iedere dienst een eigen beleidsplan te formuleren voor het bevorderen van elektronische informatievoorziening aan burgers en bedrijven.

2.3.7. Verenigd Koninkrijk

Sedert de publikatie, in 1996, van het beleidsdocument '*government.direct*'[78] is in het Verenigd Koninkrijk in diverse rapporten en plannen aandacht besteed aan de ontwikkeling van de elektronische overheid. Genoemd kan onder meer worden het rapport *E.gov. Electronic Government Services for the 21st Century*[79], waarin voor een groot aantal overheidsdomeinen (onderwijs, rechterlijke macht, sociale zekerheid, milieu, etc.) nieuwe projecten en doelstellingen worden geformuleerd. Hiervan kunnen vanuit een B2G-perspectief worden genoemd de realisatie van online verlening van octrooi, elektronische bedrijfsregistratie en de verdere digitalisering van de rechterlijke macht. Het *UK Online Annual Report*[80] uit december 2001 somt een groot aantal nieuwe initiatieven op, waarvan hier genoemd worden de ontwikkeling van een elektronisch systeem voor betalingen aan overheidsinstanties, het aanpakken van de huidige problemen voor authentificatie en beveiliging bij alle vormen van elektronische communicatie (in de private en publieke sector), het opzetten van pilots voor elektronisch aanbesteden en het optimaliseren van toegang tot overheidsinformatie en overheidsdiensten via de éénloketgedachte. Interessant is ook het plan om ieder bedrijf en iedere burger een eigen elektronische agent te geven "to act on your behalf for one or more Government services."
Om de doelmatigheid van elektronische communicatie met de overheid te verhogen te verhogen gaf e-Envoy Pinder (de speciaal ter stimulering van ICT-ontwikkelingen aangestelde hoge ambtenaar), bij de presentatie van het rapport aan dat dwingende standaarden voor elektronische overheidsdiensten zullen worden ontwikkeld.[81]
Inmiddels heeft het bureau van de e-Envoy acht richtlijnen voor beleidsmakers gepubliceerd die veel overeenkomsten vertonen met de handvatten zoals door het Nederlandse kabinet gepresenteerd in de Notitie 'Internationalisering en rechtsmacht' uit 2000. Het betreft richtlijnen als 'consider self and co-regulation', 'regulation should be technology neutral', 'check proposals are enforceable in an electronic age' en 'take account of the global market place – the EU and the international angle'.[82] De laatste van de acht richtlijnen wijst beleidsmakers op implicaties in relatie tot het onderwerp elektronische overheid: 'consider the implications for e-government'.

2.3.8. Verenigde Staten

In de afgelopen jaren heeft de federale overheid van de Verenigde Staten diverse beleidsdocumenten gepubliceerd op het terrein van de elektronische overheid. In 1993 namen de VS, zoals bij veel ICT-gerelateerde ontwikkelingen, als eerste land ter wereld het initiatief op dit terrein met een rapport over de toekomst van de e-overheid.[83] Sedertdien verscheen een groot aantal beleidsdocumenten, waarvan in ieder geval hier genoemd moet worden het op 24 juni 2000 door president Clinton gepresenteerde rapport waarin plannen werden gepresenteerd om het volk te voorzien van – in de woorden van president Clinton – "the "Information Age"

---

[77] Beschikbaar via <http://www.kantei.go.jp/foreign/it/network/0626_e.html>, p. 8-9.
[78] Office of Public Service, *Government.direct. A Green Paper on the Electronic Delivery of Government Services*, Cm 3438, HMSO, november 1996. Beschikbaar via <http://www.citu.gov.uk/greenpaper.htm>. Zie voor een bespreking: Ch. Bellamy, J.A. Taylor , 'Understanding government.direct', *Information Infrastructure and Policy,* 1997-1, p. 1-16.
[79] Beschikbaar via <http://www.cabinet-office.gov.uk/innovation/2000/delivery/intro.htm>, p. 14-92.
[80] *UK Online Annual Report 2001*, p. 46-54 <http://www.e-envoy.gov.uk/ukonline/progress/anrep2001/default.htm>.
[81] *Computer Law & Security Report,* maart/april 2002, p. 137.
[82] <www.e-envoy.gov.uk/ecommerce_index.htm>.
[83] *National Performance Review*, Washington 1993. Zie tevens Office of the Vice President, *Re-engineering Government Through IT, Accompanying Report to the National Performance Review,* Washington DC, 1993 (<http://www.npr.gov/library/reports/it.html>).

government they deserve".[84] Mede naar aanleiding van deze maatregelen, kunnen burgers en bedrijven in de VS momenteel niet alleen zoeken in alle elektronische bronnen van de federale overheid, maar ook diverse zaken met deze overheid afhandelen via de webpagina <www.firstgov.gov> en de daaronder liggende pagina's.
Nadat hier door het Office of Management and Budget in oktober 2001 reeds met een publicatie op werd geanticipeerd,[85] presenteerde President Bush op 27 januari 2002 zijn eigen beleidsplan. Onder de titel *E-Government Strategy: Simplified Delivery of Services to Citizens* werden 24 initiatieven gelanceerd met als doel "to streamline service delivery to citizens, reduce paperwork burdens on businesses, and apply the best commercial practices to improve government operating efficiency."[86] Expliciet wordt aangegeven dat bij de verdere ontwikkeling van de elektronische overheid gekeken dient te worden in hoeverre geleerd kan worden van de eerdere ontwikkelingen en ervaringen op het terrein van de elektronische handel.
Van de initiatieven die in het beleidsplan worden gepresenteerd, kunnen in het licht van ontwikkelingen op het terrein van B2G hier worden genoemd:

- de verdere ontwikkeling van overheidsdienstverlening op maat 'in a privacy-protected environment';
- de realisatie van een 'online rulemaking management'-systeem dat fungeert als "a single portal for businesses and citizens to access the rulemaking process, creating a more collaborative and transparant atmosphere in which to make policy and public safety decisions";
- de ontwikkeling van een 'One-Stop Business Compliance'-portaalpagina, waar alle voor bedrijven relevante wet- en regelgeving beschikbaar is, specifieke uitleg over deze regels wordt gegeven alsmede vastgesteld kan worden in hoeverre de regelgeving van toepassing is en bedrijven zoveel als mogelijk de relevante formaliteiten online kunnen afhandelen.
- De introductie van een overheidsbreed e-authenticatiesysteem om op deze wijze een betrouwbare, uniforme en consistentie voorziening te krijgen voor de vaststelling van identiteit bij alle vormen van e-overheidsdienstverlening.

Voor het jaar 2002 is een bedrag van $10 miljoen gereserveerd als eerste bijdrage aan een fonds waaruit de komende drie jaar voor een totaalbedrag van $100 miljoen diverse projecten op het terrein van e-overheidsinitiatieven zullen worden gefinancierd. Met de middelen van dit fonds zal ook verder vorm worden gegeven aan "The Administration's ability to implement the Government Paperwork Elimination Act of 1998, which calls upon agencies to provide the public with optional use and acceptance of electronic information, services and signatures, when practicable, by October 2003."[87] Genoemd moet ook worden de ambitie om ICT grootschalig is te zetten bij alle procedures rondom overheidsaanbestedingen. Op deze wijze beoogt men de financiële en administratieve lasten voor het bedrijfsleven terug te dringen. Om een en ander te realiseren zullen ook de wettelijke regels zodanig worden (geher)formuleerd dat elektronische aanbestedingsovereenkomsten tussen bedrijven en overheid tot de mogelijkheden behoren.
Wat betreft de voor e-overheid relevante wettelijke initiatieven, kan worden gewezen op het voorstel voor de *E-Government Act of 2001* dat op 21 maart 2002 werd aangenomen door het Government Affairs Committee van de Senaat.[88] De wet beoogt onder meer:

- de toegankelijkheid en bruikbaarheid van overheidsinformatie verder te verbeteren;
- een *privacy impact assessment* verplicht te stellen bij het vergaren van informatie door overheidsdiensten;
- een speciale Federal Chief Information Officer aan te stellen.

De diverse staten blijven ook niet achter in de ontwikkeling van elektronische overheidsdiensten. Van alle initiatieven noemen we hier het plan van de Supreme Court van Michigan om de eerste

---

[84] Zie: <http://www.whitehouse.gov/textonly/WH/EOP/nec/html/egov000624.html>.
[85] <http://www.cio.gov/fpkisc/documents/pressrelease_omb_oct25.pdf>.
[86] Beschikbaar via <www.whitehouse.gov/omb/inforeg/egovstrategy>.
[87] *A Blueprint For New Beginnings – IX.Government Reform*, 28 februari 2001 <http://www.whitehouse.gov/news/usbudget/blueprint/budix.html>.
[88] Beschikbaar via <http://www.cdt.org/legislation/107th/e-gov/>.

U.S. *Cybercourt* op te richten. De eerste stap hiervoor werd op 9 januari 2002 gezet, toen de gouverneur van de staat een wet ondertekende waarmee het project tot de oprichting van een virtuele pendant van traditionele rechtbank van start ging. Inmiddels is een concept gepubliceerd van het juridisch kader voor de virtuele rechtspraak. Hierin worden onder meer de huidige regels voor en definities van de (veelal op basis van fysieke aanwezigheid en schriftelijke documenten gebaseerde) procedures aangepast. De jurisdictie van de rechtbank zal vooralsnog beperkt blijven tot geschillen over commerciële aangelegenheden. Beoogd wordt de virtuele rechtbank op 1 oktober 2002 'in de lucht' te hebben.[89]

2.3.9. Zweden

Zweden werd begin 2002 in de in paragraaf 2.3.1 genoemde ijkdoelstudie van de Europese Commissie, aangemerkt als Europees leider in e-overheidsdiensten. Uit deze studie werd overigens ook duidelijk dat in Zweden de aandacht primair uitgaat naar e-overheidsdiensten voor burgers en niet zozeer naar B2G-initiatieven.
Vanuit het perspectief B2G is wel vermeldenswaard de aandacht die in Zweden momenteel uitgaat naar het opzetten van zogenaamde 24/7-diensten. Deze diensten kenmerken zich door een elektronische beschikbaarheid van niet slechts enkele onderdelen van een bepaalde overheidsdienst, maar een volcontinue (24 uur per dag, 7 dagen in de week) elektronische beschikbaarheid van de gehele overheidsorganisatie. Daarbij dient deze beschikbaarheid vorm te krijgen via een enkel loket en dienen de diensten voor burgers en bedrijven transparant en uniform opgezet te zijn. In het voorjaar van 2000 werden voor de 24/7-diensten diverse criteria geformuleerd en momenteel vindt halfjaarlijks een rapportage van de vorderingen plaats.[90] Het project moet op 30 juli 2003 zijn afgerond.[91] Vanuit de Zweedse overheid wordt opgemerkt dat men verwacht dat de kracht van e-overheidsdiensten voor burgers en bedrijven niet uitsluitend moet liggen in éénloketfaciliteiten, maar juist in de combinatie van éénloketfaciliteiten en gespecialiseerde toegangsfaciliteiten, waarbij bedrijfsleven en overheid gezamenlijk moeten optrekken.[92]
Andere Zweedse projecten die van belang zijn voor de relatie B2G:

- het project om alle juridische belemmeringen en vragen voor elektronische communicatie door de overheid aan te pakken (waaronder vragen inzake aansprakelijkheid voor fouten bij de communicatie);
- het opzetten van een PKI-infrastructuur en stimuleren van betrouwbare communicatiesystemen;
- een verdere uitbouw van zogenaamde *one-stop shops* waar bepaalde overheidsinformatie op eenvoudige en transparante wijze verkregen kan worden, zoals 'the LawRoom' <www.lagrummet.gov.se/>, waar alle juridische documenten zijn te verkrijgen.

2.3.10. Samenvatting

Uit het voorgaande kan worden afgeleid dat Nederland vergeleken met de besproken landen zich zeker niet – zoals Japan – in de achterhoede bevindt, maar ook niet tot de koplopers behoort. Ook in ons land worden momenteel diverse plannen uitgewerkt die meer omvatten dan uitsluitend het automatiseren van traditionele processen, maar waarin ICT wordt ingezet om tot een vernieuwing van het functioneren van de overheid te komen. Genoemd kunnen hier worden de plannen rondom authentieke registraties, eenmalige gegevensverstrekking, de digitale kluis in combinatie met een bepaalde vorm van een recht op regie voor burgers. Nederland kent nog geen concrete wetgeving voor elektronische afhandeling van rechtspraak, zoals dit bijvoorbeeld op statelijk niveau in de VS wel het geval is.

---

[89] *Electronic Commerce & Law Report* 10 april 2002, p. 327-329.
[90] *Criteria for 24/7 Agencies in the Networked Public Administration*, mei 2000 <www.statskontoret.se/pdf/200041.pdf>.
[91] Swedish Agency for Public Management, *Country Report from Sweden for the GOL Portals Project Government On-Line International Network*, 20 juli 2001, p. 7.
[92] Swedish Agency for Public Management, *Country Report from Sweden for the GOL Portals Project Government On-Line International Network*, 20 juli 2001, p. 11.

Wat uit de beschreven plannen kan worden opgemaakt is dat diverse landen de ontwikkelingen rondom de elektronische overheid niet langer in een isolement bezien, maar aandacht vragen voor de interactie tussen diverse domeinen (dat wil zeggen elektronische handel en elektronische overheid). Men stelt zich de vraag welke eerdere ervaringen bij (de regulering van) elektronische handel kunnen worden benut bij de te maken keuzes op het terrein van de elektronische overheid. In het VK wordt van beleidsmakers zelfs gevraagd expliciet vast te stellen welke consequenties de gemaakte keuzes op het terrein van regulering van onder meer elektronische handel hebben voor het terrein van de elektronische overheid. Verder wordt ook op het terrein van de elektronische overheid steeds meer over de landsgrenzen heen gekeken en waar mogelijk samengewerkt. Ook op Europees niveau wordt hier expliciet de aandacht voor gevraagd. Als voorbeeld kan dienen de samenwerkingsovereenkomst gesloten tussen Canada en het VK om te komen tot het uitwisselen van *best practices* en informatie.
Wat betreft specifieke ontwikkelingen op het terrein van B2G gaat in de diverse landen meer algemeen de aandacht uit naar e-voorzieningen om de administratieve lasten voor het bedrijfsleven terug te dringen, 24 uur per dag en 7 dagen in de week elektronisch beschikbaar te zijn, bedrijven op maat gesneden informatie beschikbaar te stellen en de betrouwbaarheid van de elektronische communicatie (met PKI voorzieningen en digitale handtekeningen) te verbeteren. Meer concreet gaat het om de ontwikkeling van faciliteiten voor elektronische aanbesteding, het elektronisch betalen voor bepaalde overheidsdiensten en (in het VK) het beschikbaar stellen van een persoonlijke elektronische *agent* voor het afhandelen van communicatie met de overheid.
Ten slotte stellen we op basis van de landenvergelijking vast dat de beleidsplannen voor de (verdere) ontwikkeling van de elektronische overheid onderstrepen dat het niet alleen de overheidsinstellingen zijn die verantwoordelijkheid dragen voor het vormgeven van de elektronische overheid. Ook de private sector moet hier een actieve rol spelen en concreet bij de initiatieven worden betrokken. Met name binnen de uitwerking van het Europese *eEurope*-initiatief is dit naar voren gebracht. In ieder geval zien we reeds dat bij de discussie over de inrichting van een betrouwbare en uniforme elektronische identiteitsinfrastructuur (ontwikkeling van onder meer een Public Key Infrastructure) er ook daadwerkelijk een noodzaak is dat bedrijfsleven en overheid samen optrekken.

3. Bieden van rechtszekerheid

3.1. Privacy op het Internet

Een belangrijke remmende factoren voor de bloei van elektronische handel is de onzekerheid over de mate van bescherming van privacy op het Internet. Veel consumenten hebben weinig vertrouwen in de veiligheid en de privacybescherming in Internettransacties. Met name de bescherming van persoonsgegevens is van belang: via elektronische middelen zijn vele persoonsgegevens te verzamelen, vaak ongemerkt, waarbij koppeling van gegevens en bestanden een schat aan informatie kan opleveren over personen en hun voorkeuren. Dit faciliteert enerzijds het aanbieden van op maat gemaakte diensten, waardoor webhandel aantrekkelijker wordt, maar kan anderzijds een ongewenste inbreuk op de privacy opleveren, omdat de webhandelaar van de consument helemaal niet hóéft te weten welke voorkeuren hij heeft. De vraag is dan ook relevant in hoeverre e-bedrijven persoonsgegevens mogen verzamelen en gebruiken.
In deze paragraaf wordt met name aandacht besteed aan deze vraag. Er zijn diverse andere privacygerelateerde onderwerpen relevant voor e-handel; deze komen aan bod in andere paragrafen, zoals 3.3 (computercriminaliteit), 3.4 (terrorismebestrijding), 5.4 (cryptografie), 5.5 (commerciële communicatie en spam) en 5.6 (gedragscodes).

3.1.1. Internationaal

Voor privacy op het Internet is de aanbeveling van de Raad van Europa R (99)5 ter bescherming van de privacy op het Internet vermeldenswaard.[93] Deze aanbeveling bevat richtlijnen ter bescherming van personen met betrekking tot het verzamelen en verwerken van hen betreffende persoonsgegevens via het Internet. Deze richtlijnen zijn uitdrukkelijk tevens bestemd ter opneming in gedragscodes. Deze aanbeveling kwam tot stand tegen de achtergrond van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens[94] en diverse sectorale aanbevelingen ter bescherming van persoonsgegevens, in het bijzonder bij het gebruik van betalingsystemen,[95] de verstrekking van persoonsgegevens aan derden door overheidsorganisaties[96] en bij gebruik van telecommunicatiediensten.[97] De richtlijnen zijn bedoeld om Internetgebruikers en -aanbieders nogmaals te wijzen op de toepasselijkheid van de voorschriften in Verdrag no. 108 op het verzamelen en verwerking van persoonsgegevens in het licht van het Internet.

In de Europese Unie is de Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[98] inmiddels in de meeste lidstaten geïmplementeerd (maar nog niet in Frankrijk, Ierland, Italië en Luxemburg, hoewel dit uiterlijk 24 oktober 1998 had moeten plaatsvinden). Hierdoor is in de lidstaten de bescherming van persoonsgegevens grotendeels geharmoniseerd, met name de meldingsplicht, transparantie voor de burger, doelbinding, rechtmatige grondslag voor gegevensverwerking, kwaliteit van de gegevens, rechten voor betrokkenen, beveiliging van de gegevensverwerking, relatie met een eventuele bewerker en gegevensverkeer met landen buiten de EU.
Op dit laatste punt is bepaald dat alleen Hongarije, Zwitserland en Canada een passend beschermingsniveau kennen voor persoonsgegevens. De VS kent alleen een passend niveau indien de organisaties aldaar zich bij de Safe Harbor Principles hebben aangesloten, waarin de

---

[93] <http://cm.coe.int/ta/rec/1999/99r5.htm>.
[94] Verdrag van Straatsburg, 1981, no. 108,
<http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=>.
[95] R(90) 19, <http://cm.coe.int/ta/rec/1990/90r19.htm>.
[96] R(91) 10, <http://cm.coe.int/ta/rec/1991/91r10.htm>.
[97] R(95) 4, <http://cm.coe.int/ta/rec/1995/95r4.htm>.
[98] *PbEG* L281 van 23 november 1995, p. 0031-0050.

EU en de VS minimumeisen zijn overeengekomen voor de bescherming van persoonsgegevens (zie par. 3.1.8). Voor andere landen, en indien art. 26 lid 1 van de richtlijn niet van toepassing is, is het alleen toegestaan persoonsgegevens door te geven naar een derde land wanneer de verantwoordelijke een passend beschermingsniveau kan garanderen. Dat is bijvoorbeeld mogelijk door middel van een contract. Ten behoeve daarvan heeft de Commissie modelcontractbepalingen vastgesteld voor de doorgifte naar een andere verantwoordelijke of bewerker in een derde land.[99] Gebruikmaking van deze modelcontractbepalingen laat onverlet dat in sommige landen, waaronder Nederland, voor de doorgifte alsnog een vergunning van de minister verkregen dient te worden.

Naast de algemene richtlijn bescherming persoonsgegevens kent de EU de richtlijn 97/66/EG inzake privacy in de telecommunicatiesector. Deze richtlijn wordt vervangen door een richtlijn inzake privacy in de elektronischecommunicatiesector.[100] Eind mei 2002 werd in het Europees Parlement in tweede lezing overeenstemming bereikt over de meest omstreden punten: bewaring van verkeersgegevens voor opsporings- en veiligheidsdoeleinden, zie par. 3.3.1, en spam, zie par. 5.5.1, en het gebruik van cookies en andere middelen ter verzameling van persoonsgegevens via Internet, zoals *spyware* en webbugs.
In november 2001 stemde het Europees Parlement, op voorstel van de Nederlandse Europarlementariër Van Velzen, voor een verbod op ongevraagde cookies. Een dergelijk verbod zou het vertrouwen in het gebruik van Internet ten goede moeten komen. In het desbetreffende amendement werd voorgesteld om het verplicht te stellen voorafgaande toestemming (opt-in) te vragen voor het gebruik van verborgen volgmiddelen, zoals cookies. De Raad van de Europese Unie heeft deze eis tot voorafgaande toestemming echter niet overgenomen, maar omgezet in een kennisgevingplicht en een recht voor de gebruiker om dergelijke middelen te weigeren (opt-out). De Raad was van mening dat het gebruik van volgmiddelen in veel gevallen dient om de levering van diensten via elektronische communicatienetwerken te vergemakkelijken, zodat voorafgaande toestemming een ongerechtvaardigde belemmering voor dit soort toepassingen zou gaan vormen. Door gebruikers volledig te informeren over de bedoeling van detectiemiddelen en het recht te geven dergelijke middelen van hun eindapparatuur te weren, kan eveneens worden voldaan aan de doelstelling om het recht op privacy van de gebruiker te waarborgen. De Commissie aanvaardt deze aanpak en is van mening dat hiermee de juiste balans is gevonden tussen het amendement van het EP en de ongerustheid van de exploitanten over dit amendement. De opt-out regeling met betrekking tot cookies is neergelegd in art. 5, derde lid, van de richtlijn.[101]

3.1.2. Nederland

Nederland heeft de Europese richtlijn uit 1995 geïmplementeerd in de Wet bescherming persoonsgegevens, die op 1 september 2001 in werking is getreden.[102] Deze wet is ook van toepassing op het verwerken van persoonsgegevens via Internet. De belangrijkste materiële normen uit de Wbp betreffen (1) de vaststelling van een gerechtvaardigd doel waarvoor persoonsgegevens worden verzameld, (2) een rechtmatige grondslag die voor de verwerking van persoonsgegevens is vereist en (3) dat eenmaal verzamelde gegevens slechts verder mogen worden gebruikt wanneer dat niet onverenigbaar is met het doel of de doelen waarvoor de gegevens oorspronkelijk zijn verzameld.

---

[99] Voor een verantwoordelijke: Beschikking van 15 juni 2001, *PbEG* 2001 L181/19, en voor een bewerker: Beschikking van 27 december 2001, *PbEG* 2002 L6/52.
[100] Voorstel voor een richtlijn betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEG* C365 E van 19 december 2000.
[101] Mededeling van de Commissie aan het Europees Parlement, overeenkomstig artikel 251, lid 2, van het EG-Verdrag over het gemeenschappelijk standpunt van de Raad met het oog op de vaststelling van 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. Brussel, 30.01.2002. SEC(2002) 124def. 2000/0189 (COD).
[102] Stb. 2000, 302.

Naast deze materiële normen is een webstekaanbieder voorts gebonden aan een informatieplicht. Alvorens persoonsgegevens via Internet mogen worden verzameld, dient de betrokkene te worden geïnformeerd over de identiteit van de verantwoordelijke en het doel van de verwerking. Aan deze informatieplicht wordt door veel organisaties tegenwoordig voldaan door middel van een privacyverklaring op de weblocatie.
De Nederlandse overheid heeft rond de inwerkingtreding van de Wbp een publiekscampagne gevoerd om het publiek bewust te maken van hun rechten en plichten ingevolge de wet.

De wettelijke bescherming van persoonsgegevens en privacy wordt ingevuld of aangevuld met enkele zelfreguleringinstrumenten in de vorm van gedragscodes. De Model Gedragscode voor Elektronisch Zakendoen van ECP.NL (zie par. 5.6.2) heeft met betrekking tot privacybescherming uitgesproken dat wederpartijen een bepaalde mate van zekerheid dienen te hebben dat vertrouwelijke informatie ook vertrouwelijk wordt behandeld. Het recht op privacy dient aldus gewaarborgd te zijn. In een eigen gedragscode kan een aanbieder uitspreken dat hij de privacy van zijn wederpartij respecteert en kan hij aangeven op welke wijze hij daaraan invulling zal geven. De Model Gedragscode bevat daartoe een voorbeeldbepaling. De NLIP-gedragscode voor Internetaanbieders (zie par. 5.6.2) bepaalt dat de aanbieder het briefgeheim met betrekking tot persoonlijke e-mail respecteert en hanteert (art. G.1). Artikel G.2 over privacy heeft vooral betrekking op de omgang met persoonsgegevens. De bepaling schrijft voor dat een aanbieder het abonneebestand niet aan derden ter beschikking stelt. Een aanbieder informeert een abonnee duidelijk en vooraf met betrekking tot welke gegevens evt. wel aan derden (kunnen) worden doorgegeven. Deze gegevens zijn binnen de organisatie van de aanbieder alleen toegankelijk ten behoeve van de bedrijfsvoering. Voorts dient een aanbieder zorg te dragen voor een beveiliging als bedoeld in de Wet bescherming persoonsgegevens en de Telecommunicatiewet.
Overigens blijkt in de praktijk de bescherming van persoonsgegevens door Internetaanbieders te wensen over te laten. De (toenmalige) Registratiekamer concludeerde in juni 2000 dat veel onduidelijkheid bestaat over het vastleggen en het gebruik van persoonsgegevens door de Internetaanbieders en dat deze zich niet altijd bewust zijn van de regels ter bescherming van de persoonlijke levenssfeer van hun abonnees. De doelen waarvoor de persoonsgegevens worden verzameld en verder gebruikt zijn vaak niet helder en eenduidig. Dit geldt ook voor de mededelingen hierover aan de (potentiële) abonnees. Verder is niet altijd duidelijk in welke rol de aanbieder zijn activiteiten verricht, en wat de relatie is tussen de beoogde doelstellingen en de gegevens die daartoe worden vastgelegd. Het is volgens de Registratiekamer dan ook maar zeer de vraag of de vastgelegde gegevens ook echt noodzakelijk zijn om deze doelstellingen te realiseren. In het algemeen trekt de Registratiekamer uit haar onderzoek de conclusie dat de bescherming van persoonsgegevens door aanbieders bij het gebruik van Internet in aanzienlijke mate tekortschiet.[103]

3.1.3. Canada

De Canadese regering heeft uitgesproken dat het geen regels van bovenaf wil opleggen ter controle van electronic commerce, tenzij zelfregulering op dit terrein zou mislukken. De regering maakt daarbij evenwel expliciet een uitzondering voor de bescherming van privacy: daarvoor is overheidsregulering juist noodzakelijk. Privacybescherming is in Canada vooral onderworpen aan provinciale wetgeving; niettemin acht de Canadese regering op dit terrein een geharmoniseerd systeem het meest wenselijk. Derhalve is overheidsregulering tot stand gebracht die van toepassing is op federale ondernemingen.[104]
De Canadese *Personal Information Protection and Electronic Documents Act* van 13 april 2000[105] is van toepassing op organisaties in de particuliere sector die in het kader van commerciële activiteiten

[103] Registratiekamer 2000.
[104] Martha Kessler, 'Save for Privacy Rights, Canadian Officials Favor Self-Regulation of Online Commerce', *Electronic Commerce & Law Report* 12 april 2000.
[105] *Second Session, Thirty-sixth Parliament, 48-49 Elizabeth II, 1999-2000. STATUTES OF CANADA 2000 CHAPTER 5. An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or*

persoonsgegevens verzamelen, gebruiken of verstrekken, en wordt in drie fasen ingevoerd. Vanaf 1 januari 2001 is de Canadese wet van toepassing op persoonsgegevens, andere dan medische persoonsgegevens, die in het kader van een commerciële activiteit worden verzameld, gebruikt of verstrekt door organisaties die een op federaal niveau opererende onderneming zijn. Hiertoe behoren luchtvaartmaatschappijen, banken, omroepen, in meer dan één provincie opererende er vervoersondernemingen en telecommunicatiebedrijven. De Canadese wet geldt ook voor alle organisaties die tegen betaling persoonsgegevens verstrekken aan ontvangers in een andere provincie of in een ander land en voor werknemersgegevens betreffende personeel van een op federaal niveau opererende onderneming.
Met ingang van 1 januari 2002 is de Canadese wet ook van toepassing op medische persoonsgegevens ten aanzien van de organisaties en activiteiten die onder de eerste fase vallen. Met ingang van 1 januari 2004 zal de werkingssfeer van de Canadese wet worden uitgebreid tot iedere organisatie die persoonsgegevens verzamelt, gebruikt of verstrekt bij de uitoefening van een commerciële activiteit, ongeacht of de organisatie onder de federale regelgeving valt. De Canadese wet is niet van toepassing op organisaties die onder de *Federal Privacy Act* of onder de regelgeving van de provinciale overheid vallen, noch op non-profitorganisaties en liefdadigheidsinstellingen, tenzij deze commercieel actief zijn. Voorts is de wet niet van toepassing op werknemersgegevens die voor niet-commerciële doeleinden worden gebruikt, met uitzondering van werknemersgegevens betreffende personeel van particuliere bedrijven die onder de federale regelgeving vallen. De Canadese Federal Privacy Commissioner kan in dergelijke gevallen nadere informatie verstrekken.
Aangezien de reikwijdte van de federale wetgeving beperkt blijft tot commerciële activiteiten, wordt de privacybescherming aangevuld met provinciale wetten. Zo heeft Ontario op 4 februari 2002 een wetsontwerp voorgesteld voor een *Privacy of Personal Information Act 2002*, dat zich ook uitstrekt over niet-commerciële activiteiten.[106]

Bij beschikking van 20 december 2001 heeft de Europese Commissie besloten dat voor de toepassing van artikel 25, lid 2, van Richtlijn 95/46/EG Canada geacht wordt een passend beschermingsniveau te waarborgen voor de doorgifte van persoonsgegevens van de Gemeenschap naar ontvangers die onder de *Personal Information Protection and Electronic Documents Act* vallen.[107]

3.1.4. Duitsland

De privacy op Internet valt in Duitsland onder de regels van de *Bundesdatenschutzgesetz* (BDSG). De nieuwe BDSG is op 23 mei 2001 in werking getreden.[108] Daarmee heeft Duitsland de oude versie van deze privacywet aangepast aan de EU richtlijn 95/46/EG. De BDSG is van toepassing op de publieke en private sector. In navolging hiervan hebben zes Duitse *Länder* hun privacywetten eveneens aangepast aan de Europese richtlijn: Brandenburg, Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, Schleswig-Holstein. Deze *Landesdatenschutzgesetze* zijn van toepassing op de publieke sector binnen deze *Länder*.[109]
Naast deze algemene privacywet bestaan in Duitsland talrijke bijzondere privacyvoorschriften. Deze zijn onder andere te vinden in het *Sozialgesetzbuch*, *Straßenverkehrsgesetz*, *Melderechtsrahmengesetz*, *Bundeszentralregistergesetz*, *Ausländerzentralregistergesetz*, *Bundesverfassungsschutzgesetz*, *Bundesgrenzschutzgesetz*, *Telekommunikationsgesetz*, *Postgesetz*, *Informations- und Kommunikationsdienste-Gesetz* en vele andere. Deze zogenoemde *bereichsspezifischen Regelungen* hebben voorrang boven de algemene privacyregels.[110]

---

transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act. BILL C-6, 13 april 2000.
[106] Zie *Technology Law Update*, maart 2002, p. 7-14; <http://www.e-laws.gov.on.ca>.
[107] *PbEG* L2 van 4 januari 2002, p. 13.
[108] Bundesgesetzblatt I Nr. 23/2001, 22 mei, p. 904.
[109] <http://www.europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm>.
[110] BfD-INFO 1 – Bundesdatenschutzgesetz – Text und Erläuterung. 8e Druk, april 2002.

Duitse ISP's mogen op grond van de *Teledienstedatenschutzgesetz* slechts persoonsgegevens van Internetgebruikers verwerken wanneer en zolang dat noodzakelijk is voor het leveren van de dienst en voor het afrekenen daarvan of voor zolang de gebruiker daarmee instemt.[111]

In opdracht van het Duitse ministerie van Binnenlandse Zaken is onderzoek gedaan naar zelfregulering bij privacybescherming in Duitsland. Het rapport beveelt aan dat zelfregulering wordt bevorderd, onder diverse voorwaarden: (1) zelfregulering dient niet vervangend maar aanvullend te zijn, (2) overheid en wetgever dienen zelfregulering te stimuleren, (3) zelfregulering dient op overheidsregulering te zijn gebaseerd, (4) de erkenning van zelfregulering dient te zijn geregeld, (5) zelfregulering dient vrijwillig maar wel verbindend te zijn, (6) zelfregulering mag niet in strijd zijn met de voorschriften op het terrein van economische mededinging, (7) zelfregulering dient regelmatig (jaarlijks) te worden geëvalueerd.[112]

3.1.5. Frankrijk

Het Franse wetsvoorstel ter implementatie van de EU richtlijn 95/46/EG is in juli 2001 aan het parlement aangeboden.[113] Het wetsvoorstel dient ter vervanging van een van de oudste privacywetten in Europa, te weten de *Wet op de informatietechnologie, gegevensbestanden en persoonlijke vrijheden* (*Loi N° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés*).
Op 30 januari 2002 is het wetsvoorstel in eerste lezing door de Nationale Assemblee aangenomen. Daarmee is Frankrijk het laatste EU-land dat richtlijn 95/46/EG implementeert. Intussen is Frankrijk ook al veroordeeld door het Hof van Justitie wegens nalatigheid bij deze implementatie.

Op 26 februari 2002 publiceerde de Franse regering een Witboek over de elektronische overheid en de bescherming van persoonsgegevens. Het witboek verlangt dat de burger in relatie tot de elektronische overheid meer zeggenschap krijgt over diens persoonsgegevens dan op dit moment het geval is, en het roept overheid en consumenten- en burgerrechtenorganisaties op om vertrouwenwekkende maatregelen te treffen voordat de elektronische overheid in Frankrijk haar deuren (of Windows) in 2005 zal openen.[114] Zie hierover nader par. 2.3.5.

Op 12 juni 2001 publiceerde de Franse toezichthouder op de privacybescherming, de Commission Nationale de l'Informatique et des Libertés (CNIL), een rapport over het verzamelen van persoonsgegevens van minderjarigen via Internet: *Internet et la collecte de données personnelles auprès des mineurs*. Het rapport gaat in op de vraag of de Franse wet van 6 januari 1978 voldoende bescherming biedt aan minderjarigen wanneer zij op Internet surfen. In het bijzonder stelt het rapport de vraag aan de orde of de regel dat persoonsgegevens niet mogen worden verzameld zonder de toestemming van de ouders wel realistisch is en geaccepteerd in de online omgeving. Het rapport geeft een aantal aanbevelingen die betrekking hebben op het verzamelen van persoonsgegevens via weblocaties, het online chatten of deelnemen aan een discussieforum door minderjarigen, het plaatsen van foto's van minderjarigen op Internet en het onderhouden van contacten met minderjarigen door middel van e-mail of nieuwsbrieven.
De CNIL heeft in februari 2000 op haar webstek[115] speciaal voor minderjarigen een aparte ruimte ingericht met informatie over hun privacy op Internet.

---

[111] *Tätigkeitsbericht 1999 und 2000 des Bundesbeauftragten für den Datenschutz.* Deutscher Bundestag, 14. Wahlperiode. Drucksache 14/5555, 13.03.2001, p. 23.
[112] Rossnagel, Pfitzmann & Garstka 2001.
[113] Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, n° 3250, déposé le 18 juillet 2001. Op Internet: <http://www.assemblee-nat.fr/projets/pl3250.asp>.
[114] Truche 2002.
[115] <http://www.cnil.fr>.

3.1.6. Japan

De huidige Japanse privacywetgeving is sectoraal; er bestaat geen overkoepelende privacywet, hetgeen als een gemis wordt ervaren.[116] De *Law Concerning the Protection of Personal Information Related to the Processing by Public Organization-owned Computers* uit 1988 biedt onvoldoende bescherming van privacy op Internet. Zo is het aantal gevallen waarin Japanse mannen een vrouw beledigen door het plaatsen van haar naam, adres en expliciete seksuele commentaren op Internet, sterk toegenomen. Om die reden heeft de Japanse regering in oktober 2001 een nieuw stel regels geïntroduceerd, de *Personal Information Bill*, gericht op Internetaanbieders (ISP's). ISP's die een klacht ontvangen van een slachtoffer van privacyschending op Internet, zijn verplicht de gegrondheid van de klacht te onderzoeken en indien dat het geval is, vervolgens de desbetreffende informatie terstond te verwijderen.[117]
De nieuwe wet stelt voorts als voorwaarde dat persoonsgegevens door personen en organisaties uitsluitend op een behoorlijke en zorgvuldige manier mogen worden verwerkt. Bedrijven mogen op grond daarvan geen persoonsgegevens verzamelen wanneer dat onredelijk zou zijn. Voorts zijn zij verplicht de toestemming van de betrokkenen te vragen alvorens hun persoonsgegevens worden doorgegeven aan derden. Deze regels zullen overigens in beperkte mate van toepassing zijn op de verwerking van persoonsgegevens voor het doel van nieuwsgaring, wetenschappelijk onderzoek of politieke en godsdienstige activiteiten.
Een reeks van Japanse mediaorganisaties heeft echter protest aangetekend tegen de nieuwe wet. Zij stellen dat de overheid onder het mom van privacybescherming probeert de vrijheid van meningsuiting door de media aan banden te leggen.[118]
Op 7 november 2001 heeft het Japanse parlement (Diet) de behandeling van de Personal Information Bill uitgesteld tot in het nieuwe parlementaire jaar 2002.[119]

Japan kent ook zelfregulering in de vorm van een privacykeurmerk, uitgegeven door het Japan Information Processing Development Center (JIPDEC), dat in april 1998 van start is gegaan. JIPDEC geeft een privacywaarborg af aan aanbieders van Internetpagina's die voldoen aan de industriële standaard van het Japanse ministerie van Internationale Handel en Industrie (MITI). In mei 2002 had de instantie 136 webstekbeheerders met een privacywaarborg erkend.
JIPDEC heeft in mei 2000 een overeenkomst gesloten met het Amerikaanse BBB Online, waarbij beide organisaties elkaars privacyprogramma's officieel erkend hebben. Door deze wederzijdse erkenning hoeven webbeheerders die in aanmerking wensen te komen voor privacy-erkenning, niet langer van beide organisaties een waarborg op hun webstek te presenteren.

3.1.7. Verenigd Koninkrijk

De Europese richtlijn 95/46/EG is in het Verenigd Koninkrijk geïmplementeerd door middel van de *Data Protection Act* 1998,[120] die op 1 maart 2000 in werking is getreden.
Het VK heeft voorts de laatste jaren diverse wetten aangenomen die de privacy sterk inperken ten behoeve van opsporing en veiligheid, de *Regulation of Investigatory Powers Act 2000* (zie par. 3.3.7) en de *Anti-terrorism, Crime and Security Act 2001* (zie par. 3.4.7).

---

[116] Zie het advies van de Personal Information Production Study Subcommittee of the Advanced Information/Communication Society Headquarters, dat voorstelt een 'omnibus-wet' te maken ter bescherming van de privacy in plaats van de sectorale privacywetgeving, mede gebaseerd op de acht algemene privacybeginselen van de OESO-privacyrichtlijn uit 1981. *Electronic Commerce & Law Report* 8 december 1999.
[117] *Mainichi Shimbun* 16 oktober 2001, <www12.mainichi.co.jp>.
[118] Op grond van de nieuwe privacywet moet het verzamelen van informatie transparant zijn voor het lijdend voorwerp. Als een journalist aan een politicus een vraag stelt op basis van vertrouwelijk verkregen informatie, kan de journalist als tegenvraag verwachten hoe deze dat weet. Vervolgens is hij wettelijk verplicht tekst en uitleg te geven. De privacywet wordt door de mediaorganisaties derhalve beschouwd als een bedreiging voor de vrijheid van meningsuiting. 'Nieuwe privacy-wet bedreigt persvrijheid in Japan.' *NRC Handelsblad* 3 juni 2002.
[119] 'Diet to carry over personal info bill', *Asahi Shimbun* 8 november 2001, <www.asahi.com>.
[120] Te vinden op <http://www.dpr.gov.uk>.

Op het gebied van zelfregulering is vermeldenswaard dat in oktober 2000 de Data Protection Commissioner een *Draft Code of Practice* heeft gepubliceerd voor het gebruik van persoonsgegevens in werkgevers-werknemers-relaties. Bedrijven en instanties kunnen deze gedragscode overnemen ter regeling van monitoring door werkgevers van het e-mailverkeer en Internetgebruik van werknemers.

3.1.8. Verenigde Staten

De VS is van oudsher een voorstander om de bescherming van privacy over het algemeen aan zelfregulering over te laten.[121] Voor bepaalde specifieke situaties bestaat echter wel wetgeving. Zo is in 1998 de *Children's Online Privacy Protection Act* (COPPA) aangenomen ter bestrijding van oneerlijke of misleidende praktijken bij het verzamelen, gebruiken en verstrekken van persoonsgegevens van kinderen via Internet. De COPPA is op 21 april 2000 in werking getreden en legt verplichtingen op aan webbeheerders of aanbieders van online diensten wanneer die weten dat zij via Internet persoonsgegevens verzamelen van kinderen jonger de 13 jaar. De Federal Trade Commission heeft recentelijk de periode waarbinnen webbeheerders die onderworpen zijn aan de COPPA mogen vertrouwen op een netbericht, in combinatie met andere verificatiemethoden, om de ouderlijke toestemming te verifiëren voor het verzamelen van persoonsgegevens van kinderen, verlengd tot 21 april 2005.[122] De FTC baseerde de beslissing op het feit dat betaalbare beveiligde elektronische middelen ter verificatie van de ouderlijke toestemming momenteel nog ontbreken. Ook schat de FTC het privacyrisico voor kinderen op dit moment nog redelijk laag in.
Ondanks de voorkeur voor zelfregulering, zijn er momenteel tal van wetgevingsinitiatieven in het Congres met betrekking tot privacybescherming aanhangig, zoals de *Online Privacy Protection Act of 2001* (H.R. 89). Dit wetsvoorstel voorziet in de bevoegdheid voor de FTC om regels voor te schrijven ter bescherming van persoonsgegevens die zijn verzameld via Internet van en over personen die niet vallen onder de *Children's Online Privacy Protection Act 1998*. Doel van deze wet is om die personen meer individuele controle te kunnen bieden over het verzamelen en gebruiken van hun betreffende persoonsgegevens voor andere doeleinden.[123]
In de VS is een levendig debat gaande tussen voor- en tegenstanders van overheidsregulering inzake privacy. De voorstanders benadrukken daarbij met name de geringe effectiviteit van zelfregulering. Ook binnen de overheid zijn er voorstanders te vinden: de Federal Trade Commission concludeerde in een rapport uit mei 2000 dat 'ongoing consumer concerns regarding privacy online and the limited success of self-regulatory efforts to date make it time for government to act to protect consumers' privacy on the Internet.'[124] Dat de voorkeur voor zelfregulering evenwel nog steeds zeggingskracht heeft, blijkt uit het feit dat deze aanbeveling van de FTC met een meerderheid van drie tegen twee werd gedaan; de minderheid achtte zelfregulering nog steeds adequaat. Vanwege de verdeeldheid die ook in het parlement bestaat, wordt niet verwacht dat binnenkort serieuze privacywetgeving tot stand komt.[125]

De VS beschikt naar de maatstaven van het Europese privacyrecht in het algemeen niet over een passend beschermingsniveau met betrekking tot persoonsgegevens. Daardoor zou de uitwisseling van persoonsgegevens tussen de EU en de VS juridisch onmogelijk worden. Met de EU heeft het Amerikaanse Department of Commerce daarom in juli 2000 een Safe Harbor Agreement gesloten, die volgens de EU wel een passend beschermingsniveau bieden.[126] Door zich aan te sluiten bij het Safe Harbor-programma garanderen Amerikaanse organisaties dat zij de *Safe Harbor*

---

[121] Zie Landwell 2000, p. 50-53.
[122] 67 Fed. Reg. 18,818, 17 april 2002.
[123] Zie voor een overzicht van aanhangige privacywetsvoorstellen <http://www.epic.org>.
[124] FTC 2000a. De opvatting werd herhaald in een rapport over *online profiling*: 'the Commission recommends legislation that would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites with respect to profiling', FTC 2000b.
[125] Electronic Commerce & Law Report 30 januari 2002, p. 105-6.
[126] Besluit 520/2000/EG van 26 juli 2000, *PbEG* L 215 25/08/2000, p. 7-47. Zie ook: Gillian Bull, 'Data Protection-Safe Harbor. Transferring Personal Data to the USA', *Computer Law & Security Report*. Vol. 17 no. 4, 2001, p. 239-243.

Principles (SHP) zullen naleven, waardoor voor de verstrekking van persoonsgegevens vanuit de EU naar die Amerikaanse organisatie een passend beschermingsniveau aanwezig wordt geacht. Het Safe Harbor-programma verlangt van de organisaties die zich daarbij aansluiten dat zij de Safe Harbor Privacy Principles, inclusief de Veel Gestelde Vragen (FAQ's), die door de Amerikaanse overheid zijn vastgesteld, zullen naleven. Voorts wordt van hen verwacht dat zij hun privacybeleid publiceren. De SHP zijn slechts van toepassing op organisaties die vallen onder de jurisdictie van de Federal Trade Commission, voorzover het oneerlijke of misleidende handelspraktijken betreft (zoals niet naleven van het gepubliceerde privacybeleid). De organisaties kunnen zich bij het Safe Harbor-programma aansluiten door te registreren bij het Amerikaanse Department of Commerce, waardoor ze op de openbare *Safe Harbor List* terechtkomen.[127]

Door de Commissie is op 13 februari 2002 een werkdocument van de diensten van de Commissie gepubliceerd, over de toepassing van de beschikking 520/2000/EG dat de SHP een passen beschermingsniveau bieden.[128] De conclusies van het werkdocument luiden als volgt.

- In alles is voorzien om de veiligehavenregeling te laten functioneren.
- De regeling betekent, in vergelijking met de situatie vóór de invoering ervan, een vereenvoudiging voor degenen die persoonsgegevens exporteren naar organisaties die deel uitmaken van de veilige haven en vermindert de onzekerheid voor VS-organisaties die gegevens vanuit de EU willen invoeren.
- Personen die van oordeel zijn dat hun rechten zijn geschonden, kunnen een klacht indienen, maar dit is tot dusverre weinig gebeurd en voorzover de Commissie op de hoogte is, is nog geen enkele klacht onopgelost gebleven.
- Een groot aantal organisaties die tot de veilige haven zijn toegetreden, houdt zich niet aan de verwachte transparantie ten aanzien van hun algemene verplichtingen of de inhoud van hun privacybeleid. Transparantie is in zelfreguleringsystemen van vitaal belang en het is dan ook noodzakelijk dat organisaties hun praktijken op dit gebied verbeteren, zo niet dan dreigt de geloofwaardigheid van de regeling in haar geheel te worden aangetast.
- Geschillenafhandelingsmechanismen beschikken over sancties om naleving van de veiligehavenregels af te dwingen. Deze mechanismen zijn nog niet getest in de veiligehavencontext. Niet alle mechanismen hebben openlijk aangegeven dat zij erop toe zullen zien dat de veiligehavenregels worden nageleefd en niet alle mechanismen hebben een privacybeleid op zichzelf van toepassing dat in overeenstemming is met de beginselen die de veiligehavenregels vereisen. Gezien het belang van rechtshandhaving en de rol van deze instanties daarin is het noodzakelijk dat veiligehavenorganisaties alleen een beroep doen op geschillenafhandelingsmechanismen die volledig aan de vereisten van de veilige haven voldoen.

De EC en het Department of Commerce beschouwen de gesignaleerde tekortkomingen als kinderziekten. De EC stelt het op prijs dat het Department of Commerce bereid is zich te richten tot die organisaties die in gebreke blijven. De EC is ervan overtuigd dat waakzaamheid van en handhaving door de bevoegde autoriteiten in de VS het Safe Harbor programma geloofwaardig blijft en een passend beschermingsniveau voor persoonsgegevens in de VS kan garanderen.

3.1.9. Zweden

Zweden staat bekend als het land dat als eerste in 1973 een nationale privacywet had: de *Data Act*. Deze wet is in 1998 vervangen door de *Personal Data Act* (1998:204) waarmee Zweden de Europese richtlijn 95/46/EC heeft geïmplementeerd. Deze nieuwe wet regelt de opslag van persoonsgegevens in computers, inclusief op webpagina's op het Internet. Voor journalistieke en artistieke doeleinden is de wet niet van toepassing.

---

[127] De Safe Harbor List en overige documentatie met betrekking tot het Safe Harbor Programma is te vinden op <http://www.export.gov/safeharbor>.

[128] Werkdocument van de diensten van de Commissie over de toepassing van Beschikking 520/2000/EG, SEC(2002) 196, 13 februari 2002, <http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_nl.pdf>.

De *Personal Data Act* is in 1999 door het Zweedse parlement gewijzigd. De wetswijziging is mede het gevolg van een aantal webpagina's waarop persoonsgegevens werden gepubliceerd. Zo publiceerde een medewerker van het Zweedse Leger des Heils op een webpagina: "Pinochet is a murderer". Vervolgens vroeg hij de Zweedse toezichthouder (Data Inspection Board) bij wijze van proefproces hem te vervolgen wegens het verwerken van strafrechtelijke persoonsgegevens, die als bijzondere gegevens worden beschouwd.
Sinds de wetswijziging worden geringe inbreuken op de wet niet langer vervolgd. Bovendien is de verstrekking van persoonsgegevens naar ontvangers buiten de EU toegestaan, als dat land met betrekking tot persoonsgegevens een passend beschermingsniveau kent. In Zweden wordt elke informatie met inbegrip van persoonsgegevens op Internet beschouwd als verstrekking naar een land buiten de EU, omdat eenieder waar ook ter wereld toegang heeft tot die informatie.[129]
Dit standpunt heeft tot gevolg gehad dat een absoluut verbod op verstrekking aan landen buiten de EU (indien daar geen passend beschermingsniveau bestaat) strijdig is met de vrijheid van meningsuiting. De Zweedse Hoge Raad sprak in juni 2001 iemand die belastende gegevens over een bank had gepubliceerd op het Internet, vrij van overtreding van verstrekken aan derde landen.[130]

In Zweden is voorts een wetsvoorstel ingediend ter bescherming van de privacy op de werkplek. Dit wetsvoorstel verbiedt de werkgever toegang te hebben tot de privé e-mailberichten van een werknemer. Niettemin mag een werkgever wel toegang hebben tot de privé e-mail van een werknemer als de werknemer daarvoor toestemming geeft of als er een redelijk vermoeden is dat de werknemer een strafbaar feit heeft gepleegd met gebruikmaking van de apparatuur van de werkgever.[131]

3.1.10. Samenvatting

De beleidsinitiatieven in de EU-lidstaten worden nog steeds gedomineerd door de implementatie van Richtlijn 95/46/EG. Hoewel Nederland te laat is geweest met de implementatie van deze richtlijn in de nationale regelgeving (de implementatietermijn eindigde op 24 oktober 1998, terwijl de Wet bescherming persoonsgegevens pas op 1 september 2001 in werking is getreden), staat Nederland daarin niet alleen. Ook Frankrijk, Luxemburg, Duitsland en Ierland zijn door de EU aangesproken op hun verlate implementatie. Wat de inhoud betreft heeft de Nederlandse wetgever gekozen voor een genuanceerde benadering waarin de precisering van de richtlijnnormen in de Wbp slechts deels in de wet heeft plaatsgevonden. Nederland lijkt hierin niet fundamenteel af te wijken van andere EU-lidstaten. Interessant in de implementaties in andere landen is het standpunt van Zweden dat het plaatsen van persoonsgegevens op het Internet het verstrekken van persoonsgegevens naar derde landen (buiten de EU) oplevert, omdat die gegevens in elk geval van daaruit toegankelijk zijn.
Zelfregulering van privacy op het Internet staat nog steeds in de belangstelling. In de EU en Canada gebeurt dat vooral ter invulling van de wettelijke kaders; in de VS staat zelfregulering voorop. In Japan wordt de sectorale privacywetgeving als te gebrekkig ervaren; een voorstel voor een nieuwe privacywet beoogt betere bescherming van persoonsgegevens te bewerkstelligen, maar de bescherming zal in diverse situaties beperkt zijn. Ook in de VS bestaat inmiddels aandacht voor overheidsregulering op dit terrein, en dat niet alleen in specifieke wetten en wetsvoorstellen; ook binnen de overheid gaan er stemmen op voor meer overheidsregulering op privacygebied, met als argument dat de handhaving van zelfregulering in de praktijk niet effectief is gebleken. Tegelijkertijd heeft de EU gesignaleerd dat de naleving van zelfregulering in de VS door middel van het Safe Harbor Programma vooralsnog te wensen overlaat, hetgeen overigens voorlopig als een kinderziekte wordt beschouwd.
De VS is wel tevens een land waar men met overheidsregulering van privacy van kinderen op Internet verder is dan Nederland – en de meeste overige lidstaten van de EU. In de VS bestaat de

[129] Palme 2000.
[130] Högsta domstolen 12 juni 2001, B 293-00 (Ramsbro), beschikbaar op <http://www.bankrattsforeningen.org.se/hddomslut.html>. Zie hierover *Computer Law & Security Report* 2002/1, p. 56-58.
[131] *Baker & McKenzie Global E-law Alert* 11 maart 2002.

Children's Online Privacy Protection Act (COPPA) reeds sinds 1998; in Frankrijk heeft de Registratiekamer aandacht gevraagd voor de privacy van kinderen, onder andere met een voorlichtingspagina. In Nederland bestaat nog nauwelijks aandacht voor de bijzondere kwetsbaarheid van de doelgroep van jonge Internetgebruikers.
Diverse organisaties doen aan publieksvoorlichting over privacy op het Internet. Veelal vindt die voorlichting plaats via Internet, niet alleen door private organisaties (zoals EPIC),[132] maar ook door privacytoezichthouders, zoals in Frankrijk (CNIL) en Duitsland (Datenschutz und Technik), en de overheid (Nederland).

[132] Zie *EPIC Online Guide to Practical Privacy Tools*, <http://www.epic.org/privacy/tools.html>.

3.2. Handhaving van intellectuele-eigendomsrechten

De intellectuele eigendom (IE) is van groot belang voor de elektronische handel. De bescherming van intellectueel eigendom kan innovatie en aanbod van nieuwe producten stimuleren; aan de andere kant kan een te grote bescherming van IE-rechten belemmerend werken voor de toegang tot informatie en daarmee juist innovatie beperken. Het slaan van een balans tussen deze twee is met name bij nieuwe technologie een uitdaging.
IE beslaat een breed gebied in relatie tot elektronische handel. Wij beperken ons hier tot twee belangrijke onderwerpen: het auteursrecht en de naburige rechten op informatie (tekst, beeld, geluid), met name in relatie tot het Internet, en het octrooirecht op software en bedrijfsmethoden. Dit hoofdstuk bespreekt de ontwikkelingen op deze gebieden en zal waar nodig aandacht besteden aan andere relevante ontwikkelingen. Voor de aan IE gerelateerde recente ontwikkelingen op het gebied van domeinnamengeschilbeslechting, zie par. 5.7.

3.2.1. Internationaal

Twee belangrijke recente verdragen met betrekking tot de handhaving van IE-rechten op het Internet zijn het *WIPO Copyright Treaty* (WCT 1996) en het *WIPO Phonograms and Performances Treaty* (WPPT 1996).[133] Op 6 maart 2002 is het WCT in werking getreden door toetreding van Gabon en per 15 april 2002 waren 35 landen aangesloten, waaronder de VS en Japan. Op 20 mei 2002 is de WIPO Phonograms and Performances Treaty (WPPT) in werking getreden door aansluiting van Honduras. Op 15 april 2002 zijn 34 landen aangesloten bij het WPPT, waaronder de VS. Ingezetenen van verdragsluitende partijen kunnen zich nu in andere verdragsluitende landen beroepen op de bescherming die deze verdragen bieden. Hoewel de EG de verdragen heeft ondertekend, zijn deze voor de EG nog niet in werking getreden.[134] Mede om de nationale wetten in overeenstemming te brengen met de bescherming waarin de beide verdragen (en het oudere TRIPs-verdrag) voorzien, heeft Europa de Auteursrechtrichtlijn[135] aangenomen.

Het WCT en WPPT beschermen de auteurs- en naburige rechten in de fysieke wereld, maar benadrukken daarnaast de bescherming van deze rechten in het digitale domein. Zo worden databanken en software expliciet beschermd, evenals digitale 'content'.

Een aantal WIPO-verdragen die de rechten van andere betrokkenen in het informatieverwerkingsproces veilig moeten stellen, zijn momenteel in de ontwerpfase. Het betreft de bescherming van de bijdragen van uitvoerende kunstenaars (acteurs, dansers, en dergelijke) aan audiovisuele werken (zoals film, tv, reclamefilmpjes, videoclips), de bescherming van omroeporganisaties, en de bescherming van databanken.

De onderhandelingen over een *WIPO Audiovisual Performances Treaty* zijn in december 2000 vastgelopen. Dit verdrag zou uitvoerende kunstenaars (m.n. acteurs) exclusieve rechten en morele rechten geven met betrekking tot het gebruik van hun bijdrage aan audiovisuele vastleggingen. Struikelblok is met name de vraag of en in welke mate de producenten (exclusieve) exploitatierechten toekomt. De VS is geen voorstander van het toekennen van de rechten aan de uitvoerende kunstenaars zonder meer, de EU ziet de positie van producenten liefst buiten het verdrag gehouden. In het najaar van 2002 zal de Algemene Vergadering van de WIPO beslissen of het zinvol is weer een diplomatieke conferentie bijeen te roepen.

---

[133] Zie <http://www.wipo.org>.
[134] De Europese Raad heeft wel ingestemd met aansluiting door de EG: Besluit 2000/278/EG van de Raad houdende goedkeuring van de verdragen op 16 maart van 4 november 2000 (*PbEG* 2000 L 89/6).
[135] Richtlijn 2001/29/EG van 22 mei 2001 van het Europees Parlement en de Raad betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (*PbEG* L 167/10).

De bescherming van omroeporganisaties in de digitale omgeving stond ten tijde van het WCT en WPPT al op de internationale agenda, maar omroeporganisaties werden buiten het WPPT gehouden. Het verdrag van Rome[136] van 1961 die op dit moment de rechten van omroeporganisaties beschermt, is niet uitgerust voor toepassing in het digitale domein. Inmiddels zijn er diverse voorstellen gedaan voor een *WIPO Broadcast Treaty*, door de EU op 21 september 2001. Het EU-voorstel voorziet in een toestemmingsrecht van omroeporganisaties om door of namens hen uitgezonden signalen vast te leggen, door te zenden en openbaar te maken. Het voorstel bevat tevens een afdeling over de bescherming van technische voorzieningen en *Digital Rights Management*-systemen (DRM). Gezien de snelle technologische ontwikkelingen en convergentie in de media- en communicatiesectoren, wil de WIPO zich bezinnen op een grondige herziening van de aard en omvang van intellectuele-eigendomsrechten voor omroeporganisaties. De beraadslagingen hierover worden eind 2002 voortgezet.

In een priller stadium verkeert de totstandkoming van een *WIPO Database Treaty*, mede omdat ontwikkelingslanden huiverig zijn voor de effecten van exclusieve rechten op gegevensverzamelingen in aanvulling op de bescherming die het auteursrecht reeds biedt. De EU is voorstander van een internationaal verdrag dat databanken beschermt zoals de Databankrichtlijn doet. Eind 2002 worden binnen WIPO de beraadslagingen over databanken voortgezet, waarbij met name aandacht besteed wordt aan de sociale en economische uitwerking van een dergelijke bescherming op de informatievoorziening in ontwikkelingslanden.

Naast de WIPO wordt de Wereldhandelsorganisatie (WTO) in de toekomst wellicht een steeds belangrijker forum voor intellectuele-eigendomsvraagstukken. De eerste handelsgeschillen over intellectuele eigendom zijn inmiddels in het kader van Trade Related Aspects of Intellectual Property Agreement (TRIPs, 1994) voorgelegd aan het Dispute Settlement Body (DSB) van de WTO. Het DSB heeft op 27 juli 2000 (DS160) haar eerste uitspraak gedaan over de toepassing van TRIPs op het gebied van het auteursrecht. De Verenigde Staten stond bepaalde winkels en horeca-aangelegenheden toe om zonder toestemming van rechthebbenden muziek te draaien. Ingevolge artikel 9 TRIPs zijn beperkingen op het auteursrecht alleen onder bepaalde voorwaarden toegestaan en in deze zaak achtte het DSB de vrijstelling ruimer dan het TRIPs toestaat. De beslissing kan belangrijk blijken in de discussie over de reikwijdte van het auteursrecht in de digitale omgeving, nu het DSB rekening hield met de economische waarde van verschillende distributievormen. Zij liet zich in dit geschil niet uit over distributie via het Internet, maar zij zal dat in de toekomst ongetwijfeld doen. Geschillen die specifiek op Internet of ICT betrekking hebben zijn op dit moment niet aanhangig bij het DSB.

Europa

In Europa is op 22 mei 2001 de Auteursrechtrichtlijn aangenomen, welke op 1 december 2002 door de lidstaten moet zijn geïmplementeerd.[137] Op bepaalde vlakken laat de Richtlijn de lidstaten weinig ruimte voor een eigen invulling van haar verplichtingen. Op deze punten zullen de nationale wetten dan ook vrijwel gelijk zijn. Op andere vlakken, met name op het gebied van de beperkingen van het auteursrecht, houden lidstaten veel vrijheid, zodat in de praktijk slechts een gedeeltelijke harmonisatie plaats zal vinden. Wetgevingsvoorstellen in de verschillende landen zijn reeds onderweg. Hieronder worden de belangrijkste bepalingen van de Richtlijn besproken.

De Richtlijn regelt het openbaarmakings- en verveelvoudigingsrecht van de auteur, de film- en muziekproducent, de uitvoerende kunstenaar en de omroeporganisaties. Onder deze rechten wordt ook de distributie via het Internet begrepen. De Auteursrechtrichtlijn kent op bepaalde punten een belangrijke rol toe aan zelfreguleringinitiatieven waarbij lidstaten slechts mogen optreden als partijen niet tot een vergelijk kunnen komen.

---

[136] Verdrag inzake de bescherming van de rechten van uitvoerende kunstenaars, producenten van fonogrammen en omroeporganisaties (Trb. 1986, 182).

[137] Richtlijn 2001/29/EG van 22 mei 2001 van het Europees Parlement en de Raad betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (*PbEG* L 167/10).

De Richtlijn voorziet in een expliciete beperking op het auteursrecht voor kopieën die plaatsvinden in het kader van de verzending over een netwerk. Hiermee tracht men een effectief functioneren van het Internet te waarborgen. De overige expliciet genoemde beperkingen (bijv. ten gunste van bibliotheken, privékopie) zijn facultatief: het staat de lidstaten vrij om deze te implementeren. Bij bepaalde van deze beperkingen, in het bijzonder de kopie voor eigen gebruik, kan een Lidstaat besluiten dat toch een vergoeding aan de auteur moet worden betaald. Zij krijgen de vrijheid om de hoogte van deze vergoeding vast te stellen en de wijze waarop deze wordt geïnd. Niet in de Richtlijn genoemde beperkingen die reeds in nationale wetgeving voorkomen mogen onder bepaalde voorwaarden worden gehandhaafd voor het analoge domein. De Richtlijn stelt verder expliciet dat het auteursrecht op gemeenschapsniveau is uitgeput met betrekking tot stoffelijke exemplaren van een beschermd werk.

Een van de meest vernieuwende aspecten van de Richtlijn is de bescherming die wordt geboden aan beschermingsmaatregelen tegen kopiëren, de zogenaamde 'technische voorzieningen'. De lidstaten voorzien in een passende rechtsbescherming tegen het omzeilen van doeltreffende technische voorzieningen door een persoon die weet of redelijkerwijs behoort te weten dat hij aldus handelt. Ook is het verboden om DRM-informatie te verwijderen en materiaal waaruit deze informatie is verwijderd te verspreiden. Hierbij kan men denken aan een muziekbestand informatie bevat over hoe vaak het bestand is beluisterd en deze informatie doorgeeft aan een incassomaatschappij. Beide bepalingen, die geïnspireerd zijn op het WCT, hebben een Amerikaanse evenknie in de DMCA (zie par. 3.2.8). In de Verenigde Staten bestaat reeds vier jaar ervaring met deze regels en het is interessant om aan de hand van deze ervaring de ontwikkeling in Europa te bestuderen.

Bepaalde wettelijke beperkingen op het auteursrecht kunnen door technologische beschermingsmaatregelen van hun effect worden ontdaan. Lidstaten mogen daarom voorzien in een effectieve bescherming van deze bij wet aan gebruikers toegestane handelingen. Hiertoe dienen de lidstaten rechthebbenden aan te sporen tot het nemen van vrijwillige maatregelen om deze beperkingen te effectueren. Als dit soort maatregelen niet wordt genomen dienen de lidstaten passende maatregelen nemen om begunstigden van die beperkingen te laten profiteren. Met betrekking tot de distributie over het Internet dient het sluiten van collectieve licentieovereenkomsten gestimuleerd te worden. Een dergelijke regeling geldt ook voor de toepassing van de beperking voor privé-gebruik. De Richtlijn stimuleert dus een bepaald soort zelfregulering, namelijk de 'private' regulering door middel van technische normen, waarbij de overheid slechts een aanvullende rol krijgt toebedeeld. De moeite waarmee in Amerika Internet-radiotarieven worden vastgesteld, is illustratief voor de problemen die dit soort zelfregulering in de praktijk kan opwerpen (zie ook 3.2.8).

Naast de Auteursrechtrichtlijn worden er pogingen gedaan om het octrooirecht op Europees niveau te unificeren. Onder het beschermingsbereik zouden de uitvindingen in het fysieke domein vallen, maar ook software- en Internetgerelateerde uitvindingen. Een voorstel voor een Europese octrooiverordening van 5 juli 2000 is nog in behandeling bij het Europees Parlement.[138] Het Europees Parlement heeft op 19 februari 2002 een reactie gegeven op het voorstel in eerste lezing. Het is, gezien de weerstand in het verleden, niet waarschijnlijk dat een dergelijke verordening op korte termijn zal worden aangenomen.

Om deze reden tracht de Europese Commissie tegelijkertijd regels op te stellen over de octrooieerbaarheid van softwarevindingen in het bijzonder. Op 19 oktober 2000 heeft de Commissie een consultatiedocument gepubliceerd over de octrooieerbaarheid van software. Na inventarisatie van de reacties heeft de Europese Commissie op 20 februari 2002 een voorstel

[138] Voorstel voor een verordening van de Raad betreffende het Gemeenschapsoctrooi, 5 juli 2000, COM(2000) 412.

gedaan voor een softwareoctrooirichtlijn.[139] Het Europees Parlement heeft op dit voorstel nog niet gereageerd.

Het voorstel harmoniseert de octrooieerbaarheidsdrempel zoals die door de nationale octrooibureaus wordt gehanteerd met betrekking tot software. Als maatstaf dienen de richtlijnen die door het Europees Octrooi Bureau (EOB) zijn uitgezet. Deze heeft op 31 augustus 2001 nieuwe richtlijnen aangenomen met betrekking tot de bescherming van methoden van bedrijfsvoering en computergerelateerde vindingen. Het voorstel en de beleidsregels van het EOB stellen als norm dat de vinding een technische bijdrage dient leveren aan de stand van de techniek en op uitvinderswerkzaamheid dient te berusten. Software zal daarnaast niet meer als product kunnen worden geoctrooieerd, maar slechts als werkwijze. In de verschillende Europese lidstaten worden inmiddels onderzoeken door de overheid uitgevoerd over de wenselijkheid van dit soort octrooien.[140]

Het is de vraag of de term 'technische bijdrage' voldoende duidelijk is en daarnaast de ongewenst geachte 'business method'-octrooien uitsluit. De toepassing van octrooibescherming heeft in het verleden tot gevolg gehad dat uitvindingen zonder echte uitvindingshoogte toch werden beschermd. In Europa lopen de meningen met betrekking tot de bescherming van softwareoctrooien uiteen, maar de octrooieerbaarheid van methoden van bedrijfsvoering wijst men over het algemeen af.

3.2.2. Nederland

De Nederlandse regering heeft op 6 september 2000 de Commissie Auteursrecht om advies gevraagd inzake de implementatie van de (toen nog ontwerp-)Auteursrechtrichtlijn. De Commissie heeft op 17 juli 2001 advies uitgebracht, waarna een voorontwerp van wet is opgesteld ter circulatie voor commentaar. Begin 2002 is vervolgens een wetsvoorstel aan de Raad van Sate voorgelegd, maar het wetsvoorstel is op dit moment (juni 2002) nog niet bij de Tweede Kamer ingediend.
Wel heeft het Ministerie van Justitie in december 2001 een rapport uitgebracht dat zich richt op de hoofdlijnen van een langetermijnvisie en strategie voor het auteursrecht.[141]

De regelgeving omtrent de begrippen openbaarmaking en verveelvoudiging behoeft nauwelijks verandering. De term reproductie in de Wet naburige rechten zal echter gewijzigd moeten worden zodat deze de tijdelijke technische kopie uitsluit. De uitputtingsregeling van artikel 12b Auteurswet geldt na implementatie op communautair niveau en niet, zoals tot op heden het geval is, wereldwijd. Daarnaast dient voor naburig-rechthebbenden een terbeschikkingstellingsrecht expliciet in de wet te worden opgenomen.

De auteursrechtbeperkingen die Nederland reeds heeft, dienen volgens het wetsvoorstel te worden behouden. Daarnaast dient – bij gebreke van een algemene *fair use*-exceptie – zo veel mogelijk op andere wijze een hardheidsclausule te worden geïntroduceerd. Voor privékopieën wordt een onderscheid gemaakt tussen verveelvoudiging en reproductie. De bestaande verveelvoudigingsbeperking voor eigen oefening, studie of gebruik wordt gehandhaafd. Reproductie voor eigen gebruik wordt echter gekoppeld aan een redelijke vergoeding, te betalen door de producent van de mediadrager. Tevens worden de parodie-, verwerkings-, wetenschappelijkonderzoeks-, archief- en terminalexceptie opgenomen in de wet.

De wetgever wil het begrip 'redelijke tegemoetkoming' introduceren, in plaats van het begrip 'billijke compensatie'. De eerste term impliceert dat de tegemoetkoming ook op een nultarief kan worden vastgesteld of in andere vorm dan geld kan geschieden. Indien de rechthebbende zijn

---

[139] Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende de octrooieerbaarheid van in computers geïmplementeerde uitvindingen, 20 februari 2002, COM(2002) 92 def.
[140] Zie <http://pauillac.inria.fr/~lang/reperes/patents/>.
[141] Ministerie van Justitie, *Auteursrecht in de informatiemaatschappij*, december 2001. Zie <http://www.ivir.nl/documenten/auteursrechtecorap.pdf.>.

materiaal ook kan beschermen door middel van technische voorzieningen, zal hij minder gauw voor een redelijke vergoeding in aanmerking komen.

Het wetsvoorstel sluit in haar bepalingen inzake technische voorzieningen zo nauw mogelijk aan bij de formulering van de Auteursrechtrichtlijn. Het maken, gebruiken en handelen in producten die technische voorzieningen omzeilen wordt strafbaar gesteld. De Minister kan bij besluit rechthebbenden verplichten om de middelen ter beschikking te stellen die de gebruiker in staat stellen van de beperkingen te profiteren, als deze in de praktijk niet blijken te werken.

Veel Internetgerelateerde zaken worden mede op grond van het databankrecht beslist, omdat veel informatie op het Internet als databank kan worden aangemerkt.[142] De Databankwet, die een implementatie is van de Databankrichtlijn, verbiedt (kort gezegd) een buitenproportionele extractie van gegevensverzamelingen. Om voor bescherming in aanmerking te komen dient de verkrijging, controle of presentatie van de gegevensverzameling te getuigen van een substantiële investering. De interpretatie van het begrip substantiële investering is in de Nederlandse rechtspraak niet eenduidig uitgelegd, waarbij het debat zich met name spitste rond de vraag of een databank die een *spin-off* is een andere activiteit, ook bescherming verdient. De Hoge Raad heeft dit debat recentelijk geslecht met de vaststelling dat de vraag of een databank een *spin-off* is van andere activiteit op zich niet relevant is voor het bestaan van een databankrecht.[143]

3.2.3. Canada

Canada is rond 2000 begonnen met een aanpassing van de Auteurswet aan het digitale tijdperk. Rond september 2002 is de deadline voor een parlementaire herziening van de Auteurswet.[144] Vooralsnog is op dit brede vlak geen vooruitgang geboekt. Momenteel is echter wel een wetsvoorstel in behandeling dat het mogelijk maakt om heruitzending van radio- en televisiesignalen op het Internet te licentiëren.[145] Canada heeft daarnaast onlangs haar octrooirecht aangepast om de 17-jarige beschermingsduur voor octrooien uit te breiden tot 20 jaar, waartoe zij op grond van het TRIPs verplicht is.

3.2.4. Duitsland

Op 18 maart 2002 is door het Ministerie van Justitie een wetsvoorstel bij het Parlement gelegd ter implementatie van de Auteursrechtrichtlijn.[146] Dit is de uitwerking van het conceptwetsvoorstel dat in 2000 reeds was voorgesteld door de Duitse regering. Duitsland heeft op 25 januari 2002 het *Gesetz zur Stärkung der vertraglichen Stellung von Urhebern und ausübenden Künstler* aangenomen, een wet die de positie van auteurs ten opzichte van exploitanten tracht te verbeteren.[147] De geboden bescherming gaat minder ver dan in voorontwerpen was beoogd. Auteurs krijgen op grond van deze wet een dwingend recht op een billijke vergoeding voor het gebruik van hun werk. Indien later blijkt dat deze vergoeding niet in redelijke verhouding staat tot de exploitatieopbrengsten, is er de mogelijkheid tot het vragen van een extra vergoeding. De wet voorziet tevens in een niet-bindende bemiddelingsprocedure om de hoogte van de vergoeding vast te stellen. De wet treedt 1 augustus 2002 in werking.

3.2.5. Frankrijk

Ten tijde van de *Internationale ICT-toets 2000* waren reeds plannen voor het oprichten van een forum voor co-regulering van het Internet. Dit forum is medio 2001 opgericht en op het Internet te vinden.[148] Het forum doet aanbevelingen met betrekking tot de regulering van verschillende

---

[142] Zie <http://www.ivir.nl/publications/hugenholtz/fordham2001.html.>.
[143] HR 22 maart 2002, *Mediaforum* 2002/5, nr. 17 (*NVM v.. de Telegraaf*).
[144] Zie <http://strategis.ic.gc.ca/SSG/rp01100e.html>.
[145] *Bill C-48*, zie <http://www.parl.gc.ca/>.
[146] *Referentenentwurf für ein Gesetz zur Regelung des Urheberrecht in der Informationsgesellschaft*, zie <http://www.nethics.net/nethics/de/themen/urheberrecht/referentenentwurf-urhR180302.pdf.>.
[147] BGB I 2002/21, 28 maart 2002, p. 1155.
[148] Zie <http://www.foruminternet.org>.

aspecten van het Internet (zoals bijvoorbeeld de aansprakelijkheid voor 'hyperlinks'), hetzij middels co-regulering, hetzij middels zelfregulering. Hiertoe kan eenieder participeren in een openbare discussie die wordt gevoerd op de webstek. Verder heeft de Franse regering een weblocatie ingericht waar informatie wordt gegeven over wetsvoorstellen en andere activiteiten van de overheid die betrekking hebben op het Internet.[149]

De Franse regering heeft op 1 maart 2002 in een brief aan de Europese Commissie zich uitgesproken tegen het Europese voorstel met betrekking tot de bescherming van softwareoctrooien. Zij heeft in dit kader ook een webstek opgericht waar verschillende rapporten en consultaties die door de overheid zijn uitgevoerd, zijn gepubliceerd.[150] Hoewel de meningen uiteenlopen, wordt gewaarschuwd voor een te lage beschermingsdrempel van software-uitvindingen. Op 14 juni 2001 is een wetsvoorstel gedaan voor een wet met betrekking tot de informatiemaatschappij.[151] Dit wetsvoorstel regelt bepaalde aspecten van het informatievoorzieningproces, maar ziet niet op de het auteursrecht of andere IE-rechten op het Internet; bovendien is het met de parlementsverkiezingen van 2002 komen te vervallen. Een wetsvoorstel ter implementatie van de Auteursrechtrichtlijn zou in de lente van 2002 worden gepresenteerd, maar het voorstel is ten tijde van schrijven nog niet gepubliceerd.[152]

3.2.6. Japan

Zoals aangegeven in de *Internationale ICT-toets 2000*, was Japan in juli 2000 nog niet toegetreden tot het WPPT.[153] Dit is nog steeds zo, hoewel het WCT op 6 maart 2002 voor Japan wel in werking is getreden. Japan had reeds in 1999 verschillende wetten gewijzigd om in lijn te komen met het WCT. Een voorstel tot ratificatie van het WPPT zal waarschijnlijk in januari 2003 worden voorgelegd aan het Parlement, tezamen met de noodzakelijke wijzigingen van de Japanse Auteurswet. In juni 2001 heeft het Japanse parlement een wet aangenomen die domeinkapen verbiedt.[154] Het Ministerie van Economische zaken van Japan heeft een initiatief genomen om een private groep te organiseren van uitgevers van muziek, film en spelletjes om piraterij in Azië te bestrijden. Het is de bedoeling dat de groep informatie uitwisselt en bijeenkomsten organiseert, waarbij het Ministerie als secretariaat fungeert.[155]

Het Japanse Octrooi Bureau heeft in december 2000 nieuwe standaarden voor het octrooieren van softwarevindingen uitgevaardigd. Op 10 januari 2001 traden de nieuwe regels in werking. Een computerprogramma dat meerdere functies vervult is octrooieerbaar volgens de standaarden van het octrooibureau. Om de wet op een lijn te brengen met deze ontwikkelingen kondigde het Ministerie van Economische zaken van Japan aan de octrooiwet aan te passen, teneinde de intellectuele eigendom van Internetbedrijven te beschermen. Deze wet zou de bescherming van computerprogramma's moeten verduidelijken.[156]

3.2.7. Verenigd Koninkrijk

Ook het Verenigd Koninkrijk zal de Auteursrechtrichtlijn moeten implementeren. Behalve het afschaffen van een heffing op IE-transacties op 28 maart 2000 zijn er geen noemenswaardige ontwikkelingen op dit front buiten het Europese kader.
Op 31 juli 2001 is de eerste prejudiciële vraag met betrekking tot het recente Europese databankrecht gesteld.[157] Tevens beëindigde het *Office of Fair Trading* op 28 februari 2002 het

---

[149] Zie <http://www.internet.gouv.fr>.
[150] Zie <http://www.industrie.gouv.fr/observat/innov/carrefour/f2o_brevet.htm>.
[151] *Projet de loi sur la société de l'information* (n°3143), <http://www.assemblee-nationale.fr/projets/pl3143.asp>, 14 juni 2001.
[152] *Journal Officiel* 3 september 2001.
[153] Landwell 2000, p. 91.
[154] EIPR N-34, 2002/3.
[155] Zie voor een Engelstalig overzicht van recente gebeurtenissen <http://www.japantimes.co.jp/>.
[156] Zie voor een Engelstalig overzicht het Japans Octrooi Bureau: <http://www.jpo.go.jp/>.
[157] *British Horseracing Board Ltd. v. William Hill Organisation Ltd. II*, Court of Appeal 31 juli 2001.

consultatieproces met betrekking tot de toepassing van mededingingsrecht op de exploitatie van IE-rechten. De overheid heeft onlangs besloten om octrooibescherming uit te breiden zodat deze ook Internetmethoden van bedrijfsvoering zal omvatten.[158] Tot slot heeft de overheid onlangs een uitgebreide webstek opgericht met informatie over IE-rechten voor rechthebbenden en gebruikers.[159]

3.2.8. Verenigde Staten

Reeds in 1998 heeft de Verenigde Staten de *Digital Millennium Copyright Act* (DMCA) aangenomen om de nationale wetgeving aan te passen aan het Internet-tijdperk en in overeenstemming te brengen met de normen van het WCT en het WPPT. De ervaring die in dit land is opgedaan met de DMCA is leerzaam en kan een indruk geven van de situatie in Europa na de implementatie van de Auteursrechtrichtlijn.

De Amerikaanse rechter heeft een aantal interessante uitspraken gedaan op grond van de DMCA. Veel van deze zaken hadden betrekking op de bescherming en omzeiling van technische voorzieningen. Actueel zijn de geschillen over het publiceren van en linken naar software om DVD's mee te kopiëren. Andere zaken die hebben gespeeld betroffen het kraken van een Nintendo Playstation, het bewerken van *webcasting*software om uitzendingen op te slaan, de kopieerbeveiliging op Adobe's e-Books en het publiceren van een nota over audiodecryptie. In Amerika woedt momenteel een verhitte discussie over de reikwijdte van de bepalingen met betrekking tot technische voorzieningen. Er gaan stemmen op om de bepalingen te wijzigen teneinde misbruik door rechthebbenden te voorkomen.[160] Over de bescherming van DRM-informatie heeft de Amerikaanse rechter nog geen uitspraak gedaan.

Een andere kwestie die illustratief is voor de problemen waar de Europese lidstaten binnenkort mee te maken zullen krijgen, is de vaststelling van royalty-tarieven voor Internet-radio.[161] De DMCA bepaalt dat rechthebbenden een vergoeding toekomt voor het openbaarmaken van hun werken via digitale media. Indien partijen echter geen overeenstemming bereiken over de tarieven die voor deze *webcasting* gelden, stelt het Copyright Office deze vast. Nu op dit punt geen overeenstemming werd bereikt tussen omroeporganisaties en de platenmaatschappijen, heeft het Copyright Office een adviescommissie, het Copyright Arbitration Royalty Panel (CARP), een adviestarief laten voorstellen.[162] Op 21 mei 2002 is dit advies door de Copyright Office niet aangenomen en op 20 juni 2002 moet de Copyright Office met een nieuw voorstel komen. Het geschil, zowel in de onderhandelingen tussen partijen en in het advies van het CARP, draait om de vaststelling van de economische waarde van uitzendingen via het Internet. De onduidelijkheid die hierover bestaat kan zelfreguleringinitiatieven zoals die ook zijn opgenomen in de Auteursrechtrichtlijn van hun effectiviteit ontdoen.

Een aantal nieuwe wetten op het gebied van de bescherming van het auteursrecht is in de maak. Hiervan is het voorstel voor een *Consumer Broadband and Digital Television Promotion Act* (CBDTPA) van 21 maart 2002 de interessantste.[163] Dit tamelijk controversiële wetsvoorstel wil de verkoop en distributie van vrijwel elke digitale machine verbieden, tenzij deze machine kopiebeschermingsstandaarden bevat die door de overheid zijn goedgekeurd. Dit zou bijvoorbeeld tot gevolg kunnen hebben dat CD-opnemers en computers technische standaarden moeten bevatten die goedgekeurd zijn door de overheid. Het Witte Huis is vooralsnog sceptisch over dit voorstel en lijkt meer te zien in een marktgestuurde oplossing. Gezien de controverse die het voorstel oproept is het niet aannemelijk dat deze bepalingen zonder slag of stoot tot wet zullen worden verheven.

---

158 EIPR 2001/7, N-111.
159 Zie <http://www.intellectual-property.gov.uk>.
160 Zie <http://www.eff.org/IP/DMCA/>.
161 Zie <http://www.saveinternetradio.org/>.
162 Zie <http://www.loc.gov/copyright/carp/webcasting_rates.html>.
163 S. 2048.

Ook verdient de *Music Online Competition Act* vermelding. Dit wetsvoorstel tracht de verstrekking van online-muziek te bevorderen.[164] Het wetsvoorstel voorziet in een beperking in het openbaarmakingsrecht ter promotie van online muziek, door een citaatrecht van 30 á 60 seconden toe te staan aan Internetwinkels. Tevens zou dit voorstel omroeporganisaties de vrijheid geven om voor online transmissie op verschillende snelheden één vergoeding te betalen. Een overzicht van deze wetten is te vinden op de webstek van het Copyright Office.[165]

Tot slot is relevant dat de Business Software Alliance (BSA), die in de praktijk een belangrijk deel van de handhaving van auteursrechten op software voor haar rekening neemt, heeft aangegeven dat voorlichting aan consumenten cruciaal is om duidelijk te maken wat de waarde is van auteursrechtelijk beschermd materiaal. 'BSA is trying to get this message out before it has to resort to enforcement measures'.[166]

Octrooirecht
In de Verenigde Staten worden methoden van bedrijfsvoering en softwareoctrooien sneller beschermd dan in Nederland. Een controversieel voorbeeld van deze bescherming is de octrooibescherming die rust op de eenkliks-winkelmethode van Amazon. Op 3 april 2001 is de *Business Method Patent Improvement Act* voorgesteld. Het doel van de wet is om octrooien van lage kwaliteit – dat wil zeggen verleend voor bedrijfsmethoden die nauwelijks een uitvinding zijn te noemen – tegen te gaan.[167]

3.2.9. Zweden

Met betrekking tot Zweden is geen relevante recente informatie aangetroffen.

3.2.10. Samenvatting

De handhaving van intellectuele-eigendomsrechten op het Internet wordt primair internationaal aangestuurd (TRIPs, WIPO-verdragen). Op Europees niveau gebeurt dit met name door implementatie van de Auteursrechtrichtlijn van 22 mei 2001. Duitsland loopt voorop in de implementatie hiervan; Nederland heeft hierover echter een uitgebreide maatschappelijke consultatie gehouden.
Op internationaal niveau zijn er de nodige initiatieven om producenten van informatiediensten (auteurs, uitvoerend kunstenaars, databankproducenten, omroeporganisaties) adequaat te beschermen in de digitale omgeving, maar het blijkt niet eenvoudig om op wereldwijde schaal om overeenstemming te bereiken over de noodzaak en precieze invulling van die bescherming. Op nationaal niveau is te zien hoe de toepassing van nieuwe en bestaande regels van intellectuele eigendom in de digitale omgeving geen sinecure is. Met name de ervaringen in de VS laten zien dat het behouden van een goede balans tussen de belangen van producenten en gebruikers een uitdaging is, evenals het duiden van het economisch belang van nieuwe distributievormen in verband met de bepaling van redelijke gebruiksvergoedingen.

De ontwikkeling van een Europees eenheidsoctrooi vordert maar langzaam. Voor de ICT-sector is het vraagstuk van bescherming van computergerelateerde uitvindingen (software) en bedrijfsmethoden zeer relevant. De verschillende wetgevers achten het beschermen van softwareoctrooien over het algemeen wenselijk, hoewel triviale uitvindingen niet moeten worden beschermd wegens de mogelijk negatieve gevolgen voor innovatie. Europa hanteert over het algemeen strengere selectiecriteria voor de bescherming van softwareoctrooien dan de Verenigde

---

164 H.R. 2724.
165 Zie <http://www.copyright.gov/legislation/>.
166 *Electronic Commerce & Law Report* 1 mei 2002, p. 405.
167 Zie <http://thomas.loc.gov/cgi-bin/query/r?c107:patent>.

Staten en Japan. Of en onder welke voorwaarden dergelijke bescherming een bijdrage levert aan innovatie en gezonde concurrentie is overigens omstreden, hetgeen naar verwachting de aanname van de door de Europese Commissie voorgestelde Richtlijn inzake softwareoctrooien niet zal bespoedigen.

3.3. Computercriminaliteit

In de jaren tachtig en negentig van de vorige eeuw hebben de meeste landen wetgeving ingevoerd op het gebied van computercriminaliteit, mede als gevolg van de aanbevelingen van de Raad van Europa uit 1989 (materieel strafrecht) en 1995 (formeel strafrecht).[168] De laatste jaren concentreert de wetgevende activiteit zich internationaal rond het Cybercrime-verdrag, dat eind 2001 werd aangenomen.
Dit hoofdstuk bevat een beknopt overzicht van de belangrijkste activiteiten van de laatste paar jaar op computercriminaliteitsgebied. De nadruk zal hierbij liggen op de internationale afstemming en verfijning van bestaande wetgeving.

3.3.1. Internationaal

Bij het totstandkomen van de genoemde aanbeveling van de Raad van Europa uit 1995, bleek dat de implementatie van de landen van de aanbeveling uit 1989 dermate uiteenliep dat van de gewenste harmonisatie geen sprake was; hetzelfde werd verwacht voor de implementatie van de aanbeveling uit 1995. Daarom besloot men te streven naar een bindend instrument, een verdrag over cybercriminaliteit (Cybercrime-verdrag). Aan dit verdrag is van 1997 tot 2001 gewerkt; het werd op 23 november 2001 te Boedapest voor ondertekening opengesteld, en dertig landen ondertekenden het.[169] Hieronder bevonden zich ook de niet-lidstaten Canada, de VS, Zuid-Afrika en Japan, die bij de voorbereiding van het verdrag waren betrokken.
Het verdrag beoogt 'approximatie' (een lichte vorm van harmonisatie) van wetgeving op het gebied van materieel en formeel strafrecht, rechtshulp en jurisdictie in verband met computercriminaliteit. Hoofdstuk 1 bevat bepalingen van materieel strafrecht, hoofdstuk 2 van opsporingsbevoegdheden, en hoofdstuk 3 van internationale rechtshulp. De bepalingen stellen minimumeisen aan de wetgeving van de lidstaten; op diverse punten is er ruimte gelaten voor nationale invulling. Een minimumniveau aan harmonisatie is evenwel wenselijk, gezien het vereiste van dubbele strafbaarheid dat voor wederzijdse rechtshulp bijna altijd wordt gesteld.
De materiële bepalingen komen grotendeels overeen met de bekende vormen van computercriminaliteit: strafbare feiten tegen de integriteit, authenticiteit, vertrouwelijkheid of beschikbaarheid van computers, netwerken of gegevens. Voor de inhoudgerelateerde delicten (uitingsdelicten) kon alleen overeenstemming worden bereikt over kinderpornografie (waaronder virtuele kinderporno). Voor andere uitingsdelicten, racisme en vreemdelingenhaat, is nadien een aanvullend Protocol opgesteld, dat vermoedelijk eind 2002 voor ondertekening zal worden opengesteld. Voor inbreuken op het auteursrecht sluit het Cybercriminaliteitsverdrag aan bij het Verdrag van Rome, TRIPs en de WIPO-verdragen (vgl. par. 3.2.1). De rechtsmachtbepalingen sluiten aan bij de traditionele beginselen uit het internationale recht; het ontwikkelen van nieuwe rechtsmachtconcepten in verband met de wereldomvattendheid van netwerken werd niet nodig geacht.[170] Positieve rechtsmachtconflicten (indien meerdere staten rechtsmacht opeisen) moeten worden opgelost door onderlinge consultatie.
De formele bepalingen komen voor een groot deel overeen met de Nederlandse bevoegdheden uit de Wet computercriminaliteit van 1993 (doorzoeking van computers en netwerken, onderzoek van telecommunicatie en medewerkingsplichten). Een nieuw fenomeen is evenwel het bevriezingsbevel, dat kan worden gegeven om te voorkomen dat gegevens verdwijnen, in afwachting van een (rechtshulpverzoek tot een) opsporingshandeling ter verkrijging van de gegevens. Van belang is op te merken dat bepaald geen volledige harmonisatie van

---

[168] *Recommendation No. R (89) 9 on computer-related crime; Recommendation No. R (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology.*
[169] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, Trb. 2002, 18. Zie
<http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>. Zie Kaspersen 2002 voor een uitvoerige bespreking van het verdrag.
[170] Kaspersen 2002, par. 9.5.6.3.

opsporingsbevoegdheden is bereikt in het verdrag, gezien de grote diversiteit aan rechtsstelsels op dit gebied.[171]
De rechtshulpbepalingen betreffen uitlevering en kleine rechtshulp wanneer daartoe geen verdragsrechtelijke basis bestaat; hieronder vallen onder andere het bevriezingsbevel en het versneld uitleveren van verkeersgegevens indien een buitenlandse dienstaanbieder bij de communicatie blijkt te zijn betrokken. Een grensoverschrijdende netwerkzoeking is alleen toegestaan bij publiek toegankelijke gegevens of met toestemming van de rechthebbende. Van belang is tot slot de oprichting van een 24/7-netwerk in elke lidstaat, dat adviseert, faciliteert en waar toegestaan zelf uitvoert in geval van internationale rechtshulpverzoeken.
Het verdrag zal in werking treden zodra vijf staten, waaronder ten minste drie lidstaten, het hebben geratificeerd.[172]

Naast het Cybercrime-verdrag is voorts van belang het EU-rechtshulpverdrag tussen lidstaten, dat in mei 2000 werd aangenomen.[173] Artikelen 17-22 van dit verdrag bevatten bepalingen over grensoverschrijdend aftappen van telecommunicatie; hieronder valt de mogelijkheid om, indien een staat geen technische hulp nodig heeft om iemand af te tappen in een andere staat, dit pas achteraf te melden aan deze andere staat. Dit verdrag treedt in werking op het moment dat ten minste acht lidstaten het hebben geratificeerd.
Ook verdient vermelding een recent ingediend voorstel voor een Kaderbesluit over aanvallen op informatiesystemen,[174] dat de desbetreffende strafbaarstellingen in de lidstaten meer op één lijn beoogt te brengen. Het voorstel verplicht lidstaten tot strafbaarstelling van onrechtmatige toegang tot en onrechtmatige verstoring van informatiesystemen, waaronder een poging daartoe.

Een van de meestbediscussieerde actuele onderwerpen op het gebied van opsporing van computercriminaliteit is de vraag of en in hoeverre verkeersgegevens verplicht moeten worden opgeslagen door telecomaanbieders voor strafrechtelijke of nationaleveiligheidsdoeleinden. Bij het Cybercrime-verdrag is verplichte opslag van de hand gewezen. In de EU vond hierover een scherpe discussie plaats bij de herziening van de Richtlijn privacy in de telecommunicatiesector,[175] die vervangen wordt door een Richtlijn privacy in de elektronischecommunicatiesector. Op 30 mei 2002 heeft het Europees Parlement een gewijzigd voorstel voor deze richtlijn aangenomen, waarin bepaald is dat lidstaten verplichte bewaring van verkeersgegevens in hun nationale wetgeving kunnen opnemen, voorzover dit verenigbaar is met de bescherming van de mensenrechten.[176]

Strafrecht is niet van nature een gebied voor zelfregulering. Niettemin is een belangrijke ontwikkeling dat in vele landen van onderop meldpunten zijn ontstaan voor schadelijke of illegale inhoud. Daarbij zijn ook internationale samenwerkingsverbanden ontstaan, zoals de Internet Hotline Providers in Europe Association (Inhope).[177] Dergelijke ontwikkelingen worden ook ondersteund door de EU met het *Safer Internet Action Plan*.[178] Een internationaal overzicht van meldpunten is beschikbaar op <http://www.saferinternet.org/hotlines/map.asp>.[179]

---

[171] Kaspersen 2002, par. 9.5.7.2.
[172] Zie <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm> onder *Chart of signatures and ratifications* voor een overzicht van de landen die het verdrag hebben ondertekend en geratificeerd.
[173] *Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union* (2000/C197/01), *OJ* 12 juli 2000.
[174] Voorstel voor een Kaderbesluit van de Raad over aanvallen op informatiesystemen, 19 april 2002, COM(2002) 173def.
[175] Richtlijn 97/66/EG van 15 december 1997.
[176] Besluit Europees Parlement van 30 mei 2002 bij aanvaarding herziene richtlijn 97/66/EG (DMN: IP/02/783).
[177] <http://www.inhope.org>.
[178] <http://europa.eu.int/information_society/programmes/iap/index_en.htm>. Zie ook COM(2002) 152, 22 maart 2002, met het vervolg op dit actieplan, beschikbaar op <http://europa.eu.int/information_society/programmes/iap/docs/pdf/programmes/followup/follow-up%20decision_acte_nl_%20fin.pdf>.
[179] Zie ook <http://www.qlinks.net/quicklinks/hotlines.htm>.

3.3.2. Nederland

Nederland was met de uitgebreide Wet computercriminaliteit[180] een van de eerste landen ter wereld met een samenhangend stelsel van wetgeving op het gebied van computercriminaliteit; met name met de opsporingsbevoegdheden in een geautomatiseerde omgeving was Nederland internationaal koploper. Aangezien de wet inmiddels verouderd wordt geacht, is in juli 1999 een wetsvoorstel Computercriminaliteit II bij het parlement ingediend,[181] dat enkele lacunes vult en schoonheidsfoutjes corrigeert van de Wet computercriminaliteit. De belangrijkste voorstellen betreffen het strafbaarstellen van netpostbommen, de uitbreiding van de ontsleutelplicht tot telecommunicatie en de mogelijkheid om gegevens ontoegankelijk te maken ('in beslag te nemen'). De behandeling van het wetsvoorstel voorloopt niet voorspoedig; in juni 2002 lag het nog steeds in de Tweede Kamer.

Nederland heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd. In het Actieplan terrorismebestrijding (zie par. 3.4.2) heeft Nederland aangegeven het verdrag "bij voorrang" te willen uitvoeren[182] (al wordt niet aangegeven ten opzichte waarvan de voorrang wordt verleend).
De Nederlandse overheid is overigens actief op het gebied van voorlichting over en bewustwording van veilig Internetgebruik, onder andere ter preventie van computercriminaliteit. De campagne surfopsafe[183] is gestart door de ministeries van Economische Zaken en Verkeer & Waterstaat naar aanleiding van de nota KWINT[184] en richt zich op de particuliere en kleinzakelijke gebruiker van het Internet. Met deze campagne worden private initiatieven, zoals veiligophetweb van de Safe Internet Foundation,[185] aangevuld.

In Nederland zijn als zelfreguleringinitiatief drie meldpunten opgezet, het Meldpunt Kinderporno, het Meldpunt Discriminatie Internet, alsmede het Meldpunt voor overig illegaal materiaal van de NLIP.[186]

3.3.3. Canada

Bij de bestrijding van computercriminaliteit legt de Canadese overheid een topprioriteit bij de bestrijding van kinderporno. In maart 2001 heeft de federale regering van Canada een omvattend wetsvoorstel tot wijziging van het Wetboek van Strafrecht ingediend, onder andere ter bestrijding van kinderpornografie via het Internet.[187] De gedragingen die in de voorgestelde wet strafbaar worden gesteld zijn onder andere de overdracht, de verspreiding en de uitvoer van kinderpornografie tussen gebruikers of via het web en het zoeken van toegang tot kinderpornografie, alsmede het gebruiken van het Internet om kinderen mee te lokken met een seksueel oogmerk. Tevens wordt het bezit van kinderpornografische afbeeldingen met het oogmerk ze te verspreiden strafbaar gesteld; het strafmaximum bedraagt 10 jaar.
Een ander nieuw fenomeen waar Canada oog voor heeft is identiteitsfraude (*identity theft*): na het verzamelen van persoonsgegevens neemt iemand de identiteit van iemand anders aan teneinde diens krediet te exploiteren. Vooralsnog bestrijdt Canada dit evenwel alleen via de wettelijke bescherming van persoonsgegevens (*Personal Information Protection and Electronic Documents Act* van

---

[180] Stb. 1993, 33.
[181] TK 1998-1999, 26 671, nrs. 1-2.
[182] TK 2001-2002, 27 925, nr. 10, p. 14.
[183] Zie <http://www.surfopsafe.nl/?catid=7&pageid=66>.
[184] <http://www.dgtp.nl/data/scriptgifs/1000372325-1.pdf>.
[185] <http://www.veiligophetweb.nl/>.
[186] <http://www.meldpunt.org/>, <http://www.meldpunt.nl> resp. <meldpunt@nlip.nl> (zie <http://www.nlip.nl/> onder Meldpunten).
[187] Zie <http://www.parl.gc.ca/PDF/37/1/parlbus/chambus/house/bills/government/C-15_1.pdf>, bezocht in mei 2002. Zie met name de wijzigingen in de artt. 161, 163, 164 en 172 van het Canadese wetboek van strafrecht.

2000 (zie par. 3.1.3) en voorlichting door de Privacy Commissioner[188]), niet via strafbaarstelling.[189]

Canada heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd.

Voor de internationale bestrijding van computercriminaliteit is van belang dat in Canada in januari 2001 de dader is veroordeeld van de verstikkingsaanvallen (*denial-of-service attacks*) die in februari 2000 veel weblocaties van internationale groothandels, met name in de VS, platlegden.[190]

De Canadian Association of Internet Providers heeft een *Protection Portal* opgericht ter voorlichting over veilig gebruik van het Internet.[191] In Canada is evenwel geen herkenbaar meldpunt voor schadelijke of illegale inhoud opgezet; de strategie van de Canadese overheid voor een veilig gebruik van het Internet meldde in februari 2001 dat de overheid en de marktsector nog de mogelijkheden bestuderen voor een dergelijk meldpunt.[192]

3.3.4. Duitsland

Duitsland kent al de nodige tijd wetgeving op het gebied van computercriminaliteit.[193] Sinds 2000 zijn er geen nieuwe initiatieven op dit gebied bekend. Op het gebied van opsporing is een recent wetsvoorstel noemenswaard, dat beoogt om het *Telekommunikationsgesetz* aan te passen met een bepaling dat telecomaanbieders verplicht identificerende gegevens van abonnees vast te leggen, waartoe de abonnees een identiteitsbewijs moeten tonen. De regeling beoogt om ook mobiele bellers met vooruitbetaalde kaarten te kunnen traceren. Hierop is kritiek gekomen van de Duitse persoonsgegevenstoezichthouders vanwege inbreuk op het recht op *informationelle Selbstbestimmung*.[194]

Duitsland heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd.

Ter voorkoming van computercriminaliteit heeft de Duitse overheid een voorlichtingscampagne opgezet, *Sicherheit im Internet*.[195] De Internetaanbieders (of multimedia-aanbieders) hebben in 1997 als zelfreguleringinitiatief vrijwillige zelfcontrole op zich genomen in het verband Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, waaronder een meldpunt voor schadelijke en illegale inhoud.[196] Ook heeft de Bertelsmann-Stichting een project opgezet voor zelfregulering van Internetinhoud, met gedragscodes, een filtersysteem en meldpunten.[197] Daarnaast heeft inmiddels ook het Electronic Commerce Forum een meldpunt voor illegale inhoud, *Newswatch*.[198]

---

188 <http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp>.
189 Zie het jaarverslag Technologie van de Criminal Intelligence Service Canada, <http://www.cisc.gc.ca/AnnualReport2001/Cisc2001/technology2001.html>.
190 *Electronic Commerce & Law Report* 24 januari 2000, p. 87.
191 <http://www.caip.ca/portal/portal-main.htm>.
192 <http://www.rcmp-grc.gc.ca/html/safe_wise_internet.htm> onder punt 4.
193 Zie Landwell 2000, p. 20-21, en <http://www.rz.uni-augsburg.de/connect/9701/compstrf.shtml> voor een beknopt overzicht.
194 Entschließung zwischen der 63. und 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002, <http://www.bfd.bund.de/information/DS-Konferenzen/63_64_ent1.html>.
195 <http://www.sicherheit-im-internet.de>.
196 <http://www.fsm.de/> en <http://www.fsm.de/beschwerde/arbeit/>.
197 Zie <http://www.bertelsmann-stiftung.de/project.cfm?lan=de&nid=33&aid=868>.
198 <http://www.eco.de/ictf/hotline/kontakt/kontakt_de.htm>.

3.3.5. Frankrijk

Frankrijk kent al de nodige tijd wetgeving op het gebied van computercriminaliteit, waaronder strafrechtelijke wetgeving voor de bescherming van minderjarigen op het Internet.[199] Sinds 2000 zijn er geen nieuwe wetgevingsinitiatieven op dit gebied bekend.

Teneinde computercriminaliteit beter te kunnen aanpakken, heeft Frankrijk in 2000 een *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* (Centraal bureau voor de strijd tegen ICT-criminaliteit) opgericht.[200] Dit bureau dient de activiteiten van de handhavingsinstanties tegen computercriminaliteit te coördineren en te stroomlijnen.

Frankrijk heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd.

De Franse overheid heeft in september 2001 een voorlichtingscampagne opgesteld voor veilig gebruik van het Internet, *Familles en ligne* (Families online).[201] Frankrijk kent ook meldpunten, die voornamelijk vanuit de overheid zijn geïnitieerd; er zijn al langere tijd meldpunten tegen kinderporno,[202] en in 2001 is een meldpunt opgezet voor illegale inhoud bij het Centraal bureau voor de strijd tegen ICT-criminaliteit.[203]

3.3.6. Japan

Japan kent al langere tijd wetgeving op het gebied van computercriminaliteit, waaronder valsheid, fraude, gegevensmanipulatie en -aantasting, en diefstal van elektriciteit,[204] alsmede computervredebreuk.[205]
Voor de handhaving is vooral van belang dat Japan sinds kort (als een van de laatste landen van de geïndustrialiseerde wereld) een wet heeft voor het aftappen van telecommunicatie.[206] Deze wet werd voor het eerst voorgesteld in 1997 en in aangepaste vorm (met een nieuw vereiste dat een onafhankelijke derde instantie aanwezig is bij het aftappen) in augustus 1999 door het parlement aangenomen; de wet trad in augustus 2000 in werking.[207] Er bestaat overigens grote maatschappelijke weerstand tegen de wet, en de politie gebruikte de tapbevoegdheid ook pas voor het eerst in 2002.[208]

Japan heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd. Japan heeft inmiddels een wetsvoorstel gepubliceerd voor ratificatie, alsmede ter aanpassing van de computercriminaliteitswetgeving aan het verdrag.[209]

In Japan is door de Internet Japan Association gediscussieerd over een meldpunt voor kinderpornografie en kinderuitbuiting op het Internet.[210]

---

[199] Zie Landwell 2000, p. 41.
[200] <http://www.interieur.gouv.fr/police/oclctic>.
[201] <http://www.social.gouv.fr/famille-enfance/fam_lign/>.
[202] <https://www.internet-mineurs.gouv.fr/> en
<http://www.bouclier.org/campagne/fr/formulaire.shtml>.
[203] <http://www.pointdecontact.org/>.
[204] Volgens de Japanse Wet computercriminaliteit, bepalingen ingevoerd in het Japanse Wetboek van Strafrecht, officieuze vertaling beschikbaar op <http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm>.
[205] Volgens de Wet op de ongeoorloofde toegang tot computers (No. 128 van 1999), officieuze vertaling beschikbaar op <http://www.npa.go.jp/hightech/fusei_ac2/UCAlaw.html>.
[206] Volgens sommigen was het niet nodig om daarvoor een wet uit te vaardigen; op basis van jurisprudentie leek het aftappen van telecommunicatie al geoorloofd. Zie <http://www.insite-tokyo.com/column/itaru/index2.html>.
[207] Zie <http://www.ccsr.cse.dmu.ac.uk/sara/assign/c1/Sur-Jap.htm>.
[208] *Japan Times* 24 mei 2002, <http://www.asiamedia.ucla.edu/Weekly2002/05.21.2002/Japan5.htm>.
[209] *World Internet Law Report* juni 2002, p. 10.
[210] <http://www.iajapan.org/hotline/20011217unicef-en.html>.

3.3.7. Verenigd Koninkrijk

Het VK kent reeds lange tijd wetgeving op het gebied van computercriminaliteit, zoals de *Computer Misuse Act 1990* en de *Telecommunications (Fraud) Act 1997*.[211] Recentelijk heeft een parlementslid een wetsontwerp ingediend, de *Computer Misuse (Amendment) Bill*, om verstikkingsaanvallen (*denial-of-service attacks*) strafbaar te stellen, aangezien die in het algemeen niet onder de *Computer Misuse Act 1990* vallen.[212]
Voor de handhaving is met name de *Regulation of Investigatory Powers Act 2000* (RIPA)[213] van belang, waarin vergaande bevoegdheden worden toegekend voor onder andere het onderscheppen van (tele)communicatie. Een gedragscode voor de uitvoering van de interceptiebevoegdheden wordt momenteel ontwikkeld. Nog niet alle delen van de wet zijn overigens in werking getreden.

De *Anti-terrorism Crime and Security Act*,[214] die op 14 december 2001 werd aangenomen (zie par. 3.4.7) bevat een bepaling die de bewaring van verkeersgegevens toestaat (art. 102-107), niet alleen voor terrorismebestrijdings- maar ook voor opsporingsdoeleinden voorzover daarbij een direct of indirect verband zou kunnen bestaan met de nationale veiligheid. Een gedragscode van de Secretary of State, vast te stellen na consultatie van de persoonsgegevenstoezichthouder en de markt, zal dit nader vormgeven.

Het VK heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd.

Een van de eerste Internmeldpunten voor illegale inhoud ter wereld werd ingesteld door de Britse Internet Watch Foundation (IWF), opgericht in 1996.[215] De eerste prioriteit van dit meldpunt is kinderpornografie. De IWF onderneemt naast dit meldpunt ook andere activiteiten om schadelijke en illegale inhoud te bestrijden, zoals het ontwikkelen van een classificatie- en filtersysteem voor Internetinhoud.

3.3.8. Verenigde Staten

De VS kent al lange tijd wetgeving op het gebied van computercriminaliteit, zowel federaal als op het niveau van de staten.[216] Op federaal niveau zijn de belangrijkste vormen van computercriminaliteit strafbaar gesteld, voorzover deze zich betrekking hebben op computers van de federale overheid of financiële instellingen of computers gebruikt voor interstatelijke of buitenlandse handel of communicatie. Op statelijk niveau loopt de wetgeving aanzienlijk uiteen, zowel qua inhoud als qua aanpak.[217]
Binnen de statelijke wetgeving zijn er enkele onderwerpen die nieuw zijn voor het gebied van computercriminaliteit. Zo zijn er diverse staten die 'identiteitsdiefstal' (*identity theft*) strafbaar hebben gesteld. Voorts hebben enkele staten wetgeving voorgesteld die verbiedt om op het Internet adresgegevens van opsporingsambtenaren te publiceren. Louisiana heeft het aanbieden van online gokken strafbaar gesteld, en enkele staten hebben voorgesteld het aanbieden van sigaretten op het Internet strafbaar te stellen. Ook interessant is dat Utah een strafrechtelijk gesanctioneerde verplichting kent tot het doen van aangifte van computercriminaliteit.[218]

Voor de handhaving is van belang dat de *PATRIOT Act of 2001*, die eind 2001 werd aangenomen, niet alleen bevoegdheden heeft uitgebreid voor bestrijding van terrorisme, maar

---

[211] Zie voor een beknopt overzicht Landwell 2000, p. 66-67.
[212] *World Internet Law Report* juni 2002, p. 12-13.
[213] De wet heeft een eigen webstek: <http://www.homeoffice.gov.uk/ripa/ripact.htm>.
[214] <http://www.hmso.gov.uk/acts/acts2001/20010024.htm>.
[215] <http://www.iwf.org.uk/hotline/index.htm>.
[216] Zie een overzicht op <http://www.usdoj.gov/criminal/cybercrime/cclaws.html>. Algemene informatie over computercriminaliteit in de VS is te vinden op <http://www.usdoj.gov/criminal/cybercrime/>.
[217] Brenner 2001, die een overzicht en analyse biedt van de statelijke computercriminaliteitswetgeving.
[218] Brenner 2001.

ook van computercriminaliteit, zoals het aftappen van computerkrakers (par. 217 van de wet). (Zie hierover par. 3.4.8.)

Ter preventie van computercriminaliteit heeft de VS bij de FBI het National Infrastructure Protection Centre opgericht, dat bedreigingen van de (Internet-)infrastructuur opspoort en analyseert en waarschuwingen publiceert.[219]

De VS heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd.

In de VS is een meldpunt actief voor bestrijding van kindermisbruik, de CyberTipline,[220] opgericht door het National Center for Missing and Exploited Children, in samenwerking met de FBI en diverse opsporingsinstanties.

3.3.9. Zweden

Het Zweedse strafrecht kent enkele specifieke bepalingen over computercriminaliteit, maar wordt in het algemeen geacht om voldoende toegesneden te zijn op computercriminaliteit. De in de *Internationale ICT-toets 2000* vermelde mening dat geen specifieke wetgevende maatregelen op dit terrein nodig zijn,[221] lijkt nog steeds de heersende te zijn.
Voor de handhaving kent Zweden diverse ICT-gerelateerde opsporingsbevoegdheden, zoals aftappen van telecommunicatie, het opvragen van verkeersgegevens en observatie met een technisch hulpmiddel.[222] Er vindt al sinds langere tijd een discussie plaats over de vraag of ook direct afluisteren toegelaten moet worden in Zweden; de Minister van Justitie heeft in januari 2001 aangegeven dat een wetsvoorstel daartoe echter pas kan worden overwogen indien het probleem van bijvangst (*överskottsinformation*) adequaat kan worden geregeld.[223]

Zweden heeft het Cybercrime-verdrag op 23 november 2001 ondertekend maar nog niet geratificeerd.

In Zweden is een meldpunt actief op het gebied van kinderpornografie, opgericht door Rädda Barnen (Red de kinderen).[224]

3.3.10. Samenvatting

De laatste twee jaar hebben individuele landen weinig activiteiten ondernomen op het gebied van wetgeving van computercriminaliteit. Deels kan dit worden verklaard door het feit dat de wetgeving van de meeste landen op dit vlak grotendeels als voldoende werd beschouwd. De belangrijkste reden voor de inactiviteit is echter de ontwikkeling van het Cybercrime-verdrag van de Raad van Europa, waar alle in dit onderzoek onderzochte landen bij betrokken waren. Alle inspanningen waren hierop gericht, en staten hebben gewacht tot het verdrag definitief vormkreeg alvorens nieuwe wetsvoorstellen te doen.
Het Cybercrime-verdrag biedt dan ook de belangrijkste vernieuwing in computercriminaliteitswetgeving. Dit is minder het geval om de inhoud, die vooral consolidatie betekent van de reeds langer bekende catalogus van computercriminaliteit en ICT-opsporingsbevoegdheden, dan om de internationale dimensie. Waar bestrijding van computercriminaliteit tot nu toe voor een belangrijk deel een nationale aangelegenheid was van individuele landen, ligt er met het Cybercrime-verdrag de mogelijkheid om grensoverschrijdende computercriminaliteit aan te pakken. De approximatie van materiële bepalingen (waardoor aan het vereiste van dubbele strafbaarheid meestal zal worden voldaan) en de rechtshulpbepalingen,

---

[219] <http://www.nipc.gov/index.html>.
[220] <http://www.missingkids.org/cybertip/ncmec_default_cybertipline.htm>.
[221] Landwell 2000, p. 80.
[222] Zie Zila 2000.
[223] <http://www.riksdagen.se/debatt/fragor/svar.asp?rm=0102&nr=496>.
[224] <http://www.rb.se/hotline/>.

alsmede de oprichting van een 24/7-netwerk, betekenen een belangrijke stap voorwaarts in de bestrijding van computercriminaliteit op een internationaal niveau.
De zegeningen van het Cybercrime-verdrag moeten echter ook niet worden overschat. Voor uitingsdelicten is bijvoorbeeld geen overeenstemming bereikt, met uitzondering van kinderporno; hier moet men toevlucht nemen tot aanvullende protocollen met een kleiner draagvlak. Bovendien kunnen staten op tal van punten voorbehouden maken of slechts een minimumniveau implementeren. De belangrijkste beperking is misschien dat op het vlak van rechtsmacht nauwelijks vooruitgang is geboekt: staten houden onverkort vast aan nationale soevereiniteit, voor positieve rechtsmachtconflicten (die zich bij computercriminaliteit snel voordoen) wordt geen structurele oplossing geboden, en de interpretatie van de situaties waarin een staat rechtsmacht kan opeisen kan behoorlijk uiteenlopen.
Desondanks is het Cybercrime-verdrag wel een succes: zelden is een verdrag van de Raad van Europa zo snel door zoveel landen ondertekend. De wil om computercriminaliteit internationaal aan te pakken is duidelijk zeer groot.

Naast de wetgevingsinitiatieven is in dit onderzoek vooral gekeken naar zelfregulering via meldpunten voor schadelijke of illegale inhoud. Nederland was hierin een van de voorlopers. De laatste jaren zijn in alle onderzochte landen, met uitzondering van Canada en Japan, meldpunten opgezet of uitgebreid. De VS en Zweden, en een Japans voorstel voor een meldpunt, beperken zich hierbij tot kinderporno en uitbuiting van kinderen via het Internet; de overige landen, waaronder Nederland, kennen meldpunten voor ook andere vormen van illegale inhoud. Overigens zijn de meldpunten niet alle landen een zuivere zelfregulering: in Frankrijk en de VS worden de meldpunten nadrukkelijk door de overheid ondersteund.
Tot slot verdient aandacht dat in diverse landen, waaronder Nederland, Canada, Duitsland en de VS, de overheid actief Internetpagina's onderhoudt ter voorlichting en waarschuwing aan het publiek, teneinde veilig gebruik van het Internet te stimuleren.

3.4. Terrorismebestrijding

Als reactie op de terroristische aanslagen op (en in) de Verenigde Staten van 11 september 2001 ontwikkelen veel landen nu antiterrorismewetgeving. Daarnaast worden in veel landen bestaande of bevroren wetsvoorstellen uit de kast gehaald en plotseling van de hoogste (wetgevings)prioriteit voorzien. Angst en paniek spelen na 11 september mogelijk bij veel westerse landen een rol. Daarbij speelt vooral de vraag op welke wijze dient te worden omgegaan met de zichtbaar geworden terroristische dreiging. Er is evenwel dermate veel gebeurd op het terrein van terrorismebestrijding dat we in dit rapport geen volledig overzicht kunnen geven. We beperken ons grotendeels tot de belangrijkste initiatieven die een verband hebben met ICT-regulering.
Voor (de regulering van) elektronische handel is dit onderwerp om twee redenen van belang. In de eerste plaats behoeft e-handel een veilige infrastructuur; beveiliging van netwerken tegen terroristische aanslagen is daarom een aandachtspunt. In de tweede plaats kan antiterrorismewetgeving leiden tot bijzonder vergaande bevoegdheden voor opsporings- en veiligheidsdiensten, en het is niet ondenkbaar dat bijvoorbeeld een *carte blanche* voor deze diensten om elektronische communicatie af te luisteren een verkillend effect (*chilling effect*) op e-handel zouden kunnen hebben, mede gegeven de (al dan niet vermeende) belangstelling van veiligheidsdiensten voor bedrijfsspionage.

3.4.1. Internationaal

Verenigde Naties
Als reactie op de aanslagen in de VS komt de Veiligheidsraad op 'the day after' met een resolutie waarin de desbetreffende aanslagen sterk veroordeeld worden.[225] Op 28 september wordt een tweede resolutie[226] in het leven geroepen. Hierin komt de Veiligheidsraad tot een aantal maatregelen die door elke lidstaat afzonderlijk nageleefd dienen te worden. De maatregelen zien vooral op het lamleggen of bevriezen van fondsen of andere financieringswijzen die uiteindelijk (direct of indirect) bestemd zijn voor terroristische acties, personen of groeperingen. Daarnaast dient de financiering strafbaar gesteld te worden. Tevens wordt aan de diverse lidstaten opdracht gegeven geen steun te bieden (ook geen andere dan financiële steun) aan terroristen. De lidstaten moet dus als het ware een ontmoedigingsbeleid voeren en het daarmee zo moeilijk mogelijk voor terroristen maken. Daarnaast moeten ze op de behoorlijke wijze informatie uitwisselen met andere staten.

Net zoals de Veiligheidsraad, veroordeelt ook de Algemene Vergadering middels een resolutie de aanslagen van 11 september 2001.[227] Op 30 januari 2002 neemt de AV een resolutie aan waarin een aantal te nemen antiterrorismemaatregelen en aanbevelingen (*Measures to eliminate international terrorism*) vermeld staan.[228] In de tekst wordt gewezen op de al eerder aangenomen resolutie 49/60 (9 december 1994) waarin de AV de verschillende deelstaten aanmoedigt tot adequate antiterrorismewetgeving te komen. Naast deze verwijzing wordt in de resolutie van dit jaar aangedrongen op een intensivering van internationaal optreden tegen terrorisme en wordt de noodzaak tot uitbreiding van het totale VN-arsenaal tegen terrorisme benadrukt.

Er bestaan in totaal twaalf multilaterale VN-verdragen of protocollen die een of andere manier de nadruk leggen op te nemen verantwoordelijkheden en maatregelen van nationale staten ter bestrijding van het terrorisme.[229] De *Supression of Terrorist Financing Convention*[230] was reeds op 9 december 1999 aangenomen door de Algemene Vergadering van de Verenigde Naties. Per 10

---

[225] S/RES. 1368(2001), <http://www.un.org/Docs/scres/2001/res1368e.pdf>.
[226] S/RES. 1373(2001).
[227] <http://www.un.org/documents/ga/res/56/a56r001.pdf>.
[228] <http://www.un.org/documents/ga/res/55/a55r158.pdf>.
[229] Beschikbaar op <http://www.undcp.org/terrorism_conventions.html>.
[230] De tekst van dit VN-verdrag is beschikbaar op <http://www.undcp.org/resolution_2000-02-25_1.html>.

april 2002 is het verdrag van kracht geworden.[231] Dit verdrag geeft aan dat financiering het hart van elke terroristische operatie is en dat er afdoende maatregelen voorhanden dienen te zijn om deze financiering te dwarsbomen. Een maatregel is het 'bevriezen' van bankrekeningen of fondsen klaarblijkelijk bestemd voor terroristisch optreden. De inbeslaggenomen gelden kunnen uiteindelijk ter compensatie van slachtoffers van terroristische aanslagen dienen. Financiële instellingen dienen bepaalde vermoedens (dat bepaalde gelden afkomstig zijn van of bestemd voor terroristische groeperingen) op tijd door te spelen naar overheidsinstanties.

Europese Unie
Hoewel ook voor de aanslagen van 11 september 2001 in de EU stappen werden ondernomen voor terrorismebestrijding,[232] is er na de aanslagen een groot aantal initiatieven ontplooid binnen de EU op dit gebied.[233] We beperken ons hier tot enkele belangrijke activiteiten die relevant zijn voor ICT-regulering.
De JBZ-raad van 20 september 2001 en de bijzondere vergadering van de Europese Raad op 21 september 2001 stelden diverse maatregelen voor, waaronder verbeterde politiële en justitiële samenwerking, het stimuleren van internationale verdragen en bestrijding van terrorismefinanciering.[234] De Commissie deed voorstellen voor een kaderbesluit inzake terrorismebestrijding, dat onder andere minimumbepalingen van strafbare terroristische activiteiten in de strafwetgeving van lidstaten verplicht stelt,[235] en voor een Europees arrestatiebevel[236]. Veel nadruk wordt gelegd op samenwerking en informatie-uitwisseling tussen veiligheidsdiensten en politie, zowel tussen lidstaten als met Europol en Eurojust en met niet-lidstaten.[237] Ook de bestaande inspanningen op het gebied van veiligheid van netwerken[238] worden versterkt.

3.4.2. Nederland

De aanslagen van 11 september hebben ook in Nederland voetsporen achtergelaten. Naar aanleiding van de aanslagen zijn (telling eind mei 2002) maar liefst 59 kamerstukken gepubliceerd in de serie *Terroristische aanslagen in de Verenigde Staten*.[239] Centraal hierin staat het *Actieplan terrorismebestrijding en veiligheid*, dat op 5 oktober 2001 aan de Tweede Kamer werd aangeboden.[240] Hierin wordt voortgebouwd op lopende initiatieven, die met nieuwe maatregelen worden aangevuld. Voor ICT-regulering zijn hierbij vooral de volgende actiepunten van belang:

- betere wisselwerking tussen inlichtingen- en veiligheidsdiensten (ivd's) en politie (Nederlandse politie en Europol);
- ontwikkeling van biometrische identificatiemethoden;
- ontwikkeling van een samenhangend pakket van maatregelen ter bescherming van de infrastructuur van overheid en bedrijfsleven (waaronder ICT);
- uitbreiding recherche- en analysecapaciteit voor terrorismebestrijding;

---

231 Zie <http://www.un.org/law/cod/sixth/54/english/r54109e.pdf>.
232 Zie bijvoorbeeld Aanbeveling van 5 september 2001 van het Europees Parlement betreffende de rol van de Europese Unie in de terreurbestrijding (2001/2016(INI)) *PbEG* 21 maart 2002, <http://europa.eu.int/eur-lex/nl/dat/2002/ce072/ce07220020321nl01350141.pdf>.
233 Zie COM(2001) 611, <http://europa.eu.int/comm/justice_home/news/terrorism/documents/com_2001_611_report_en.pdf> voor een overzicht.
234 Zie <http://europa.eu.int/comm/justice_home/news/terrorism/documents/concl_council_21sep_en.pdf>.
235 COM(2001) 521def, 19 september 2001, beschikbaar op <http://europa.eu.int/eur-lex/nl/com/pdf/2001/nl_501PC0521.pdf>, formeel aangenomen door de Raad op 13 juni 2002.
236 COM(2001) 522def, 19 september 2001, formeel aangenomen door de Raad op 13 juni 2002.
237 Zie bijvoorbeeld Initiatiefvan het Koninkrijk Spanje met het oog op de aanneming van een besluit van de Raad betrefende de toepassing van specifieke maatregelen op het gebied van politiële en justitiële samenwerking ter bestrijding van terrorisme (2002/C 126/15), *PbEG* 28 mei 2002.
238 Zie COM(2000) 890def en COM(2001) 298def.
239 Serie 27 925.
240 TK 2001-2002, 27 925, nr. 10. Zie nr. 50 van 15 maart 2002 voor een overzicht van de stand van zaken rond de uitvoering van de actiepunten.

- uitvoering regelgeving met betrekking tot aftapverplichtingen uit de Telecommunicatiewet afronden;
- het project herziening tapkamers (voorzien voor eind 2003) versnellen;
- versnellen van besluitvorming over rechtmatige toegang voor veiligheidsdiensten en politie in cryptografische voorzieningen bij derde partijen (TTP's) en streven naar regulering van krachtige cryptografie voor publiek gebruik;
- onderzoek verrichten naar de categorieën gegevens die telecomaanbieders bewaren en de belemmeringen die de opsporings- en ivd's ondervinden door de afwezigheid van bewaarplichten voor historische verkeersgegevens; versterken van de mogelijkheden van analyse van internationaal telefoonverkeer (afgestemd met Europese lidstaten);
- uitbreiding satellietinterceptiecapaciteit voor terrorismebestrijding;
- snelle uitvoering van het Nationaal Actieplan Digitaal Rechercheren.
- verbetering van uitwisseling van informatie tussen de betrokken partners bij financieel rechercheren;
- Nederland zal alle inspanningen erop richten de EU-rechtshulpovereenkomst eind 2002 te ratificeren; daarmee worden ook gemeenschappelijke onderzoeksteams mogelijk;
- Nederland zal in november 2001 het Cybercrime-verdrag ondertekenen en het vervolgens bij voorrang uitvoeren.

Er wordt dus vooral ingezet op meer uitwisseling van gegevens, uitbreiding van capaciteit en versnelling van bevoegdhedengerelateerde initiatieven. Opvallend is dat *en passant* in het actieplan *terrorisme*bestrijding diverse aanbevelingen worden gedaan die ook of vooral *opsporings*doeleinden beogen te bereiken. Voor een deel betreft dit lopende initiatieven (zoals het project tapkamers, biometrie, rechtmatige toegang bij TTP's (zie par. 5.3.2)), maar voor een deel ook lijkt via een U-bocht gepoogd te worden eerder afgewezen voorstellen of stokpaardjes alsnog in te voeren (regulering van sterke cryptografie (zie par. 5.4.2), bewaarplicht verkeersgegevens (zie par. 3.3.2).

3.4.3. Canada

Als reactie op de aanslagen in de Verenigde Staten van 11 september 2001 voert de Canadese regering op 24 december de *Anti-Terrorism Act* in.[241] Met deze federale wet worden onder meer de twee (van de twaalf) nog niet eerder geratificeerde VN-verdragen door de Canadese autoriteiten alsnog geratificeerd en daarmee uiteindelijk in de nationale strafwetgeving opgenomen.
De nieuwe federale wet heeft tevens grote gevolgen voor de tot dan toe bestaande strafproceswetgeving (*Criminal Code*) in Canada. Op de officiële weblocatie van de Canadese autoriteiten staan de belangrijkste wetswijzigingen vermeld.[242] Zo wordt het op basis van de nieuwe wet het voor de strafvorderlijke autoriteiten een stuk gemakkelijker om terroristische groeperingen (direct) af te luisteren of af te tappen. Daarbij komt de eis te vervallen dat de interceptie van communicatie (*electronic surveillance*) het laatste redmiddel (*last resort*) dient te zijn.[243] De voorgestelde wetgeving verlengt de periode dat er afgetapt mag worden van maximaal 60 dagen naar maximaal één jaar. Als voorwaarde geldt dan wel dat het object van onderzoek een terroristische groepering dient te zijn. Daarnaast blijft de eis bestaan dat een rechter interceptie van communicatie vooraf dient goed te keuren (warrant). Tot slot wordt tevens de notificatieplicht aangepast. Pas na drie jaar dient de gedupeerde te worden ingelicht over het feit dat zij object van onderzoek is geweest.

Op basis van de *Anti-Terrorism Act* wordt naast de *Criminal Code* tevens de *National Defence Act* gewijzigd om daarmee het mandaat van de zogenaamde *Communications Security Establishment* (CSE) te verduidelijken. Op basis van de nieuwe regeling is het voor de CSE (veiligheidsdienst) toegestaan communicatie van buitenlandse doelen buiten het grondgebied van Canada te

---

[241] De bedoelde antiterrorismewet is in december 2001 in werking getreden. Zie hiervoor het persbericht op <http://canada.justice.gc.ca/en/news/nr/2001/doc_29513.html>. De wet wordt ook wel aangeduid als 'Bill C-36'. De tekst van deze wet is onder meer beschikbaar op <http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_3/C-36_cover-E.html>.
[242] <http://canada.justice.gc.ca/en/news/nr/2001/doc_27787.html>.
[243] Beschikbaar op <http://canada.justice.gc.ca/en/news/nr/2001/doc_29513.html>.

onderscheppen, alsmede *security-checks* van overheidscomputers uit te voeren om deze te beschermen tegen terroristisch handelen.
Tevens wordt de *Canadian Human Rights Act* gewijzigd om duidelijk te maken dat het verbod om haatberichten te verspreiden bij telefoonmaatschappijen toeziet op alle telecommunicatievormen. Ook de *Canada Evidence Act* is met invoering van de nieuwe federale wet gewijzigd. Bepaalde 'gevoelige' informatiestromen kunnen op basis van deze wetswijziging van het publiek afgeschermd worden. Daarnaast wordt ook de *Proceeds of Crime (money laundering) Act* gewijzigd met het oog op het verlenen van bijzondere bevoegdheden aan het zogenaamde Financial Transactions and Reports and Analysis Centre om daarmee financiële transacties ter herkennen en op te sporen die eventueel de veiligheid van de Staat zouden kunnen aantasten en de eventueel verzamelde informatie door te spelen aan de Canadese Inlichtingendienst (Canadian Security Intelligence Service).
Tot slot wordt tevens de Canadese DNA-databank uitgebreid tot terroristisch en daarmee samenhangend strafbaar optreden.
Op de nieuwe wetgeving is kritiek gekomen van onder andere de CCPA (Canadian Civil Liberties Association).[244]

3.4.4. Duitsland

Vrijwel direct na de aanslagen van 11 september start de Duitse minister van Binnenlandse Zaken Schily een stevige antiterrorismecampagne, die uiteindelijk leidt tot het *Gesetz zur Bekämpfung des internationalen Terrorismus* (*Terrorismusbekämpfungsgesetz*). Zowel de Duitse Bundesrat als Bundestag hebben uiteindelijk hun groene licht voor deze nieuwe antiterrorismewet gegeven. [245] De wet is per 1 januari 2002 van kracht geworden. Daarbij dient overigens opgemerkt te worden dat de Duitse regering in eerste instantie was vergeten de wet via publicatie in het *Bundesgesetzblatt* (het Duitse Staatsblad) openbaar te maken. Uiteindelijk wordt deze slordigheid rechtgezet en wordt de wet als nog in het Duitse Staatsblad gepubliceerd en wel op 11 januari 2002.[246]
In de periode na de aanslagen van 11 september wordt het voor Otto Schily tevens mogelijk een reeds eerder op 5 september 2001 ingediend wetsvoorstel alsnog door te voeren. Het gaat hier om de zogenaamde *Abschaffung des Religionprivilegs*. Na door zowel de Duitse Bundesrat als de Bundestag te zijn goedgekeurd, wordt het nieuwe wetsvoorstel door publicatie in het Duitse Staatsblad op 8 december tot wet verheven.[247]

Met het *Geldwäschebekämpfungsgesetz* worden in samenhang met het op 1 januari in werking getreden *Terrorismusbekämpfungsgesetz* aanvullende en voor de toekomst noodzakelijke maatregelen getroffen met het oog op een (meer) effectieve bestijding van de financiering van internationale terroristische geldstromen. Duitsland zal met het van kracht worden van de *Geldwäschebekämpfungsgesetz* als een van de eerste Europese landen de Europese richtlijn[248] ter wijziging van de antiwitwasrichtlijn uit 1991 (91/308/EEG) in nationaal recht omzetten.[249]

Talrijke wetten worden met de nieuw ontstane terroristische dreiging gewijzigd. Dit zijn onder meer het *Bundesverfassungsschutzgesetz*, *MAD-Gesetz*, *BND-Gesetz*, *Bundesgrenzschutzgesetz* (Douanewet), *Bundeskriminalamtgesetz* alsook de *Ausländergesetz* (Vreemdelingenwet). De wetten worden onder meer gewijzigd om de openbareordediensten (Sicherheitsbehörden) in staat te stellen:

- de verkregen gegevens efficiënter met elkaar uit te wisselen;
- preventief de binnenkomst van een vermeend terrorist te verhinderen;

---

[244] Zie <http://www.ccla.org/> en <http://www.policyalternatives.ca/publications/c-36.html>.
[245] <http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_65812.htm>.
[246] De antiterrorismewet wordt uiteindelijk gepubliceerd in het *Bundesgesetzblatt*, nr. 3, 11 januari 2002. Deze publicatie is beschikbaar op <http://www.bundesanzeiger.de/bgbl1f/b1f01q1.htm>.
[247] De wet (*Änderung des Vereingesetzes*) wordt gepubliceerd in het *Bundesgesetzblatt*, nr. 64, p. 3319 van 7 december 2001. De inhoud is beschikbaar op <http://217.160.60.235/BGBL/bgbl1f/b101064f.pdf>.
[248] Richtlijn 2001/97/EG van 28 december 2001, *PbEG* 2001, L 344/76, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_344/l_34420011228en00760081.pdf>.
[249] <http://www.bmi.bund.de/top/dokumente/Pressemitteilung/ix_76935.htm>.

- identificerende maatregelen verbeteren (visum);
- grenscontroles aan te scherpen;
- de reeds in Duitsland bevindende extremisten (terroristen) te herkennen;
- de inzet van bewapende diensten en personen in vliegtuigen mogelijk te maken.

Het zwaartepunt van de nieuwe wetswijzigingen ligt in de stelling dat de veiligheids- of zekerheidsdiensten, zoals bijvoorbeeld het Bundeskriminalamt (Rijkspolitie), de Bundesgrenzschutz (douanedienst), het Bundesamt für Verfassungsschutz (geheime dienst) en de Bundesnachrichtendienst (Inlichtingendienst) over voldoende wettelijke bevoegdheden dienen te beschikken met het oog op de bestrijding van het terrorisme.
De Verfassungsschutz (geheime dienst) krijgt de bevoegdheid om in de pro-actieve fase (Vorfeldaufklärung) tevens bepaalde handelingen of gedragingen (stelselmatig) te observeren die zich tegen de samenleving richten en die een gevaarlijke voedingsbodem voor het opkomende terrorisme kunnen vormen.[250] Ook bepaalde geldstromen van extremistische organisaties of personen kunnen in de gaten gehouden worden om daarmee uiteindelijk aanknopingspunten te krijgen.
De traditionele onderzoeksbevoegdheden van de Rijkspolitie worden verder uitgebreid. Op eigen initiatief (lees: zonder machtiging of bevel) kunnen bepaalde vormen van zware computercriminaliteit opgespoord worden. Daarnaast worden de opsporingsbevoegdheden meer op centraal niveau uitgeoefend. Dit dient voor een betere informatiepositie te zorgen.

3.4.5. Frankrijk

Op 31 oktober 2001 wordt in Frankrijk de *Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne* (Wet over de dagelijkse veiligheid) aangenomen.[251] Deze was al in maart 2001 voorgesteld, maar na 11 september zijn diverse extra maatregelen ingevoegd in het wetsvoorstel. Deze hebben betrekking op onder andere autodoorzoekingen, fouillering door private veiligheidsfunctionarissen en televerhoren in strafprocedures. Voor ICT-regulering zijn twee maatregelen van bijzonder belang. Artikel 29 van de wet verplicht telecomaanbieders om bij decreet aan te wijzen gegevens (zoals verkeersgegevens) te bewaren gedurende een jaar. Daarnaast zijn eerder voorgestelde bepalingen over cryptografie ingevoegd (zie par. 3.3.5). Deze maatregelen zijn geldig tot 31 december 2003.

3.4.6. Japan

Als reactie op de aanslagen in en op de Verenigde Staten wordt in Japan de zogenaamde *Anti-Terrorism Special Measures Bill* voorgesteld. Op 29 oktober 2001 wordt het nieuwe wetsvoorstel door de *Diet* (Huis van Afgevaardigden) goedgekeurd. De hier genoemde wet wijkt sterk af de antiterrorismewetten in de westerse landen. Zo stelt de wet geen nieuwe bevoegdheden voor en worden andere wetten niet gewijzigd.

De nieuwe antiterrorismewet van Japan ziet onder meer op de volgende punten:

- de bijdrage van Japan (aan de internationale gemeenschap) inzake de bestrijding van het terrorisme;
- opvang van vluchtelingen als gevolg van internationaal terrorisme en het verschaffen van materiële zaken zoals tenten en dekens voor deze vluchtelingen, dit alles op verzoek van de Hoge Commissaris voor de Vluchtelingen van de VN;
- beschikbaar stellen van diverse fondsen voor noodhulp (vluchtelingen);
- afkeuren en ontmoedigen (economisch boycotten) van kernproeven ondernomen door India en Pakistan;
- maatregelen, in overeenstemming met de VN-verdragen 1267 en 1333, door geldstromen van bepaalde groepen (meer dan 200 in totaal) te beperken en te bevriezen;
- diplomatieke onderhandelingen om internationaal optreden tegen terrorisme te bevorderen;
- *search and rescue*-ondersteuning voor slachtoffers van de VS-aanslagen.

---

[250] <http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_65812.htm>.
[251] *Journal Officiel* 16 november 2001, <http://www.assemblee-nat.fr/dossiers/securite_quotidienne.asp>.

3.4.7. Verenigd Koninkrijk

Reeds enige tijd voor de aanslagen van 11 september was er in het Verenigd Koninkrijk antiterrorismewetgeving van kracht. Dat was de *Terrorism Act 2000*, in werking getreden op 19 februari 2001.[252] Naar aanleiding van de terroristische aanslagen in de Verenigde Staten wordt op 14 december 2001 besloten de wet te laten vervangen door de *Anti-terrorism, Crime and Security Act 2001*.[253]

De oude wet zag onder meer toe op de volgende punten;

- het creëren van permanente antiterrorismewetgeving;
- het geven van een nieuwe definitie van het begrip 'terrorisme' die ziet op alle vormen van terrorisme;
- het verlenen van nieuwe onderzoeksbevoegdheden om aan de nationale grenzen verdachte terroristische geldstromen in beslag te nemen;
- strafbaarstelling van het trainen/opleiden/voorbereiden van terroristische acties;
- strafbaarstelling van het uitlokken/aanzetten tot terroristische acties in het buitenland, waarbij de uitlokking in Engeland plaatsvindt.

De *Anti-terrorism, Crime and Security Act 2001* beoogt om tot regelgeving te komen die ervoor zorgt dat de overheid op verschillende gebieden, in het licht van de nieuwe situatie na de aanslagen van 11 september, over voldoende middelen beschikt op een adequate wijze de nieuwe dreiging af te slaan. De nieuwe maatregelen zijn onder meer bedoeld om:

- financiering van terroristische organisaties tegen te gaan;
- ervoor te zorgen dat departementen en andere overheidsinstellingen informatie verzamelen en met elkaar delen om de terroristische dreiging af te slaan;
- eenvoudige immigratieprocedures mogelijk te maken;
- strategische punten (kernenergie-industrie of luchtvaart) te beveiligen;
- gevaarlijke stoffen die een verhoogd risico lopen doelwit van terroristische aanslagen te worden van extra beveiliging te voorzien;
- strafvorderlijke bevoegdheden uit te breiden.

De nieuwe antiterrorismewet bestaat uit veertien delen. Hier volgt een toelichting op enkele delen.[254] Het eerste en tweede deel bevatten regels die ervoor moeten zorgen dat terroristen geen toegang tot hun vermogen (geld) krijgen. De regels vormen een aanvulling op bestaande strafwetgeving en dienen ervoor te zorgen dat de autoriteiten te allen tijde over maatregelen beschikken die het eventueel financieren van terroristische groeperingen kunnen dwarsbomen door onder andere deze gelden te bevriezen. Andere maatregelen zijn bijvoorbeeld het vorderen van inzicht in bepaalde bankrekeningen. Deel drie bevat regels voor de afscherming van bepaalde documenten. Op deze manier kunnen bepaalde stukken ontoegankelijk voor het grote publiek gemaakt worden. Deel vier maakt het mogelijk vermeende internationale terroristen vast te zetten indien zij een mogelijk gevaar voor de nationale veiligheid vormen. Daarbij komt de oude eis te vervallen dat vastzetting (*detention*) alleen mogelijk is indien tevens uitzetting (*removal*) tot de mogelijkheden behoort. Tevens wordt de asielprocedure ten aanzien van vermoedelijke terroristen aanzienlijk versneld en wordt een beroep tot herziening van een vermeende terrorist automatisch niet herzien door de daarover te beslissen beroepsinstantie (Secretary of State) indien laatstgenoemde instantie aantoont dat hierbij het algemeen belang gediend is.
Het tiende deel bevat nieuwe strafvorderlijke bevoegdheden die het voor de politie mogelijk maken een behoorlijk identificatieonderzoek te verrichten. Daarbij kan gedacht worden aan het maken van vingerafdrukken enkel en alleen met het oog op identificatie. Daarnaast kunnen ook

---

[252] <http://www.homeoffice.gov.uk/terrorism/index.htm>. De volledige inhoud van deze wet is beschikbaar op <http://www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm>.
[253] <http://www.hmso.gov.uk/acts/acts2001/20010024.htm>. De toelichting op deze wet is beschikbaar op <http://www.hmso.gov.uk/acts/en/2001en24.htm>.
[254] Bevindingen zijn gebaseerd op de Explanatory Notes (Toelichting) behorende bij de nieuwe antiterrorismewet 2001, beschikbaar op <http://www.hmso.gov.uk/acts/en/2001en24.htm>.

foto's worden genomen, eventueel vergezeld van maatregelen conform een politiebevel om bepaalde op het gezicht aangebrachte identificatieverstorende effecten te verwijderen. Het elfde deel bevat regels die het mogelijk maken voor de (straf)autoriteiten om telecommunicatieaanbieders te verplichten bepaalde klantgegevens voor bepaalde tijd te bewaren ten behoeve van de veiligheid van de Staat en op verzoek beschikbaar te stellen aan de (strafvorderlijke) autoriteiten. De klantgegevens mogen in ieder geval op basis van deze wet langer worden bewaard dan noodzakelijk voor de eigen bedrijfsvoering indien daarmee nationale belangen gediend zijn. In die zin vormt onderhavige wet een belangrijke aanvulling op de *Regulation of Investigatory Powers Act 2000* (RIPA) (zie par. 3.3.7).

3.4.8. Verenigde Staten

Direct na de terroristische aanslagen op Amerikaanse doelen en vooral onder invloed van het feit dat de aanslagen op Amerikaans grondgebied plaatsvonden, kondigt de Amerikaanse president Bush een wereldwijde antiterrorismecampagne af. Het is niet eenvoudig zicht te krijgen op de massa's maatregelen, wetgevingsinitiatieven, wetsvoorstellen en wetten die direct voortvloeien uit de terroristische aanslagen van 11 september. Het 'getroffen' land verkeert in een shock. Op basis van de in Amerika heersende gemoedstoestand krijgen vérgaande wetten de kans als paddestoelen uit de grond te schieten en zich te nestelen tussen bestaande wetgeving, waarmee bestaande evenwichten tussen veiligheid en vrijheid worden gewijzigd.

De belangrijkste wet, met nieuwe bevoegdheden, is de *Anti-Terrorism Act 2001* (ATA), beter bekend onder de namen USA-act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) en (USA) Patriot Act.
De wet (hierna Patriot Act) is op 26 oktober 2001 van kracht geworden. Het betreft hier in feite een verzamelwet. Veel afzonderlijke wetsvoorstellen zijn uiteindelijk in de Patriot Act opgenomen, zoals de International Money Laundering Abatement Act, de Financial Anti-Terrorism Act of 2001 en de Public Safety and Cyber Security Enhancement Act of 2001 (PSCSEA).
Enkele wijzigingen zijn de volgende.[255]

- Op basis van de Patriot Act zijn opsporingsbeambten voor het eerst bevoegd telecommunicatie af te tappen (*intercept wire communications*) indien de *Fraud and Abuse Act* (18 U.S.C. § 1030) overtreden is. Het dient hier te gaan om gesprekken, dus niet om elektronische communicatie. Zo kunnen opsporingsambtenaren gesprekken van 'hackers' afluisteren die hun plannen over de telefoon maken en voorbereiden. De lijst met 'tapbare' delicten is hiermee uitgebreid.
- Op basis van de *Electronic Communications Privacy Act* (ECPA) was het voor de opsporingsinstanties niet mogelijk opgeslagen draadgebonden communicatie (*wire communications*), zoals opgeslagen stempostberichten uit te luisteren indien deze zich bij de gedupeerde zelf bevonden. Daarvoor was een afzonderlijke huiszoekingsbevel vereist. Dat is onder de Patriot Act niet meer noodzakelijk.
- Op basis van de Patriot Act mag een dienstaanbieder voor het eerst op vrijwillige basis bepaalde communicatiegegevens (verkeersgegevens en ook inhoud) ter beschikking van strafvorderlijke autoriteiten stellen, indien hij aanwijzingen heeft dat een terrorist gebruik maakt van zijn diensten. Wel dient er sprake te zijn van een noodsituatie.
- De bestaande regeling inzake verkeersgegevens (*pen and trap orders*) wordt op een aantal punten gewijzigd. De regeling omvat nu tevens de communicatie over computernetwerken. Daarmee vallen alle transportgegevens van Internetcommunicatie onder de regeling.
- Invoering van landelijk effect van het vorderen van verkeergegevens. Hiermee behoeft een rechtbank geen rekening te houden met jurisdictie en is de vordering niet beperkt tot de beperkte rechtsmacht van de lokale rechter.
- Op verzoek de gedupeerden (eigenaren van pc) mogen strafvorderlijke autoriteiten nu elektronische communicatie onderscheppen van personen die inbreken (hacken) in bepaalde computers.

[255] <http://www.cdt.org/security/011030doj.pdf>.

- Invoeren van een landelijk bevel om de inhoud van een netpostbus (opgeslagen e-mailberichten) op te vragen. Op deze wordt de bevoegdheid tot uitlevering uitgebreid tot buiten het gebied waarbinnen de rechter normaliter bevoegd is.
- Uitbreiding van de DNA-databank. Ook 'terroristisch handelen' valt nu onder het bereik van de DNA-databank.

Daarnaast zijn nog diverse andere wetten en wetsvoorstellen van belang. Vele hiervan beogen de beveiliging van infrastructuren te verbeteren tegen terroristische aanslagen, zoals de *Cyberterrorism Preparedness Act 2002 (S.1900)* en de *Cybersecurity Research and Education Act 2002 (S.1901)*, die een samenwerkingsplatform en een terrorismeteam opzetten om de veiligheid van en op de digitale snelweg te bevorderen. Denk hierbij aan de ontwikkeling van toptechniekinstrumenten en wachtwoordbeveiliging. Deze wetsvoorstellen zijn ingediend op 28 januari 2002 en zijn op dit moment nog aanhangig. De *Cyber Security Research and Development Act (HR 3394)*, die voorstelt zogenaamde *cybersecurity research centers* op te richten, is in februari 2002 door het Huis van Afgevaardigden aangenomen.
Een wet die reeds is goedgekeurd is de *Cyber Security Enhancement Act 2001 (CSEA)*. Het doel van deze wet is het verhogen van de strafmaat inzake computerdelicten. Daarnaast wordt tevens een nieuwe orgaan ingesteld, het National Infrastructure Protection Center (NIPC), dat vooral als coördinatie- en steunpunt dient.

3.4.9. Zweden

Zweden heeft relatief weinig wettelijke maatregelen genomen als gevolg van de terroristische aanslagen op de VS; het legt de nadruk op internationale samenwerking. Zweden is reeds toegetreden tot alle 12 VN-verdragen tegen terrorisme. Als uitvloeisel daarvan is op 1 november 2001 een wetsvoorstel uitgebracht dat de mogelijkheid geeft financiële tegoeden van terroristen te bevriezen.[256]
Voorts heeft Zweden samen met Finland het voorstel gedaan het de Raad van het Euro-Atlantische Partnerschap (EAPC), waarin de landen van de NAVO en het Partnership for Peace zijn verenigd, te verstevigen door nader samen te werken op het terrein van terrorismebestrijding.[257]

3.4.10. Samenvatting

De aanslagen op de VS van 11 september 2001 hebben tot een grote stroom aan beleids- en reguleringsinitiatieven geleid. Met uitzondering van Nederland en Zweden hebben alle onderzochte landen één of meer wetten aangenomen als directe reactie op de aanslagen. Nederland heeft daarentegen wel een grootschalig actieplan terrorismebestrijding gelanceerd, vol oude en nieuwe voorstellen, dat qua inhoud vergelijkbaar is met veel van de antiterrorismewetten in de overige landen. Inhoudelijk gezien hebben alleen Japan en Zweden zich relatief rustig hebben gehouden in de nasleep van 11 september, met slechts beperkte nationale wetsinitiatieven; zij leggen meer de nadruk op internationale samenwerking. De overige landen, waaronder Nederland, hebben ingrijpende wijzigingen voorgesteld of doorgevoerd naar aanleiding van 11 september. Vooral de VS, het VK en Canada voeren hierin de boventoon. Overigens is niet alle wetgeving even nieuw. Diverse bepalingen waren al eerder voorgesteld maar zijn door 11 september versneld aangenomen; bij andere eerder voorgestelde maatregelen heeft 11 september extra gewicht in de schaal gelegd – mogelijk zouden deze maatregelen anders niet zijn aangenomen.
De voorgestelde of doorgevoerde maatregelen die relevant zijn voor ICT-regulering betreffen vooral vergroting van de informatie-uitwisseling tussen veiligheidsdiensten en politie (bijvoorbeeld in de EU, Duitsland en Nederland), versterking van identificatiemogelijkheden (bijvoorbeeld in Duitsland, Nederland en het VK), het uitbreiden van DNA-databanken (Canada en de VS) en beveiliging van netwerken en infrastructuren (bijvoorbeeld in EU, Nederland en de VS). Daarnaast valt vooral op dat bevoegdheden voor het onderzoek van telecommunicatie

[256] Zie <http://www.utrikes.regeringen.se/inenglish/frontpage/terror.htm>.
[257] <http://www.regeringen.se/galactica/service=irnews/action=obj_show?c_obj_id=42160>.

worden uitgebreid: de telecomtap mag vaker worden toegepast (Canada en de VS) of wordt versneld verbeterd (Nederland), verkeersgegevens kunnen sneller worden overhandigd (de VS) of moeten verplicht worden bewaard (Frankrijk, het VK en mogelijk Nederland).
Alles overziend zijn de maatregelen en bevoegdhedenuitbreiding niet dusdanig ingrijpend dat er een verkillend effect op de elektronische handel mag worden verwacht, maar duidelijk is wel dat het bestaande grensvlak tussen veiligheid en persoonlijke vrijheden in de meeste landen is verschoven en dat er meer inbreuk op de burgerlijke vrijheden mogelijk is dan voorheen.

4. Fiscale aspecten

Voor de ontwikkeling van elektronische handel zijn fiscale aspecten van groot belang. Met name bij grensoverschrijdende handel doet zich de vraag voor waar wordt belast. Ook het fiscale klimaat is evenwel relevant: kent een land fiscale stimuleringsmaatregelen om het aantrekkelijk te maken voor webhandelaren om zich er te vestigen?
In dit hoofdstuk wordt een overzicht op hoofdlijnen gegeven van de stand van zaken van fiscale beleids- en reguleringsinitiatieven op het gebied van de elektronische handel. Daarbij wordt voortgebouwd op de *Internationale ICT-toets* van 2000.[258] Hierbij wordt een drietal onderdelen onderscheiden: directe belastingen, verbruiksbelastingen en fiscale stimulering van ICT-toepassingen.
Wat opvalt is dat de ontwikkelingen na 2000 zich met name op internationaal terrein hebben afgespeeld. Wat betreft de directe belastingen is het met name de OESO die zich manifesteert. Wat betreft de consumptiebelastingen speelt vooral de EU de eerste viool.

4.1. Internationaal

De internationale fiscale discussie over elektronische handel, hierna ook wel e-business genoemd, is intensief en omvangrijk. Wat betreft de directe belastingen heeft de OESO de leiding in die discussie naar zich toegetrokken. Alle landen die onderwerp zijn van deze studie zijn lid van de OESO en accepteren ook de leidende rol van de OESO in dezen. Wat betreft de consumptiebelastingen is met name de EU bepalend, hoewel ook de OESO zich steeds meer op dit terrein in de discussie mengt. Tot op heden heeft de EU zich op het terrein van de directe belastingen en e-business nog niet echt gemanifesteerd. Op internationaal niveau zijn ons geen initiatieven bekend die specifiek op de fiscale stimulering van ICT-toepassingen zien. Wel is het zo dat de initiatieven van de OESO en de EU in het algemeen tot doelstelling hebben om de elektronische handel te stimuleren dan wel om fiscaaljuridische belemmeringen weg te nemen of te verzachten.

4.1.1 Directe belastingen

De OESO heeft op grond van de in 1998 in Ottawa geformuleerde 'taxation framework conditions' in 2000 en 2001 een aantal belangwekkende rapporten en discussiestukken gepubliceerd.[259] Hiermee is een belangrijke stap voorwaarts gezet om een internationale consensus te bereiken over de belastingheffing van elektronische handel. Met de rapporten wordt met name beoogd om binnen het bestaande fiscale kader, vooral belastingverdragen, zekerheid te verschaffen aan zowel het bedrijfsleven als overheden. De OESO is in het algemeen nog niet toe aan de beantwoording van de vraag of het huidige fiscale instrumentarium nog wel voldoet in de door e-handel veranderde en veranderende wereld. De OESO-rapporten zijn in het algemeen tot stand gekomen in samenwerking met het bedrijfsleven en niet-OESO-landen (de zogenaamde Technical Advisory Groups), waardoor het draagvlak voor de voorgestelde oplossingen of oplossingsrichtingen niet beperkt is tot de OESO-lidstaten. Opgemerkt zij dat de discussies nog lang niet zijn afgerond, hoewel op een enkel terrein al wel voorlopige eindconclusies zijn getrokken. Door het werk van de OESO zal wereldwijd een grotere uniforme fiscale behandeling van elektronische handel mogelijk worden, hetgeen de verdere ontwikkeling van de elektronische

---

[258] Zie Landwell 2000.

[259] De rapporten zijn gebundeld in OECD 2001a. Hierin zijn ook rapporten opgenomen inzake de invloed van ICT op consumptiebelastingen en het functioneren van belastingadministraties. Bij dit laatste wordt niet alleen ingegaan op de problemen en mogelijkheden van belastingadministraties bij de heffing van, de controle op en de invordering van belastingen, maar ook op de mogelijkheden om de dienstverlening aan belastingplichtigen te verbeteren, zoals bijvoorbeeld informatieverstrekking en het doen van een elektronische aangifte. In veel landen is het mogelijk om een elektronische aangifte te doen. Zie bijvoorbeeld Duitsland, Frankrijk, Nederland, het Verenigd Koninkrijk en de Verenigde Staten. In Verenigde Staten is zelfs de mogelijkheid geopend om een het doen van een elektronische aangifte af te dwingen (Section 6001, lit e, para. 1 Internal Revenu Code). Ook in het Verenigd Koninkrijk bestaan daartoe plannen wat betreft de Britse *wage tax*. Vergelijk ook Käbisch en Unruh 2000, p. 33-39

handel ten goede zal komen. De kans op dubbele belasting van e-handel of het in het geheel geen belasting heffen zal als gevolg van die grotere uniforme behandeling worden verkleind. De meeste staten wachten overigens nog wel met nationale initiatieven totdat binnen de OESO definitieve overeenstemming is bereikt. Op het terrein van de toepassing van belastingverdragen is een viertal rapporten verschenen:
(1) *Clarification on the application of the permanent establishment definition in e-commerce: changes to the commentary on Article 5*;
(2) *Treaty characterisation issues*;
(3) *Attribution of profit to a permanent establishment involved in electronic commerce transactions* (*A discussion paper from the Technical Advisory Group on monitoring the application of existing treaty norms for the taxation of business profits*);
(4) *Impact of the communications revolution on the application of "place of effective management" as a tie breaker rule* (*A discussion paper from the Technical Advisory Group on monitoring the application of existing treaty norms for the taxation of business profits*).
Hieronder wordt nader ingegaan op de afzonderlijke rapporten.

4.1.1.1 Vaste inrichting
Een vaste inrichting en een vaste vertegenwoordiger zoals behandeld in het eerste rapport vormen voor een verdragsstaat aanknopingspunten om belastingjurisdictie te kunnen claimen. Het gaat hierbij om de andere verdragsstaat dan waarin de ondernemer in fiscale zin woont of is gevestigd, de zogenaamde bronstaat. De woonstaat van de ondernemer geeft dan een tegemoetkoming voor aan een vaste inrichting of vaste vertegenwoordiger toe te rekenen winst, waardoor dubbele belasting wordt voorkomen. Zonder vaste inrichting of vaste vertegenwoordiger is alleen de zogenaamde woonstaat bevoegd om over de winst uit onderneming te heffen. Er bestaat in het algemeen consensus over het volgende:
(a) Een weblocatie van een zogenaamde inhoudsaanbieder vormt geen vaste inrichting. Portugal en Spanje nemen hierbij evenwel een afwijkend standpunt in.
(b) Een server voldoet aan de algemene verdragsdefinitie van een vaste inrichting, ook al is er op de plaats van de server geen sprake van menselijke activiteiten die aan de ondernemer kunnen worden toegerekend. Het feit dat een server gemakkelijk verplaatsbaar is doet daaraan niet af. Het Verenigd Koninkrijk vormt een uitzondering met zijn standpunt dat een dergelijke enkele server (*stand-alone server*)[260] geen vaste inrichting kan vormen.
(c) Voor veel ondernemers zal een enkele server echter als een werkzaamheid van voorbereidende aard zijn aan te merken of het karakter van een hulpwerkzaamheid hebben, waardoor met een beroep op de uitzonderingsregels alsnog een vaste inrichting wordt voorkomen. Een Internetdienstaanbieder (ISP) en telecommunicatieondernemers zullen deze uitzonderingsregels niet kunnen inroepen, omdat een dergelijke server onderdeel is van de kernactiviteiten.
(d) De server van een ISP vormt in het algemeen geen vaste inrichting voor de inhoudsaanbieder die van de diensten van de desbetreffende ISP gebruik maakt.
(e) Een weblocatie en een server kunnen geen vaste vertegenwoordiger zijn, onder andere, omdat zij geen persoon zijn in de zin van een belastingverdrag.
(f) Een ISP vormt in het algemeen ook geen vaste vertegenwoordiger voor een inhoudsaanbieder omdat de ISP doorgaans geen contracten namens de inhoudsaanbieder afsluit.
De OESO heeft voorgesteld om het bovenstaande in 2002 in het OESO-Commentaar op het OESO-Modelverdrag in te voegen (Draft 2002).[261] Naar verwachting zal over de Draft 2002 in de tweede helft van 2002 een beslissing worden genomen. In veel landen wordt het OESO-Commentaar gebruikt bij de interpretatie en toepassing van belastingverdragen, ook in de

[260] Dat wil zeggen, een server die op zijn locatie verder niet is ingebed in een organisatie van arbeid en kapitaal van de onderneming. Vanwege mogelijke verwarring door het begrip 'stand-alone' (dat bij pc's aanduidt dat deze niet met een netwerk zijn verbonden), wijken wij hier af van de OESO-terminologie van *stand-alone server* en hanteren wij het begrip 'enkele server'.
[261] Zie OECD 2001b.

jurisprudentie. Het is echter de vraag of rechters in de verschillende landen ook deze aanpassingen van het OESO-Commentaar zullen overnemen.[262]
In het algemeen kan een inhoudsaanbieder zijn ondernemingsactiviteiten zo vorm geven dat de keuze aan hem is of hij in een bepaald land wel of niet een aanknopingspunt voor belastingheffing heeft. Dit biedt mogelijkheden tot belastingplanning en dat kan de concurrentieverhoudingen weer beïnvloeden.

4.1.1.2 Classificatie van inkomen
Het tweede rapport ziet met name op vraag of een bepaald inkomen als ondernemingswinst of als een royalty moet worden geclassificeerd. Zoals hierboven aangegeven mag winst uit onderneming alleen in de woonstaat worden belast, tenzij er sprake is van een vaste inrichting of vaste vertegenwoordiger. Indien een vaste inrichting of vaste vertegenwoordiger ontbreekt, dan mag de bronstaat geen belasting heffen. Indien het inkomen echter als een royalty kan worden aangemerkt, dan mag een bronstaat vaak toch een (bron)heffing opleggen. De percentages variëren, maar een percentage van tien over de bruto betalingen is dan wel gangbaar. Soms biedt een belastingverdrag voor een bronstaat naast royalty's nog andere aanknopingspunten om belastingjurisdictie te claimen. Soms geven ook betalingen voor knowhow, voor het gebruik of recht van gebruik van industriële, commerciële of wetenschappelijke uitrusting, of voor diensten van technische, management- of adviserende aard een bronstaat het recht om belasting te heffen. Uitgangspunt is dat dient te worden vastgesteld waarvoor de vergoeding hoofdzakelijk wordt betaald. Bijvoorbeeld, bij het onderscheid tussen winst uit onderneming en royalty's zal het dan met name van belang zijn om vast te stellen of hoofdzakelijk voor andere dingen wordt betaald dan voor het auteursrecht en of het gebruik van het auteursrecht beperkt is. Indien dit het geval is, dan zal er in het algemeen geen sprake zijn van een royalty maar van winst uit onderneming. De algemene conclusie van het rapport komt erop neer dat slechts in een beperkt aantal situaties er sprake zal zijn van royalty's, bijvoorbeeld het elektronisch bestellen en binnenhalen van digitale producten teneinde het auteursrecht daarop commercieel te exploiteren. Het rapport bevat ook aanbevelingen om het OESO-Commentaar aan te passen. In de Draft 2002 wordt voorgesteld om het Commentaar inderdaad aan te passen.[263]

4.1.1.3 Toerekening van winst aan vaste inrichting
Het derde rapport, dat in wezen een discussiestuk is, gaat nader in op de toerekening van winst aan een vaste inrichting (daaronder begrepen vaste vertegenwoordiger) in een e-business. Het discussiestuk bouwt voort op de conclusies van het eerste rapport. Het besteedt met name aandacht aan de toerekening van winst aan een enkele server door middel waarvan volledig geautomatiseerde functies worden uitgeoefend. Het gaat daarbij met name om het online verwerken van transacties en verzenden van digitale producten. Het rapport geeft aan dat de toepassing van het *arm's length*-beginsel in een dergelijke situatie problematisch is, omdat er op de locatie van de server geen menselijke activiteiten worden verricht die aan de ondernemer kunnen worden toegerekend. Voor de toerekening van winst geldt dat op grond van dit beginsel de vaste inrichting moet worden gezien als een "functionally separate entity". De vaste inrichting en het hoofdhuis worden geacht met elkaar te handelen zoals zelfstandige ondernemingen onder dezelfde of soortgelijke omstandigheden zouden doen. De omvang van de toe te rekenen winst wordt dan met name bepaald door de uitgevoerde functies rekening houdend met de aan de vaste inrichting toe te rekenen activa en de toe te rekenen veronderstelde risico's. In het kader van een enkele server wordt het voorbeeld van een webhandelaar (*retail distribution of entertainment products*) met een aantal variaties daarop uitgewerkt. Het voorbeeld wordt geacht een wijdere werking te hebben. De conclusie is dat er maar weinig inkomen aan een dergelijke vaste inrichting kan worden toegerekend, omdat het zwaartepunt van de functies en de daarbij horende activa en risico's bij het hoofdhuis en niet bij de vaste inrichting ligt. Als er geen mensen voor de ondernemer op de plaats van de server actief zijn, dan kan er volgens het discussiestuk slecht een *cost-plus*-benadering worden toegepast omdat de vergelijking dient te worden gemaakt met een

[262] Vergelijk Kemmeren 2001, p. 337-340 en 366-368. Zie voor een bespreking van nationaalrechtelijke concepten, onder andere, Doernberg, Hinnekens, Hellerstein & Li 2001, p. 175-203.
[263] Zie OECD 2001b.

"contract service provider" of "independent service provider". Dit betekent dat niet meer dan de toerekenbare kosten met een geringe winstmarge als winst aan de enkele server zou kunnen worden toegerekend.
De OESO heeft om commentaar gevraagd op het rapport. Er zal derhalve een vervolg op komen. In de literatuur is uitgebreid op de toerekening van winst in een dergelijke situatie ingegaan.[264] In dit verband wordt ook wel verdedigd dat juist een substantieel deel of misschien wel alle winst aan de vaste inrichting moet worden toegerekend, omdat de enkele server een, zo niet de, essentiële en significante functie(s) van de onderneming uitoefent. Verder kan men zich afvragen of in geval van een *e-tailer* een vergelijking met een *bricks and mortar retailer* niet meer voor de hand ligt en derhalve de toepassing van een *resale-minus*- in plaats van een *cost-plus*-toerekening. Bovendien is het nog maar de vraag of het voorbeeld van de e-tailer ook model kan staan voor het toerekenen van winst in andere gevallen van e-business. Zo lijken de traditionele toerekeningsmethoden waaronder worden begrepen de op transactie basis gebaseerde methoden van *comparable uncontrolled price*, *cost-plus* en *resale minus* en de op transactiewinst gebaseerde methoden van *profit split* en *transactional net margin* minder goed toepasbaar te zijn op grensoverschrijdende netwerken van toegevoegde waarden, die in de e-business steeds meer de plaats van ketens van toegevoegde waarden zullen innemen. Op dit terrein heerst derhalve nog veel onduidelijkheid, hetgeen de verdere ontwikkeling van e-handel geen goed zal doen. De OESO zou het proces om tot een internationale consensus te komen moeten versnellen.

4.1.1.4 Dubbele woonplaats lichamen
Het vierde rapport inzake de verdragswoonplaats is ook een discussiestuk. Als gevolg van de nationale fiscale regels van de verdragsstaten kunnen natuurlijke personen en lichamen onder omstandigheden als inwoners van beide verdragsstaten worden aangemerkt. Voor de toepassing van een belastingverdrag is het echter noodzakelijk om tot een enkelvoudige woonplaats van inwoners van de betrokken verdragsstaten te komen – anders kunnen de toewijzingsregels niet goed worden toegepast, waardoor dubbele belasting of zogenaamde "double dips" (bijvoorbeeld eenzelfde verlies in twee landen en dus dubbel in aanmerking nemen) in stand blijven. De ICT-ontwikkelingen lijken met betrekking tot de vaststelling van een enkelvoudige woonplaats van natuurlijke personen voor de toepassing van belastingverdragen tot weinig problemen te leiden. Dit is anders met betrekking tot lichamen. Als gevolg van het Internet, intranets, videovergaderingen, telefonische vergaderingen, e-mail en dergelijke is het voor de bestuursleden van een lichaam minder of niet noodzakelijk om op één plaats als bestuur te functioneren. De bestuursleden kunnen gemakkelijk(er) in en vanuit verschillende jurisdicties functioneren, waardoor de verdragsregel die uitkomst moet brengen in geval van een dubbele woonplaats van lichamen bij een gedecentraliseerd functionerend bestuur geen uitkomst meer lijkt te bieden. Het huidige criterium is namelijk dat een lichaam met een dubbele vestigingsplaats voor de toepassing van het verdrag slechts inwoner wordt geacht te zijn van de staat waarin *de* plaats van werkelijke leiding van het lichaam zich bevindt. Echter *de* plaats van werkelijke leiding van een lichaam zal bij een sterk gedecentraliseerd functionerend bestuur niet meer zijn vast te stellen. Het bestuur zal dan op meerdere plaatsen de werkelijke leiding van het lichaam uitvoeren. Het gevolg kan dus zijn dubbele belasting of "double dips", hetgeen niet wenselijk is. Het discussiestuk komt zelf met een viertal mogelijke oplossingen en nodigt uit tot commentaar of andere alternatieven.[265] Als mogelijke oplossingen worden in het discussiestuk genoemd:
(a) het vervangen van de plaats van werkelijke leiding door het incorporatiebeginsel;
(b) verdere verfijning van het criterium van plaats van werkelijke leiding;
(c) de introductie van een rangorderegeling, startend met de plaats van werkelijke leiding, gevolgd door plaats van oprichting, economische nexus en tot slot een regeling gebaseerd op onderlinge overeenstemming;
(d) een combinatie van de drie voorgaande alternatieven.
Ook hier ligt derhalve een terrein dat nog niet is uitgekristalliseerd. Hoewel het probleem op dit moment in omvang wellicht nog niet heel erg groot is, dient er toch van te worden uitgegaan dat

[264] Zie bijvoorbeeld Strunk 2000, p. 9-17, Sprague en Boyle 2001, p. 21-63, Kemmeren 2001, p. 368-372, Ackerman, Danziger, Faiferlick & Lim, 2001, p. 1465-1484.
[265] Zie voor een alternatief, bijvoorbeeld, Kemmeren 2001, p. 259-265 en 280-282.

het probleem steeds prangender wordt, niet alleen vanwege de voortschrijdende ICT-ontwikkelingen, maar ook door toenemende grensoverschrijdende fusies en overnames, waardoor de raden van bestuur ook steeds internationaler van samenstelling zullen worden.

De OESO heeft in het kader van e-business al heel wat werk verricht en zal nog veel werk dienen te verrichten. Verder lijkt ons er ook een rol te zijn weggelegd voor de Europese Commissie. Immers het terrein van de directe belastingen raakt ook het functioneren van de interne markt van de EG. Het bevorderen van die interne markt kan niet aan de OESO worden overgelaten. De instellingen van de EU hebben daarvoor een eigen verantwoordelijkheid. In het kader van de traditionele handel is er al een aantal initiatieven geweest.[266] Nu wordt het ook tijd om na te gaan of, bijvoorbeeld, in het kader van het creëren van een *level playing field* ingrijpen op Europees niveau gewenst is.

4.1.2 Verbruiksbelastingen

Tijdens de Ottawa-conferentie in 1998 is op het gebied van de verbruik- of consumptiebelastingen overeenstemming bereikt over het feit dat belastingheffing plaats dient te vinden op de plaats van consumptie, en dat digitaal geleverde producten niet anders belast mogen worden dan hun fysieke pendanten. Zoals reeds onder 4.1.1 is opgemerkt, heeft de OESO op grond van de in Ottawa geformuleerde 'taxation framework conditions' in 2000 en 2001 een aantal rapporten en discussiestukken gepubliceerd. Op het terrein van de toepassing van verbruiks- of consumptiebelastingen is in 2001 het rapport *Consumption tax aspects of electronic commerce* verschenen. In het rapport wordt op grond van de in Ottawa geformuleerde 'taxation framework conditions' gekozen voor belastingheffing op de plaats van consumptie. Het is dan ook van groot belang dat de plaats van consumptie van elektronische diensten helder wordt gedefinieerd. Tevens gaat het rapport in op mogelijke oplossingen om eenvoudiger tot invordering van belasting te kunnen overgaan. Verder wordt in het rapport wederom benadrukt dat de internationale samenwerking van belastingadministraties dient te worden verbeterd en dat fiscale en administratieve regelingen zo eenvoudig mogelijk moeten worden gehouden.

Naast de initiatieven binnen de OESO is in EU-verband steeds geijverd voor een aanpassing van de regelgeving met betrekking tot (Europese) BTW bij e-handelprestaties aan EU-consumenten. Een aanpassing van de Europese Zesde BTW-richtlijn werd nodig geacht, omdat thans buiten de EU gevestigde dienstverrichters in tegenstelling tot binnen de EU gevestigde dienstverrichters geen BTW in rekening hoeven te brengen voor de levering van digitale producten. Op 12 februari 2002 is een richtlijn inzake BTW en e-handel[267] door de EU-Ministerraad aangenomen. In het kort komt de regeling erop neer dat elektronisch geleverde producten van buiten de EU-aan consumenten binnen de EU belastbaar worden in de lidstaat waar de consument woont. De niet in de EU gevestigde leveranciers mogen zich in een lidstaat naar keuze registreren, maar worden desalniettemin BTW verschuldigd op basis van de wetgeving van de lidstaat waarin de afnemende consument woonachtig is, zij het dat afdracht aan de lidstaat van registratie volstaat. De EU-lidstaten zullen het mogelijk moeten maken dat de administratieve afwikkeling (zo veel mogelijk) via elektronische weg kan geschieden.

Scherp in het oog dient te worden gehouden dat de nieuwe regeling enkel ziet op digitale prestaties van niet in de EU gevestigde ondernemingen aan EU-consumenten (B2C). Indien de prestaties worden geleverd aan EU-ondernemingen (B2B), zal de verschuldigde BTW worden verlegd naar de afnemer, die de BTW aan de fiscus zal moeten afdragen. Naar verluidt vormen de B2B-transacties ongeveer 90% van de markt.
De lidstaten moeten de nieuwe regels uiterlijk 1 juli 2003 in hun nationale wetgevingen hebben geïmplementeerd. De nieuwe regels zullen vervolgens vóór 30 juni 2006 door de lidstaten worden geëvalueerd, waarna een definitieve aangepaste regeling in werking zal treden of de

---

[266] Zie, bijvoorbeeld, Commissie van de Europese Gemeenschappen, *Naar een interne markt zonder belastingbelemmeringen, Een strategie voor het verschaffen van een geconsolideerde heffingsgrondslag aan ondernemingen voor de vennootschapsbelasting op hun activiteiten in de gehele EU*, 23 oktober 2001, COM(2001) 582def.
[267] Richtlijn 2002/38/EG van de Raad van 7 mei 2002, *PbEG* 15 mei 2002, L 128/41.

onderhavige regeling zal worden voortgezet voor een verlengde periode. De richtlijn bevat een lijst van producten waarop de nieuwe regeling in ieder geval van toepassing is indien deze via elektronische weg worden verstrekt. De lijst is evenwel niet limitatief. De lidstaten hebben derhalve de bevoegdheid de lijst uit te breiden, hetgeen een belemmering zou kunnen opwerpen voor een uniforme behandeling van e-handelactiviteiten in de verschillende lidstaten. De lijst omvat de volgende digitale producten:

- het leveren en onderbrengen van computersites, het onderhoud op afstand van programma's en uitrustingen;
- de levering van software en het actualiseren ervan;
- de levering van beelden, geschreven stukken en informatie en de terbeschikkingstelling van databanken;
- de levering van muziek of films, van spelen, met inbegrip van kans- of gokspelen, en van uitzendingen of manifestaties op het gebied van politiek, cultuur, kunst, sport, wetenschappen of ontspanning;
- de levering van onderwijs op afstand.

De Verenigde Staten hebben evenwel reeds hun bezwaren tegen de Europese fiscale benadering van B2C kenbaar gemaakt.[268] Amerikaanse bedrijven zullen, anders dan hun Europese concurrenten, bijvoorbeeld BTW verschuldigd worden conform de wetgeving van het land van consumptie. Dit levert extra kosten op voor Amerikaanse bedrijven en kan leiden tot een tariefnadeel ten opzichte van EU-bedrijven die gevestigd zijn in lidstaten met een relatief laag BTW-tarief (ten opzichte van EU-bedrijven gevestigd in lidstaten met een relatief hoog BTW-tarief vormt het een concurrentievoordeel). Voorts hebben de Verenigde Staten er bezwaar tegen dat producten in digitale vorm onder omstandigheden zwaarder belast worden dan dezelfde producten in fysieke vorm. Dit laatste bezwaar geldt uiteraard niet alleen voor niet in de EU gevestigde ondernemers, maar tevens voor in de EU gevestigde ondernemers en vormt mitsdien geen concurrentievervalsing waarvan met name Amerikaanse bedrijven last van zouden kunnen hebben.

Inmiddels heeft de EU-Ministerraad ook de Richtlijn inzake elektronisch factureren aangenomen.[269] Deze richtlijn, die overigens meer aspecten van het factureren omvat dan enkel het elektronisch factureren, moet door de lidstaten uiterlijk op 1 januari 2004 in hun nationale wet- en regelgeving zijn geïmplementeerd. Voornoemde richtlijn wijzigt de Europese Zesde BTW-richtlijn om deze aan de huidige tijd aan te passen. De voorwaarden waaraan een factuur moet voldoen zijn geharmoniseerd. Daarnaast is geregeld dat bedrijven elektronisch mogen factureren. Voorwaarde daarbij is dat de afnemer accepteert dat de leverancier elektronisch factureert. Lidstaten moeten een elektronische factuur aanvaarden mits voorzien van een beveiligde handtekening,[270] EDI wordt gehanteerd[271] of deze aan andere door de lidstaat erkende voorwaarden voldoet.

Met de Richtlijn inzake BTW en e-handel is de EU erin geslaagd om de achterstandspositie van in de EU gevestigde leveranciers van digitale producten ten opzichte van hun niet in de EU gevestigde concurrenten teniet te doen. Keerzijde van de gekozen benadering is dat nu de niet in de EU gevestigde ondernemers zich in een nadeligere positie bevinden. Dit kan, gelet op de reactie van de Verenigde Staten op de richtlijn, wellicht leiden tot een klacht bij de WTO. Daarbij zal de vraag kunnen spelen of een niet in de EU gevestigde ondernemer, die zich in één van de lidstaten moet registreren terzake van elektronisch geleverde B2C-diensten, gelijk is te stellen met een wel in de EU gevestigde ondernemer die dezelfde prestaties levert. De regeling voor de niet-EU ondernemers lijkt evenwel in overeenstemming met het uitgangspunt van de OESO om

---

[268] Zie de verklaring van de onderminister van Financiën Kenneth W. Dam op 8 februari 2002, <http://www.ustreas.gov/press/releases/po1001.htm>.
[269] Richtlijn 2001/115/EG van de Raad van 20 december 2001, *PbEG* 17 januari 2002, L 15/24.
[270] Derhalve een beveiligde elektronische handtekening in de zin van art. 2 lid 2 Richtlijn 1999/93/EG (zie par. 5.1.1).
[271] Voldaan moet worden aan de definitie van art. 2 Aanbeveling 1994/820/EG.

digitale activiteiten daar te belasten waar de consumptie plaatsvindt. Voor EU-ondernemers wordt dit principe echter (nog) niet gehuldigd. Verder voorziet de Richtlijn elektronisch factureren in de behoefte om de thans geldende factuurvereisten aan te passen aan de huidige tijd.

4.2. Nederland

4.2.1 Directe belastingen

Nederland volgt de OESO op het terrein van de directe belastingen. Eerder had Nederland het standpunt ingenomen dat ingeval een enkele server als een vaste inrichting zou moeten worden aangemerkt, hieraan in beginsel geen winst zou dienen te worden toegerekend. Deze opvatting strookt niet met het OESO-discussiestuk zoals hierboven besproken. Het is afwachten of Nederland dit eigen standpunt overeind houdt dan wel de koers van de OESO gaat volgen. Dit laatste ligt wellicht in de lijn der verwachting, omdat Nederland ook heeft aangegeven dat indien al winst aan een dergelijke server dient te worden toegerekend, dit op basis van een *cost-plus* dient te gebeuren mits er sprake is van ondersteunende of soortgelijke activiteiten. Hiertoe kan ook een *advanced pricing agreement* worden overeengekomen, zodat de buitenlandse investeerder zekerheid vooraf kan krijgen over zijn fiscale positie.[272]

4.2.2 Verbruiksbelastingen

Nederland zal als lidstaat van de EU de Richtlijn inzake BTW en e-handel uiterlijk op 1 juli 2003 in haar wetgeving moeten hebben geïmplementeerd. Het is thans nog niet duidelijk of Nederland de niet-limitatieve lijst van digitale producten zal uitbreiden. Duidelijk is dat de speelruimte van Nederland op het gebied van de BTW zeer beperkt is. Nederland zal zich moeten conformeren aan de regelgeving van de EU op dit gebied. Tot het moment van implementatie van de nieuwe wetgeving kan voor de heffing van omzetbelasting met betrekking tot prestaties die over het Internet worden verricht, onder andere worden teruggevallen op in 1998 gepubliceerd beleid.[273] Hierin is vastgelegd dat het tegen vergoeding binnenhalen van spelletjes, erotische tijdschriften, muziek, films en andere standaardbeelden of -programma's via het Internet een dienst is waarop in B2C-verhoudingen geen Nederlandse BTW drukt indien, bijvoorbeeld, de leverancier buiten Europa en de consument in Nederland is gevestigd. In de spiegelbeeldsituatie zal wel Nederlandse BTW in rekening dienen te worden gebracht. Indien er geen sprake is van het binnenhalen van bestanden via het Internet maar van het tegen vergoeding raadplegen of bekijken van op een weblocatie geplaatste bestanden, dan kan er, volgens de staatssecretaris, sprake zijn van een vermakelijkheidsactiviteit, van een onderwijsactiviteit of van informatieverschaffing. In geval van een vermakelijkheids- of onderwijsactiviteit is de plaats van de dienst de plaats waar de afnemer de vermakelijkheids- of onderwijsprestatie afneemt, dat wil zeggen de plaats waar het vermaak of het onderwijs plaatsvindt. In B2C-verhoudingen dient dan wel Nederlandse BTW in rekening te worden gebracht indien, bijvoorbeeld, de leverancier buiten Europa en de consument in Nederland is gevestigd. In de spiegelbeeldsituatie zal daarentegen geen Nederlandse BTW in rekening behoeven te worden gebracht. Aan de ondernemer is in dit verband een aantal handvatten aangereikt die kunnen bijdragen aan het bewijs dat men in Nederland geen omzetbelasting is verschuldigd. Daarbij kan worden gedacht aan: de eigen opgaaf van het woonadres van de afnemer, het e-mailadres van de afnemer, de bank of de kredietkaartmaatschappij via welke de betaling binnenkomt en de vastlegging van de Internetaanbieder via welke de afnemer inbelt.

Nederland dient verder de factuurvereisten uit de Richtlijn elektronisch factureren, net als de overige lidstaten, uiterlijk 1 januari 2004 in de nationale wet- en regelgeving te hebben geïmplementeerd. In Nederland bestaat reeds een besluit waarin vereisten over elektronisch factureren zijn opgenomen.[274] De vereisten voor elektronisch factureren zoals opgenomen in het

---

[272] Notie van de Staatssecretaris van Financiën, *Belastingen in een wereld zonder afstand*, 4 mei 1998, p. 31-32.
[273] Besluit van 14 augustus 1998, nr. VB98/1785, V-N 1998/40.33.
[274] Besluit van 26 april 2001, nr. CPP2001/1104, V-N 2001/25.5.

besluit stemmen vrijwel geheel overeen met de vereisten van de Richtlijn elektronisch factureren. Het besluit is dan ook gebaseerd op het voorstel voor deze richtlijn.

4.2.3 Fiscale stimulering van ICT-toepassingen

Er zijn diverse nationale regelingen waarmee wordt beoogd om de ontwikkeling en het gebruik van ICT positief te beïnvloeden.
(1) *Willekeurige fiscale afschrijving*. In de winstsfeer zijn geen speciale regelingen op dit vlak. In de belastingwetgeving is wel een aantal mogelijkheden tot willekeurige afschrijving opgenomen die een positief effect op het gebruik van ICT zouden kunnen hebben. De aanschaffings- of voortbrengingskosten van bedrijfsmiddelen die zijn aangewezen als bedrijfsmiddelen met een hoogwaardig technologisch karakter of als bedrijfsmiddelen bestemd om gebruikt te worden bij onderzoek en ontwikkeling, zouden voor de toepassing van de inkomsten- en vennootschapsbelasting onder bepaalde voorwaarden willekeurig kunnen worden afgeschreven. Tot op heden zijn er echter geen bedrijfsmiddelen als zodanig aangewezen, vanwege de als bezwaarlijk ervaren voorwaarden die vanuit de Europese Commissie zijn opgesteld. Daarmee is deze faciliteit, die in potentie ook het gebruik van ICT zou kunnen stimuleren, vooralsnog feitelijk buiten gebruik.[275] Een vorm van willekeurige afschrijving die wat betreft regelgeving wel is geïmplementeerd en die zou kunnen bijdragen aan het stimuleren van ICT-toepassingen, is de willekeurige afschrijving voor aangewezen bedrijfsmiddelen die in het belang zijn van de bevordering van de economische ontwikkeling of de economische structuur. In dit verband is met name de willekeurige afschrijving van immateriële activa van belang. Hierbij kan bijvoorbeeld worden gedacht aan programmatuur, *knowhow* en weblocaties. Het gaat daarbij om immateriële activa in het kader van de verwerving van een onderneming (of een gedeelte daarvan) die voordien buiten Nederland werd gedreven. De aanschaffingskosten van de bedrijfsmiddelen mogen per verwerving niet meer dan € 4.537.000 bedragen.
(2) *Fiscale stimulans scholingsinspanning*. Hoewel deze regeling niet alleen op het stimuleren van ICT-toepassingen is gericht, zou van deze stimulans wel een positief effect op het gebruik van ICT kunnen uitgaan. Indien in een kalenderjaar kosten en lasten van scholing van in de onderneming werkzame personen bij een ondernemer in aftrek komen bij het bepalen van de winst over dat jaar, dan kan een bepaald bedrag aanvullend ten laste van de winst over dat jaar worden gebracht (scholingsaftrek). Als uitgangspunt geldt dat de scholingsaftrek 20% van de desbetreffende kosten en lasten bedraagt. Er zijn echter daarbovenop ook nog toeslagen mogelijk. Als bedrag aan scholingsaftrek wordt ten hoogste € 2.390.000 in aanmerking genomen. Voor de *non-profit*sector geldt een vergelijkbare afdrachtvermindering loonheffing.
(3) *Belastingvrije computers voor werknemers*. Onder bepaalde voorwaarden kunnen een computer en bijbehorende apparatuur voor de loonbelasting onbelast aan de werknemer worden verstrekt of de kosten hiervan onbelast worden vergoed. Voorwaarde is dat de apparatuur voor de dienstbetrekking wordt gebruikt. Bijbehorende apparatuur is apparatuur die bestemd is om aan de computer te worden gekoppeld om informatie uit te wisselen. Voorbeelden hiervan zijn een modem, een printer, een fax, een *docking station* (een apparaat dat wordt geplaatst tussen een draagbare computer en een bureauset) en een digitale fotocamera. Per drie kalenderjaren mag in totaal niet meer dan € 2.269 inclusief omzetbelasting belastingvrij worden vergoed. Naar verluidt zal het nieuw te vormen kabinet voorstellen doen om deze faciliteit af te schaffen.[276]
(4) *Gedeeltelijke vrijstelling loonbelasting bij verstrekking en ter beschikkingstelling van telewerkruimte*. De inrichting van een werkruimte die wordt verstrekt of ter beschikking wordt gesteld, behoort bij zakelijk gebruik niet tot het loon wanneer aan bepaalde voorwaarden is voldaan. Één van de voorwaarden is dat de werknemer ten minste eenmaal per week gedurende de gebruikelijke werktijd, zonder dat ook naar een arbeidsplaats buiten de woning wordt gereisd, voor de vervulling van zijn dienstbetrekking in de werkruimte met behulp van telematica werkt. Per vijf kalenderjaren mag niet meer dan € 1.815 inclusief BTW onbelast worden verstrekt of ter beschikking wordt gesteld.

---

[275] Zie de brief van de Minister van Economische Zaken van 8 december 2000, TK 2000-2001, 27 400-XIII, nr. 43, V-N 2001/4.16.
[276] Zie *NRC Handelsblad* 25 juni 2002, p. 2.

(5) *Belastingvrije Internetaansluitingen*. Als een werknemer een Internetaansluiting via de kabel of via ADSL ter behoorlijke vervulling van de dienstbetrekking gebruikt, kunnen onder voorwaarden de kosten die aan dat zakelijke gebruik verbonden zijn, voor de loonbelasting onbelast worden vergoed of verstrekt. Deze regeling geldt ook voor het vaste bedrag aan gesprekskosten van een Internetaansluiting via ADSL. Het providerdeel bij ADSL kan onbelast worden vergoed of verstrekt bij zakelijk gebruik van meer dan 10%.
(6) *Belastingvrije telefoons*. Vergoedingen en verstrekkingen voor een telefoon kunnen voor de loonbelasting geheel of gedeeltelijk vrijgesteld zijn. Er gelden verschillende regelingen voor een telefoonabonnement met meer dan één aansluiting of nummer, voor tweede en volgende abonnementen, voor de (mobiele) telefoon van de werknemer en voor de tweede en volgende (mobiele) telefoon die voor 90% of meer wordt gebruikt voor de dienstbetrekking. Er zijn verschillende regelingen voor abonnementen en voor abonnementen en gesprekskosten samen.

4.3. Canada

4.3.1 Directe belastingen

Canada volgt als lid van de OESO het beleid van deze organisatie.

4.3.2 Verbruiksbelastingen

Canada zoekt blijkens een in november 2001 uitgebrachte studie aansluiting bij de uitgangspunten van de OESO.[277] Digitale diensten die worden verleend aan Canadese consumenten dienen te worden belast in Canada. Niet in Canada gevestigde ondernemingen die dergelijke diensten verrichten zullen zich moeten registreren in Canada en zullen tevens de belasting aan de Canadese fiscus moeten afdragen. Indien niet in Canada gevestigde ondernemingen digitale prestaties verrichten aan Canadese bedrijven, vindt een verleggingsregeling toepassing. Dit houdt in dat de Canadese afnemer in plaats van de leverancier van de dienst de belasting verschuldigd wordt en dient af te dragen.

4.3.3 Fiscale stimulering van ICT-toepassingen

De Canadese regering wil een fiscaal klimaat scheppen dat ondernemingen helpt bij het ontplooien van e-handelactiviteiten. De Canadese regering neemt een terughoudende positie in voor wat betreft de introductie van nieuw beleid en nieuwe belastingen. Deze opstelling wordt met name ook gevoed door de gedachten dat e-handel niet door nieuwe regels mag worden belemmerd en dat ondernemingen door middel van een wereldwijde samenwerking moeten worden ondersteund.[278] Voorzover bekend zijn er overigens geen bijzondere belastingmaatregelen te melden.[279]

4.4. Duitsland

4.4.1 Directe belastingen

De Duitse fiscus volgt de OESO in zijn beleid. De Oberfinanzdirektion Karlsruhe had door middel van een mededeling laten weten dat in afwachting van een nadere standpuntbepaling binnen de OESO als voorlopig standpunt zou worden ingenomen dat een enkele server niet als een vaste inrichting voor de toepassing van een belastingverdrag zou kwalificeren, omdat er sprake zou zijn van een hulpwerkzaamheid of een werkzaamheid van voorbereidende aard.[280] Inmiddels is er in Duitsland jurisprudentie waarin het tegenovergestelde is beslist. Het gaat om een uitspraak van het Finanzgericht Schleswig-Holstein van 6 september 2001,[281] waartegen beroep in cassatie is ingesteld bij het Bundesfinanzhof. Voorzover ons bekend is deze rechterlijke

---

[277] Zie <http://www.ccra-adrc.gc.ca/tax/technical/discussion-e.pdf>.
[278] Report of the Minister's Advisory Committee on Electronic Commerce – Summary of General Recommendations (1998). Zie <http://www.ccra-adrc.gc.ca/tax/business/ecomm/ecomsue2-e.html>, Bijgewerkt: 2002-01-16.
[279] Zie <www.fin.gc.ca> en International Tax Review E-commerce 2001, nr. 4, p. 114-121.
[280] Mededeling 11-11998, S 1301 A – St 332.
[281] I R 86/01, *Entscheidungen Finanzgericht* 2001/1535.

uitspraak de eerste jurisprudentie inzake de kwalificatie van een enkele server als vaste inrichting. Het ging om een in Zwitserland geplaatste enkele server waarvan een in Duitsland gevestigde GmbH de eigenaar was. De server stond in Zwitserland in een gehuurd gebouw en werd gebruikt voor het op elektronische verzoek van Zwitserse klanten tegen betaling verstrekken van informatie. Die informatie werd door een groepsmaatschappij aan de GmbH geleverd. De GmbH zette deze informatie op haar Zwitserse server. Vervolgens werd op elektronisch verzoek de informatie aan de Zwitserse klanten tegen betaling elektronisch geleverd. Er waren in Zwitserland geen mensen actief die aan de GmbH konden worden toegerekend. Het elektronisch verstrekken van informatie werd als de kernactiviteit van de GmbH aangemerkt. Dientengevolge kon één van de uitzonderingen op de algemene vaste-inrichtingsdefinitie van het verdrag Duitsland-Zwitserland, dat op dit punt vergelijkbaar is met het OESO-modelverdrag, niet worden ingeroepen, aldus het Finanzgericht. De enkele server werd als een vaste inrichting aangemerkt. Over de winsttoerekening aan de vaste inrichting bestond tussen de partijen geen verschil van mening. Er werd een combinatie toegepast van ondernemings- en winstsplitsing. Het Finanzgericht sloot zich daarbij aan. De kwalificatie als vaste inrichting ligt in de lijn van de door de OESO voorgestane interpretatie van het begrip vaste inrichting. Het Fianzgericht refereert in zijn uitspraak ook aan het OESO-rapport en de aanpassingen van het OESO-Commentaar.[282] De door het Finanzgericht geaccepteerde winsttoerekening lijkt niet in overeenstemming met de door de OESO geformuleerde uitgangspunten. De OESO staat namelijk een *cost-plus*-benadering voor, waardoor er minder winst aan een enkele server lijkt te kunnen worden toegerekend dan in de door het Finanzgericht geaccepteerde toerekeningsmethode. Naar het arrest van het Bundesfinanzhof wordt met meer dan gewone belangstelling uitgekeken, niet alleen voor de kwalificatie van de enkele server als vaste inrichting, maar ook voor de methode van winsttoerekening. Van deze jurisprudentie kan een grote gidswerking worden verwacht.

4.4.2 Verbruiksbelastingen

Duitsland moet als lidstaat van de EU de Richtlijn inzake BTW en e-handel uiterlijk op 1 juli 2003 in haar wetgeving hebben geïmplementeerd. Het is thans nog niet duidelijk of Duitsland de niet-limitatieve lijst van digitale producten zal uitbreiden.

Duitsland dient verder de factuurvereisten uit de Richtlijn elektronisch factureren net als de overige lidstaten uiterlijk 1 januari 2004 in de nationale wet- en regelgeving te hebben geïmplementeerd.

4.4.3 Fiscale stimulering van ICT-toepassingen

Voorzover bekend zijn er op federaal niveau geen bijzondere belastingmaatregelen te melden.[283]

4.5. Frankrijk

4.5.1 Directe belastingen

Ook Frankrijk volgt de OESO. Over de vraag of aan een vaste inrichting in Frankrijk de eis van menselijke interventie kleeft, bestaat onduidelijkheid. De Franse regering heeft in een publicatie voorafgaande aan het OESO-rapport het standpunt ingenomen dat menselijke interventie inderdaad een vereiste voor het aannemen van een vaste inrichting is.[284] Vooralsnog heeft Frankrijk in de OESO geen voorbehoud tot uitdrukking gebracht. In het kader van de actualisering 2002 van het OESO-Commentaar zal de positie van de Franse fiscus duidelijk dienen te worden.

---

[282] Het Finanzgericht refereert in zijn uitspraak ook aan de zogenaamde Pipeline case (Bundesfianzhof 30 oktober 1996, II R 12/92, BSt.Bl. II 1997, 12) die de internationale discussie over de kwalificatie van een enkele server als een vaste inrichting zeer heeft gedomineerd. In deze zaak werd een in Duitsland gelegen pijpleiding van een in Nederland gevestigde BV ook als een vaste inrichting aangemerkt zonder dat daarvoor aan de BV toerekenbare menselijke arbeid in Duitsland was vereist.

[283] Zie <www.bundesfinanzministerium.de> en Baker & McKenzie 2001, p. 100.

[284] Zie Rep. Min. No. 15728 and 17729 to Mr Olivier de Chazeaux, *JO AN Q* 26 oktober 1998, p. 5849 en 5850 en Baker & McKenzie 2001, p. 70-74.

4.5.2 Verbruiksbelastingen

Frankrijk zal als lidstaat van de EU de Richtlijn inzake BTW en e-handel uiterlijk op 1 juli 2003 in haar wetgeving moeten hebben geïmplementeerd. Het is thans nog niet duidelijk of Frankrijk de niet-limitatieve lijst van digitale producten zal uitbreiden.

Frankrijk dient verder de factuurvereisten uit de Richtlijn elektronisch factureren net als de overige lidstaten uiterlijk 1 januari 2004 in nationale wet- en regelgeving te hebben geïmplementeerd.

4.5.3 Fiscale stimulering van ICT-toepassingen

Voorzover bekend zijn er geen bijzondere belastingmaatregelen te melden.[285]

4.6. Japan

4.6.1 Directe belastingen

Japan volgt voorzover bekend de beleidslijnen van de OESO.

4.6.2 Verbruiksbelastingen

Door de Japanse overheid wordt thans geen duidelijke richting gegeven aan de wijze waarop digitale prestaties voor de Japanse omzetbelasting moeten worden behandeld. De algemene Japanse omzetbelastingregels zijn van toepassing op transacties via het Internet, of het nu om goederen of diensten gaat. In het kader van de ontwikkelingen in de IT heeft het Japanse Ministerie van Financiën in februari 2001 wel een rondetafelconferentie gehouden met vertegenwoordigers van de OESO, het bedrijfsleven en de wetenschap.[286] Van de zijde van het Japanse Ministerie van Financiën is aangegeven dat Japan in navolging van de bevindingen van de OESO voor wat betreft digitale prestaties op weg is naar een de heffing van een verbruiks- of consumptiebelasting in het land van consumptie van de prestatie. Benadrukt werd dat de dialoog over Internet en verbruiksbelasting in internationaal verband moet worden gecontinueerd.

4.6.3 Fiscale stimulering van ICT-toepassingen

In het kader van het stimuleren van investeringen heeft Japan een aantal fiscale maatregelen genomen.
(1) Het midden- en kleinbedrijf kon in het jaar van verwerving tot 31 maart 2002 terzake van investeringen in machines en bepaalde installaties een extra afschrijving van 30% of een belastingkorting van 7% in aanmerking nemen.
(2) Ter bevordering van het technologische fundament van het midden- en kleinbedrijf wordt tot het einde van het belastingjaar dat aanvangt op 31 maart 2002 een extra belastingkorting van 10% voor onderzoek en ontwikkeling verstrekt.
(3) De in aanmerking te nemen levensduur van computers is verlaagd van zes jaar naar vier jaar voor PC's en naar vijf jaar voor andere computers. Hierbij zij wel opgemerkt dat de volledige aftrek van de aanschaffingskosten in het jaar van aanschaffing voor bepaalde communicatie- en informatiegerelateerde uitrusting is ingetrokken.
(4) Voor uitrusting die wordt gebruikt in het kader van hogesnelheidscommunicatienetwerken (bijvoorbeeld DSL, FWA, en WDA) is er in het eerste jaar een bijzondere afschrijving mogelijk.[287]

4.7. Verenigd Koninkrijk

4.7.1 Directe belastingen

---

[285] Zie <www.minefi.gouv.fr > en Baker & McKenzie 2001, p. 68-90.
[286] Zie <http://www.mof.go.jp/english/tax/it01.htm>.
[287] Zie <http://www.mof.go.jp/english/tax/tax.htm>.

Het Verenigd Koninkrijk lijkt te volharden in zijn standpunt dat een enkele server geen vaste inrichting kan vormen.[288] Daarmee wijkt het duidelijk af van de positie van de OESO en haar lidstaten. Wellicht moet het standpunt worden gezien tegen de achtergrond van de ambitie van het Verenigd Koninkrijk om zichzelf te profileren als de beste plaats om elektronisch handel te drijven. Terwijl een enkele server in het Verenigd Koninkrijk niet tot belastingheffing zal leiden, zou de woonstaat van de betrokken ondernemer juist wel tot een vaste inrichting kunnen concluderen. Voor de daaraan toe te rekenen winst zou de woonstaat van de ondernemer dan voorkoming van dubbele belasting kunnen verlenen. In een verrekeningsstelsel ter voorkoming van dubbele belasting zal in de woonstaat effectief geen voorkoming worden gegeven, omdat er in het Verenigd Koninkrijk geen belasting wordt geheven en er derhalve geen belasting is om te verrekenen. Indien de woonstaat echter een vrijstelling of een belastingvrijstelling als methode ter voorkoming van dubbele belasting hanteert, dan zal voor de winst toerekenbaar aan de enkele server in het Verenigd Koninkrijk wel effectief voorkoming van dubbele belasting worden gegeven. Bijvoorbeeld, Duitsland past onder verdragen terzake van vaste-inrichtingswinst in het algemeen een vrijstelling toe, terwijl Nederland in de regel een belastingvrijstelling hanteert. In een dergelijk geval kan het derhalve interessant zijn voor een in Nederland gevestigde ondernemer om zijn e-business via een in het Verenigd Koninkrijk aanwezige server te doen en niet via een in Nederland geplaatste server: geen heffing in Verenigd Koninkrijk, wel belastingvrijstelling in Nederland. Hetzelfde geldt mutatis mutandis voor een in Duitsland gevestigde ondernemer. Het hangt dan van de omvang van de aan de enkele server toe te rekenen vaste-inrichtingswinst af of het te behalen belastingvoordeel substantieel is. Nederland gaat van een *cost-plus*-benadering uit. In Duitsland is door het Finanzgericht Schlesswig-Holstein een combinatie van ondernemings- en winstsplitsing geaccepteerd (zie par. 4.4.1), waardoor waarschijnlijk meer winst aan een enkele server kan worden toegerekend dan bij de Nederlandse benadering. Zoals hierboven aangegeven vindt over de toe te rekenen winst de internationale discussie nog in volle hevigheid plaats, zodat daarover nog geen duidelijkheid bestaat.

4.7.2 Verbruiksbelastingen

Als lidstaat van de EU dient het Verenigd Koninkrijk de Richtlijn inzake BTW en e-handel uiterlijk op 1 juli 2003 in haar wetgeving te hebben geïmplementeerd.

Het is thans nog niet duidelijk of het Verenigd Koninkrijk de niet-limitatieve lijst van digitale producten zal uitbreiden. Het Verenigd Koninkrijk had overigens voorgesteld om net als in de Verenigde Staten een belastingmoratorium in te stellen op digitale diensten.
Het Verenigd Koninkrijk dient verder de factuurvereisten uit de Richtlijn elektronisch factureren net als de overige lidstaten uiterlijk 1 januari 2004 in nationale wet- en regelgeving te hebben geïmplementeerd.

4.7.3 Fiscale stimulering van ICT-toepassingen

Het Verenigd Koninkrijk gaat ervan uit dat de ICT ongekende kansen voor de modernisering van de gehele economie geeft. Rond 2002 wil het Verenigd Koninkrijk het beste land voor e-handel zijn. In het kader van het realiseren van die doelstelling is als gevolg van het *Budget 2000* een 100%-afschrijving in het eerste jaar (*first year (capital) allowance*) ingevoerd voor investeringen in ICT door het kleinbedrijf. De regeling zou in eerste instantie tot 2003 lopen. Normaal gesproken heeft het midden- en kleinbedrijf een aanspraak op een *first year allowance* van 40% voor investeringen in machines en bedrijven.[289] De Britse Treasury heeft aangegeven dat het bij voortduring maatregelen in overweging zal nemen om ervoor te zorgen dat het Britse bedrijfsleven concurrerend kan blijven en dat het volledig gebruik kan maken van de kansen die e-handel biedt.[290] In dit kader vallen waarschijnlijk ook de recente voorstellen te plaatsen. Onlangs is namelijk aangekondigd dat er een nieuwe belastingkorting wordt ingevoerd voor

---

[288] Dit standpunt was reeds door de Inland Revenue door middel van een persbericht van 11 april 2000 (84/2000) bekendgemaakt.
[289] Zie <http://www.hm-treasury.gov.uk/consultations_and_legislation/financebill2000/consult_finance_clause70a_2000.cfm>.
[290] *HM Treasury e-business strategy*, oktober 2000.

onderzoeks- en ontwikkelingsactiviteiten van grote bedrijven. Een dergelijke belastingkorting is er ook voor het kleinbedrijf. Verder is de looptijd van de 100%-*first year allowance* voor investeringen door het midden- en kleinbedrijf in ICT-uitrusting in de tijd onbeperkt geworden.[291]

4.8. Verenigde Staten

4.8.1 Directe belastingen

De Verenigde Staten is een van de leiders en opiniemakers in de internationale discussie en binnen de OESO. Dit klinkt ook door in de OESO-rapporten. Niettemin kan de vraag worden gesteld of in het concept van "trade or business" dat in de Amerikaanse nationale wetgeving wordt gehanteerd in plaats van het vaste-inrichtingsconcept wel geheel past op de interpretatie van het begrip vaste inrichting zoals dat door de OESO wordt voorgesteld. In het kader van "trade or business" lijkt een menselijke activiteit een constitutief vereiste te zijn,[292] terwijl dit voor het begrip vaste inrichting niet (meer) door de OESO wordt onderschreven. Dit zou kunnen betekenen dat een aan de Verenigde Staten op grond van een belastingverdrag toegewezen heffingsrecht terzake van een enkele server op grond van de Amerikaanse nationale wet mogelijk niet zou kunnen worden gerealiseerd. In dit verband zij verwezen naar de opmerkingen gemaakt in par. 4.7.1. Overigens zij opgemerkt dat in de Amerikaanse jurisprudentie aanwijzingen zijn te vinden dat voor de Amerikaanse interpretatie van het begrip vaste inrichting een menselijke activiteit ook een constitutief vereiste vormt.[293] In dat geval kan de interpretatie als voorgestaan door de OESO in de Verenigde Staten niet worden gerealiseerd.

4.8.2 Verbruiksbelastingen

De Verenigde Staten hebben in 1997 een driejarig belastingmoratorium afgekondigd op belastingen op Internet door middel van de Internet Tax Freedom Act. Er worden geen federale belastingen geheven ten aanzien van Internet. Op 28 november 2001 is de Internet Tax Freedom Act met twee jaar verlengd. Op federaal niveau kennen de Verenigde Staten geen indirecte belasting vergelijkbaar met de Europese BTW. Op het niveau van de individuele staten zijn er wel staten die een *Sales and Use Tax* heffen. *Sales Tax* treft de verkoop van goederen in een staat, terwijl *Use Tax* het gebruik van goederen in de staat treft wanneer de goederen zijn geleverd door een ondernemer van buiten de staat. De *Sales Tax* en *Use Tax* zijn als het ware complementair. De *Sales and Use Tax* ziet op de levering van goederen en meestal niet op diensten. Voorzover goederen worden verkocht via het Internet kan een staat *Sales and Use Tax* heffen op dezelfde wijze als dit wordt gedaan voor de levering van goederen via de reguliere kanalen. Ten aanzien van de levering van goederen aan afnemers in een bepaalde staat door ondernemers die niet in die staat gevestigd zijn, is *Use Tax* verschuldigd. Deze *Use Tax* dient evenwel door de koper zelf te worden afgedragen. Dit gebeurt bij aankopen via het Internet in de praktijk vrijwel nimmer. Uit hoofde van de *Internet Tax Freedom Act* is het verboden voor de federale regering en de staten om een nieuwe *Sales and Use Tax* voor digitale prestaties in te stellen. In het licht van deze keuze voor belastingvrijheid op Internetdiensten zijn de bezwaren van de Verenigde Staten tegen de Europese richtlijn inzake BTW en e-handel niet onbegrijpelijk. Als gevolg van deze richtlijn zullen in de Verenigde Staten gevestigde aanbieders van elektronisch geleverde diensten aan in de EU-lidstaten woonachtige consumenten (B2C) BTW in rekening moeten gaan brengen, terwijl men dat op dit moment niet hoeft te doen. Aan de andere kant dienen op dit moment de in de EU-lidstaten gevestigde ondernemers wel BTW in rekening te brengen terzake van elektronisch geleverde diensten aan in de Verenigde Staten woonachtige consumenten (B2C). Na implementatie van de nieuwe richtlijn zal op deze diensten geen BTW meer drukken. Hierdoor verdwijnt een concurrentievoordeel voor de in de Verenigde Staten gevestigde aanbieders op

---

[291] Zie *Speech by the Chancellor of the Exchequer, Gordon Brown Mp, at the Tgwu Conference – Manufacturing Matters, Press release* 30/02, 28 maart 2002.

[292] Zie *Flint v. Stone Tracy Co.* 220 U.S. 107 (1911).

[293] Zie *Consolidated Premium Iron Ores, Ltd v Commissioner*, 28 TC 127, 151 (1957), *affd*, 265 F2d 320 (6th Cir 1959). Zie ook bijvoorbeeld *Inez de Amodio*, 34 TC 894 (1960), *affd*, 299 F2d 623 (3d Cir. 1962).

zowel hun thuismarkt als de Europese afzetmarkt, waardoor ook voor in Nederland gevestigde aanbieders meer een *level playing field* ontstaat.

4.8.3 Fiscale stimulering van ICT-toepassingen

Voorzover bekend zijn er op federaal niveau geen bijzondere belastingmaatregelen te melden.[294]

4.9. Zweden

4.9.1 Directe belastingen

De lijn die Zweden volgt wijkt voorzover bekend niet af van de door de OESO uitgezette lijnen.

4.9.2 Verbruiksbelastingen

Zweden moet als lidstaat van de EU de Richtlijn inzake BTW en e-handel uiterlijk op 1 juli 2003 in haar wetgeving hebben geïmplementeerd. Het is thans nog niet duidelijk of Zweden de niet-limitatieve lijst van digitale producten zal uitbreiden.

Zweden dient verder de factuurvereisten uit de Richtlijn elektronisch factureren net als de overige lidstaten uiterlijk 1 januari 2004 in nationale wet- en regelgeving te hebben geïmplementeerd.

4.9.3 Fiscale stimulering van ICT-toepassingen

Uitgangspunt is dat de belastingregelgeving helder dient te zijn en de ontwikkeling van e-handel niet onnodig mag belemmeren, terwijl het verlies van belastingopbrengsten dient te worden voorkomen.[295] Met ingang van 2001 is er belastingvermindering voor natuurlijke personen en rechtspersonen ingevoerd. Voor kosten van bepaalde telecommunicatie- en datacommunicatieverbindingen kan voor de jaren 2001-2002 een belastingvermindering worden gekregen. De belastingvermindering bedraagt 50% van bepaalde kosten voorzover zij een bedrag van SEK 8.000 overschrijden met een maximum van SEK 5.000. Verder loopt er een studie naar het wegnemen van onnodige hindernissen in de belastingwetgeving voor e-handel. [296]

4.10. Samenvatting

Op het terrein van de directe belastingen en e-handel zet de OESO de toon. Die rol is na 2000 alleen maar toegenomen. De opvattingen van de OESO lijken in het algemeen te stroken met de Nederlandse opvattingen. Dit geldt ook voor Canada, Japan en Zweden. Dit kan niet met zoveel woorden worden gezegd voor Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten. De verschillen in belastingheffing kunnen tot concurrentieverstoringen leiden. De meest uitgesproken van de OESO afwijkende positie wordt door het Verenigd Koninkrijk ingenomen met het standpunt dat een enkele server (*stand-alone server*) geen vaste inrichting kan vormen. Hierdoor kan het Verenigd Koninkrijk een aantrekkelijker land voor de plaatsing van een enkele server zijn dan Nederland, omdat deze in het Verenigd Koninkrijk geen aanknopingspunt voor belastingheffing kan vormen, terwijl dit in Nederland wel het geval is. Aan de andere kant kan Nederland door het verschil in winsttoerekening aan een enkele servers weer aantrekkelijker zijn dan, bijvoorbeeld, Duitsland.

Op het gebied van de verbruiksbelastingen (BTW) is de speelruimte van Nederland erg beperkt. Nederland is gebonden aan de beslissingen die op Europees niveau worden genomen. Dit geldt ook voor Duitsland, Frankrijk, het Verenigd Koninkrijk en Zweden. De nieuwe richtlijn inzake BTW en e-handel raakt enkel aan de B2C-transacties (naar verluidt ongeveer 10% van de markt). Het belang van de richtlijn moet dan ook niet overschat worden. De positie van Canada verschilt niet wezenlijk van de positie binnen de EU na implementatie van de nieuwe richtlijn. De positie

---

[294] Zie <www.ustreas.gov>.

[295] Regeringskansliet, *A coordinated policy for the development of electronic commerce*, The Ministry of Industry, Employment and Communications, 16 februari 2001.

[296] Ministry of Industry, Employment and Communications, *Follow-up of Swedish Government IT Policy*, 21 februari 2002.

van Japan is vooralsnog niet duidelijk maar neigt tot belastingheffing in het land van consumptie. Dit is ook in lijn met de uitgangspunten van de EU en derhalve ook van Nederland. De nieuwe Europese richtlijn heeft wel tot gevolg dat er met name vanuit de Verenigde Staten druk op de EU wordt uitgeoefend om de richtlijn te wijzigen omdat Amerikaanse ondernemers een concurrentievoordeel gaan verliezen. Door implementatie van de richtlijn wordt de concurrentiepositie van de in de EU gevestigde aanbieders van elektronisch geleverde diensten, en derhalve ook van in Nederland gevestigde aanbieders, ten opzichte van de Amerikaanse aanbieders versterkt doordat meer een *level playing field* wordt gecreëerd.

Wat betreft de fiscale stimulering van ICT-toepassingen voert Nederland een actief beleid. Dat kan niet worden gezegd van Canada, Duitsland, Frankrijk en de Verenigde Staten. Daarentegen kennen Japan, het Verenigd Koninkrijk en Zweden op dit terrein wel fiscale stimuleringsmaatregelen. De fiscale stimuleringsmaatregelen in Zweden zijn ten opzichte van Nederland zeer beperkt te noemen. De fiscale maatregelen in Japan en Verenigd Koninkrijk zijn daarentegen aanzienlijk omvangrijker dan in Zweden. De afschrijvingen en belastingkortingen kunnen concurreren met de Nederlandse regelingen. Opgemerkt zij dat sommige Japanse maatregelen slechts een zeer beperkte looptijd hebben. Met name de recente uitbreidingen van de fiscale stimuleringmaatregelen in het Verenigd Koninkrijk versterken diens positie. Deze versterking past in de ambitie van het Verenigd Koninkrijk om het beste land voor e-handel te zijn. Voor de positie van Nederland ten opzichte van de andere landen geldt dat met name de ontwikkelingen in het Verenigd Koninkrijk in de gaten dienen te worden gehouden.

5. Vergroten van vertrouwen

5.1. Elektronische handtekeningen

De beveiliging van elektronische transacties is een essentiële voorwaarde voor het vertrouwen van consumenten en bedrijven in elektronische handel. Naast bescherming van de vertrouwelijkheid van berichten (vgl. par. 5.4) is vooral de bescherming van de authenticiteit en integriteit van berichten van belang. Elektronische vormen van authenticatie kunnen een soortgelijk vertrouwen scheppen in de veiligheid van e-handel als de traditionele handtekening op papier bewerkstelligde. De vraag is echter of elektronische authenticatie wel rechtsgeldig is: wat is de juridische bewijsstatus van een elektronische handtekening? In veel rechtsgebieden worden vormvereisten gesteld voor rechtshandelingen: ze moeten bijvoorbeeld op schrift staan of (traditioneel) zijn ondertekend. Dergelijke vormvereisten kunnen dan ook belemmerend werken voor e-handel. In deze paragraaf staat de vraag centraal welke juridische status elektronische handtekeningen hebben.[297]

5.1.1. Internationaal

Bij de UNCITRAL bestaan twee belangrijke initiatieven op het gebied van de elektronische handtekening. Ten eerste de in 1996 aangenomen en 1998 gewijzigde Modelwet betreffende elektronische handel. Deze Modelwet bepaalt dat in gevallen waarin de wet een handtekening vereist, hieraan bij elektronische communicatie kan worden voldaan door middel van: (a) een methode die de ondertekenaar identificeert en uitdrukking geeft aan diens instemming met de informatie in het document, en (b) een methode die voldoende betrouwbaar is in het licht van het doel waarvoor het elektronische bericht is gegenereerd (artikel 7). De onder (b) verwoorde aanpak wordt aangeduid als de functionele benadering en beoogt de juridische gelijkstelling tussen de traditionele handtekening en e-handtekening op een techniek-neutrale wijze op te lossen.
Het tweede initiatief is de in 2001 aangenomen Modelwet betreffende elektronische handtekeningen. Deze Modelwet beoogt aanvullende rechtszekerheid te bieden op het gebied van de e-handtekening. De modelwet neemt artikel 7 van de Modelwet betreffende elektronische handel tot uitgangspunt en borduurt aldus voort op de functionele benadering. Daarnaast geeft deze Modelwet richtlijnen ten aanzien van de verplichtingen en aansprakelijkheid van de verschillende betrokkenen (ondertekenaar, vertrouwende partij en certificatieaanbieder) bij het e-handtekeningproces.

In de Europese Unie is in 1999 Richtlijn 1999/93/EG betreffende elektronische handtekeningen aangenomen. Deze richtlijn is thans in bijna alle lidstaten van de Europese Unie geïmplementeerd. De richtlijn is gebaseerd op een tweesporenbenadering. Enerzijds mogen e-handtekeningen geen juridische status worden ontzegd op grond van onder meer de overweging dat ze in elektronische vorm zijn geschied. Anderzijds worden bepaalde, aan specifieke (betrouwbaarheids)eisen voldoende, e-handtekeningen geheel met de handmatige handtekening gelijkgesteld. In het laatste geval wordt gesproken van gekwalificeerde handtekeningen. De vereisten worden in de richtlijn verder uiteengezet. Met de gekozen benadering beoogt de Europese wetgever meer rechtszekerheid te bieden en tegelijkertijd de weg naar ontwikkelingen op e-handtekeninggebied open te laten.

5.1.2. Nederland

Begin juni 2002 was het wetsvoorstel 27 743 nog in parlementaire behandeling, dat Richtlijn 1999/93/EG in de Europese Unie beoogt te implementeren. Naast een vrij letterlijke weergave

---

[297] Deze paragraaf is gebaseerd op Van der Hof 2002, waarin alle bronnen voor deze paragraaf zijn te vinden. Zie ook Aalberts & Van der Hof 1999 en Van der Hof 2001 over de regulering van elektronische handtekeningen.

van de richtlijn bevat het wetsvoorstel tevens een op artikel 7 van de UNCITRAL-Modelwet betreffende elektronische handel gebaseerde bepaling. Dit beoogt zeker te stellen dat andere dan de technieken dan die als gekwalificeerde e-handtekening zijn te beschouwen eveneens uitdrukkelijke juridische erkenning genieten.

5.1.3. Canada

Federaal niveau
In januari 2001 is de *Personal Information Protection and Electronic Documents Act* in werking getreden. Deze wet zal slechts van toepassing zijn op specifiek aangewezen wettelijke bepalingen, maar tot op heden zijn er – voorzover bekend – geen aanwijzingen geweest.

Statelijk niveau
In september 1999 hebben de *Uniform Law Conference of Canada* en het Ministerie van Justitie de *Uniform Electronic Commerce Act* (UECA) aangenomen. De wet is gebaseerd op de functionele benadering zoals voorgesteld door de UNCITRAL-*Model Law on Electronic Commerce* en is vergelijkbaar met de *Uniform Electronic Transactions Act* in de Verenigde Staten (zie par. 5.1.8). De wet zorgt – uitzonderingen in enkele gevallen daargelaten – voor de juridische erkenning van elektronische documenten en elektronische handtekeningen. Ook bevat de wet regels voor bewaring van elektronische bestanden en staat het gebruik van e-documenten en e-handtekeningen in communicatie tussen burgers en overheid toe. Tot slot geeft de wet de vereisten voor rechtsgeldig contracteren door middel van e-bestanden en e-handtekeningen. UECA is al in verschillende staten van Canada geïmplementeerd.[298]

5.1.4. Duitsland

In Duitsland zijn in het kader van de elektronische handtekening twee wetgevingsinitiatieven relevant. In 1997 is in Duitsland wetgeving over de digitale handtekening afgekondigd. Deze wet is als gevolg van de implementatie van Richtlijn 1999/93/EG betreffende elektronische handtekening per mei 2001 vervangen door het *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*.[299] Verdere uitwerking van de wet heeft door middel van een verordening plaatsgevonden, de *Verordnung zur elektronischen Signatur*.[300]

Naast het zogeheten *Signaturgesetz* is in 2001 tevens het *Gesetz zur Anpassung von Formvorschriften im Privatrecht und anderer Vorschriften an den Modernen Geschäftsverkehr* in werking getreden. Het doel van deze wet is aanpassing van de in het privaatrecht voorkomende vormvoorschriften aan de eisen die het elektronische rechtsverkeer stelt. Daartoe worden twee nieuwe vormen in het privaatrecht geïntroduceerd, te weten de elektronische vorm en de *Textform*. De elektronische vorm die is voorzien van de gekwalificeerde e-handtekening ofwel een e-handtekening die voldoet aan de eisen van het *Signaturgesetz 2001*, is gelijkgesteld aan het getekende geschrift. Bij de *Textform* is geen (gekwalificeerde) elektronische handtekening vereist. Wel moet er sprake zijn van een duurzame weergave van een leesbare elektronische verklaring, die voorzien is van de naam van de verklarende en afgesloten is hetzij door nabootsing van de handtekening van de verklarende hetzij op andere wijze.
In het procesrecht kan in plaats van een geschrift eveneens de elektronische vorm worden gebruikt onder voorwaarde dat het e-document geschikt is voor verwerking door het gerecht. Voorts wordt in het bewijsrecht voorzien in een verlichting van de bewijslast ten aanzien van de elektronische vorm. Tenzij ernstige twijfel bestaat over de overeenstemming van de in elektronische vorm afgegeven verklaring met de wil van de sleutelhouder, wordt aangenomen deze verklaring authentiek is (*Anscheinsbeweis*).

---

[298] Zie <http://www.e-commercecanada.net/Archives/Sept26/table/body_table.html> voor een (licht verouderd) overzicht van e-handtekeningbepalingen op statelijk niveau.
[299] *BGBl* Teil I, Nr. 22,
<http://www.bmwi.de/Homepage/download/infogesellschaft/Signaturgesetz.pdf>.
[300] *BGBl* Teil I, S. 3074, <http://www.internetrecht-info.de/rechtsn/sigv.pdf>.

5.1.5. Frankrijk

In april 2001 is in Frankrijk wetgeving (nr. 2000-230 van 13 maart 2000) betreffende het gebruik van elektronische handtekeningen en elektronische documenten als bewijs in werking getreden, waarmee richtlijn 1999/93/EG is geïmplementeerd in het Franse recht. De voorwaarden voor betrouwbaarheid van elektronische handtekeningen zijn verder uitgewerkt in een decreet (nr. 2001-272 van 31 maart 2001). Hierin worden enkele voorschriften omtrent de betrouwbaarheid van gekwalificeerde elektronische handtekeningen gegeven.[301]

5.1.6. Japan

In april 2001 is in Japan wetgeving betreffende elektronische handtekeningen en certificatiediensten in werking getreden. De wetgeving is in het bijzonder gericht op de digitalehandtekeningtechnologie (dat wil zeggen, op asymmetrische encryptie gebaseerde elektronische handtekeningen).

5.1.7. Verenigd Koninkrijk

In maart 2002 traden de *Electronic Signatures Regulations* in werking. De *Regulations* implementeren bepalingen uit richtlijn 1999/93/EG betreffende elektronische handtekeningen die betrekking hebben op onder meer het toezicht op certificatieaanbieders (CA's), aansprakelijkheid van CA's en de bescherming van persoonsgegevens. De juridische erkenning van e-handtekeningen wordt bestreken door §7 van de in mei 2000 in werking getreden *Electronic Communications Act 2000*.[302]

5.1.8. Verenigde Staten

Federaal niveau
In oktober 2000 werd de *Electronic Signatures in Global and National Commerce Act* (E-Sign) van kracht. De wet volgt de functionele benadering zoals voorgesteld in de UNCITRAL-*Model Law on Electronic Commerce*. Voor wat betreft *business-to-consumer*-contracten is het in beginsel vereist dat de consument instemt met elektronisch getekende contracten en het ontvangen van e-bestanden via het Internet. E-Sign ontkracht statelijke wetgeving op het gebied van e-handtekeningen, met uitzondering van de hierna te behandelen UETA. E-sign is echter beperkt tot interstatelijke en internationale transacties en is alleen toepasselijk buiten gevallen die worden bestreken door de *Uniform Commercial Code* (UCC).
De *E-Sign Act* draagt de overheid ook op om het gebruik van elektronische handtekeningen, ook internationaal, te stimuleren.

De *E-government Act of 2001* die op 1 mei 2001 in de senaat is voorgesteld (S. 803),[303] bepaalt in paragraaf 202 dat elk overheidsorgaan (*executive agency*) moet waarborgen dat diens methoden voor gebruik en acceptatie van elektronische handtekeningen overeenstemmen met de procedures en standaarden van de directeur van het *Office of Management and Budget*.

Statelijk niveau
De *National Conference of Commissioners on Uniform State Laws* heeft in de *Uniform Electronic Transactions Act* (UETA) en de *Uniform Computer Information Transactions Act* (UCITA) bepalingen met betrekking tot e-handtekeningen opgenomen. Daarbij is de functionele benadering zoals gepropageerd door de UNCITRAL-*Model Law on Electronic Commerce* gevolgd. Beide modelwetten zijn of worden momenteel in verschillende staten geïmplementeerd.

---

[301] Zie uitgebreider Menais 2001.
[302] <http://www.hmso.gov.uk/acts/acts2000/20000007.htm>.
[303] <http://www.cdt.org/legislation/107th/e-gov/s803.pdf>.

5.1.9. Zweden

In januari 2001 is de wet betreffende gekwalificeerde e-handtekeningen in werking getreden.[304] Deze wet implementeert richtlijn 1999/93/EG betreffende e-handtekeningen. De gelijkstelling van gekwalificeerde elektronische handtekeningen met traditionele handtekeningen bij vormvereisten is vastgelegd in art. 17; voor communicatie met de overheid kunnen evenwel aanvullende voorwaarden worden gesteld.
De bijbehorende verordening[305] bepaalt dat de post- en telecomautoriteit (Post- och telestyrelsen) de toezichthouder is.

5.1.10. Samenvatting

Alle onderzochte landen hebben inmiddels wetgeving op het gebied van e-handtekeningen afgekondigd. Inhoudelijk kan de wetgeving verschillen, in het bijzonder ten aanzien van de vereisten die aan de e-handtekeningtechniek worden gesteld. In sommige landen – Duitsland en Japan – zijn deze strenger en voornamelijk gericht op de digitalehandtekeningtechniek. Andere landen – Verenigde Staten en Canada – hebben een open en functionele benadering gekozen, op grond waarvan in beginsel – eventueel afhankelijk van het doel waarvoor de e-handtekening wordt gebruikt – iedere techniek voor e-ondertekenen kan worden toegepast. Een tussenvorm is richtlijn 1999/93/EG betreffende e-handtekeningen, die de open benadering voor e-handtekening in algemene zin koppelt aan een striktere benadering voor gekwalificeerde e-handtekening. Onder deze laatste valt voornamelijk de digitalehandtekeningtechniek.
Nederland volgt in het implementatiewetsvoorstel tamelijk letterlijk de bepalingen van voornoemde richtlijn, maar heeft omwille van de technologieonafhankelijkheid tevens een open bepaling toegevoegd. Dit is niet verrassend, aangezien de Nederlandse wetgever steeds een duidelijke voorkeur voor een open en functionele benadering in de geest van de UNCITRAL-*Model Law on Electronic Commerce* heeft gehad.
Ondanks de harmonisatie die met Richtlijn 1999/93/EG wordt beoogd, blijven er binnen de Europese Unie nochtans verschillen op het gebied van de regulering van elektronische handtekeningen bestaan.

---

[304] Lag (2000:832) om kvalificerade elektroniska signaturer (Wet op de gekwalificeerde elektronische handtekeningen), <http://www.notisum.se/rnp/SLS/LAG/20000832.HTM>, beschikbaar in het Engels op <http://rechten.kub.nl/simone/QESA.pdf>.
[305] Förordning (2000:833) om kvalificerade elektroniska signaturer (Verordening op de gekwalificeerde elektronische handtekeningen), <http://www.notisum.se/rnp/sls/lag/20000833.htm>.

5.2. Elektronisch betalen

Naast de juridische status van e-handtekeningen is ook de juridische status van elektronische betaalinstrumenten van belang voor het elektronisch rechtsverkeer. Er bestaan tal van e-betaalwijzen, die deels zijn gebaseerd op 'betaling op afstand' (bijvoorbeeld kredietkaarten of pinpassen) en deels zijn gebaseerd op een elektronische variant van contant geld (zoals e-cash). Dergelijke betaalwijzen zullen alleen worden geaccepteerd indien ze zijn ingekaderd in de financiële regelgeving, waarbij met name het toezicht op uitgevers van dergelijke instrumenten van groot belang is. In deze paragraaf staat de juridische status van elektronisch geld centraal. Daarnaast zullen ook elektronische financiële diensten aan bod komen.

5.2.1. Internationaal

De belangrijkste internationale initiatieven op het gebied van elektronisch betalen zijn de volgende.

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[306]

Om de markt voor de uitgifte van elektronisch geld open te breken, wordt in de richtlijn een nieuw type kredietinstelling ingevoerd. Dit is de instelling voor elektronisch geld, die naast de reeds bestaande en uit verschillende richtlijnen en wetten, zoals de Wet Toezicht Kredietwezen, bekende 'traditionele' kredietinstellingen komt te staan. Voor dit type instelling moet volgens de richtlijn een gericht toezichtregime gaan gelden dat in vergelijking met het toezichtregime voor traditionele kredietinstellingen enerzijds minder streng is ten aanzien van zaken als aanvangskapitaal, terwijl het aan de andere kant de werkzaamheden en de beleggingsmogelijkheden van instellingen voor elektronisch geld beperkt (Overwegingen 11 en 12 en artikelen 4 en 5). Verder is ook opgenomen dat in principe uitgevers uitgegeven elektronisch geld weer moeten omwisselen in gewoon geld en dat ontheffing van toepassing van de richtlijn in bepaalde gevallen mogelijk is. De richtlijn had uiterlijk 27 april 2002 in de lidstaten geïmplementeerd moeten zijn.

Door diverse critici, waaronder het Britse Ministerie van Financiën, is opgemerkt dat indien de definitie van elektronisch geld uit de richtlijn letterlijk wordt genomen, systemen waarbij meer elektronische waarde aan consumenten wordt gegeven dan zij in traditioneel geld aanbieden, niet onder het bereik van de richtlijn vallen.[307] Immers, bij systemen waarbij consumenten voor bijvoorbeeld € 25 een digitale tegenwaarde van € 30 krijgen, is volgens de definitie in de richtlijn geen sprake van elektronisch geld. Aangezien in dergelijke systemen de digitale euro zwakker is dan de contante of girale euro, worden zij in het vervolg geïnflateerde systemen genoemd. Na de definitie van elektronisch geld in artikel 1 van de richtlijn, is in artikel 3 een bepaling opgenomen die voorschrijft dat uitgevers van elektronisch geld uitgegeven waarde op verzoek van gebruikers in principe ook weer moeten omruilen voor traditioneel geld, en wel in een één-op-één-verhouding. De gedachte achter deze bepaling was dat de toepasselijkheid ervan met zich zou brengen dat geïnflateerde systemen op economische gronden geen realiteit zouden worden. Echter, genoemde omwisselbepaling geldt alleen voor systemen die onder de definitie van elektronisch geld vallen. Aangezien geïnflateerde systemen niet onder die definitie vallen, geldt hiervoor ook geen omwisselplicht.[308] De geschetste situatie is des te interessanter omdat de Europese Centrale Bank geïntervenieerd heeft, juist om de invoering van geïnflateerde systemen te voorkomen. Ook volgens het Britse Ministerie van Financiën is een ongecontroleerde uitgave van monetaire waarde ongewenst en het Ministerie spreekt daarom van een 'loophole' in de Europese richtlijn.[309] Kennelijk vonden de regelgevers het, gezien de moeilijke politieke discussie

---

[306] *PbEG* L 275, 27.10.2000, p. 39-43.

[307] Zie HM Treasury 2001, p. 4-5, punten 13-15 en Lelieveldt 2001.

[308] Lelieveldt 2001.

[309] HM Treasury 2001, p. 5, punten 14-15.

omtrent de totstandkoming van de richtlijn, beter om deze 'constructiefout' in de richtlijn te laten zitten, met als gevolg dat mogelijke problemen die eruit voortvloeien in de nationale wetgeving van de verschillende lidstaten gladgestreken moeten worden.[310]

Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verkoop op afstand van financiële diensten aan consumenten en tot wijziging van de richtlijnen 90/619/EEG van de Raad en 97/7/EG en 98/27/EG
De bedoeling is dat deze richtlijn zaken op het gebied van consumentenbescherming met betrekking tot de verkoop op afstand van financiële diensten gaat regelen. Voorgesteld wordt aan aanbieders van dergelijke diensten bepaalde informatieverplichtingen op te leggen, zoals adresinformatie, beschrijving van de dienst, etc. In bepaalde gevallen moet een consument ook een bedenkperiode krijgen waarin hij een aankoop ongedaan kan maken.
Het voorstel is momenteel in afwachting van de tweede lezing door de Raad.

Van voor 2000, maar van algemeen belang voor het gebruik van elektronische betaalinstrumenten is *Aanbeveling 97/489/EG van de Commissie van 30 juli 1997 betreffende transacties die met een elektronisch betaalinstrument worden verricht, in het bijzonder inzake de betrekking tussen uitgever en houder*.[311] In deze aanbeveling worden zaken als verplichtingen en aansprakelijkheid voor zowel uitgevers als houders geregeld. Voor uitgevers houden de verplichtingen onder andere in dat de contractvoorwaarden op tijd bij de consument bekend moeten zijn, terwijl consumenten hun persoonlijke codes, zoals PIN-codes, geheim moeten houden.[312] Deze aanbeveling wordt in de toekomst waarschijnlijk omgezet in een richtlijn.[313]

5.2.2. Nederland

Op het moment is bij het parlement een wetsvoorstel in behandeling ter implementatie van richtlijn 2000/46/EG. Dit wetsvoorstel is inmiddels in gewijzigde vorm, aan de Eerste Kamer voorgelegd.[314] Het voorstel moet leiden tot aanpassing van de Wet Toezicht Kredietwezen, maar net als het oorspronkelijke voorstel van januari 2002,[315] wijkt ook het gewijzigde voorstel van wet op een aantal punten waarschijnlijk ten onrechte af van de bepalingen in de richtlijn. Waar de richtlijn in artikel 1, lid 3 sub b onder andere bepaalt dat elektronisch geld een monetaire waarde is vertegenwoordigd door een vordering op de uitgevende instelling, welke is uitgegeven in ruil voor ontvangen geld dat ten minste dezelfde waarde vertegenwoordigt als de uitgegeven monetaire waarde, wordt in het wetsvoorstel gesproken van een geldswaarde en bepaald dat het door een kredietinstelling uitgegeven elektronisch geld een waarde vertegenwoordigt die ten minste gelijk is aan de waarde van de voor de uitgifte ontvangen gelden. Deze laatste bepaling is vrijwel het tegenovergestelde van wat in de richtlijn staat. Bovendien is een geldswaarde niet noodzakelijkerwijs hetzelfde als een monetaire waarde.[316]

Van juli 1999 zijn de beleidsregels media WTK 1992 van De Nederlandsche Bank. Deze beleidsregels zijn uitgevaardigd aangezien bij personen, ondernemingen en instellingen die via het Internet, andere elektronische media of via papieren media activiteiten ondernemen die onder een van de verbodsbepalingen van de Wet Toezicht Kredietwezen 1992 kunnen vallen, onduidelijkheid kan bestaan over de mate van toepasselijkheid van deze wet op de genoemde bancaire activiteiten. In de regels worden indicatoren aangereikt om te beoordelen of een

---

[310] Zie hierover nader Schudelaro 2002, waarop deze bespreking mede is gebaseerd, alsmede Lelieveldt 2001.
[311] *PbEG* L 208, 2.8.1997, p. 52-58.
[312] Voor toepassing van de aanbeveling in de lidstaten zie <http://www.europa.eu.int/comm/internal_market/en/finances/payment/instrument/reports.htm>.
[313] *A possible legal framework for the single payment area in the internal market*, MARKT/208/2001-Rev. 1 van 26 april 2002.
[314] TK 2001-2002, 28189, nr. 8.
[315] TK 2001-2002, 28189, nrs. 1-2; Memorie van Toelichting TK 2001-2002, 28189, nr. 3.
[316] Schudelaro 2002.

bepaalde activiteit op Nederland is gericht. Een voorbeeld van zo'n indicator is het gebruik van Nederlands als voertaal bij de activiteiten.[317]

5.2.3. Canada

Er is thans geen verbod op de uitgifte van elektronisch geld door niet-financiële instellingen. Toestemming kan noodzakelijk zijn voor een gereguleerde financiële instelling om een dochteronderneming op te zetten die elektronisch geld gaat uitgeven. Tot nu toe hebben alleen gereguleerde financiële instellingen die ook deposito's aannemen elektronisch geld uitgegeven. Momenteel heeft de Bank of Canada geen plannen om zelf elektronisch geld uit te gaan geven.[318]

5.2.4. Duitsland

Voorzover nu na te gaan, is richtlijn 2000/46/EG nog niet volledig in het *Kredietwesengesetz* geïmplementeerd. Zaken als aanvangskapitaal, eigen vermogen, wederzijdse erkenning en terugbetaalbaarheid moeten nog geregeld worden. Hiertoe is op 18 januari 2002 een wetsvoorstel ingediend.[319] In dit wetsvoorstel, het *Viertes Finanzförderungsgesetz*, zijn naast de veranderingen vanwege elektronisch geld ook veranderingen opgenomen met betrekking tot beursrecht, waardepapierenrecht, investeringsrecht, verzekeringsrecht en hypotheekbankrecht. In tegenstelling tot het Nederlandse wetsvoorstel ter implementatie van richtlijn 2000/46/EG staat in het Duitse voorstel geen relatie waaraan de waardes van uitgegeven elektronisch geld en in ruil daarvoor ontvangen geld moeten voldoen. Wat deze relatie betreft wordt elektronisch geld gedefinieerd als waarde-eenheden in de vorm van een vordering op de uitgevende instelling die tegen in ontvangstname van een geldbedrag worden uitgegeven.[320]

5.2.5. Frankrijk

Met betrekking tot elektronisch geld is geen specifieke wet- of regelgeving van kracht. De wetgever is van mening dat het bestaande rechtskader de nieuwe ontwikkelingen volledig omvat. Alleen kredietinstellingen mogen elektronisch geld uitgeven.[321] Dit zou aangepast kunnen worden wanneer Frankrijk richtlijn 2000/46/EG implementeert, maar daartoe is nog geen wetsvoorstel verschenen.

5.2.6. Japan

Er is weinig recente informatie over Japan aangetroffen over dit onderwerp. In het CPSS-rapport uit november 2001 wordt slechts een aantal beleidsrapporten uit 1997 en 1998 vermeld.[322] De *Law on Sales of Financial Products* van 2001, die verplichtingen oplegt aan financiële instellingen voor onder andere informatievoorziening, geldt voor alle financiëledienstaanbieders maar is niet in het bijzonder gericht op elektronische financiële dienstverlening.[323] De Japan Bankers Association heeft echter wel in april 2000 richtlijnen gepubliceerd voor banktransacties via het Internet, die onder andere betrekking hebben op identificatie, beveiliging, informatievoorziening, de inrichting van de webstek (inclusief koppelingen) en reclame.[324]

5.2.7. Verenigd Koninkrijk

Ook in het Verenigd Koninkrijk wordt gewerkt aan implementatie van richtlijn 2000/46/EG. Dit heeft geleid tot publicatie van twee consultatiedocumenten in oktober en december 2001 door het Britse Ministerie van Financiën en de Financial Services Authority respectievelijk.[325] In maart

---

[317] Zie voor de beleidsregels 1999: <http://www.dnb.nl/toezicht/pdf/3210.pdf>.
[318] Committee on Payment and Settlement Systems, 2001, p. 16.
[319] <http://www.uni-leipzig.de/bankinstitut/dokumente/2002-01-18-01.pdf>.
[320] <http://www.uni-leipzig.de/bankinstitut/dokumente/2002-01-18-01.pdf>, p. 41.
[321] Committee on Payment and Settlement Systems, 2001, p. 31.
[322] Committee on Payment and Settlement Systems 2001, p. 48
[323] Beschikbaar op <http://www.fsa.go.jp/topics/law_e/law_002.pdf>.
[324] Baker & McKenzie 2000, p. 6.
[325] HM Treasury 2001, FSA 2001.

en april van dit jaar zijn hierop *response*documenten gepubliceerd.[326] In het laatste document heeft de Financial Services Authority haar regels omtrent de uitgifte van elektronisch geld bekend gemaakt. Wat betreft de relatie tussen de waarde van uitgegeven elektronisch geld en van het in ruil daarvoor ontvangen traditionele geld, wordt in de Britse implementatie slechts opgemerkt dat elektronisch geld wordt uitgegeven in ruil voor de ontvangst van geld ('funds'). Dit lijkt op de Duitse aanpak, maar verschilt van nogal van de afwijkende Nederlandse aanpak.

De vraag of het aanbieden van financiële diensten via Internet onder Britse wetgeving valt, wordt behandeld in de *Financial Services and Markets Act 2000*.[327] Voor de inwerkingtreding van deze wet was het zo dat in principe elke aanbieding die via het Internet in het Verenigd Koninkrijk geraadpleegd kon worden, ook onder Britse wetgeving viel. Hoewel in theorie allesomvattend, werd in de praktijk gekeken of de Britse consumentenbescherming in het geding was. Hierbij werd gebruik gemaakt van verschillende indicatoren. Voorbeeld hiervan zijn de vragen of een weblocatie in het Verenigd Koninkrijk is gevestigd en in hoeverre Britten van een aanbieding gebruik kunnen maken.[328]

5.2.8. Verenigde Staten

Op 3 augustus 2000 is door de National Conference of Commissioners on Uniform State Laws (NCCUSL) de *Uniform Money Services Act* aangenomen.[329] De modelwet heeft betrekking op *Money Services Businesses*, niet-bancaire instellingen die geen deposito's aannemen of leningen verstrekken. In plaats daarvan verschaffen zij alternatieve betaalmechanismen. Een activiteit van *Money Services Businesses* is de uitgifte van 'stored-value'-kaarten. Internetbetaalsystemen vallen onder de wet zolang het de verkoop en uitgifte betreft van monetaire waarde (nieuw gedefinieerd als 'een ruilmiddel al dan niet terugbetaalbaar in geld') of het overmaken van monetaire waarde door een niet-bancaire instelling. In het laatste geval moet de instelling het geld van de klant voor eigen rekening bewaren.[330] *Money Services Businesses* moeten geregistreerd worden en voldoen aan bepaalde veiligheids- en betrouwbaarheidsvereisten. Opvallend verschil tussen de Verenigde Staten en Europa is dat in de Verenigde Staten elektronisch geld niet als een aparte klasse behandeld wordt, maar als een van de vele alternatieve betalingsmethoden. Dit heeft tot gevolg dat de *Uniform Money Services Act* niet alleen regelgeving over elektronisch geld harmoniseert, maar ook die voor andere alternatieve betaalmethoden. Bovendien schijnt de wet minder streng te zijn dan de Europese richtlijn.[331] Zo is in de wet geen terugbetaalverplichting voor uitgevers opgenomen. Het ziet ernaar uit dat in de Verenigde Staten bij regelgeving de nadruk eerder ligt op transacties dan op instellingen.[332]

Ook in de Verenigde Staten bestaan er regels om vast te stellen of een financiële dienst die via Internet wordt aangeboden van buiten de Verenigde Staten op de Verenigde Staten gericht is. Hierbij wordt onder andere gekeken of er vrijwaringclausules op een weblocatie zijn die aangeven dat een aanbod niet op de Verenigde Staten gericht is en of een aanbieder bijvoorbeeld de adressen van klanten controleert om te voorkomen dat toch aan iemand in de Verenigde Staten geleverd wordt.[333]

5.2.9. Zweden

Zweden heeft richtlijn 2000/46/EG geïmplementeerd bij wet van 4 april 2002, de *Lag (2002:149) om utgivning av elektroniska pengar* (Wet op de uitgifte van elektronisch geld).[334] De wet geeft geen voorschrift voor een relatie waaraan de waardes van uitgegeven elektronisch geld en in ruil

---

[326] HM Treasury 2002, FSA 2002.
[327] <http://www.fsa.gov.uk/fsma>.
[328] Le Goueff 2001, p. 26-27.
[329] <http://www.law.upenn.edu/bll/ulc/moneyserv/UMSA2001Final.htm>.
[330] Taft 2000.
[331] Krueger 2001, p. 19.
[332] Böhle & Krueger 2001.
[333] Le Goueff 2001, p. 27-28.
[334] Beschikbaar via <http://.194.52.125.3>.

daarvoor ontvangen geld moeten voldoen. Elektronisch geld wordt gedefinieerd als een waarde in de vorm van een vordering op de uitgevende instelling, die opgeslagen is op een elektronisch medium, en die als betaalmiddel te gebruiken is bij andere instellingen dan de uitgevende instelling (art. 2). De Finansinspektionen oefent het toezicht uit.

5.2.10. Samenvatting

Op het gebied van elektronisch betalen is momenteel in Europa de belangrijkste ontwikkeling de implementatie van de Richtlijn instellingen voor elektronisch geld. De richtlijn kent een constructiefout in het voorkomen van geïnflateerde systemen voor elektronisch geld (een instelling die onder de richtlijn valt mag niet meer waarde aan e-geld uitgeven dan zij aan gewoon geld krijgt, maar een instelling die dat laatste doet valt per definitie niet onder de richtlijn); deze fout moet door de lidstaten rechtgezet worden. Duitsland, het Verenigd Koninkrijk en Zweden doen dit op een vergelijkbare manier, maar Nederland lijkt uit de pas te lopen door een afwijkende implementatie van de richtlijn. Terwijl de richtlijn beoogt om geïnflateerde systemen te voorkomen (een instelling mag niet meer waarde (maar wel minder) aan e-geld uitgeven dan zij in ruil hiervoor aan contanten of giraal geld ontvangt), kiest Nederland in het wetsvoorstel voor een consumentenbeschermende richting (een instelling mag niet minder (maar wel meer) waarde aan e-geld uitgeven dan zij in ruil hiervoor aan contanten of giraal geld ontvangt).
De Verenigde Staten hebben bij de regulering van elektronisch geld een andere aanpak gekozen dan de Europese Unie. In plaats van elektronisch geld als een aparte categorie van betaalsystemen te behandelen, is een aanpak gekozen waarbij elektronisch geld op dezelfde wijze behandeld wordt als andere alternatieve betaalmethoden. Dit leidt ertoe dat een groter gebied van betaalsystemen door de Amerikaanse wetgeving wordt geharmoniseerd. Bovendien lijken de Verenigde Staten zich meer te concentreren op transacties dan op het type instelling dat met deze transacties gemoeid is.
Op het gebied van financiële diensten is vooral van belang het Europese voorstel voor een Richtlijn verkoop op afstand van financiële diensten. Deze richtlijn beoogt consumentenbescherming bij verkoop op afstand van dergelijke diensten te regelen (vergelijkbaar met de Richtlijn verkoop op afstand voor verkoop van producten).

5.3. Trusted Third Parties (TTP's)

Een Trusted Third Party (TTP) is een vertrouwde onafhankelijke partij die diensten aanbiedt die de betrouwbaarheid van elektronische gegevensuitwisseling en gegevensopslag vergroten. Zij helpen de integriteit en authenticiteit, vertrouwelijkheid en beschikbaarheid van gegevens te waarborgen. Het eerste is vooralsnog de belangrijkste toepassing: de huidige TTP's beperken zich hoofdzakelijk tot het faciliteren van authenticiteit van berichten, met name door certificaten uit te geven die de band van een ondertekenaar met zijn publieke cryptografische sleutel waarborgen (zie par. 5.1 over digitale handtekeningen). Deze TTP's heten certificatie-aanbieders (Certification Authorities, CA's) of certificatiedienstverleners (Certification Service Providers, CSP's). Andersoortige TTP's kunnen versleuteling voor vertrouwelijkheid van gegevens faciliteren, waarbij de aanbieder sleutels genereert of in bewaring kan houden, of ten behoeve van bewijs en bewaring documenten bijvoorbeeld tijdstempelen of authenticeren.

De infrastructuur van certificatiedienstverleners wordt vaak aangeduid met de term *Public Key Infrastructure* (PKI). Veel landen zijn momenteel bezig om voor de overheid een dergelijke PKI op te zetten teneinde de interne (en uiteindelijk ook de externe) communicatie te beveiligen.

5.3.1. Internationaal

De UNCITRAL heeft in 2001 de Modelwet betreffende elektronische handtekeningen aangenomen (zie par. 5.1.1), die landen als uitgangspunt kunnen gebruiken bij het reguleren van elektronische handtekeningen. In deze modelwet zijn de verplichtingen (art. 9 lid 1) en aansprakelijkheid (art. 9 lid 2) van CSP's opgenomen. Artikel 10 bevat enkele indicatoren die van invloed zijn op het oordeel over de benodigde betrouwbaarheid van CSP's.

De Europese richtlijn elektronische handtekeningen[335] bevat ook uitgebreide bepalingen voor CSP's. Gekwalificeerde elektronische handtekeningen (die gelijkgesteld worden met traditionele handtekeningen) kunnen alleen worden geplaatst met een gekwalificeerd certificaat uitgegeven door een CSP die voldoet aan de voorwaarden van bijlage II bij de richtlijn. Anders dan in de UNCITRAL-modelwet zijn gekwalificeerde CSP's volgens de richtlijn verplicht een herroepingdienst (*revocation service*) aan te bieden, waardoor personen kunnen nagaan of een certificaat nog geldig en ongeschonden is. Voor niet-gekwalificeerde CSP's (die dus geen gekwalificeerde handtekeningen kunnen faciliteren) gelden minder specifieke eisen; de richtlijn bepaalt dat voor dergelijke CSP's geen eis mag worden gesteld van voorafgaande autorisatie. Voor wat betreft de aansprakelijkheid bepaalt de richtlijn dat op CSP's in beginsel het gewone, nationale aansprakelijkheidsrecht van toepassing is (overweging 22). In artikel 6 van de richtlijn wordt een aparte aansprakelijkheidsregel geformuleerd voor aanbieders van gekwalificeerde certificaten: voor hen geldt een omkering van de bewijslast ten aanzien van de (on)zorgvuldigheid waarmee zij gehandeld hebben.

Er zijn geen internationale regelingen bekend voor andersoortige TTP's dan CSP's.

5.3.2. Nederland

De Nederlandse overheid heeft in 1999 de notitie *Nationaal TTP-project* uitgebracht, waarin randvoorwaarden zijn opgenomen voor TTP's. Als uitvloeisel hiervan is de projectgroep TTP.NL opgezet binnen ECP.NL, een vorm van zelfregulering.[336] Inmiddels heeft deze projectgroep een schema en criteria voor TTP's vastgesteld; in juni 2002 is voorts een richtsnoer (Guidance) voor interpretatie van de criteria uitgebracht.[337] TTP's die aan het schema voldoen,

---

[335] Richtlijn 1999/93/EG, zie par. 5.1.1.

[336] TK 1998-1999, 26581, nr. 1, resp. <http://www.ecp.nl/taakgebied/vertrouwen/ttp.html>. Zie hierover uitgebreider Landwell 2000, p. 103-105.

[337] Zie *TTP.NL Certification in the area of electronic signatures* (juni 2001) en *Guidance on ETSI TS 101 456* (30 mei 2002) beschikbaar op <http://www.ecp.nl/publicatie/pub.html>.

kunnen een keurmerk aanvragen bij een Certificerende Instantie, dat wordt beheerd door ECP.NL. Hiermee wordt vormgegeven aan de mogelijkheid van de Richtlijn elektronische handtekeningen een vrijwillig systeem op te zetten voor certificatie van TTP's. De eisen van dit keurmerk zijn overigens een uitwerking van de eisen uit de bijlagen bij de richtlijn, zodat TTP's die het keurmerk verkrijgen gekwalificeerde certificaten kunnen uitgeven. Voor wat betreft dit keurmerk is vermeldenswaard dat TTP.NL met de keurmerkinstantie van het VK (tScheme) overlegt over wederzijdse erkenning van de keurmerken.[338]

Het toezicht op TTP's die gekwalificeerde certificaten uitgeven wordt ondergebracht bij de OPTA.[339] Dergelijke TTP's hebben een registratieplicht. Dit wordt geregeld in het wetsvoorstel van 18 mei 2001 ter implementatie van de richtlijn, dat begin juni 2002 nog bij de Eerste Kamer lag. Daarin wordt de regulering van certificatiedienstverleners ondergebracht in de Telecommunicatiewet; de eisen van bijlage II van de richtlijn worden opgenomen in een AMvB. De aansprakelijkheid van certificatiedienstverleners voor gekwalificeerde certificaten wordt geregeld in voorgesteld art. 6:196b BW.

Voor vertrouwelijkheiddienstverleners is het project Rechtmatige toegang van TTP.NL van belang, zie daarover par. 5.4.2.

De overheid heeft een Taskforce Public Key Infrastructure ingesteld om een PKI voor de overheid op te zetten, die ook voor externe communicatie met de overheid zal worden gebruikt.[340] In 2001 is het voorlopig programma van eisen van PKI-diensten en -producten opgesteld, dat verder wordt uitgewerkt in aanbestedingsdocumenten. De belangrijkste aanbesteding zal de uitgifte van het basiscertificaat zijn, dat het ankerpunt is voor de PKI. De overheid beoogt in 2003 een grootschalige uitrol van de PKI te doen plaatsvinden.[341]

5.3.3. Canada

Canada heeft bij de regulering van elektronische handtekening gekozen voor een open, functionele benadering, die niet gestoeld is op de techniek van cryptografiegerelateerde handtekeningen. De *Uniform Electronic Communications Act* (zie par. 5.1.3) bevat dan ook geen bepalingen over CSP's.
De Canadese overheid acht authenticatie een belangrijk aandachtspunt voor elektronische handel. Industry Canada (een federaal overheidsdepartement) heeft in consultatie met belanghebbenden een beleidsdocument opgesteld met uitgangspunten voor dit onderwerp. Hierbij staat een marktgeoriënteerde aanpak voorop, maar dit moet met name vorm krijgen door co-regulering ("a need to develop a co-ordinated approach"). Actieve deelname van Canada in internationale fora over authenticatie-onderwerpen is gewenst; bovendien is publieke bewustwording en educatie essentieel voor het gebruik van cryptografische authenticatietechnieken in elektronische handel.[342] Het beleidsdocument treedt niet in details, en TTP's of CSP's komen er niet expliciet in aan bod.

De Canadese overheid is zeer actief met het opzetten van een PKI, mede omdat de overheid een rolmodel heeft te vervullen[343] (zie par. 2.3.3). Bij deze PKI kiest de overheid niet voor een hiërarchische opbouw, maar voor een systeem van departementale *Certification Authorities* die elkaar kruiscertificeren op basis van de *Canada Public Key Infrastructure Certificate Policies*, gefaciliteerd door de Canadian Central Facility.[344]

---

[338] Marjolijn Durinck, ECP.NL, persoonlijke mededeling 30 mei 2002.
[339] TK 2000-2001, 27 743, nr. 3, p. 9-10.
[340] TK 1999-2000, 26 387, nr. 5.
[341] TK 2001-2002, 26 387, nr. 13, p. 10.
[342] Industry Canada, Electronic Commerce Branch, *Addressing the Trust Agenda: Electronic Authentication*, februari 2001, <http://e-com.ic.gc.ca/english/authen/doc/authen_summary.pdf>, p. ii.
[343] Industry Canada, Electronic Commerce Branch, *Addressing the Trust Agenda: Electronic Authentication*, februari 2001, <http://e-com.ic.gc.ca/english/authen/doc/authen_summary.pdf>, p. 10.
[344] *Government of Canada PKI*, <http://www.cio-dpi.gc.ca/pki-icp/gocpki/gocpki_e.asp>.

5.3.4. Duitsland

Duitsland was een van de eerste landen ter wereld met wetgeving voor digitale handtekeningen. Deze wetgeving (het *Signaturgesetz*, de *Signaturverordnung* en de *Massnahmenkatalog*)[345] was geënt op digitale handtekeningen (dat wil zeggen, op cryptografie gebaseerd) en stelde vereisten voor een PKI, waarbij ook voorwaarden werden gesteld voor CSP's. Onder invloed van de Europese richtlijn Elektronische handtekeningen heeft Duitsland deze wetgeving evenwel in mei 2001 vervangen door het *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften,*[346] nader uitgewerkt in de *Verordnung zur elektronischen Signatur*[347] van november 2001 (zie par. 5.1.4). Hoofdstuk II van de wet bevat uitgebreide vereisten voor CSP's; op basis van hoofdstuk III is vrijwillige accreditatie van CSP's mogelijk. Beide punten worden nader uitgewerkt in de onderliggende verordening.

5.3.5. Frankrijk

Frankrijk kende in de jaren negentig een uitgebreide regulering van TTP's, in verband met de beperking op cryptografie (zie par. 5.4.5).[348] Deze gold primair voor TTP's die (cryptogerelateerde) vertrouwelijkheidsdiensten aanboden, maar ook deels voor authenticatie-TTP's.[349] Met de liberalisering van het cryptobeleid in 1999 werd het dwingende karakter van de regeling voor vertrouwelijkheids-TTP's opgeheven. Sinds kort zijn dergelijke TTP's wel specifiek verplicht op bevel cryptosleutels van hun klanten te overhandigen of zelf te ontsleutelen, op straffe van maximaal twee jaar gevangenisstraf (art. 31(I) Wet op de dagelijkse veiligheid[350]).

In het wetsvoorstel *Projet de loi sur la société de l'information* van 14 juni 2001 is vervolgens een andere regeling voor TTP's opgenomen. Het aanbieden van TTP-diensten is onderworpen aan een registratieplicht (art. 38), en TTP's zijn onder omstandigheden aansprakelijk (art. 39-40). Wanneer een TTP zich niet houdt aan de regels, kan de premier de circulatie van cryptografie van deze aanbieder verbieden (art. 41). Het wetsvoorstel is evenwel vervallen door de verkiezingen van 2002, zodat deze bepalingen vooralsnog niet zijn geïmplementeerd.
Wel zijn inmiddels met de wet op de elektronische handtekeningen[351] en de daarop gebaseerde verordening[352] specifieke bepalingen opgesteld voor authenticatie-TTP's, de CSP's, die sterk leunen op de Europese Richtlijn Elektronische handtekeningen.

In Frankrijk bestaan diverse initiatieven voor een PKI binnen de overheid, maar vooralsnog lijken deze gefragmenteerd te zijn en gebruik te maken van certificatiediensten uit de private sector. Er wordt wel nagedacht over het ontwikkelen van een interne PKI tussen alle ministeries, maar hiervoor zijn nog geen concrete plannen ontvouwd.[353]

---

345 <http://www.iid.de/rahmen/iukdgebt.html#a3> en <http://www.iid.de/rahmen/sigv.html>.
346 <http://www.bmwi.de/Homepage/download/infogesellschaft/Signaturgesetz.pdf>.
347 <http://www.internetrecht-info.de/rechtsn/sigv.pdf>.
348 Zie hierover Landwell 2000, p. 42, en Koops 2002.
349 De enige toegelaten vertrouwelijkheids-TTP was overigens SCSSI, het onderdeel van de Franse overheid dat verantwoordelijk was voor het cryptobeleid. Koops 2002.
350 *Loi no. 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne*, <http://www.legifrance.gouv.fr/citoyen/jorf_nor.ow?numjo=INTX0100032L>.
351 *Loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, *Journal Officiel* 62 van 14 maart 2000, p. 3968, <http://www.legifrance.gouv.fr/citoyen/jorf_nor.ow?numjo=JUSX9900020L>.
352 *Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique*, *Journal Officiel* 77 van 31 maart 2001, p. 5070, <http://www.legifrance.gouv.fr/citoyen/jorf_nor.ow?numjo=JUSC0120141D>.
353 Clarisse Girot, persoonlijke mededeling 6 juni 2002.

5.3.6. Japan

De Japanse overheid stimuleerde al vroeg het opstellen van richtlijnen voor CSP's,[354] waaronder aansprakelijkheid,[355] via het *Electronic Commerce Promotion Project*. Met de wet op de elektronische handtekeningen van 2000[356] zijn er inmiddels ook wettelijke bepalingen voor CSP's, die met name zien op accreditatie (art. 4-14). Ook in internationale afstemming van geaccrediteerde CSP's is voorzien (art. 15-16). Artikel 34 draagt de overheid op om publiekscampagnes te voeren ter bewustwording van elektronische handtekeningen en CSP-diensten.
Voor de aansprakelijkheid van CSP's gelden de normale regels van het Japanse Burgerlijk Wetboek; het Ministry of Economy, Trade and Industry (METI, voorheen MITI) heeft daarbij in een document uit mei 2002 een interpretatie gegeven hoe de algemene aansprakelijkheidsregels kunnen worden toegepast op CSP's.[357]

Japan is ook actief in het opzetten van een PKI voor de overheid, zowel een PKI voor de centrale overheid dat gebruikmaakt van het Kasumigaseki-WAN van de centrale overheden, als een PKI voor 3200 decentrale overheden dat gebruikmaakt van het Local Government WAN. De diverse ministeries krijgen elk een certificatieautoriteit, waarbij een Bridge Certification Authority zorgt voor kruiscertificering.[358]

5.3.7. Verenigd Koninkrijk

De Britse overheid heeft in de jaren negentig voorstellen gedaan voor regulering van TTP's, die zowel zou gelden voor vertrouwelijkheids- als authenticatie-TTP's. Deze stuitten echter op weerstand, met name omdat de overheid via de TTP's toegang wenste tot cryptografische sleutels van gebruikers (zie par. 5.4.7).
Vervolgens heeft de overheid in deel I van de *Electronic Communications Act 2000*[359] een uitgebreide regeling voor *Cryptographic Service Providers* getroffen, die zowel geldt voor vertrouwelijkheids- als authenticatie-TTP's (art. 6). Registratie is niet verplicht maar wordt wel gestimuleerd. De overheid gaf in de toelichting op deze wet aan dat de voorkeur uitging naar een zelfreguleringmechanisme en dat deel I niet zou worden uitgeoefend indien zo'n mechanisme zou blijken te voldoen; een dergelijk zelfreguleringmechanisme, tScheme van de Alliance for Electronic Business, werd daarbij als voorbeeld genoemd.[360] In het consultatiedocument van maart 2001 over de implementatie van de Europese richtlijn Elektronische handtekeningen geeft het Department of Trade and Industry aan: "Government has no plans therefore at present to introduce a *voluntary accreditation* scheme and notes that the conduct of the tScheme appears to fulfil the broad objectives for schemes which might be introduced by Member States in accordance with the Directive."[361] Als gevolg hiervan is deel I van de Electronic Communications Act 2000 (vooralsnog) niet in werking getreden.[362]
In de nadere implementatie van de Europese richtlijn, *The Electronic Signatures Regulations 2002* van 13 februari 2002,[363] wordt wel het toezicht op CSP's geregeld die gekwalificeerde certificaten uitgeven, waarvan ook een register wordt bijgehouden (art. 3). Artikel 4 regelt de

---

[354] Minoru Yasuda, *Certification Authority Guidelines in Japan*, 1997, <http://www.electronicmarkets.org/netacademy/publications.nsf/all_pk/92>.
[355] *Proposal for Liability of Certification Authority*, <http://www.ecom.or.jp/ecom_e/report/no7/wg05.html>.
[356] Law Concerning Electronic Signatures and Certification Services, mei 2000, <http://www.meti.go.jp/english/report/data/gesignconte.html>, inwerkingtreding 1 april 2001.
[357] *Interpretative Guidelines on Electronic Commerce (Provisional Translation)*, 28 mei 2002, <http://www.meti.go.jp/english/information/data/c0205EleCome.pdf>, p. 15-18.
[358] Zie hierover het rapport van Dialogic voor pijler E van de Internationale ICT-toets 2002.
[359] <http://www.hmso.gov.uk/acts/acts2000/20000007.htm>.
[360] *Explanatory Notes to Electronic Communications Act 2000*, punt 10, <http://www.hmso.gov.uk/acts/en/2000en07.htm>. Voor tScheme, zie <http://www.tscheme.org/>.
[361] DTI, *Consultation on EC Directive 1999/93/EC of the European Parliament and Council on a Community Framework for Electronic Signatures*, maart 2001, <http://www.dti.gov.uk/cii/ecommerce/europeanpolicy/esigncondoc.pdf>.
[362] <http://www.dti.gov.uk/cii/datasecurity/electronicsignatures/electronic_communication.shtml> (inzage 29 mei 2002).
[363] SI 2002 No. 318, <http://www.legislation.hmso.gov.uk/si/si2002/20020318.htm>.

aansprakelijkheid van CSP's voor gekwalificeerde certificaten. Het toezicht is vormgegeven door een 'light touch approach', waarbij het Department of Trade and Industry het register bijhoudt van deze CSP's en waar nodig publiciteit geeft aan opmerkingen over de prestaties van die CSP's.[364]

5.3.8. Verenigde Staten

In de jaren negentig hebben diverse beleidsinitiatieven en wetsvoorstellen voorgesteld om via een TTP-systeem het binnenlands gebruik van cryptografie te reguleren (zie par. 5.4.8), doch deze initiatieven hebben niet tot daadwerkelijke regulering geleid.

De federale *E-Sign Act* en de statelijke modelwet *Uniform Electronic Transactions Act* (UETA, zie par. 2.1.8 en 5.1.8), bevatten geen bepalingen over CSP's, aangezien ze niet geënt zijn op digitale handtekeningen en een certificatie-infrastructuur.
Wel geeft de toelichting bij de UETA aan dat registratie door een Trusted Third Party ingezet kan worden om de exclusieve beschikkingsmacht (*control*) te garanderen die noodzakelijk is bij verhandelbare elektronische documenten (*transferable records*).[365] Hetzelfde geldt voor de analoge bepaling in de *E-Sign Act*. Dergelijke TTP-systemen bestaan al voor het overdragen van waardepapieren (*securities entitlements*) onder art. 8 *Uniform Commercial Code*, aldus de toelichting bij art. 16 UETA.[366]

Voor de overheid wordt gewerkt aan het opzetten van een Public Key Infrastructure, onder de coördinatie van het Federal PKI Steering Committee.[367] Vele overheidsorganen zijn druk bezig met de uitvoering van een PKI.[368] Bij de inrichting van deze overheids-PKI is bewust afgezien van een centrale, hiërarchische structuur met één basiscertificaat, onder andere vanwege privacybezwaren[369] en de onwil van overheidsinstanties om hun PKI uit te besteden.[370] In plaats daarvan is in juni 2001 een *Federal Bridge Certification Authority* in het leven geroepen, die de interoperabiliteit van certificatie binnen de overheid moet faciliteren, waarbij overheidsinstanties hun eigen PKI kunnen opzetten.[371] De *E-government Act of 2001* die op 1 mei 2001 in de senaat is voorgesteld (S. 803)[372] bevat bepalingen ter stimulering van deze FBCA.

5.3.9. Zweden

De Zweedse overheid benadrukt in haar cryptografiebeleid (*On cryptography*, 6 mei 1999, zie par. 5.4.9)[373] dat een infrastructuur van CSP's belangrijk is voor de ontwikkeling van elektronische handel. Zweden heeft daarop snel de Europese richtlijn E-handtekeningen geïmplementeerd in een wet (inwerkingtreding januari 2001) waarin de bepalingen over CSP's voor gekwalificeerde certificaten vrijwel direct zijn overgenomen.[374] De aansprakelijkheid van deze CSP's is gereregeld in art. 14 van deze wet. De bijbehorende verordening[375] bepaalt dat de post- en telecomautoriteit (Post- och telestyrelsen) de toezichthouder op deze wet is.

---

[364] Geoff Smith, DTI, persoonlijke mededeling, 7 juni 2002.
[365] Zie de toelichting bij art. 16 UETA, <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>.
[366] <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>.
[367] <http://www.cio.gov/fpkisc/>. Zie ook de Legal & Policy Working Group hiervan, <http://www.cio.gov/fpkisc/legal-policy/index.htm>.
[368] Zie het overzicht op <http://www.cio.gov/fpkisc/evolving_fpki/index.htm>.
[369] Een centrale PKI met één elektronische identiteitskaart voor burgers zou de overheid toestaan om te veel persoonsgegevens centraal te verzamelen.
[370] Peter Alterman, 'The U.S. Federal PKI and the Federal Bridge Certification Authority', 7 mei 2001, <http://www.cio.gov/fbca/documents/altermanpaper.pdf>.
[371] <http://www.cio.gov/fbca/>.
[372] <http://www.cdt.org/legislation/107th/e-gov/s803.pdf>.
[373] Beschikbaar op <http://cryptome.org/se-crypto99.htm>.
[374] Lag (2000:832) om kvalificerade elektroniska signaturer (Wet op de gekwalificeerde elektronische handtekeningen), <http://www.notisum.se/rnp/SLS/LAG/20000832.HTM>, beschikbaar in het Engels op <http://rechten.kub.nl/simone/QESA.pdf>.
[375] Förordning (2000:833) om kvalificerade elektroniska signaturer (Verordening op de gekwalificeerde elektronische handtekeningen), <http://www.notisum.se/rnp/sls/lag/20000833.htm>.

Ook Zweden is bezig een vrijwillig accreditatieschema voor CSP's op te stellen, waarbij de Raad voor Accreditatie rechtstreeks TTP's 'accrediteert'.[376]

5.3.10. Samenvatting

'Trusted Third Parties' blijkt een verouderde term als men de internationale initiatieven en reguleringen op een rij zet. In het buitenland wordt deze term niet (meer) gebruikt; men spreekt hoofdzakelijk van cryptografische dienstaanbieders of van certificatiedienstaanbieders.
De terminologie hangt samen met een onderscheid in soorten dienstaanbieders: er zijn dienstaanbieders die vertrouwelijkheidsdiensten faciliteren (waarbij het depot van cryptosleutels een mogelijkheid is) en dienstaanbieders die authenticiteit en integriteit faciliteren.[377] Nederland staat samen met Frankrijk en het VK alleen in het geïntegreerd willen aanpakken van beide soorten aanbieders; de overige landen beperken zich tot certificatieaanbieders (CSP's). De aanpak van Nederland, Frankrijk en VK verschilt overigens nogal. Frankrijk kende van oudsher beperkingen op cryptoaanbieders en stelt weliswaar liberalisering voor, maar blijft verder gaan in regulering dan Nederland en het VK. Deze landen staan geconditioneerde zelfregulering voor: in beginsel wordt aan de markt overgelaten om een adequaat reguleringsmechanisme op te stellen voor crypto-dienstaanbieders, met eventuele nadere wetgeving op de achterhand. Deze aanpak lijkt ook in Canada te bestaan.
Voor certificatieaanbieders loopt de regulering uiteen. De EU-lidstaten hebben deze geënt op de richtlijn Elektronische handtekeningen; Nederland loopt hierbij overigens achter met de implementatie. Voor wat betreft gekwalificeerde CSP's zijn de eisen redelijk geüniformeerd conform de richtlijn; voor niet-gekwalificeerde CSP's loopt de regeling van accreditatie, certificatie en toezicht soms uiteen (waar de richtlijn ook ruimte voor biedt).
Buiten de EU heeft Japan een uitgebreide regeling voor accreditatie van CSP's, maar Canada en de VS kennen evenwel geen specifieke regulering van certificatieaanbieders, mede omdat hun elektronischehandtekeningwetgeving niet is geënt op cryptografische handtekeningen.

Diverse landen zijn bezig een *Public Key Infrastructure* op te zetten voor communicatie binnen of met de overheid. De VS en Canada lopen hiermee voorop, direct gevolgd door Nederland. De aanpak van Nederland verschilt van daarbij van die van de VS, Canada en Japan: Nederland ontwerpt een centrale, hiërarchische infrastructuur die opgehangen is aan één basiscertificaat; de VS en Canada kiezen voor een systeem van kruiscertificering door autonome overheids-certificatieaanbieders, die elkaar kruiscertificeren (Canada) of waarbij een centrale instantie als facilitator optreedt (VS, Japan).

Tot slot is vermeldenswaard dat Canada en Japan de noodzaak benadrukken van voorlichting aan het publiek om hen bewust te maken van elektronische handtekeningen en certificatieaanbieders; Japan heeft dit zelfs bij de wet aan de overheid opgedragen.

---

[376] Jacob Boersma, ECP.NL, persoonlijke mededeling 6 juni 2002.
[377] Over andersoortige TTP-diensten dan deze twee is niets aangetroffen. Overigens kunnen certificatieaanbieders ook indirect vertrouwelijkheid faciliteren, aangezien een sleutelpaar met een gecertificeere publieke sleutel ook gebruikt kan worden om gegevens te versleutelen en aldus vertrouwelijk te houden. Een certificatieaanbieder biedt evenwel als zodanig niet een vertrouwelijkheidsdienst aan.

5.4. Cryptografie

Beveiliging is essentieel voor het scheppen van vertrouwen in elektronische handel, en cryptografie – systemen die gegevens versleutelen zodat onbevoegden er geen kennis van kunnen nemen – is één van de belangrijkste technieken voor beveiliging. Daarom is het zinvol de juridische status van het gebruik van cryptografie te beschouwen.
Aangezien staten van oudsher bang waren dat cryptografie in handen zou vallen van staatsvijandige personen (zodat hun communicatie niet meer zou kunnen worden afgeluisterd), bestaan er van oudsher exportbeperkingen op cryptografie. Sinds medio jaren negentig van de twintigste eeuw zijn staten daarnaast in toenemende mate bezorgd dat het gebruik van cryptografie door misdadigers de opsporing in grote mate belemmert; daarom worden er ook juridische maatregelen overwogen of genomen die het binnenlands gebruik van cryptografie beperken. Een van de maatregelen betreft het inbouwen van een achterdeur voor de overheid, via depot van sleutels (*key escrow*) of het scheppen van een mogelijkheid de sleutel in voorkomende gevallen te achterhalen, sleutelherwinning (*key recovery*).
Beide soorten regelingen – export- en binnenlandse beperkingen – kunnen een drempel opwerpen voor elektronische handel.

5.4.1. Internationaal

Exportregulering
De export van cryptografie valt onder het Wassenaar Akkoord, een internationaal instrument dat de export van wapens en goederen voor tweeërlei gebruik (zowel voor militaire als civiele toepassingen) reguleert.[378] Cryptografie valt hieronder als goed voor tweeërlei gebruik (*dual-use good*). Het Wassenaar Akkoord is niet-bindend; lidstaten dienen de afspraken te implementeren in nationale wetgeving.
Het Wassenaar Akkoord dateert van 1995 (ter vervanging van het daarvoor geldende COCOM)[379] en is ondertekend door 33 landen. De regeling legde aanvankelijk strenge beperkingen op aan de export van cryptografie, maar deze is in december 2000 versoepeld. Cryptografie die bestemd is voor breed gebruik (*mass-market crypto*) is sindsdien vrijelijk uitvoerbaar. Voor export van de meeste andere sterke cryptografie wordt een vergunningvereiste gesteld.[380]

De Europese Unie heeft een regeling met een soortgelijke inhoud, de *Council Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology*,[381] zoals geamendeerd door regeling Nr. 458/2001 van 6 maart 2001[382] (implementatie van de wijziging in het Wassenaar Akkoord, waarbij de limiet van 64 bits voor mass-market crypto is geschrapt) en door regeling Nr. 2432/2001 van 20 november 2001, die de bijlagen bij de oude regeling vervangt.[383] In het algemeen is export binnen de Europese Unie geheel vrij (op enkele zeer specifieke uitzonderingen na), en voor export naar Australië, Canada, Tsjechië, Hongarije, Japan, Nieuw Zeeland, Noorwegen, Polen, de VS en Zwitserland kan men een *Community General Export Authorisation* (CGEA) aanvragen, die geldt voor alle EU-lidstaten. Voor export naar andere landen is meestal een nationale vergunning vereist.

Een overzicht van nationale reguleringsinstanties verantwoordelijk voor cryptografie-exportregulering is te vinden op <http://rechten.kub.nl/koops/cryptolaw/cls-addr.htm>.

---

[378] <www.wassenaar.org>.
[379] Zie Koops 2002.
[380] Zie <http://www.wassenaar.org/list/Table%20of%20Contents%20-%2099web.html>, kategorie 5, deel 2.
[381] *PbEG* 2000, L159, 30 januari 2000.
[382] *PbEG* 2001, L65/19, 7 maart 2001, beschikbaar op <http://www.dti.gov.uk/export.control/pdfs/councilregulations.pdf>.
[383] *PbEG* 2001, L 338/1, beschikbaar op <http://www.dti.gov.uk/export.control/pdfs/dual-use-regulation-1101.pdf>.

Binnenlandse regulering
Voor binnenlandse regulering bestaan weinig internationale richtlijnen of reguleringen. Alleen de OESO heeft richtlijnen opgesteld voor cryptoregulering, de Aanbeveling van de Raad over richtlijnen voor cryptografiebeleid (*Recommendation of the Council concerning Guidelines for Cryptography Policy*) van 27 maart 1997.[384] Deze zijn echter dermate algemeen dat zij weinig richtinggevend zijn; staten kunnen de richtlijnen naar believen interpreteren om cryptografiegebruik te stimuleren of juist aan banden te leggen.

5.4.2. Nederland

Exportregulering
Nederland volgt het Wassenaar Akkoord. De export van cryptografie wordt gereguleerd door de In- en uitvoerwet[385] en het daarop gebaseerde In- en uitvoerbesluit strategische goederen[386]. Vergunningen voor uitvoer worden uitgegeven door de *Afdeling Exportcontrole en Sanctiebeleid* van het Ministerie van Economische Zaken.

Binnenlandse regulering
Na een hevig omstreden wetsontwerp uit 1994 dat cryptografie sterk aan banden wilde leggen, staat Nederland op het standpunt dat gebruik van cryptografie vrij is.[387] Om de opsporingsproblemen toch tegen te gaan, heeft de Nederlandse overheid een tweesporenbeleid gevoerd.

Ten eerste bekijkt men de mogelijkheid om via TTP's (onafhankelijke instanties die de betrouwbaarheid van elektronisch verkeer verhogen, zie par. 5.3) toegang tot cryptografische sleutels te waarborgen. De Nota Nationaal TTP-project van 3 juni 1999 bevat daartoe randvoorwaarden die kunnen worden gesteld aan TTP's voor vertrouwelijkheidsdiensten. De nota laat de uitwerking hiervan in het midden. In het project Rechtmatige toegang (een onderdeel van TTP.nl, 2000-2001), waarin overheid en bedrijfsleven zitting hadden, is nader bekeken welke randvoorwaarden voor dergelijke TTP's gesteld kunnen worden. De laatste fase van het project betreft een economische effectrapportage, die momenteel (juni 2002) wordt afgerond. Deze rapportage moet de effecten bekijken van de mogelijkheden om van crypto-gerelateerde TTP's te eisen dat zij toegang hebben tot sleutels van gebruikers. Mocht het project niet het beoogde resultaat bereiken, dan kan de overheid alsnog wettelijke maatregelen treffen,[388] al valt vanwege de belangentegenstellingen en de aard van de materie niet te verwachten dat er een wettelijke regeling kan worden gevonden die tegelijk realistisch en effectief is.

Ten tweede heeft de Nederlandse overheid gekozen voor een ontsleutelplicht; dit gebeurde al bij de Wet computercriminaliteit uit 1993.[389] Deze is vooralsnog beperkt tot de situatie van een huiszoeking (art. 125k lid 2 Sv), en een ontsleutelbevel mag niet aan een verdachte worden gegeven (art. 125m lid 1 Sv). Het wetsvoorstel Computercriminaliteit II beoogt het bevel uit te breiden tot situaties na afloop van een huiszoeking (wijziging in art. 125k lid 2 Sv) en bij afgetapte telecommunicatie (voorgesteld art. 126m/t lid 5-8).[390] Een eerder voorstel in het wetsontwerp Computercriminaliteit II van januari 1998 om het bevel ook aan verdachten te kunnen geven, werd ingetrokken, wellicht vanwege heftige discussie in juridisch Nederland.[391]

---

[384] Beschikbaar op <http://www.cybercrime.gov/oeguide.htm>.
[385] *Wet van 5 juli 1962, houdende een regeling op het gebied van de invoer en de uitvoer van goederen*, laatstelijk gewijzigd bij wet van 12 februari 2001 *Stb.* 2001, 191.
[386] *Besluit van 26 april 1963, houdende regelen ten aanzien van de uitvoer van bepaalde goederen, die van strategische betekenis zijn of kunnen zijn*, laatstelijk gewijzigd in *Stct.* 2001, 249.
[387] Nota WES, TK 1997-1998, 25 880, nrs. 1-2, p. 10.
[388] De TTP-nota dreigt: "Indien het bedrijfsleven niet voldoende actief meewerkt aan de ontwikkeling van genoemd instrumentarium, zal de overheid nadrukkelijk overwegen om met nadere wetgeving de behoefte aan rechtmatige toegang in te vullen." TK 1998-1999, 26 581, nr. 1, p. 24.
[389] Stb. 1993, 33.
[390] TK 1998-1999, 26 671, nrs. 1-2.
[391] Zie daarover Koops 2000, p. 20-23.

Ook ten behoeve van nationale veiligheid kan sinds kort een ontsleutelbevel worden gegeven. De Wet op de inlichtingen- en veiligheidsdiensten 2002[392] bevat een ontsleutelplicht (art. 24 lid 3, art. 25 lid 7 Wiv), die wordt gesanctioneerd met een gevangenisstraf van maximaal zes maanden (onopzettelijk) of twee jaar (opzettelijk) (art. 89 Wiv). Van belang is voorts dat de inlichtingen- en veiligheidsdiensten de bevoegdheid hebben technische voorzieningen te plaatsen om cryptografie te omzeilen (art. 24 lid 1 Wiv); zij mogen daartoe hacken in computers van burgers en programma's installeren die heimelijk wachtwoorden "opsnuiven" en doorzenden.

5.4.3. Canada

Exportregulering
Canada volgt het Wassenaar Akkoort (zie boven).[393] Na een discussiedocument uit februari 1998, *A Cryptography Policy Framework for Electronic Commerce*, waarop de reacties overwegend een vrijer exportbeleid voorstonden, kondigde de regering op 1 oktober 1998 een nieuw cryptobeleid aan dat vooral versoepelingen in andere landen als argument hanteerde voor versoepeling van het nationale beleid. Dit is dan ook een van de uitgangspunten van het Canadese cryptobeleid.[394]

Binnenlandse regulering
Canada formuleerde een cryptobeleid op 1 oktober 1998, dat aangaf dat de overheid geen verplichte toegang tot sleutels (*key recovery* of *key escrow*) zou eisen, maar dat het bedrijfsleven wel gestimuleerd zou worden zelf dergelijke systemen te gebruiken.[395] Het sindsdien staande beleid zegt dan gebruik van cryptografie vrij is, teneinde elektronische handel te stimuleren. Om opsporingsbelemmeringen tegen te gaan, stelt Canada bepalingen voor die het gebruik van cryptografie ter bevordering van een misdrijf of om bewijs te verdonkeremanen moeten tegengaan. Bestaande medewerkingsverplichtingen worden geacht ook van toepassing te zijn in situaties waarin cryptografie wordt aangetroffen.[396]

5.4.4. Duitsland

Exportregulering
Duitsland volgt de EU-regeling, geïmplementeerd in de *Algemeine Genehmigung Nr. 16*, zoals gewijzigd bij besluit van 18 augustus 1999.[397] Bedrijven kunnen grotendeels zelf bepalen of een cryptoproduct voor de massamarkt bestemd is en derhalve een algemene vergunning voor deze cryptografie volstaat; het *Bundesausfuhramt* kan daarbij assisteren.

Binnenlandse regulering
Na een lange en gepolariseerde maatschappelijke discussie, waarin diverse voorstellen voor een sleuteldepotachtige regulering door regeringsvertegenwoordigers werden gedaan, stelde de Duitse overheid in juni 1999 een algemeen cryptobeleid vast, de *Eckpunkte der deutschen Kryptopolitik*. Het algemene uitgangspunt is dat cryptogebruik vrij is, en dat de overheid het gebruik van cryptografie voor informatiebeveiliging stimuleert. De opsporingsproblemen leidden vooralsnog niet tot regulering; de overheid legde vooral de nadruk op het versterken van de technische capaciteit van opsporings- en nationaleveiligheidsinstanties.[398]

5.4.5. Frankrijk

Exportregulering

---

[392] Stb. 2002, 148.
[393] Zie *Summary of Canada's Cryptography Policy*, <http://e-com.ic.gc.ca/english/fastfacts/43d7.html>. Zie <http://www.dfait-maeci.gc.ca/~eicb/> voor het verantwoordelijke overheidsorgaan van het Department of Foreign Affairs and International Trade.
[394] *Summary of Canada's Cryptography Policy*, <http://e-com.ic.gc.ca/english/fastfacts/43d7.html>.
[395] Koops 2002.
[396] *Summary of Canada's Cryptography Policy*, <http://e-com.ic.gc.ca/english/fastfacts/43d7.html>.
[397] <http://www.sicherheit-im-internet.de/download/ag_16.pdf>.
[398] Koops 2002.

Frankrijk heeft lange tijd cryptografie sterk aan banden gelegd, zowel voor wat betreft de import en export, als voor wat betreft de productie, handel en het gebruik. Eind jaren negentig van de vorige eeuw heeft Frankrijk echter de regulering sterk versoepeld, vooral onder invloed van de Europese Unie, waarin Frankrijk op dit vlak een eenzame positie innam.
De export wordt gereguleerd door een wet van 26 juli 1996 en de daarop gebaseerde decreten van 24 februari 1998 (*Journal Officiel* 25 februari 1998), en van 17 maart 1999 (decreet 99-200[399] en decreet 99-199[400]). Voor export van sterke cryptografie is een vergunning nodig; voor diverse andere cryptografie geldt een registratieverplichting.[401]
In januari 1999 kondigde premier Jospin een versoepeling aan, die werd opgenomen in hoofdstuk II van het wetsvoorstel *Projet de loi sur la société de l'information* van 14 juni 2001.[402] Het wetsvoorstel is evenwel vervallen door de verkiezingen van 2002, zodat deze bepalingen vooralsnog niet zijn geïmplementeerd. Vooralsnog houdt Frankrijk strengere exportregulering dan de andere EU-landen, en heeft het bovendien als enige EU-land enige mate van importregulering.

Binnenlandse regulering
De binnenlandse productie van, handel in en gebruik van cryptografie is lange tijd sterk beperkt in Frankrijk door een vergunningen- en registratiesysteem. In 1996 voerde Frankrijk de mogelijkheid in om een vergunning te krijgen wanneer men zijn cryptosleutels bij een TTP in depot gaf. In 1999 werd het binnenlands cryptobeleid evenwel aanzienlijk versoepeld door de algemene maatregelen van bestuur van 17 maart 1999 (decreet 99-200 en decreet 99-199, zie boven). Gebruik van cryptografie werd daardoor grotendeels vrij en het TTP-systeem is afgeschaft, in afwachting van een volledige liberalisering van cryptogebruik, die gestalte krijgt in het voornoemde wetsvoorstel *Projet de loi sur la société de l'information* van 14 juni 2001. Het aanbieden van cryptografie is in dat voorstel nog onderworpen aan een registratieplicht. Gebruik van cryptografie wordt volledig vrij, maar wanneer cryptografie wordt gebruikt ter bevordering van een strafbaar feit, zal de maximumstraf kunnen worden verhoogd (art. 45 van het wetsvoorstel). Bovendien bevat het wetsvoorstel diverse bepalingen over crypto-gerelateerde TTP's (zie par. 5.3.6). Nu het wetsvoorstel is vervallen door de verkiezingen van 2002, worden deze bepalingen vooralsnog niet ingevoerd.
Wel zijn inmiddels enkele bepalingen uit het wetsvoorstel versneld opgenomen in de wet 2000-1062 van 15 november 2001 over dagelijkse veiligheid *(Loi no. 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne*)[403]. De *Code d'Instruction Criminelle* is uitgebreid met een ontsleutelbevel (art. 230-1 lid 1). Bij misdrijven met een maximumgevangenisstraf van minstens twee jaar kan de politie de veiligheidsdiensten inschakelen om aangetroffen versleutelde gegevens te kraken (art. 230-1 lid 2 tot en met 230-5). Het niet voldoen aan een ontsleutelbevel is strafbaar met maximaal drie jaar gevangenisstraf, of met maximaal vijf jaar gevangenisstraf als de ontsleuteling de effecten van een strafbaar feit had kunnen voorkomen of verzachten (art. 434-15-2 *Code Criminelle*).

5.4.6. Japan

Exportregulering
Japan volgt het Wassenaar Akkoord (zie boven).[404]

Binnenlandse regulering
In een ontwerprapport van het Ministry of Trade and Industry (MITI), *Towards the Age of Digital Economy*,[405] van mei 1997, wordt ontwikkeling en gebruik van cryptografie sterk gestimuleerd; dit

[399] <http://www.internet.gouv.fr/francais/textesref/cryptodecret99200.htm>.
[400] <http://www.internet.gouv.fr/francais/textesref/cryptodecret99199.htm>.
[401] Zie het overzicht in Koops 2002.
[402] <http://www.assemblee-nationale.fr/projets/pl3143.asp>.
[403] *Journal Officiel* 16 november 2001, p. 18215.
[404] Koops 2002.
[405] <http://www.meti.go.jp/english/aboutmeti/data/a228101e.html>.

wordt bevestigd in het door MITI en diens opvolger METI geformuleerde informatiebeleid.[406] Het mogelijk gebruik van cryptografie door misdadigers of terroristen speelt traditioneel geen belangrijke rol voor de overheid.[407]

5.4.7. Verenigd Koninkrijk

Exportregulering
Export van cryptografie wordt gereguleerd in *The Dual-Use Items (Export Control) Regulations 2000*.[408] Deze regeling is overeenkomstig het Wassenaar Akkoord en de EU-regulering.

Binnenlandse regulering
In het VK is lang gediscussieerd over binnenlandse cryptoregulering, waarbij de overheid lange tijd het verplichten van *key escrow* of *key recovery* leek voor te staan. Een consultatiedocument *Licensing of Trusted Third Parties for the Provision of Encryption Services* van 19 maart 1997 bevatte daartoe voorstellen, maar de reacties op verplicht gebruik van TTP's waren overwegend negatief. Na een volgend consultatiedocument, *Building Confidence in Electronic Commerce* van 5 maart 1999, waarin sleuteldepot niet werd verplicht maar werd gestimuleerd, sloeg de regering een andere richting in,[409] namelijk een ontsleutelplicht.
Deze is opgenomen in deel III van de *Regulation of Investigatory Powers Act 2000*[410] en kan worden gegeven door de politie, nationaleveiligheidsdiensten en de douane. Het opzettelijk niet voldoen aan een ontsleutelbevel is strafbaar met maximaal twee jaar gevangenisstraf (art. 53 lid 1 en 5 RIPA). Mede voor de uitvoering hiervan is een National Technical Assistance Centre (NTAC) opgericht.[411] Een gedragscode zal de autoriteiten nader richting geven bij het uitvoeren van het ontsleutelbevel; een voorontwerp hiervan werd gepubliceerd op 10 juli 2000, maar deze is niet meer beschikbaar op het Internet.[412] Aan een nieuwe versie wordt momenteel nog gewerkt. Van belang is dat deel III van de RIPA nog niet in werking is getreden; de inwerkingtreding wordt ook niet verwacht voor eind 2002.

5.4.8. Verenigde Staten

Exportregulering
De VS hebben het Wassenaar Akkoord ondertekend, maar hanteerden van oudsher over het algemeen zwaardere beperkingen op cryptografie dan het Akkoord. De *Export Administration Regulations*[413] van het Department of Commerce vereisen in het algemeen een individuele vergunning voor export van sterke cryptografie. De exportbeperkingen zijn echter sinds 1998 geleidelijk versoepeld, waarbij voor diverse landen en diverse toepassingen uitzonderingen op de vergunningplicht zijn gemaakt. Met name de regelingen van 12 januari en 19 oktober 2000 betekenden een aanzienlijke versoepeling,[414] waarmee de VS grosso modo in de pas lopen met de andere Wassenaar-landen.

Binnenlandse regulering

---

[406] *MITI's Information Policy, Specific Policy*, <http://www.gip.jipdec.or.jp/policy/infopoli/indivipoli-e.html>; METI, *Key Points. 2002 Economic and Industrial Policy*, augustus 2001, p. 14-15, <http://www.meti.go.jp/english/information/data/c2002polie.pdf>.
[407] Koops 2002.
[408] SI 2000/2620, <http://www.hmso.gov.uk/si/si2000/20002620.htm>.
[409] Vgl. de *Electronic Communications Act 2000* van 25 mei 2000, <http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm>, die een verbod bevat voor de overheid om een sleuteldepotregeling te baseren op bepalingen uit deze wet.
[410] <http://www.legislation.hmso.gov.uk/acts/acts2000/10000023.htm>, 2000 Chapter 23.
[411] Zie <http://www.homeoffice.gov.uk/oicd/ntac/>.
[412] De pagina met Codes of Practices van de RIPA <http://www.homeoffice.gov.uk/ripa/ripadcp.htm> bevat niet de onderhavige ontwerpgedragscode, die voorheen beschikbaar was op <http://www.homeoffice.gov.uk/ripa/part3.htm>.
[413] 15 C.F.R. Parts 730-774 (zie met name paragrafen 740.13, 740.17 en 742.15).
[414] Zie voor een samenvatting van deze regelingen Koops 2002 en de informatiepagina van het Bureau of Industry and Security (voorheen Bureau of Export Administration, BXA) <http://www.bxa.doc.gov/Encryption/Default.htm>.

In de jaren negentig van de vorige eeuw is er in de VS een verhit beleidsdebat gevoerd over cryptobeperkingen. Het debat begon met de Clipper-chip (een sleuteldepotsysteem), door de regering in 1993 voorgesteld, die door overheidsstimulering op vrijwillige basis zoveel mogelijk zou moeten worden gebruikt; hiervan kwam evenwel niets terecht. Daarna volgden diverse regeringsinitiatieven voor sleuteldepot of sleutelherwinning (door tegenstanders vernoemd tot Clipper II en Clipper III), waar ook grote maatschappelijke weerstand tegen bestond. Tegelijkertijd werden in het Congres diverse wetsvoorstellen ingediend om cryptogebruik aan banden te leggen, maar geen van deze wetsvoorstellen werd aangenomen. Het laatste wetsvoorstel van regeringszijde, de *Cyberspace Electronic Security Act of 1999*, liet verplichte sleutelherwinning vallen en concentreerde zich op het geldelijk ondersteunen van het FBI's Technical Support Center; ook dit wetsvoorstel is evenwel niet aangenomen.[415]
Sinds eind 1999 heeft de overheid geen concrete wetsvoorstellen of beleid meer ontwikkeld voor binnenlandse regering van cryptografie. Mogelijk wordt volstaan met het vervolmaken van technische onderscheppingsmaatregelen als een *key sniffer*, een programmaatje dat – op afstand geïnstalleerd op de computer van een verdachte – kort gezegd een cryptosleutel onderschept; volgens een uitspraak van het District Court New Jersey van 26 december 2001 is dit toegestaan op grond van aftapwetgeving.[416]

5.4.9. Zweden

Exportregulering
De export van cryptografie werd gereguleerd in overeenstemming met het Wassenaar Akkoord. Dit gebeurde in de *Förordning om strategiska produkter* (SFS 1998:400, Verordening over strategische producten);[417] deze verordening is evenwel ingetrokken en vervangen door de *Lag om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd* (SFS 2000:1064) (Wet voor de controle op producten voor tweeërlei gebruik en op technische hulp)[418] en de bijbehorende verordening (SFS 2000:1217).

Binnenlandse regulering
Na een consultatiedocument uit 1997, *Cryptography Policy: Possible Courses of Action for Sweden*, bepaalde de Zweedse overheid een cryptografiebeleid in het document *On cryptography* van 6 mei 1999.[419] De regering ziet geen reden om cryptografie te beperken in Zweden. Indien toekomstige ontwikkelingen daartoe nopen, zal de regering alsnog passende maatregelen nemen om overheidstoegang tot versleutelde gegevens te waarborgen (maar er wordt geen indicatie gegeven welke dat zullen zijn).

5.4.10. Samenvatting

Exportregulering
De export van cryptografie wordt voor het overgrote deel internationaal aangestuurd via het Wassenaar Akkoord. Vrijwel alle landen, waaronder Nederland, hebben de afspraken uit dit akkoord in nationale wetgeving geïmplementeerd. Waar tot eind jaren negentig van de vorige eeuw de nationale regelingen behoorlijk uiteen konden lopen (de VS en Frankrijk kenden strengere regelingen), zijn de laatste jaren de regelingen steeds meer naar elkaar toe gegroeid. Bovendien zijn de exportbeperkingen de laatste twee, drie jaren behoorlijk versoepeld, waardoor de maatschappelijke weerstand ertegen verstomd lijkt. Kennelijk functioneren de vergunningstelsels en de uitzonderingen op de vergunningplicht afdoende. Een voorzichtige conclusie zou kunnen luiden dat de exportbeperkingen op cryptografie geen wezenlijk obstakel voor internationale elektronische handel meer lijken te vormen.

---

[415] Zie Koops 2002 voor een overzicht van al deze wetsvoorstellen.
[416] *United States v. Scarfo*, <http://lawlibrary.rutgers.edu/fed/html/scarfo2.html-1.html>.
[417] <http://www.notisum.se/rnp/sls/lag/19980400.HTM>.
[418] <http://www.notisum.se/rnp/SLS/LAG/20001064.HTM>.
[419] Beschikbaar op <http://cryptome.org/se-crypto99.htm>.

Binnenlandse regulering

De binnenlandse regulering van cryptografie is, in tegenstelling tot de exportbeperkingen, vooral een nationale aangelegenheid. Internationale afstemming kon men op dit punt niet bereiken. Ook hier lijken de regelingen echter naar elkaar toe te groeien. In de jaren negentig helden diverse overheden (met name de VS en het VK) over naar het inbouwen in cryptosystemen van een mogelijkheid tot overheidstoegang (sleuteldepot of sleutelherwinning); Frankrijk was het enige land dat hiertoe daadwerkelijk wetgeving kende. In deze landen is men echter teruggekomen van deze richting, mede onder invloed van grote maatschappelijke weerstand.

De meeste landen beperken zich nu tot een wettelijke ontsleutelplicht: wanneer de overheid versleutelde gegevens aantreft, kan zij een bevel geven deze te ontsleutelen of een sleutel te overhandigen. Nederland was het eerste land dat – al in 1993 – een ontsleutelplicht invoerde, zij het op beperkte schaal. Frankrijk en het VK hebben een verdergaande ontsleutelplicht (ook voor verdachten), waarbij niet-naleving met hoge straffen wordt bedreigd.[420] Naast een wettelijke ontsleutelplicht leggen diverse landen (Duitsland, Frankrijk en de VS) de nadruk op het versterken van de technische kraakcapaciteit van de overheid; Nederland heeft daartoe vooralsnog geen stappen ondernomen.

In algemene zin kan men stellen dat het geworstel met binnenlandse cryptoregulering lange tijd rechtsonzekerheid heeft opgeleverd over de toelaatbaarheid van cryptogebruik, hetgeen belemmerend heeft gewerkt op het gebruik van cryptografie voor informatiebeveiliging. Nu overheden niet meer overwegen om cryptogebruik zelf aan banden te leggen, maar slechts maatregelen nemen om in voorkomende gevallen ontsleuteling te bevelen, zal het gebruik van cryptografie kunnen toenemen, waardoor het vertrouwen in elektronische handel wordt gestimuleerd. De enige kanttekening is dat de straffen op het niet naleven van een ontsleutelbevel in sommige landen (Frankrijk, VK en in Nederland bij de Wiv) dermate hoog zijn dat hiervan een "verkillend effect" op cryptogebruik zou kunnen uitgaan; hiervoor zijn echter vooralsnog geen aanwijzingen te vinden.

[420] Ook diverse landen die buiten dit rapport vallen, zoals Singapore, kennen inmiddels een ontsleutelplicht. Zie Koops 2002.

5.5. Commerciële communicatie en spam

Het begrip 'commerciële communicatie' kan gedefinieerd worden als 'alle vormen van adverteren, direct marketing, sponsoring, sales promotion en public relations waarmee producten en diensten worden gepromoot'.[421] De officiële, uitgebreidere definitie luidt: 'elke vorm van communicatie bestemd voor het direct of indirect promoten van goederen, diensten of het imago van een onderneming, organisatie of persoon, die een commerciële, industriële of ambachtelijke activiteit of een gereglementeerd beroep uitoefent. Het navolgende vormt op zich geen commerciële communicatie: informatie die rechtstreeks toegang geeft tot de activiteit van een onderneming, organisatie of persoon, in het bijzonder een domeinnaam of een elektronisch postadres; mededelingen over de goederen of diensten of het imago van een onderneming, organisatie of persoon, die onafhankelijk van deze en in het bijzonder zonder financiële tegenprestatie zijn samengesteld'.[422]
'Spam' is de populaire aanduiding voor ongevraagde commerciële e-mail, hetgeen ook wel aangeduid wordt als UCE (*unsolicited commercial e-mail*).[423]

Voor e-handel is dit onderwerp relevant omdat ter promotie van die handel veelal gebruik wordt gemaakt van commerciële communicatie, en meer specifiek UCE oftewel 'spam'. Vanwege het belang van zelfregulering bij dit onderwerp, wordt in deze paragraaf steeds apart aandacht besteed aan regelgeving en zelfregulering.

5.5.1. Internationaal

Europese regelgeving
De Europese regelgeving ten aanzien van commerciële communicatie c.q. spam wordt gevormd door vier belangrijke EG-richtlijnen; twee hiervan stellen direct regels voor (het versturen van) commerciële e-mail, de 2 andere stellen indirect regels doordat ze (kort gezegd) voorschrijven in hoeverre onder meer e-mailadressen kunnen worden gebruikt voor het toezenden van zulke e-mail.
Deze richtlijnen zijn:
1. *Distance Selling Directive* (Verkoop op afstand, 97/7/EC, 20 mei 1997),
2. *Electronic Commerce Directive* (Elektronische handel, 2000/31/EC, 8 juni 2000),
3. *Data Protection Directive* (Bescherming persoonsgegevens, 95/46/EC, 24 oktober 1995) en
4. *Telecommunications Privacy Directive* (Privacy in de telecomsector, 97/66/EC, 15 december 1997).

Omdat deze laatste twee richtlijnen eigenlijk geen directe regels stellen en deze eigenlijk onder het onderzoeksgebied 'privacy' vallen, zal het overzicht wat betreft de EU en EU-landen hier zich name gericht zijn op de regels die voortvloeien uit de eerste twee richtlijnen.

De Richtlijn Verkoop op afstand (artikel 10) maakt, ten aanzien van het versturen van berichten voor direct-marketing-doeleinden, een onderscheid tussen enerzijds 'automatische belmachines' en faxen (lid 1) en anderzijds de overige communicatiemiddelen (lid 2), onder welke laatste categorie ook e-mail begrepen kan worden. Voor de eerste categorie communicatiemiddelen geldt dat consumenten daarmee alleen benaderd mogen worden als ze daarmee vooraf hebben ingestemd ('opt-in'), middels de overige communicatiemiddelen staat het vrij consumenten te benaderen mits deze daartegen geen bezwaar hebben gemaakt ('opt-out' systeem).

Overigens zijn er mensen die menen dat spam onder lid 1 valt nu de werking van de meeste systemen waarmee spam wordt verstuurd, veel lijkt op de werking van automatische belsystemen. De officiële uitleg is evenwel dat UCE niet onder lid 1, maar onder lid 2 valt, en dat een lidstaat

---

[421] Definitie gehanteerd in *Groenboek Commerciële communicatie in de interne markt*, COM(96) 192, 8 mei 1996.
[422] Definitie in artikel 2 sub f van de Richtlijn Elektronische handel, 2000/31/EG.
[423] Zie Lodder & Bergfeld 2002 voor nadere begripsbepaling.

dus kan kiezen tussen ofwel een opt-in- ofwel een opt-out-regime. Ook in de VS bestaat een soortgelijke stroming, zie par. 5.5.8.

De *Richtlijn Elektronische handel* stelt, voorzover hier relevant, als regel dat indien een lidstaat het toezenden van UCE toestaat, deze lidstaat de op zijn grondgebied gevestigde verzenders van UCE moet verplichten deze UCE duidelijk als zodanig herkenbaar te maken. Als de commerciële communicatie deel uitmaakt van een 'dienst van de informatiemaatschappij', of zo'n dienst vormt, moet in die communicatie ook duidelijk gemaakt worden namens welke natuurlijke of rechtspersoon de communicatie is verstuurd (artikelen 6 en 7). Kortom: als UCE toegestaan wordt, moet deze duidelijk als zodanig herkenbaar zijn en moet de afzender duidelijk vermeld worden.

De *Richtlijn Bescherming persoonsgegevens* stelt een kader voor de wijze waarop persoonsgegevens (naam, adres, telefoonnummer, mailadres, etc.) kunnen worden verzameld, verwerkt en gebruikt, ook voor direct-marketing-doeleinden. De richtlijn stelt, kort samengevat, diverse regels voor het verzamelen, opslaan en gebruik van persoonsgegevens (onder meer: deze mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld worden, en deze mogen alleen verwerkt worden als de betrokkene dit heeft goedgekeurd of als de gegevensverwerking noodzakelijk is gezien een limitatief aantal gronden, artikelen 6 en 7). Relevant is voorts dat de betrokkene geïnformeerd moet worden over het gebruik van zijn gegevens en de mogelijkheden om deze gegevens te corrigeren (artikelen 10, 11 en 12). Zeer belangrijk wat betreft UCE is de bepaling dat, indien persoonsgegevens naar verwachting gebruikt zouden worden voor direct-marketing-doeleinden, de betrokkene daarover geïnformeerd moet worden en hij de mogelijkheid moet krijgen tegen dat gebruik bezwaar te maken (artikel 14 sub b).

De *Richtlijn Privacy in de telecomsector* stelt voor het hier relevante onderwerp feitelijk dezelfde regel als gesteld wordt in de Richtlijn Verkoop op afstand; voor communicaties via fax en automatische belapparaten geldt een opt-in-regime, voor communicaties via andere communicatiemiddelen geldt een opt-out-regime (artikel 12 leden 1 en 2).

Laatstgenoemde richtlijn zal overigens op korte termijn vervangen worden door een herziene richtlijn, waarbij de keuze tussen een opt-in- en opt-out-regime zal worden vervangen door een verplicht opt-in-regime voor UCE.[424] Er zal wel een uitzondering gelden voor het sturen van e-mail naar bestaande klanten, onder voorwaarde dat op het moment dat de klantgegevens worden verkregen en bij elke direct-marketing-boodschap een duidelijke en gemakkelijke mogelijkheid wordt geboden om dit gebruik te stoppen. Voorts moet, volgens de nieuwe richtlijn, het gebruik van communicatiegegevens beperkt blijven tot degene die deze gegevens oorspronkelijk heeft verzameld.
Als gevolg van deze richtlijn zullen, zo mag aangenomen worden, de opt-out-regelingen ingevolge de voorgaande richtlijnen irrelevant en krachteloos worden en zal in plaats daarvan in alle EU-landen een opt-in-regime van kracht moeten worden.

Europese zelfregulering
De Europese federatie van nationale direct-marketing-organisaties (FEDMA) heeft de FEDMA *Code of Conduct on E-commerce and Interactive Marketing* opgesteld. Deze gedragscode bepaalt onder meer dat elke commerciële communicatie duidelijk als zodanig herkenbaar moet zijn, en dat consumenten geïnformeerd moeten worden over het gebruik van hun gegevens en hun rechten daaromtrent. Deze bepalingen gaan geven geen verdere bescherming dan al ingevolge de eerdergenoemde richtlijnen bestond, dus de meerwaarde en relevantie van deze gedragscode is zeer beperkt.

[424] Besluit Europees Parlement van 30 mei 2002 bij aanvaarding herziene richtlijn 97/66/EG (DMN: IP/02/783).

Als tegenhanger van de belangenpleitgroep van de Europese direct-marketing-organisaties (FEDMA) is de CAUCE ontstaan, de Coalition Against Unsolicited Commercial E-mail. Op dit moment is er een Europese poot van CAUCE (EuroCAUCE),[425] een Indiase[426] en een Canadese[427] poot.

5.5.2. Nederland

Regelgeving
In Nederland is gekozen voor invoering van een wettelijk opt-out-regime; consumenten kunnen zich bij de Nederlandse brancheorganisatie voor direct marketing (DMSA) opgeven, waarna de bij de DMSA (en haar Europese zusterorganisaties) aangesloten bedrijven aan de desbetreffende consument geen UCE meer mogen toezenden. Het regime van artikel 10 van de Richtlijn Verkoop op afstand is dus in Nederland ingevoerd als een *opt-out*-regime (artikel 7:46h leden 2 en 3 BW).
De 'informatieplicht' van de Richtlijn Elektronische handel zal worden neergelegd in het voorgestelde artikel 3:15e lid 2 BW.[428]

De privacyregels van de Richtlijn Bescherming persoonsgegevens zijn neergelegd in de Wet bescherming persoonsgegevens,[429] en die van de Richtlijn Privacy in de telecomsector in artikel 11.7 Telecommunicatiewet (zie voor deze regels boven, bij de desbetreffende richtlijn).

Zelfregulering
De DMSA (de Nederlandse brancheorganisatie van direct-marketing-bedrijven) biedt consumenten de mogelijkheid om zich bij haar op een opt-out-lijst te laten zetten, waarna de bij de DMSA aangesloten bedrijven volgens haar reglement verplicht zijn om de desbetreffende consumenten geen UCE meer te sturen.

Overigens staan in de *Model Gedragscode voor elektronisch zakendoen* van ECP.NL (Electronic Commerce Platform Nederland)[430] als hier relevante bepalingen dat de aanbieder van e-handeldiensten ervoor moet zorgdragen dat 'zijn reclame-uitingen herkenbaar en herleidbaar zijn' en dat, indien hij een opt-in- of opt-out-mogelijkheid hanteert, hij daarover duidelijke informatie moet geven (paragraaf 2.3.2 van de Model Gedragscode). Deze Model Gedragscode is evenwel slechts bedoeld als 'inspiratiebron' voor bedrijven die een gedragscode willen opstellen en deze kunnen naar eigen believen bepalingen negeren of andere daarvoor in de plaats zetten.

5.5.3. Canada

Regelgeving
De Canadese overheid vindt dat spam niet gereguleerd behoeft te worden, aangezien marktwerking hiervoor volstaat.[431] Bovendien is er in een civiele zaak een uitspraak geweest tegen spam. Er gaan echter stemmen op om spammen wel te reguleren.[432]

Voor reclame op het Internet is nog van belang dat Quebec wetgeving kent die eist dat reclame voornamelijk Franstalig is. Het Office of the French Language heeft aangegeven dat dit ook geldt voor weblocaties van bedrijven met een adres in Quebec, ongeacht waar de netwerkcomputer van het bedrijf staat.[433]

---

[425] <http://www.euro.cauce.org>.
[426] <http://www.india.cauce.org>.
[427] <http://www.cauce.ca>, weblocatie nog niet actief.
[428] TK 2001-2002, 28 197, nrs. 1-2.
[429] Wbp, Stb. 2000, 302, inwerkingtreding 1 september 2001.
[430] <http://www.ecp.nl>.
[431] Canadian Radio-Television and Telecommunications Commission, New media decision, 17 mei 1999, <http://www.crtc.gc.ca/archive/eng/Notices/1999/PB99-84.htm>.
[432] Michael Geist, 'Time to hit delete key on weak spam policy', *Globe and Mail* 30 mei 2002.
[433] Office of the French Language (Quebec), *The Charter of the French Language and Web Sites*, <http://www.olf.gouv.qc.ca/index.html>.

Zelfregulering
Over zelfregulering is geen materiaal aangetroffen in dit onderzoek.

5.5.4. Duitsland

Regelgeving
Er is geen materiaal gevonden over regelgeving voor UCE in Duitsland.

Zelfregulering
Het Duitse Interessenverband Deutsches Internet (IDI)[434] heeft voor haar leden een *opt-out*-systeem ontwikkeld, de zogenoemde 'E-robinson Liste'.[435]

Het Deutscher Multimedia Verband (DMMV)[436] stelt zich daarentegen in haar *Definition für akzeptables E-Mail-Marketing*[437] op het standpunt dat alleen sprake is van acceptabele e-mailmarketing als de ontvanger het toezenden van dergelijke e-mailberichten uitdrukkelijk heeft goedgekeurd. Deze belangenvereniging voor de Internet- en multimedia-branche pleit dus voor een *opt-in*-regime. Het is onduidelijk of de richtlijn verplicht is voor de leden van DMMV.

5.5.5. Frankrijk

Regelgeving
In Frankrijk bestaat geen regelgeving (noch initiatieven daartoe) die het toezenden van UCE reguleert.

Op het gebied van privacyregulering is hier relevant dat de Commission Nationale de l'Informatique et des Libertés (CNIL)[438] in haar rapport *Le publipostage électronique et la protection des données personelles*[439] van oktober 1999 een aantal beleidsuitgangspunten heeft geformuleerd voor de privacyregulering op het gebied van UCE, waarbij aangesloten wordt bij de beginselen van de eerdergenoemde Richtlijn Bescherming persoonsgegevens. De Commissie neemt als uitgangspunt dat er geen recht bestaat om consumenten middels UCE te benaderen zonder toestemming daartoe van die consumenten. Een opt-out-regime zou, aldus het rapport, ook geen recht doen aan de bescherming die geboden wordt door de eerdergenoemde privacyrichtlijn. Voorzover nagegaan kon worden, heeft de regering nog geen inhoudelijke reactie gegeven op de conclusies van het rapport.

Zelfregulering
De Franse brancheorganisatie voor direct-marketing-bedrijven (Fédération des Enterprises de Vente à Distance, FEVAD)[440] heeft voorgesteld tot een wettelijke opt-out-regeling te komen. De FEVAD heeft zelf al op eigen initiatief een opt-out-systeem opgezet, de zogenoemde 'Liste E-Robinson'.[441]

5.5.6. Japan

Regelgeving
In april 2002 is de *Law concerning the Proper Transmission of Specific Electronic Mails* door het Japanse parlement aangenomen, die verbiedt om UCE te sturen naar personen die hebben aangegeven

---

434 <http://www.idi.de>.
435 <http://www.mailrobin.de>.
436 <http://www.dmmv.de>, <http://www.werbeformen.de>.
437 <http://www.dmmv.de/de/7_pub/homepagedmmv/themen/emarketing/emailmarketing/aktivitaetenemailmarketing/definition_e_mail.cfm>.
438 <http://www.cnil.fr>.
439 <http://www.cnil.fr/init/index.htm>.
440 <http://www.fevad.com>.
441 <http://www.e-robinson.com>.

deze niet te willen ontvangen. Voorts bepaalt de wet dat in de UCE duidelijk de aard van de communicatie en het e-mailadres van de afzender vermeld moeten worden.[442]

Zelfregulering
Over zelfregulering van UCE in Japan is niets aangetroffen in dit onderzoek.

5.5.7. Verenigd Koninkrijk

Regelgeving
In het VK wordt artikel 10 van de Richtlijn Verkoop op afstand niet als zodanig geïmplementeerd, evenmin als artikel 7 lid 2 van de Richtlijn Elektronische handel over een opt-outregister. De Engelse overheid (bij monde van het Department of Trade and Industry, DTI)[443] heeft gesteld dat er voldoende bescherming tegen spam wordt geboden door 'de bestaande zelfreguleringinitiatieven'.[444]
Er zijn dus in het VK geen wettelijke regelingen voor regulering van het toezenden van commerciële communicatie via e-mail.

Zelfregulering
De Engelse DMA (brancheorganisatie van direct-marketing-bedrijven)[445] heeft een *Code of Practice for Electronic Commerce* voor haar leden opgesteld,[446] waarin bepaald is dat de leden geen 'ongerichte' UCE (spam) mogen uitsturen, dat UCE als zodanig herkenbaar moet zijn, en dat de leden de 'opt-out-lijst' van de DMA in acht moeten nemen en dat zij derhalve geen UCE meer mogen toezenden aan consumenten die daartegen bezwaar hebben gemaakt. Ook bepaalt de gedragscode dat de leden bij het verzamelen en gebruik van persoonsgegevens de regels van de Richtlijn Bescherming persoonsgegevens in acht moeten nemen.

5.5.8. Verenigde Staten

Regelgeving
Op federaal niveau is er geen regelgeving die UCE reguleert. Er liggen daartoe wel diverse wetsvoorstellen bij het Congres (waaronder de *Unsolicited Commercial Electronic Mail Act*, *Anti-spamming Act*, *E-Mail User Protection Act*, *Inbox Privacy Act*, *Can Spam Act*),[447] maar het is onzeker of deze aangenomen zullen worden, mede gezien de intensieve lobby tegen die regelgeving door de direct-marketing-branche.

Wel is er in 21 individuele staten anti-spam-regelgeving.[448] De aard en strekking van deze regelgeving verschilt aanzienlijk van staat tot staat. Zo is het bijvoorbeeld in Delaware verboden massa-UCE te versturen, in Californië en Nevada moeten UCE-berichten opt-out-instructies en diverse gegevens van de afzender (zoals telefoonnummer en adres) bevatten en moeten de verzenders van UCE de opt-out-lijsten respecteren, in bijvoorbeeld Utah moet UCE bovendien een etiket in het onderwerpsveld hebben ('ADV' voor 'advertisement', met daarbij 'ADLT' als de inhoud niet geschikt is voor personen onder de 18 jaar), en in West Virginia is het verboden om valse routeringsinformatie in bij het mailen te gebruiken. In al deze 21 staten bestaat de anti-spam-wetgeving uit een of meerdere van deze genoemde elementen.

Overigens is in de VS een stroming die argumenteert dat spam te brengen valt onder de verbodsregeling die oorspronkelijk voor een andere soort communicatie bedoeld was; de definitie

---

[442] *Electronic Commerce & Law Report* 2002, p. 351.
[443] <http://www.dti.gov.uk>.
[444] <http://213.38.88.195/coi/coipress.nsf/2b45e1e3ffe090ac802567350059d840/0edb179246bfae9580256950003cf6cf?OpenDocument> en par. 5.10 van de *Guidance Notes* bij de voorgestelde *Electronic Commerce (E.C. Directive) Regulations 2002*.
[445] <http://www.dma.org.uk>.
[446] Te vinden via <http://www.dma.org.uk/shared/lgl_code.asp>.
[447] Te vinden via <http://www.spamlaws.com/us.html>, onder 'federal laws', en *Electronic Commerce & Law Report*, Vol. 6, no. 12, p. 290.
[448] Te vinden via <http://www.spamlaws.com/us.html>, onder 'state laws'.

van 'telephone facsimile machine' in de *Telephone Consumer Protection Act 1991*[449] is volgens hen zo breed uit te leggen dat deze wet, naast het sturen van ongevraagde reclame-faxen, ook het sturen van UCE of spam verbiedt.[450] Deze uitleg is evenwel vooralsnog niet in de rechtspraak aangetroffen.

Zelfregulering
De Amerikaanse branchorganisatie van direct-marketing-bedrijven (DMA)[451] heeft de zogenoemde *E-Mail Preference Service* (E-MPS)[452] opgezet, waarbij consumenten zich bij haar op een opt-out-lijst kunnen laten plaatsen. De bij de DMA aangesloten bedrijven zijn verplicht de op de E-MPS-lijst voorkomende e-mailadressen uit hun adressenbestanden te verwijderen.

5.5.9. Zweden

Regelgeving
In Zweden is de bescherming tegen spam aanwezig zoals voorzien in artikel 10 van de Richtlijn Verkoop op afstand. Per 1 mei 2000 is namelijk in de *Marknadsföringslag* (Marktwet, par. 13a) de regeling van artikel 10 van de Richtlijn Verkoop op afstand opgenomen, met daarin nog een uitbreiding; de regeling van artikel 10 lid 1 (opt-in) is daar ook van toepassing op 'andere gelijksoortige automatische systemen voor individuele communicatie die niet door iemand worden bediend'.[453] Het is aan de rechter overgelaten om te beoordelen of in deze toevoeging van 'gelijksoortige geautomatiseerde systemen voor individuele communicatie' ook e-mail gelezen kan worden; een amendement om de toevoeging te expliciteren als doelende op e-mail werd in het Parlement afgewezen. Feitelijk is daarmee nog onzeker of er in Zweden sprake is van een opt-in of opt-out-regime ten aanzien van UCE, maar redelijkerwijs moet in deze bepaling een opt-in voor e-mail worden gelezen, nu de wijze waarop de meeste spam wordt verstuurd onder de formulering van die bepaling valt.

Zelfregulering
Over zelfregulering van UCE in Zweden is in dit onderzoek niets aangetroffen.

5.5.10. Samenvatting

Globaal bezien is in de meeste landen op dit moment een opt-out-systeem van kracht, ofwel krachtens een wettelijke regeling ofwel ingevolge zelfregulering. Opvallend is dat in Duitsland en Frankrijk – die toch gerekend worden tot belangrijke economieën – er door de regeringen (nog) geen concrete stappen zijn genomen ter regulering van UCE. In Frankrijk geldt een opt-out-regime als gevolg van zelfregulering, maar in Duitsland is (voorzover nagegaan kon worden) de situatie nog onduidelijk; de ene belangenorganisatie pleit voor opt-out, de andere voor opt-in.

De algemene 'Europese richting' ten aanzien van commerciële communicatie via e-mail (oftewel spam, UCE) is op dit moment nog de opt-outbenadering:[454] UCE versturen mag, mits aan een aantal voorwaarden is voldaan (waaronder: de consument heeft geen bezwaar gemaakt, de communicatie is duidelijk als zodanig herkenbaar, de consument wordt geïnformeerd over het gebruik van zijn persoonsgegevens). Deze benadering gaat veranderen in een opt-inbenadering zodra de nieuwe Richtlijn Privacy in de elektronischecommunicatiesector (opvolger van de ISDN-richtlijn) van kracht zal worden; deze herziene richtlijn zal als hoofdregel bepalen dat

---

[449] 47 U.S.C. § 227.
[450] Zie David E. Sorkin, 'Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991', 45 *Buffalo L. Rev.* 1001 (1997) en de verdere daar genoemde bronnen, alles te vinden via <http://www.spamlaws.com> onder 'articles'.
[451] <http://www.the-dma.org>.
[452] <http://www.e-mps.org>.
[453] Informatie gevonden op <http://www.euro.cauce.org/en/countries/c_se.html>. De tekst van deze Marktwet is (in het Zweeds) te vinden op <http://www.sverigedirekt.se>, en daar via een zoekopdracht onder 'Lagar och förordningar' (wetten en verordeningen) en dan 'sök lagar' (zoek wetten).
[454] Overigens kennen vier EU-lidstaten, die niet in dit onderzoek zijn opgenomen, momenteel wel een opt-inregeling: Denemarken, Finland, Italië en Oostenrijk. Lodder & Bergfeld 2002, p. 1055.

bedrijven consumenten alleen met UCE mogen benaderen als deze hiervoor vooraf toestemming hebben gegeven. De lidstaten van de EU zullen deze hoofdregel op een termijn van waarschijnlijk ongeveer twee jaar in hun nationale regelgevingen hebben moeten implementeren, waarna de opt-inbenadering de hoofdregel zal worden in de EU-landen. Alle nationale opt-out-regelingen (regelgeving en zelfregulering) zullen daarmee worden vervangen door het opt-in-regime. Deze hoofdregel kent overigens wel een nuance; zo mag een bedrijf haar bestaande klanten wel met e-mailberichten benaderen.

Bovenbedoelde opt-out-benadering wordt in de praktijk veelal gerealiseerd doordat landelijke brancheorganisaties voor direct marketing een opt-out-regeling in het leven hebben geroepen. Het is niet na te gaan uit welke motieven elk van deze organisaties tot deze regelingen gekomen zijn; in veel gevallen is wel aannemelijk dat dit is gebeurd om regulering van overheidswege (opt-out of zelfs opt-in), waarbij de branche dan verder buitenspel zou komen te staan, te voorkomen.

Nederland loopt, in vergelijking met de meeste andere landen, in de pas; ook hier geldt op dit moment een opt-out-regime waarbij voor de consument een aantal garanties geldt (hij kan zich op een opt-out-lijst laten plaatsen, een wet beschermt zijn persoonsgegevens, etc.). Mede omdat dit regime en de bijbehorende garanties (ook) duidelijk in wetgeving zijn vastgelegd, kan gezegd worden dat de Nederlandse situatie zelfs beter is geregeld dan diverse van de besproken landen. Wel kan gezegd worden dat Nederland niet sterk is in het ontwikkelen van eigen (beleids)initiatieven; Nederland implementeert slechts de regelgeving uit Brussel (waarbij zij ook vaak de implementatietermijn niet eens haalt), en heeft het aan de Nederlandse brancheorganisatie voor direct marketing overgelaten om een (standaard) opt-out-regeling te bieden, waarbij ook niet of nauwelijks wordt gedaan aan consumentenvoorlichting om de consument optimaal gebruik te laten maken van deze mogelijkheid. Al met al kan gezegd worden dat de Nederlandse overheid geen actieve belangenbehartiger is van consumentenbelangen op dit punt. Het laatste geldt overigens ook voor de andere landen in dit onderzoek: er zijn geen voorlichtingscampagnes van overheden aangetroffen om consumenten te wijzen op de mogelijkheden van opt-out.

Overigens is in dit verband een saillant punt dat in Zweden al wel een opt-in-regime lijkt te gelden, nu dat land de ISDN-richtlijn (Richtlijn Privacy in de telecomsector) zo heeft geïmplementeerd dat, evenals 'spam' middels automatische belmachines en faxen, ook – zo mag worden aangenomen – e-mail onder het opt-in-regime valt. Hoewel er bijvoorbeeld ook in de VS stemmen opgaan om, gezien de bestaande regelingen (zoals de *Telephone Consumer Protection Act*), in dit verband e-mail hetzelfde te behandelen als faxberichten (waarvoor een verbod geldt voor ongevraagde toezending), hebben de meeste Europese landen – waaronder ook Nederland – ervoor gekozen e-mail en fax niet op één lijn te zetten, maar e-mail te brengen onder een opt-out-regime. Hoewel laatstgenoemde benadering wordt toegestaan door de richtlijn, illustreert de vergelijking met Zweden wel dat de bedoelde landen, waaronder Nederland, op dit punt eerder neigen naar bescherming van de belangen van de direct-marketing-industrie dan naar bescherming van consumentenbelangen.

5.6. Gedragscodes en keurmerken voor webhandel

Zelfregulering is een belangrijk instrument voor het bevorderen van vertrouwen in elektronisch zakendoen. Het kan, onder bepaalde voorwaarden, een mechanisme zijn dat bestaande wetgeving kan aanvullen en soms zelfs als (voorlopige) vervanging van wetgeving kan dienen. Wel geldt dat er een belangrijke rol is weggelegd voor aanbieders (bedrijfsleven) om zelf een behoorlijke inspanning te leveren om dat vertrouwen te creëren. Dat kan onder andere door aan te geven dat de aanbieder zich volgens bepaalde regels zal gedragen. Zulke regels liggen bijvoorbeeld in wetgeving vast, maar kunnen ook duidelijk gemaakt worden door middel van contracten of door het onderschrijven van een gedragscode over de wijze waarop een organisatie omgaat met elektronisch zakendoen. Veelal wordt door middel van certificering in de vorm van keurmerken aangeduid dat een aanbieder een zekere gedragscode onderschrijft en ook naleeft.

5.6.1. Internationaal

Er bestaan internationale richtsnoeren zoals de *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*. Deze richtsnoeren worden echter volgens onderzoek van ConsumersInternational door erg veel online aanbieders niet nageleefd: "However, these guidelines are voluntary and our research shows that many sites do not follow them."[455]

Een onderdeel van de Verenigde Naties, de United Nations Commission on International Trade Law (UNCITRAL), zet zich in om wetgeving rond elektronisch zakendoen in de wereld te bevorderen en te stroomlijnen. Hiertoe worden modelwetten opgesteld die door landen gebruikt worden voor het maken van nationale wetgeving. Zo heeft UNCITRAL in 1996 de *Model Law on Electronic Commerce* ontworpen, die in 1998 is aangepast. Deze modelwet is inmiddels aangenomen in de landen Australië, Bermuda, Colombia, Filippijnen, Frankrijk, Hong Kong, Ierland, Singapore, Slovenië, Zuid-Korea en de staten Jersey (Verenigd Koninkrijk) en Illinois (Verenigde Staten). In Canada (Uniform Electronic Commerce Act) en de Verenigde Staten (Uniform Electronic Transactions Act) is de wetgeving gebaseerd op de principes van de UNCITRAL-modelwet.[456]

De Europese Richtlijn elektronische handel stimuleert in artikel 16 het gebruik van zelfregulering en de ontwikkeling van gedragscodes met onder meer als doel het vertrouwen van consumenten in de elektronische handel te doen groeien. Lidstaten en de Commissie dienen zich in te spannen om consumentenorganisaties te betrekken bij het opstellen en implementeren van gedragscodes.[457]

In de EU is een Webtrader-keurmerk opgezet, een internationaal project gefinancierd door de Europese Commissie. Hierbij hebben zich een tiental Europese consumentenorganisaties aangesloten.[458] Deze verschillende organisaties verwijzen dan ook naar elkaar. Tussen de verschillende nationale implementaties een uitvoeringen van de Webtrader-gedragscode bestaan echter wel behoorlijke verschillen.[459]

---

[455] Kate Scribbins, 'Should I buy? Shopping online 2001. An international comparative study of electronic commerce', Consumers International, Office for Developed and Transition Economies 2001, p. 8. <http://www.consumersinternational.org/CI_Should_I_buy.pdf>.

[456] <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

[457] Richtlijn 2000/31/EG, *PbEG* 2000, L 178/1.

[458] Argentinië (ADELCO), Italië (Altroconsumo), Frankrijk (CLCV), Nederland (Consumentenbond), Portugal (DECO), Zwitserland (FRC), Griekenland (Kepka), Spanje (OCU), België (Test Aankoop), Verenigd Koninkrijk (Which).

[459] Zie G. Nannariello, *E-commerce and Consumer Protection: A Survey of Codes of Practice and Certification Processes*, EC-Joint Research Centre, Institute for the Protection en Security of the Citizen, Cybersecurity Sector 2001, §3.2.2. Hierin wordt ook meer in detail getreden over dit specifieke keurmerkstelsel, beschikbaar via <http://www.aptsec.org/seminar/meeting-2001/ecs2001/study%20on%20consumer%20protection.pdf>. Zie tevens M. Demoulin, *The webtrader*

Een voorbeeld van een hoog aangeschreven keurmerk is *WebTrust*.[460] Dit keurmerk is ontwikkeld door het *American Institute of Certified Public Accountants* (AICPA) en het *Canadian Institute of Chartered Accountants* (CICA). *WebTrust* biedt bedrijven een scala aan *best practices* die voor het creëren van consumentenvertrouwen dienen te zorgen. WebTrust omvat programma's op het gebied van online privacy, integriteit van transacties, veiligheid, onloochenbaarheid, vertrouwelijkheid en beschikbaarheid. De WebTrust-programma's worden momenteel aangeboden in meerdere landen, waaronder Argentinië, Australië, Canada, Denemarken, Duitsland, Frankrijk, Ierland, Italië, Nederland, Nieuw-Zeeland, Spanje, het Verenigd Koninkrijk en de Verenigde Staten.

5.6.2. Nederland

Als een van de eerste landen ter wereld[461] had Nederland een gedragscode voor elektronisch zakendoen. Deze Model Gedragscode voor elektronisch zakendoen van ECP.nl[462] beschrijft hoe bedrijven zich moeten gedragen bij het doen van zaken via het Internet. Dit beschermt niet alleen de consument, maar ook de bedrijven onderling. ECP.NL heeft in oktober 2001 een definitieve Model Gedragscode opgesteld.[463]
De Model Gedragscode is toegespitst op de praktijk en opgesteld in overeenstemming met het geldende recht. Met betrekking tot een aantal onderwerpen bevat de Model Gedragscode aanvullende regels (vergelijk bijvoorbeeld par. 5.4.2). Daar waar er sprake is van een overlapping van de inhoud van de Model Gedragscode met wettelijke regels heeft zij een voorlichtende functie. De toepasselijke wettelijke regels worden voor de gebruiker van de Model Gedragscode herhaald en geplaatst in de context van het elektronisch zakendoen temidden van regels over aanverwante onderwerpen.
De Model Gedragscode heeft een aanvullende functie indien zij regels bevat die (nog) niet in wetgeving zijn vastgelegd. Meer in het bijzonder kan daarvan sprake zijn indien de wetgever bepaalde materie niet heeft geregeld of er wettelijke regels in voorbereiding zijn maar deze nog niet van toepassing zijn. In deze laatste gevallen loopt de Model Gedragscode van ECP.nl vooruit op nieuwe wetgeving.
De Model Gedragscode is opgebouwd rond drie begrippen:

1. *transparantie*: regels voor het duidelijk, inzichtelijk, overzichtelijk en zo mogelijk verifieerbaar handelen;
2. *betrouwbaarheid*: regels voor de juistheid en volledigheid van verstrekte informatie, van systemen en organisatie; en
3. *vertrouwelijkheid en privacy*: vertrouwelijkheid van informatie en het waarborgen van de persoonlijke levenssfeer van (potentiële) handelspartners.

Deze Model Gedragscode kan als voorbeeld of als inspiratiebron dienen voor organisaties bij het opstellen van een gedragscode voor elektronisch zakendoen. Ook kan de Model Gedragscode dienen als vinklijst bij het beoordelen van de mate waarin contracten, algemene voorwaarden, reglementen en dergelijke bijdragen aan het vergroten van het onderling vertrouwen bij elektronisch zakendoen.

Een voorbeeld van een in de praktijk uitgegeven certificaat of keurmerk in het kader van vertrouwen en webhandel was het WebTrader-logo dat in Nederland door de Consumentenbond

---

Schemes: Comparative study, Analysis of the codes of practice, Université de Liège, mei 2001, <http://www.droit.fundp.ac.be/textes/webtrader.pdf>.
[460] <http://www.webtrust.org>.
[461] Voorzover bekend had Japan een jaar eerder al een gedragscode gepubliceerd.
[462] ECP.NL, het platform voor elektronisch zaken doen, is een nationaal samenwerkingsverband van partijen met als doel de versnelde en gecoördineerde invoering van elektronisch zaken doen in Nederland, <http://www.ecp.nl>.
[463] Model Gedragscode voor elektronisch zakendoen (Definitieve versie, oktober 2001), <http://www.ecp.nl/publicatie/publicaties/cocdraft4.0NL.pdf>. Er is ook een Egelse versie beschikbaar (Model Code of Conduct Draft 4.0), <http://www.ecp.nl/ENGLISH/publication/cocdraft4.0ENG.pdf>.

werd verstrekt.[464] Webtrader waakte voor consumentonveilige e-handelweblocaties. De Consumentenbond besloot echter met ingang van 1 januari 2002 te stoppen met de uitgifte van dit keurmerk. De redenen hiervoor zijn dat de Consumentenbond van mening is dat, mede dankzij de komst van het keurmerk, de discussie over consumentenbescherming op Internet is aangewakkerd, dat zelfregulering vanuit het bedrijfsleven plaatsvindt en dat het Burgerlijk Wetboek per 1 februari 2001 is aangepast met bepalingen die de bescherming van de consument bij op afstand gesloten overeenkomsten beter kunnen waarborgen dan voorheen het geval was.[465] Bovendien is er met het Thuiswinkel Waarborg-keurmerk (waaraan de Consumentenbond heeft bijgedragen) een volwaardig alternatief met een onafhankelijke geschillencommissie.[466]
Het is niet op voorhand evident dat de Nederlandse Consumentenbond zich om deze redenen zou terugtrekken uit het Webtrader-keurmerk; het betreft immers een internationaal project (zie par. 5.6.1). Diverse buitenlandse consumentenorganisaties die deelnemen in het project verwijzen nog steeds naar de Nederlandse Consumentenbond, hoewel de webstek <www.webtrader.nl> al geruime tijd niet meer bestaat. Kennelijk vindt er geen goede onderlinge afstemming plaats. Het Nederlandse webtrader-keurmerk wordt ook nog steeds door verschillende weblocaties gebruikt, maar dat blijkt na een snelle rondgang over het Internet een uitzondering te zijn.[467]

Met het wegvallen van Webtrader lijkt de weg geopend voor een wildgroei aan keurmerken. Het Nederlandse Keurmerkinstituut ziet op het Internet, naast bonafide keurmerken, ook *pseudo-keurmerken* opduiken. Dit geeft een vals gevoel van vertrouwen bij de consument. De catalogus van keurmerken, die het Keurmerkinstituut bijhoudt op zijn webstek, telt momenteel vier keer zoveel Internetkeurmerken als een jaar geleden (zie bijlage).[468] Dit wordt mede veroorzaakt door het feit dat elke subsector een eigen keurmerk lijkt te ontwikkelen; hierdoor vermindert de kenbaarheid en daarmee de zeggingskracht van keurmerken voor consumenten.

Diverse brancheorganisaties, waaronder DMSA (zie par. 5.5.2), de Nederlandse Thuiswinkel Organisatie[469] en de NLIP, hanteren gedragscodes voor de aangesloten bedrijven. Zo zijn er bijvoorbeeld gedragscodes voor de telemarketing- en postorderbranche. Bedrijven die aangesloten zijn bij de Nederlandse Thuiswinkel Organisatie bieden de consument een geschillenregeling waarop het Thuiswinkel Waarborg van toepassing is, met een onafhankelijke geschillencommissie. De gedragscode van de NLIP voor Internetaanbieders, die sinds 23 november 1999 bestaat, bevat onder andere bepalingen over bescherming van het briefgeheim, omgang met persoonsgegevens en beveiliging.[470]

Verder zijn er in Nederland overheidsinitiatieven om de elektronische handel te stimuleren en bedrijven voor te lichten.[471]

Vooralsnog lijkt het effect van keurmerken en gedragscodes alsook van overheidsregulering en -voorlichting op het gebied van consumentenbescherming nog niet volmaakt. De resultaten van een onderzoek van de Consumentenbond, die op 19 september 2001 bekend werden gemaakt, gaven aan dat Internetwinkels zich niet blijken te houden aan de nieuwe regels voor kopen op afstand. De Consumentenbond pleitte dan ook voor streng toezicht door de overheid.[472]

---

[464] Te vinden op <http://www.consumentenbond.nl> (bezocht: 14 mei 2002).
[465] Wet van 21 december 2000, Stb. 2000, 617, ter implementatie van Richtlijn 97/7/EG inzake verkoop op afstand.
[466] Persbericht Consumentenbond, *Consumentenbond stopt met Web Trader*, 5 september 2001.
[467] Zie bijvoorbeeld punt 8 onder de helpfunctie van <http://www.psxshop.nl>.
[468] <http://www.keurmerk.nl/Certificatie/Catalogus.html>.
[469] <http://www.thuiswinkel.org>.
[470] <http://www.nlip.nl>.
[471] Zie bijvoorbeeld <http://www.nederlandgaatdigitaal.nl>.
[472] Persbericht Consumentenbond*, Internetwinkels lappen wetten aan hun laars*, 19 september 2001.

5.6.3. Canada

Canada's wettelijk kader in relatie tot consumentenbescherming bestaat uit zowel federale als provinciale wetgeving. De belangrijkste federale regeling is de *Consumer Protection Act*; daarnaast bestaan allerlei sectorale wetten. De verschillende Canadese deelstaten hebben op hun beurt wetgeving in de vorm van verschillende *Consumer Protection Acts* in het leven geroepen. Het nadeel van deze verscheidenheid aan regelgeving op dit gebied is met name te vinden kwesties rondom jurisdictie. Dit laatste vergroot bij consumenten zeker niet het vertrouwen en daarom gaan er in Canada stemmen op (bij consumentenorganisaties en ook bij het *Office of Consumer Affairs*) om de provinciale wettelijke regels op het gebied van consumentenbescherming onderling te harmoniseren en tegelijkertijd deze wettelijke regelingen in overeenstemming te brengen met internationale regelgeving.[473] Daarnaast heeft een werkgroep met vertegenwoordigers van het bedrijfsleven, consumenten en de overheid eerder al richtlijnen ontwikkeld voor consumententransacties via het Internet, met de nadruk op informatieplichten en transparantie van toepasselijke regels. De richtlijnen gaan gepaard met voorlichtingspagina's op het Internet voor consumenten (*Shopping on the Internet. Get informed*) en voor bedrijven (*Your Internet business. Earning consumer trust*).[474]

Een andere, wat directere, manier om het vertrouwen van Canadese consumenten in de webhandel te vergroten is, naast voorlichting, het certificeren van deze webhandel. Verschillende keurmerkprogramma's zijn in Canada aan een opmars bezig. Inhoudelijk verschillen deze keurmerken echter nog wel eens. Zo zijn er aan de ene kant keurmerken die 'slechts' bevestigen dat het bedrijf achter een bepaalde webstek ook daadwerkelijk op het opgegeven adres bestaat, en zijn er aan de andere kant ook keurmerken die een aanbieder van elektronische handel en zijn weblocatie volledig toetsen aan bepaalde criteria.[475] Het *Canadian Institute of Chartered Accountants* (CICA) was een van de oprichters van het internationaal opererende WebTrust (zie par. 5.6.1).

Momenteel subsidieert *Canada's advanced Internet development organization* (CANARIE) het *Canadian Online Trust Project* in opdracht van *the Office of Consumer Affairs*.[476] Uitvoerder van dit project is de Canadese *Consumers' Association*; het doel is om een basis te creëren waarmee "good online business practices" worden bevorderd door middel van het certificeren van weblocaties met keurmerken. De onderliggende gedragscode is op dit moment nog niet opgesteld.

5.6.4. Duitsland

Het Bondsministerie van Wetenschap en Technologie heeft in juli 2000 in samenwerking met de werkgroep Initiative D21, die zich bezig houdt met bepaalde aspecten van de informatiemaatschappij, een aantal kwaliteitscriteria voor het elektronisch zakendoen geformuleerd.[477] Deze criteria hebben betrekking op onderwerpen als de identiteit van de aanbieder, het transactieproces, prijsinformatie en toepasselijke voorwaarden.

In totaal zijn er in Duitsland acht aanbieders van keurmerken werkzaam op basis van deze kwaliteitscriteria. Deze aanbieders worden dan ook door Initiative D21 aanbevolen. De keurmerkaanbieders zijn met Initiative D21 een overeenkomst aangegaan waarin zij verklaren dat de kwaliteitscriteria gerespecteerd zullen worden.

In Duitsland gaat men er niet van uit dat de aanpassing van wet- en regelgeving aan de Europese e-handelrichtlijn voldoende is om het vertrouwen van de consument te vergroten. De eigen verantwoordelijkheid van de markt voor de te beschermen belangen van consumenten dient een prominente plaats in te nemen in het geheel van het elektronisch zakendoen.

---

[473] Zie hierover Tasse, Faille & Henderson 2001.
[474] Industry Canada, *Principles of Consumer Protection for Electronic Commerce: A Canadian Framework*, 1999, <http://strategis.ic.gc.ca/SSG/ca01180e.html>.
[475] Meer informatie hierover is te verkrijgen op de webstek van het *Office of Consumer Affairs*, <http://strategis.ic.gc.ca/oca>.
[476] Zie <http://www.canarie.ca/press/releases/01-03-16.html>.
[477] <http://www.initiatived21.de>.

5.6.5. Frankrijk

In Frankrijk is men van mening dat er een sterke rol voor overheidsregulering moet zijn op het gebied van de elektronische handel en dat zelfregulering daaraan ondergeschikt dient te zijn. Zelfregulering kan slechts dan een mogelijke uitkomst bieden als er van overheidswege niet is voorzien in een regeling.

Men concludeert echter wel dat de groei van de elektronische handel van bedrijf naar consument (B2C) niet verder kan groeien zolang het vertrouwen van de consument in het verrichten van online betaaltransacties niet wordt vergroot. Het vergroten van dit vertrouwen geschiedt door de uitgifte van gecertificeerde keurmerken aan weblocaties door organisaties als Fia-Net[478] en WEBCERT[479]. Er is wel een wildgroei aan "valse" keurmerken waar te nemen, waartegen in januari 2002 door het Franse ministerie van Financiën is gewaarschuwd.[480]

Een veel voorkomend keurmerk in Frankrijk is *L@belsite* van het Conseil National du Commerce, Institute International du Commerce Électronique, Fédération des Enterprises du Commerce et de la Distribution (FCD) en de Fédération des Enterprises de Vente à Distance (FEVAD).[481] De gedragscode achter dit keurmerk is ook weer opgebouwd rond drie begrippen:
1. informatie over het bedrijf achter de weblocatie;
2. naleving van wetgeving;
3. transparantie.

FEVAD heeft een handvest gepubliceerd inzake kwaliteitseisen voor verkoop op afstand, waarin wordt verwezen naar Internet.[482] Dit handvest is inmiddels zeer uitgebreid en bevat naast algemene regels ook regels die betrekking hebben op specifieke bedrijfssectoren als het verzekeringswezen, het ontwikkelen van foto's[483] en *Règles spécifiques aux Colis-Epargne* (*parcel-saving*).

5.6.6. Japan

Nadat de Electronic Commerce Promotion Council of Japan (ECOM) in 1998 de *ECOM Consumer Transaction Guidelines* heeft opgesteld, lijkt het stil te zijn geworden. Wel heeft er nog een aanpassing plaatsgevonden van deze richtlijnen op basis van de OESO-*Guidelines for Consumer Protection*, maar verdere ontwikkelingen zijn uitgebleven. Het (Engelstalige) gedeelte van de ECOM-webstek over consumentenbescherming is sinds 1999 niet meer bijgewerkt.[484] Er zijn geen andere initiatieven aangetroffen op het gebied van keurmerken of op het gebied het vergroten van consumentenvertrouwen in webhandel.
In maart 2002 heeft het Japanse Ministry of Economy, Trade and Industry (METI)[485] de *Interpretative Guidelines on Electronic Commerce*[486] uitgebracht. Dit document heeft tot doel om inzichtelijk te maken hoe de bestaande Japanse wetgeving (met name de *Civil Code*) moet worden geïnterpreteerd bij verschillende juridische problemen die te maken hebben met elektronische handel. Het onderliggende doel van deze *Interpretative Guidelines* is dat zij kunnen dienen tot aanpassing van de huidige wetgeving aan het fenomeen elektronische handel. Dergelijke aanpassingen (of voorstellen daartoe) worden gemaakt door de Rule Establishment Subcommittee of the Information Economy Committee of the Industrial Structure Council.

---

[478] <http://www.fia-net.com>.
[479] <http://www.webcert.org>.
[480] Karine Solovieff, 'Un rapport dénonce les pseudo-labels de confiance', <http://www.01net.com/rdn?oid=175006&rub=2134>.
[481] <http://www.labelsite.org>.
[482] Zie <http://www.fevad.com/informer/accueilsup.asp?sup=15>.
[483] "Les entreprises s'engagent en cas de perte ou de détérioration des travaux photographiques en laboratoire à rembourser au minimum la prestation payée et à offrir une pellicule et son développement gratuit à titre de dédommagement."
[484] Zie <http://www.ecom.or.jp/ecom_e/> en tevens <http://www.ecom.jp/qecom/ecom_e/>.
[485] <http://www.meti.go.jp>.
[486] Beschikbaar via <http://www.meti.go.jp/english/information/data/c0205EleCome.pdf>.

Deze commissie wordt in haar taak met advies bijgestaan door consumentenorganisaties, handelsorganisaties en verscheidene overheidsdiensten.
Het lijkt er dus op dat in Japan de wetgeving de boventoon voert en er relatief weinig aandacht is voor zelfreguleringinitiatieven als gedragscodes en keurmerken die het vertrouwen in webhandel vergroten.

5.6.7. Verenigd Koninkrijk

TrustUK is een non-profitorganisatie, erkend door de Britse regering, die zich tot doel stelt het consumentenvertrouwen in de elektronische handel te bewerkstelligen of te vergroten.[487] Ten opzichte van de vorige *Internationale ICT-toets* is er voor TRUSTUK niets veranderd.[488]

In het Verenigd Koninkrijk wordt het webtrader-keurmerk *(Which? Webtrader Scheme)* nog steeds uitgegegeven, door de Britse consumentenbond (Consumers' Association). De *Which? Webtrader Code* is goedgekeurd door TrustUK.

5.6.8. Verenigde Staten

Ook in de Verenigde Staten is de tendens waar te nemen dat consumenten weinig vertrouwen hebben in het online winkelen. Om het elektronisch zakendoen toch te bevorderen zoeken veel Internetondernemers hun heil in keurmerken die gekoppeld zijn aan een bepaalde gedragscode.

Er zijn verschillende keurmerken en gedragscodes in omloop. De bekendste keurmerken zijn *BBBOnline*,[489] dat is gebaseerd op de *Guidelines for Merchant-to Consumer Transactions, Code of Online Business Practices* van een bedrijvencoalitie, *Betterweb* van PricewaterhouseCoopers[490] en TRUSTe[491]. De keurmerken richten zich met name op het onderwerp privacy, om langs deze weg het vertrouwen van de consument te winnen (vgl. par. 3.1.8).

5.6.9. Zweden

Over Zweden is geen materiaal aangetroffen met betrekking tot keurmerken of gedragscodes.

5.6.10. Samenvatting

In de onderzochte landen worden gedragscodes en keurmerken belangrijk geacht voor het vergroten van het vertrouwen in elektronische handel, wellicht met uitzondering van Japan en Zweden. Zelfregulering wordt aldus in de meeste landen een belangrijke rol toegedicht bij het adequaat reguleren van e-handel.
Gedragscodes kunnen – vaak in afwachting van overheidsregulering – een rol spelen bij het scheppen van rechtszekerheid voor consumenten. Naarmate er meer overheidsregulering komt, functioneren gedragscodes vooral als vertaalslag van complexe regelgeving naar de praktijk van de webhandel. Nederland heeft op het gebied van gedragscodes een voortrekkersrol gespeeld met de Model Gedragscode van ECP.nl.
Voor de zichtbaarheid van de naleving van op overheids- of zelfregulering gebaseerde minimumnormen spelen keurmerken een belangrijke rol. Met name in Canada en de VS zijn er keurmerken ontstaan als product van pure zelfregulering. In Europa worden keurmerken evenwel over het algemeen meer ondersteund door de overheid, via financiering (door de Europese Commissie van het Webtrader-netwerk), het vaststellen van kwaliteitseisen waaraan keurmerken moeten voldoen of certificatie van keurmerken (Duitsland, Frankrijk, VK) en het aanbevelen van bepaalde keurmerken die als betrouwbaar worden gezien (Duitsland).
Op het gebied van keurmerken lijkt in Nederland evenwel een stap terug te zijn gedaan door het stopzetten van Webtrader door de Consumentenbond in januari 2002. Dit kan verwarring wekken bij consumenten, nu buitenlandse organisaties nog steeds verwijzen naar de Nederlandse

[487] <http://www.trustuk.org.uk>.
[488] Over TRUSTUK zie Landwell 2000, p. 71-72.
[489] <http://www.bbbonline.org>. Zie Landwell 2000, p. 59-60.
[490] <http://www.pwcbetterweb.com>.
[491] <http://www.truste.org>.

Webtrader als internationaal afgestemd keurmerk; de onderlinge afstemming tussen de Webtraderpartijen lijkt dan ook niet groot. Bovendien groeit het aantal keurmerken de laatste tijd explosief, mede omdat elke subsector een eigen keurmerk lijkt te ontwikkelen; hierdoor vermindert de kenbaarheid en daarmee de zeggingskracht van keurmerken voor consumenten. In het buitenland is ook al geconstateerd dat de opkomst van diverse pseudo-keurmerken vertroebelend werkt. De effectiviteit van keurmerken lijkt vooralsnog dan ook niet groot.

Bijlage: Keurmerken op het Internet[492]

Animaux keurmerk
Keurmerk voor weblocaties over dieren, uitgegeven door het castingmodellenbureau voor huisdieren Animaux <www.dierencasting.nl>. Beheer: onduidelijk.

BBBOnLine
Keurmerken voor weblocaties waarop producten en diensten worden aangeboden; er zijn varianten voor betrouwbaarheid (juiste informatie geven, beloftes nakomen), privacy, en privacy van kinderen. Eigendom van en uitgegeven door BBBOnLine <www.bbbonline.org>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

Bobby
Keurmerk voor weblocaties die ook toegankelijk zijn voor gehandicapten. Eigendom van Center for Applied Special Technology <www.cast.org>. Beheer: beheerders kunnen een geautomatiseerde analyse van hun webstek laten uitvoeren, en – bij positieve uitslag – het keurmerk toepassen, en de weblocatie aanmelden voor opname in een databank op het Internet.

CaseTrust
Singaporees keurmerk voor weblocaties waar producten en diensten worden aangeboden die voldoen aan zekere eisen van duidelijkheid, veiligheid van betalingen, privacy, klachtenbehandeling en dergelijke. Eigendom van en uitgegeven door CaseTrust <www.case.org.sg>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

Clicksure
Keurmerk voor weblocaties waar producten en diensten worden aangeboden die voldoen aan zekere eisen van duidelijkheid, veiligheid van betalingen, privacy, klachtenbehandeling en dergelijke, en die beheerd worden op basis van een verantwoord kwaliteitssysteem. Eigendom van en uitgegeven door Clicksure <clicksure.com>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

EBtrust
Keurmerk voor de betrouwbaarheid van leveranciers die op het Internet producten en diensten aanbieden. Eigendom van en uitgegeven door Det Norske Veritas <www.dnv.nl>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

KeurCom
Keurmerk voor weblocaties. De criteria betreffen opmaak, navigatie en inhoud. Eigendom van en uitgegeven door KeurCom <www.keurcom.dts.nl>. Beheer: onduidelijk.

Koophits
Keurmerk voor weblocaties waar producten en diensten worden aangeboden. De criteria betreffen: veilig betalen, vertrouwelijkheid van klantgegevens, afspraken over levertijden en garantie, dienstverlening en bereikbaarheid, duidelijkheid van de webwinkel, weblocatie en te

[492] Zie <http://www.keurmerk.nl>.

leveren artikelen. Het keurmerk is verbonden aan de webstek Koophits <www.koophits.nl>. Beheer: onduidelijk.

Nationaal keurmerk internet websites
Keurmerk voor de kwaliteit van weblocaties op het Internet. Een initiatief van de Leeuwenhaeghe Groep, zie www.keurmerken.nl. Beheer: onduidelijk.

NLIP-kwaliteitskeurmerk
Keurmerk voor de kwaliteit van Internetaanbieders. Eigendom van en uitgegeven door Nederlandse Vereniging van Internet Providers <www.nlip.nl>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

SP-keur
Keurmerk voor de kwaliteit van weblocaties op het Internet. Eigendom van en uitgegeven door Startpunt Internet <startpunt.cc/spkeur>. Beheer: onduidelijk.

Square Trade
Keurmerk voor weblocaties die klantgericht zijn en bereid zijn mee te werken aan online bemiddeling bij geschillen. Eigendom van en uitgegeven door Square Trade <www.squaretrade.com>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

TNO-QMIC
Keurmerk voor betrouwbare medische informatie op het Internet, gestart in juni 2002. QMIC staat voor *Quality for Medical Information and Communication*. Door QMIC gecertificeerde webpagina's zijn te vinden via <www.gezondzoeken.nl>.

TNO Trust
Keurmerk voor de veiligheid en betrouwbaarheid van informatie, communicatie en transacties op Internet. Eigendom van en uitgegeven door TNO Preventie en Gezondheid <www.health.tno.nl>. Beheer: criteria worden opgesteld door brancheorganisaties in samenwerking met TNO; keuringen en controles worden uitgevoerd door de uitgevende instelling.

Trusted Shops
Duits keurmerk voor webwinkels die duidelijk zijn, zorgvuldig omgaan met de gegevens van hun bezoekers, en een 'niet goed – geld terug'-garantie geven. Eigendom van en uitgegeven door Trusted Shops <www.trustedshops.de>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling in samenwerking met TüV.

Trustmark
Keurmerk voor weblocaties die zorgvuldig omgaan met de gegevens van hun bezoekers; er is een speciale variant voor de privacy van kinderen. De belangrijkste eis is dat het privacybeleid op de weblocatie is in te zien, en dat men zich eraan houdt. Eigendom van en uitgegeven door TRUSTe <www.truste.org>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

TrustUK
Engels keurmerk voor weblocaties waar producten en diensten worden aangeboden die werken met een reglement (gedragscode) dat voldoet aan zekere eisen van veiligheid van betalingen, privacy, klachtenbehandeling en dergelijke. Eigendom van en uitgegeven door TrustUK <www.trustuk.org.uk>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

VeriSign Secure Site

Keurmerk voor de authenticiteit van weblocaties en de beveiliging van gegevensverkeer. Eigendom van en uitgegeven door VeriSign <www.verisign.com>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

WebAssured
Keurmerk voor de betrouwbaarheid van leveranciers die op het Internet producten en diensten aanbieden. Eigendom van en uitgegeven door WebAssured <www.webassured.com>. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling.

Web Shop keurmerk
Keurmerk voor weblocaties waarop producten en diensten worden aangeboden. De eisen betreffen onder andere de leveringsvoorwaarden, de betalingsmethode en de privacy; ze zijn grotendeels gelijk aan de eisen van WebTrader (zie hieronder). Beheer: onduidelijk, zie <www.keurmerk.info>.

WebTrader
Keurmerk voor weblocaties waarop producten en diensten worden aangeboden. De eisen betreffen onder andere de leveringsvoorwaarden, de betalingsmethode en de privacy. Voor verschillende Europese landen bestaan varianten, elk beheerd door een nationale consumentenorganisatie. De Nederlandse variant, beheerd door de Consumentenbond, is per 1 januari 2002 opgeheven. Beheer: keuringen en controles worden uitgevoerd door de uitgevende instelling; zie onder andere de WebTrader-webstek voor het Verenigd Koninkrijk <www.which.net/webtrader>.

WebTrust
Keurmerk voor weblocaties die betrouwbaar zijn (juiste informatie geven, beloftes nakomen), zorgvuldig omgaan met de gegevens van hun bezoekers, en werken met veilige betalingsmethoden <www.webtrust.org>. Beheer: American Institute of Certified Public Accountants <www.aicpa.org>; keuringen en controles worden uitgevoerd door een daartoe aangewezen accountant.

5.7. Online geschillenbeslechting

E-handel doet – veronderstellenderwijs – een behoefte ontstaan aan mogelijkheden om conflicten online te kunnen beslechten. In deze behoefte werd al enigszins voorzien door aanbieders van ADR (*alternative dispute resolution*), zoals arbitrage-instellingen. Bijzonder voor deze verslagperiode is dat nu ook enige overheidsrechters – schoorvoetend – hun eerste stapjes zetten in de wereld van de online geschillenbeslechting (zie met name de Verenigde Staten en het Verenigd Koninkrijk hierna).
Bij domeinnaamgeschillen is al behoorlijk wat ervaring opgedaan met online geschillenbeslechting. Hoewel deze geschillen enkele specifieke eigenschappen hebben, zijn ervaringen met deze procedures ook van belang voor de online geschillenbeslechting in het algemeen.

5.7.1 Internationaal

De Europese richtlijn inzake elektronische handel kent in artikel 17 enkele bepalingen over buitengerechtelijke geschillenbeslechting. Volgens het eerste lid dienen lidstaten ervoor te zorgen dat hun wetgeving geen belemmering vormt voor beslechting van geschillen tussen verleners en afnemers van diensten van de informatiemaatschappij op basis van bestaande mogelijkheden van buitengerechtelijke geschillenbeslechting. Tevens mag het gebruik van elektronische middelen voor de geschillenbeslechting geen wettelijke belemmering opleveren.
Volgens het tweede lid moedigen de lidstaten organen voor buitengerechtelijke geschillenbeslechting aan ervoor te zorgen dat passende procedurele garanties voor handen zijn; dit geldt in versterkte mate voor geschillen waarbij consumenten betrokken zijn. Ten slotte bepaalt het derde lid dat de lidstaten de organen aanmoedigen de Commissie in kennis te stellen van alle belangrijke beslissingen die zij ten aanzien van diensten van de informatiemaatschappij nemen en van alle andere informatie over de praktijk, het gebruik en de gewoonten betreffende de elektronische handel. De lidstaten (respectievelijk aanbieders van alternatieve geschillenbeslechting in die landen) dienen de bepalingen te implementeren.

Op 16 oktober 2001 is het EEJ-Net gelanceerd.[493] EEJ-Net is een Europees initiatief ter bevordering en vereenvoudiging van oplossing van grensoverschrijdende geschillen waarbij consumenten betrokken zijn. Daartoe wordt in een netwerk van nationale *clearinghouses* opgezet, die consumenten op weg helpen bij de oplossing van hun geschil door middel van ODR.

Op het gebied van domeinnamen is al meer ervaring opgedaan met ODR. Met de groei van het Internet is de spanning tussen het domeinnamensysteem en het merkenrecht toegenomen. De belangrijkste oorzaak hiervan is dat er bij een domeinregistratie niet vooraf naar mogelijke merkrechten van derden wordt gekeken. Ook de omstandigheid dat het systeem van merkenregistratie en dat van de domeinnaamregistratie van elkaar verschillen is een belangrijke oorzaak. Een merkrecht is in beginsel territoriaal begrensd. Een domeinnaam daarentegen biedt de gebruiker de mogelijkheid om wereldwijd actief te zijn. Veel zogenaamde domeinkapers hebben van de mogelijkheden van het domeinnaamsysteem gebruik gemaakt om de merken van derden als domeinnaam te registreren.
In april 1999 publiceerde de World Intellectual Property Organization (WIPO) het eindrapport van het eerste WIPO Internet Domain Name Process.[494] In dit rapport werden aanbevelingen gedaan om een alternatieve online geschillenprocedure vorm te geven. Hiermee werd recht gedaan aan het gegeven dat het voor merkhouders praktisch onmogelijk is om via de normale rechter te procederen. Procederen is vaak duurder dan een domeinkaper voor de domeinnaam te betalen, vooral wanneer de vermeende inbreukmakende domeinnaamhouder in het buitenland gevestigd is. Op basis van dit rapport is door de Internet Corporation for Assigned Names and Numbers (ICANN) – de organisatie die onder andere verantwoordelijk is voor het technische

[493] Zie <http://europa.eu.int/comm/dgs/health_consumer/newsletter/200110/02_en.htm>.
[494] Zie <http://wipo2.wipo.int/process1/report/index.html>.

systeem van het Internet – de Uniform Dispute Resolution Policy (UDRP) opgesteld.[495] De UDRP-online-geschillenprocedure is enkel gericht op de evidente gevallen van domeinnaamkaping. In juni 2002 waren er sinds de inwerkingtreding van de UDRP in december 1999 al ruim 6400 procedures[496] bij de verschillende door ICANN geaccrediteerde instituten gestart. De communicatie wordt voor het belangrijkste deel via het Internet gevoerd. Wel is het mogelijk om bepaalde stukken ook op papier aan te leveren.
Door middel van een bepaling in het registratiecontract is een domeinnaamhouder gehouden om aan de procedure mee te werken of ten minste de mogelijke overdracht van de domeinnaam te dulden. De Internetaanbieder van de verliezende domeinnaamhouder is namelijk verplicht de domeinnaam over te dragen aan de eventuele winnende eiser. Deze automatische overdracht van de domeinnaam is de belangrijkste reden van de populariteit van de procedure. Via de nationale rechter is de overdracht van een domeinnaam niet altijd zeker. Ook belangrijk is dat de procedure behoorlijk snel is.
De enige mogelijkheid een overdracht van een domeinnaam te voorkomen is om binnen 10 dagen na de uitspraak bij een nationale rechter een procedure te starten.
De procedure is van toepassing op de belangrijkste internationale domeinnamen (zoals .com, .net, .org, .biz). Enkele landencodedomeinnamen (de ccTLD's) hebben de UDRP ook aanvaard (zoals .nu, .mx en .tv). Voor verschillende andere landen zijn eigen regelingen van kracht, in sommige gevallen zijn deze op de UDRP geënt. Enkele hiervan worden hieronder besproken.

5.7.2 Nederland

Volgens de Nederlandse regering behoeft het eerste lid van art. 17 Richtlijn inzake elektronische handel geen implementatie omdat de Nederlandse wetgeving geen belemmeringen voor alternatieve geschillenbeslechting kent.[497] Wel dienen ADR-aanbieders (met name de Stichting Geschillencommissies) te bezien of hun diensten ook langs elektronische weg mogelijk gemaakt moeten kunnen worden. Ook de leden 2 en 3 van art. 17 (de Memorie van toelichting spreekt van art. 7 maar dat is een kennelijke misslag) behoeven geen implementatie van overheidswege. Onder de vleugels van ECP.nl, is een aantal brancheorganisaties ODR.nl gestart. ODR.nl heeft tot doel online afhandeling van klachten.

In Nederland is de voor de uitgifte van de .nl-domeinnamen verantwoordelijke Stichting Internet Domeinregistratie Nederland (SIDN) bezig met het opzetten van een ADR-procedure voor domeinnaamgeschillen. Eind november 2001 presenteerde het Projectteam Domeinnaamdebat het eindrapport van het in opdracht van de SIDN uitgevoerde consultatieproces.[498] Een belangrijke aanbeveling uit dit rapport is om een ADR-procedure op te richten. Deze mening wordt ondersteund door de Nederlandse overheid.[499]
Bijzonder in de voorstellen is dat er een hogerberoepsmogelijkheid wordt voorgesteld, alsook een mogelijkheid tot een kostenverdeling, dit in tegenstelling tot de eerder besproken UDRP-procedure.
Naar verwachting zal eind augustus 2002 het reglement voor de nieuwe geschillenprocedure worden vastgesteld. Op dit moment is nog onbekend wanneer de regeling van kracht zal zijn. Waarschijnlijk zal een belangrijk deel van de communicatie online plaats gaan vinden. Dit zal zeker het geval zijn wanneer men gebruik zal maken van een tweede buitenlands arbitrage-instituut. Een tweede instituut wordt voorgesteld wanneer de .nl-registratie opengesteld wordt voor buitenlandse partijen, dit om de internationale acceptatie te vergroten.[500]

---

[495] Zie <http://www.icann.org/dndr/udrp/policy.htm>.
[496] Zie <http://www.icann.org/udrp/proceedings-stat.htm>.
[497] TK 2001-2002, 28 197, nr. 3, p. 29.
[498] Zie <http://www.domeinnaam.nl>.
[499] Nota Toetsing Werkwijze SIDN, juli 2001, p. 23.
[500] Eindrapport Domeinnaamdebat, p. 38, zie <http://www.domeinnaam.nl>.

5.7.3 Canada

De vooraanstaande online geschillenbeslechter eResolution is in 2001 gestopt met zijn activiteiten.[501] eResolution is een van de geschillenbeslechters die door de ICANN zijn aangewezen om domeinnaamgeschillen onder de UDRP op te lossen. Tevens bood eResolution algemene online bemiddelings- en arbitragediensten aan.
Geschillen over .ca-domeinen kunnen binnenkort via een bemiddelings- en arbitrageprocedure worden beslecht door de Canadian Internet Registration Authority (CIRA),[502] volgens een procedure die grotendeels overeenstemt met de ICANN-procedure.[503] De procedure is alleen van toepassing wanneer een domeinnaamregistratie inbreuk maakt op merkrechten van de eiser. Er bestaat enige bezorgdheid over de objectiviteit van de procedure vanwege de mogelijkheid van *forumshoppen* naar 'merkhoudervriendelijke' arbiters.[504]

5.7.4 Duitsland

Duitsland past ter implementatie van art. 17 lid 1 Richtlijn inzake elektronische handel haar burgerlijk wetboek aan, opdat 'Schiedsvereinbarungen' (vaststellingsovereenkomsten) waarbij consumenten betrokken zijn in de toekomst ook via elektronische weg overeengekomen kunnen worden.[505]
Duitsland kent op het gebied van domeinnaamgeschillen nog geen ADR-initiatief.

5.7.5 Frankrijk

Het Franse wetsvoorstel ter implementatie van de richtlijn inzake elektronische handel kent geen bepaling over alternatieve geschillenbeslechting.[506]
Frankrijk kent op het gebied van domeinnaamgeschillen nog geen ADR-initiatief.

5.7.6 Japan

In het kader van het stimuleringsprogramma *e-Japan 2002* worden randvoorwaarden ontwikkeld om een impuls te geven aan ADR.[507] Daartoe worden de voorbereidingen voor arbitragewetgeving met meer voortvarendheid ter hand genomen. Tevens worden voorbereidingen getroffen voor een kaderwet over ADR.

5.7.7 Verenigd Koninkrijk

De Lord Chancellor's Court Service is op 4 februari 2002 het project *Money Claim Online* gestart, waarbij consumenten en kleine ondernemingen een rechtszaak online aanhangig kunnen maken en een online vonnis van een *country court* kunnen verkrijgen.[508] Het project is beperkt tot geldvorderingen tot maximaal GBP 100.000,-. Het project is een eerste stap in een ambitieus programma om de rechtbanken te moderniseren. Het loopt in ieder geval tot 16 juni 2003.
Het Britse *clearinghouse* dat participeert in EEJ-Net (zie par. 5.7.1) is inmiddels actief.[509]

Voor domeinnaamgeschillen is er ook in het Verenigd Koninkrijk een alternatievegeschillenbeslechtingsprocedure. Deze procedure is in september 2001 ingevoerd en staat open voor beweerdelijke inbreuken op een naam of een merk. Er moet hierbij sprake zijn

---

501 Zie <http://www.eresolution.ca/>.
502 <http://www.cira.ca>.
503 Zie <http://www.cira.ca/en/cat_Dpr.html>.
504 *Technology Law Update* maart 2002, p. 18.
505 Zie het *Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr* (*Elektronischer Geschäftsverkehr-Gesetz*, EGG) van 14 december 2001, *Bundesgesetzblatt* 2001, 20 december 2001, p. 3721-3728, zie <http://www.iid.de/iukdg/EGG/index.html> en <http://217.160.60.235/BGBL/bgbl1f/b101070f.pdf>.
506 Zie <http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi.htm>.
507 <http://www.kantei.go.jp/foreign/it/network/0626_e.html>.
508 'U.K. Claimants may sue in new cyber courtroom', *World Data Protection Report*, 2002/3, p. 19-20. Het *cybercourt* zelf is te vinden onder <http://www.courtservice.gov.uk/mcol>.
509 <http://www.eej-net.org.uk/index.html>.

van *abusive registration*.[510] Op dit moment zijn 55 uitspraken gepubliceerd. Een deel van de communicatie in deze procedure gaat online. Enkele stukken moeten ook op papier aangeleverd worden.

5.7.8 Verenigde Staten

In de Amerikaanse staat Michigan start in oktober 2002 een *cybercourt*.[511] Een aanpassing van wetgeving (*Michigan House Bill 4140*)[512] is daartoe noodzakelijk. Het project wordt geregisseerd door het hooggerechtshof van Michigan. Het *cybercourt* wordt bemenst met staatsrechters die ervaring hebben met handelszaken en die belangstelling hebben voor rechtsbedeling met technologische middelen. Het *cybercourt* heeft alleen jurisdictie indien beide partijen daarin toestemmen.
De *E-commerce and ADR Task Force* van de American Bar Association (ABA) heeft in maart 2002 richtlijnen opgesteld voor *best practices* in ODR.[513] Het is geen gewone gedragscode maar veeleer een meta-code aan de hand waarvan bestaande of toekomstige gedragscodes gewaardeerd kunnen worden. In de code wordt sterk de nadruk gelegd op informatievoorziening door ODR-aanbieders. De achtergrond daarvan is dat ODR nog zo nieuw en onbekend is dat het nog te vroeg is om met 'inhoudelijke standaarden' te komen. Tevens wordt voorgesteld een informatiecentrum, het iADR Center, in te richten.

5.7.9 Zweden

De Zweedse wet ter implementatie van de richtlijn inzake elektronische handel[514] kent geen bepaling over alternatieve geschillenbeslechting.[515]
In Zweden is op het gebied van domeinnaamgeschillen nog geen ADR-initiatief.

5.7.10 Samenvatting

De mogelijkheid om geschillen online te kunnen beslechten (ODR) staat sinds enkele jaren in de belangstelling. Aanbieders van alternatieve geschillenbeslechting (ADR), zoals arbitrage-instellingen, beginnen voorzichtig in een dergelijke mogelijkheid te voorzien. De Europese richtlijn elektronische handel bepaalt dat er geen wettelijke belemmeringen mogen zijn voor alternatieve geschillenbeslechting of het gebruik van ICT daarbij.
Online geschillenbeslechting verkeert nog duidelijk in de pioniersfase. Er worden wel initiatieven ondernomen, maar het lijkt er toch op dat aanbieders nog tastenderwijs hun weg aan het zoeken zijn. Ook de personen die een geschil hebben moeten hun weg naar ODR nog vinden. Het belang van informatievoorziening over ODR wordt dan ook van meerdere zijden onderstreept, bijvoorbeeld door het Europese EEJ-Net, ODR.nl en de American Bar Association, onderstreept. Het belang van adequate procedurele waarborgen bij ODR wordt ook benadrukt. Nederland heeft met ODR.nl, dat is opgezet onder de vleugels van ECP.nl en tot doel heeft de online afhandeling van klachten, een eerste stap gezet. Het VK en de VS zijn echter verder met initiatieven op het vlak van online geschillenbeslechting, waarbij bepaalde reguliere rechterlijke procedures online worden afgehandeld.

Bij domeinnaamgeschillen wordt evenwel al wel op behoorlijke schaal gebruik gemaakt van (gedeeltelijke) online geschillenbeslechting. Naast de internationale UDRP-procedure, zijn voor

---

[510] Art. 1 *DRS Policy*, zie <http://www.nic.uk/ref/drs-policy.html>.
[511] 'Michigan authorizes first-ever 'cyber-court'; online tribunal will handle business disputes', *Electronic Commerce & Law Report* 7/4, p. 73.
[512] Zie <http://www.michigancybercourt.net> en <http://www.michbar.org>.
[513] Zie <http://www.abanet.org/dispute/finaldraft.doc>.
[514] *Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster* van 6 juni 2002 (Wet op de elektronische handel en andere diensten van de informatiemaatschappij), beschikbaar via <http://.194.52.125.3>.
[515] Zie <http://europa.eu.int/comm/enterprise/tris/webdata/200274NL.doc> en <http://europa.eu.int/comm/enterprise/tris/webdata/200275NL.doc>.

vele nationale domeinnamen al procedures van kracht of wordt daaraan gewerkt.[516] Van de onderzochte landen zijn de VS en het VK hierin het verst, gevolgd door Canada en Nederland.

[516] In juni 2002 had 19% (46) van alle ccTLD's een ADR-procedure, zie <http://ecommerce.wipo.int/databases/cctld/output.html>.

5.8. Rechtsmacht en toepasselijk recht bij privaatrechtelijke geschillen

Een van de belangrijkste vraagstukken – en vermoedelijk het meest complexe – voor de internationale e-handel betreft de vraag welke rechter internationaal bevoegd en welk recht van toepassing is ten aanzien van een internationaal geschil. In deze paragraaf geven we een korte verhandeling van de problemen rondom rechtsmacht en toepasselijk recht die vanuit civielrechtelijk[517] oogpunt ontstaan bij grensoverschrijdende e-handel.
In deze paragraaf is gekozen voor een andere opzet dan bij de voorgaande onderwerpen, hoofdzakelijk omdat de kwestie binnen het beperkte bestek van dit onderzoek te complex is voor een behandeling per individueel land. We volstaan met een schetsmatige weergave van relevante problemen in de internationale context, en een voorzichtige indicatie van de (on)mogelijkheden voor internationale oplossingen.[518] Hierbij moet men in aanmerking nemen dat internationaal privaatrecht (ipr) in beginsel nationaal (of Europees) recht is, maar dat het voor de rechtszekerheid bij grensoverschrijdende elektronische handel gewenst is om internationale overeenstemming te bereiken over vraagstukken van rechtsmacht en toepasselijk recht.

5.8.1. Algemeen

Internationaal bevoegdheidsrecht (bepaling van de rechtsmacht) en het conflictenrecht (vaststelling van het toepasselijk recht) zijn verschillende, maar nauw samenhangende onderwerpen binnen het internationaal privaatrecht. In de Europese context wordt rechtsmacht bepaald door de Verordening EG/44/2001 (EEX-Vo),[519] die het Verdrag van Brussel[520] voor de meeste lidstaten heeft vervangen, en het toepasselijk recht door het Europees Overeenkomstenverdrag (EVO) uit 1980[521]. In *common law*-stelsels – waaronder de Verenigde Staten – geeft het ipr voornamelijk algemene richtlijnen voor de bepaling van de rechtsmacht en het toepasselijk recht, waarbij het resultaat sterk van de omstandigheden van het geval afhangt.

Voor wat betreft rechtsmacht kunnen onder meer algemene (denk aan de woonplaats van gedaagde of – in de VS – *doing business*) en specifieke bevoegdheidsgronden (bijvoorbeeld de plaats waar een overeenkomst is of moet worden uitgevoerd, of de plaats waar de gevolgen van een onrechtmatige daad effect hebben) een rol spelen. De systematiek in de aanwijzing van de internationaal bevoegde rechter kan in verschillende rechtsstelsels (vooral *civil law* versus *common law*) echter drastisch uiteenlopen. In de Verenigde Staten moet bijvoorbeeld rekening worden gehouden met beperkingen aan de rechtsmacht (*forum non conveniens* en *public policy*) die in het Europese systeem niet worden gehanteerd. Onder de EEX-Vo bestaan daarentegen weer bijzondere bevoegdheidsregels voor bijvoorbeeld consumentenovereenkomsten. Belangrijk is dat partijen ook een keuze voor een rechter kunnen maken door middel van een – inmiddels (bijna) wereldwijd aanvaarde – forumkeuze. Dit kan voorspelbaarheid brengen in gevallen waarin het internationaal bevoegdheidsrecht onduidelijk is. Anders dan in de Verenigde Staten, zijn de

---

[517] De strafrechtelijke jurisdictievraag is nog complexer (zie daarover par. 3.3): er wordt aangesloten bij bestaande rechtsmachtprincipes, maar de rechtsmachtproblemen die bijvoorbeeld in de Internetomgeving ontstaan (met name de interpretatie wanneer er sprake is van een handeling op een bepaald grondgebied) blijven vooralsnog grotendeels onaangeroerd.
[518] Zie hierover ook Koops e.a. 2000, p. 145-152 en Kuypers 2002.
[519] Verordening EG/44/2001 van de Raad van 22 december 2000 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, *PbEG* 2001, L 12/1, 16 januari 2001 (EEX-Vo).
[520] Verdrag inzake de rechterlijke bevoegdheid en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, Brussel, 27 september 1968, *PbEG* 1972, L 299/32. Zie ook het parallelverdrag: Verdrag betreffende de rechterlijke bevoegdheid en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, Lugano, 16 september 1988, Trb. 1989, 58 (Verdrag van Lugano).
[521] Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst, Rome, 19 juni 1980, *PbEG* 1980, L 266, p. 1.

mogelijkheden van een forumkeuze onder de EEX-Vo voor consumentenovereenkomsten evenwel beperkt.

De hoofdregel in het conflictenrecht is dat partijen het toepasselijk recht kiezen. Een rechtskeuze is gewoonlijk expliciet ("Op dit contract is Engels recht van toepassing"). Het kan echter ook in minder directe bewoordingen ("Op dit contract is het recht van toepassing van het land waar de leverancier zijn voornaamste vestigingsplaats heeft") geschieden. Bij afwezigheid van een rechtskeuze is het recht van het land dat de nauwste band heeft met de verbintenis van toepassing. De wijze waarop dit criterium wordt ingevuld, kan echter in de verschillende rechtsstelsels uiteenlopen. Voor consumentenovereenkomsten bestaat onder het EVO voorts een bijzondere conflictregel die verwijst naar het (dwingende) recht van het land van de consument. Ook in *common law*-stelsels kan de rechter bij consumentenovereenkomsten – zeker wanneer het *adhesion contracts* zijn – besluiten tot toepassing van het recht van de gewone verblijfplaats van de consument. Consumentenbescherming is daar echter niet structureel (want afhankelijk van de omstandigheden van het geval) en gebaseerd op algemene leerstukken als *unconscionability* en *public policy*. In alle gevallen (dus met of zonder rechtskeuze) kan het verwijzingsresultaat worden gefrustreerd door belangrijke regels van nationaal recht (internationaal dwingend recht of *fundamental public policies*). Gedacht moet worden aan mededingingsrecht, in- en exportbeperkingen en bijzondere regels van consumentenrecht.

Een derde dimensie van het internationaal privaatrecht is de *erkenning* en *tenuitvoerlegging* van buitenlandse vonnissen. Anders dan bij arbitragebeslissingen, waar de erkenning en tenuitvoerlegging vanwege de brede aanvaarding van het Verdrag van New York relatief eenvoudig is, is dit bij rechterlijke beslissingen over het algemeen afhankelijk van wederzijdse overeenkomsten tussen staten. Dit is anders in speciale gevallen als de EU en het Britse Gemenebest. Erkenning en tenuitvoerlegging van vreemde vonnissen levert geen specifiek door het Internet ingegeven problemen op en wordt in deze paragraaf verder buiten beschouwing gelaten.

5.8.2. Problemen bij e-handel en Internet

Het Internet roept om twee hoofdredenen vragen op omtrent rechtsmacht en toepasselijk recht. In de eerste plaats maakt het Internet het eenvoudiger om een groot aantal landen tegelijk te benaderen en aldaar goederen en diensten verhandelen. Vanwege de in aanleg a-geografische aard van het Internet is het voor iemand die iets aanbiedt op het web – zonder nadere maatregelen – niet goed te bepalen en te beheersen waar het aanbod wordt ontvangen, gelezen en aanvaard. In de tweede plaats is worden internationale overeenkomsten – anders dan voorheen – in toenemende mate afgesloten door partijen met een ongelijke marktpositie. Het aantal internationale consumentenkopen groeit sterk, en de algemene (soms ook in officieel beleid tot uitdrukking gebrachte) indruk is dat consumenten een zwakkere positie hebben dan aanbieders.[522]

Het belangrijkste pijnpunt voor het bereiken van internationale overeenstemming over regels voor de vaststelling van rechtsmacht en toepasselijk recht is het spanningsveld tussen enerzijds consumentenbescherming (gesteund door enkele machtige consumentenpleitgroepen) en anderzijds rechtszekerheid en risicobeheersing voor de bedrijven (gesteund door – mogelijk nog machtiger – marktpleitgroepen). Vanuit consumentenzijde bestaat in het bijzonder de zorg dat consumenten feitelijke rechtsgang wordt geweigerd, wanneer niet het *forum consumptoris* maar een verre en vreemde rechter internationale bevoegdheid heeft. Ook zouden consumenten de bescherming van het eigen, vertrouwde recht niet mogen worden ontzegd.
De strijd gaat er concreet om of voor online activiteiten het land-van-oorsprong-beginsel of het land-van-bestemming-beginsel moet gelden. Bij het eerste beginsel zijn online aanbieders voor

[522] Dit lijkt geen algemeen geldende aanname, aangezien er situaties zijn (bijvoorbeeld bij bedrijfjes in kleine of onderontwikkelde landen die thuisproducten aanbieden via het Internet) waarin de consument misschien de beste onderhandelingspositie heeft. Bovendien vervaagt het onderscheid tussen consument en aanbieder op het Internet, bijvoorbeeld door de opkomst van veilingweblocaties.

rechtsmacht en toepasselijk recht aangewezen op het land vanwaaruit zij hun diensten online aanbieden; bij het tweede kunnen zij worden geconfronteerd met rechtsmacht in en het recht van alle landen waarin hun online diensten worden aangeboden of waar hun online activiteiten effect hebben. In het eerste geval is het rechtsmachtrisico en conflictenrechtelijke risico van online aanbieders dus beperkt tot één land; in het tweede geval niet. In het kader van de EEX-Vo is voor de rechtsmacht ten aanzien van online consumentenovereenkomsten gekozen voor het land-van-bestemming-beginsel. Dat houdt in dat de rechter van de gewone verblijfplaats van de consument in beginsel internationaal bevoegd is, wanneer de online aanbieder zich heeft gericht op dat land. In de Verenigde Staten is voor wat betreft de forumkeuzebevoegdheid gekozen voor de belangen van de online aanbieder: deze mag – ook ten aanzien van consumenten – een keuze voor zijn eigen forum opleggen. Onder het EVO bestaat vooralsnog onduidelijkheid over de uitleg van de desbetreffende bepalingen, maar in navolging van de EEX-Vo zou een pro-consumentenuitleg ervan kunnen worden hooggehouden.
Een bijzonder geval is de Europese Richtlijn Elektronische handel, die het land-van-oorsprong-beginsel centraal stelt, maar niet tot doel heeft regels van internationaal privaatrecht te geven. Hierdoor is ten eerste onduidelijk of het land-van-oorsprong-beginsel een ipr-regel is en ten tweede wat de verhouding tussen de richtlijn en het EVO is. Aangenomen moet worden dat het land-van-oorsprong-beginsel in ieder geval niet geldt voor online consumentenovereenkomsten en gevallen waarin partijen een rechtskeuze zijn overeengekomen. Voor het overige lopen de opvattingen omtrent de desbetreffende bepalingen uiteen en draagt de richtlijn bepaald niet bij aan hetgeen daarmee wordt beoogd te creëren, namelijk rechtszekerheid.

Relevant in het kader van de rechtsmacht zijn de pogingen om binnen de Haagse Conferentie[523] tot een wereldwijd rechtsmachtverdrag te komen. Dit ambitieuze project, dat reeds is begonnen in 1992, zou moeten voorzien in op de elektronische handel gerichte bepalingen. Zo zijn in 2000 amendementen voorgesteld die voorzagen in een systeem van keurmerken voor weblocaties met een minimumniveau aan consumentenbescherming. Voor webhandelaars voorzien van een dergelijk keurmerk die tevens de mogelijkheid voor (gratis) alternatieve geschillenbeslechting aanbieden zou dan het land-van-oorsprong-beginsel gelden. Deze amendementen zijn evenwel te controversieel gebleken.[524] De hierdoor ontstane impasse is in april 2002 doorbroken met het besluit om een geheel nieuwe ontwerptekst op te stellen. Besloten is tot de formatie van een nieuw ontwerpcomité, dat begin 2003 een nieuw ontwerp moet hebben opgesteld, waarbij de meest controversiële onderwerpen achterwege zijn gelaten. Na overeenstemming over de eenvoudiger onderwerpen, kunnen vervolgens de moeilijker onderwerpen alsnog ter hand worden genomen.[525] Vanwege de controverses bestaat er weinig kans op een – alomvattend – rechtsmachtverdrag op de korte termijn. Ingevolge de toenemende internationalisering is het vanuit het oogpunt van rechtszekerheid en voorspelbaarheid niettemin van groot belang dat er een unificatie van internationaal bevoegdheidsrecht wordt bereikt.

Op het terrein van toepasselijk recht worden vooralsnog geen pogingen tot het creëren van internationale oplossingen ondernomen. Vanuit het oogpunt van *business-to-business*contracten bezien, is dit op zich niet onbegrijpelijk, aangezien er reeds eenvormig recht in de vorm van het Weens Koopverdrag bestaat. Regels van conflictenrecht zijn dan niet altijd meer noodzakelijk. De unificatie van consumentenrecht is echter een stuk problematischer en mogelijk niet goed haalbaar. Ondanks de diverse harmonisatiepogingen is er binnen de Europese Unie ten slotte ook nog sprake van duidelijke verschillen tussen het nationale consumentenrecht van de lidstaten. Wel een stap vooruit is dat op bepaalde punten op zijn minst een Europees minimumniveau van bescherming is gecreëerd. De ontwikkeling van internationaal conflictenrecht is vanuit de consumentenovereenkomst bezien aan te bevelen.

Tot slot is er nog de complicerende factor dat de discussies en ontwikkelingen zich tot nu toe vooral centreren rond rechtsmacht en toepasselijk recht bij overeenkomsten. De vragen welke

[523] Zie <http://www.hcch.net>.
[524] Zie daarover Koops e.a. 2000, p. 149.
[525] Zie *World Internet Law Report* juni 2002, p. 37-38.

rechter bevoegd is te oordelen over een onrechtmatige daad, en welk recht daarop van toepassing is, zijn tot nu toe nogal onderbelicht gebleven. Juist op het wereldwijde web, waarop van alles en nog wat wordt gepubliceerd, zullen zich veel sneller en vaker dan voorheen situaties voordoen waarin een publicatie of aanbod in een bepaald land als onrechtmatig kan worden ervaren. Een prangend voorbeeld is het internationale geschil tussen de VS en Frankrijk in de Yahoo!-zaak. De Franse rechter besloot dat het te koop aanbieden van Nazi-parafernalia op een via de webstek van Yahoo! bereikbare online veiling in Frankrijk niet is toegestaan. Yahoo! werd derhalve gesommeerd de toegang tot deze weblocatie aan het Franse publiek te ontzeggen via technische middelen. In de VS werd deze uitspraak echter beschouwd als een aantasting van de vrijheid van meningsuiting, zodat een rechter in Californië het vonnis van de Franse rechter om die reden nietig verklaarde.[526] Dergelijke tegenstrijdige uitspraken maken het onvoorspelbaar welk recht van toepassing is op publicaties op het Internet die in diverse landen toegankelijk zijn. Vanwege de grote culturele verschillen en de daarmee gemoeide uiteenlopende belangen zal het echter vrijwel onmogelijk zijn om hierover in enigermate breed verband afspraken te maken.

5.8.3. Enkele voorbeelden van aanpak

Bij afwezigheid van internationale afstemming, zullen landen in bepaalde gevallen eigen oplossingen ontwikkelen voor de vraagstukken van rechtsmacht en toepasselijk recht. Hier geven we enkele voorbeelden van richtingen die in diverse landen zijn voorgesteld.

EU

Een belangrijke recente (eerdergenoemde) ontwikkeling is dat aanbieders die met consumenten contracteren onder de EEX-Vo in beginsel gebonden zijn aan het *forum consumptoris*.[527] Als gevolg daarvan zou de aanbieder kunnen besluiten om zijn aanbod tot niet-consumenten of tot bepaalde landen te beperken. Een consument die de online aanbieder vervolgens valselijk over zijn hoedanigheid of woonplaats voorlicht, zou geen beroep op bescherming van de EEX-Vo moeten mogen doen. De keuze voor rechtsmacht van het land van de consument is toegejuicht door consumentenorganisaties, maar sterk afgekeurd door het bedrijfsleven.

Canada

Het Canadian Competition Bureau heeft ontwerprichtlijnen uitgegeven voor adverteren op het Internet, onder andere over de mate van identificatie die adverteerders in acht moeten nemen.[528] Voor toepasselijk recht is van belang dat buitenlandse adverteerders, om aansprakelijkheid onder Canadees recht te voorkomen, wordt aangeraden om duidelijk te maken tot wie de advertentie is gericht. Zij worden bijvoorbeeld geadviseerd om:

- te verzekeren dat bezoekers van de webstek hun woonplaats aangeven, zodat zij doorgekoppeld kunnen worden naar een webstek die is toegesneden op hun nationaliteit;
- de toegang tot hun weblocatie te filteren zodat alleen bezoekers komen uit landen die zij willen benaderen; en
- te verzekeren dat de woonplaats van de consument wordt aangegeven voordat een overeenkomst tot stand kan komen.

Deze adviezen tonen een soortgelijke gedachtegang als de overwegingen die ten grondslag lagen aan het debat over actieve en passieve consumenten in de EU.

Verenigd Koninkrijk

Het Department of Trade & Industry (DTI) heeft een *Guidance Note* gepubliceerd om bedrijven voor te lichten over de veranderingen die de consumentenbeschermende bepalingen van de

---

[526] Zie hierover Le Menestrel, Hunter & De Bettignies 2001.

[527] Verordening EG/44/2001 van de Raad van 22 december 2000 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, *PbEG* 2001, L 12/1, 16 januari 2001 (EEX-Vo).

[528] Competition Bureau, Industry Canada, *Staying 'On-Side' When Advertising Online: A Guide to Compliance with the Competition Act When Advertising on the Internet, Draft*, 29 mei 2001, <http://strategis.ic.gc.ca/SSG/ct02186e.html>.

EEX-Vo in de Britse wetgeving hebben bewerkstelligd.[529] Hierin wordt bijvoorbeeld een handvat gegeven voor het bepalen van de omstandigheden waaronder een weblocatie geacht kan worden gericht te zijn geweest op buitenlandse consumenten (art. 15 lid 1 onder c EEX-Vo). De enkele toegankelijkheid van een weblocatie zou hiervoor niet voldoende zijn. Relevant is bijvoorbeeld of de weblocatie iets in andere gemeenschapstalen en gemeenschapsvaluta aanbiedt, of zich beperkt tot de Engelse taal en het Britse pond; in het laatste geval kan er nauwelijks sprake zijn van een op een buitenlandse consument gerichte webstek. Ook moet worden gekeken naar de aard van de weblocatie.[530] Hiermee lijkt DTI af te wijken van het gemeenschappelijke standpunt van de Raad en de Commissie over art. 15, dat aangeeft dat de taal of de valuta hierbij geen relevante factor is.[531]

Verenigde Staten
De American Bar Association heeft in 2000 een rapport uitgebracht over wereldwijde jurisdictievraagstukken in relatie tot het Internet. Het voorstel om een wereldwijde commissie samen te stellen die uniforme beginselen voor rechtsmacht moet ontwikkelen lijkt weinig realistisch, maar een ander gedeelte van het rapport, over de rol van technologie bij de aanpak van jurisdictieproblemen, biedt interessante aanknopingspunten. Het stelt voor dat *intelligent agents* en software zodanig worden geprogrammeerd dat zij consumenten inzicht bieden in het land, de regels, de consumentenbescherming en beschikbare rechtsmiddelen, voordat zij een overeenkomst kunnen afsluiten. Verder wordt ook hier gerefereerd aan de mogelijkheid van het beperken van het online aanbod, om het rechtsmachtrisico in de hand te houden.[532]

5.8.4. Samenvatting

De vaststelling van de rechtsmacht en het toepasselijk recht roepen in relatie tot de internationale e-handel vragen op. De tegenstelling tussen het belang van rechtszekerheid voor de aanbieder en belang bij bescherming van de consument lijkt in internationaal verband, in elk geval voorlopig, niet te kunnen worden aangepakt. Tekenend is dat er binnen grootschalig internationaal verband (zoals de OESO en de Haagse Conferentie) geen vooruitgang wordt geboekt. Naar verwachting zullen de onderhandelingen binnen de Haagse conferentie niet tot een snelle afronding komen. De kans is zelfs groot dat de conferentie slechts beperkt resultaat oplevert, waarbij aan de elektronische handel gerelateerde oplossingen geheel worden vermeden. In kleiner verband (zoals in de EU) gekozen richtingen, zoals rechtsmacht in het land van de consument onder de EEX-Vo, kunnen in breder – internationaal – verband niet altijd op instemming rekenen.
Ipr-problemen spelen bij onrechtmatigedaadsituaties in versterkte mate een rol. Dit vraagstuk is tot nu toe onderbelicht gebleven en op internationaal niveau uiterst lastig aan te pakken, vanwege het bestaan van grote culturele verschillen en daarmee gemoeide uiteenlopende belangen. Ook zullen – anders dan bij overeenkomsten – over het algemeen vooraf geen afspraken zijn gemaakt in de vorm van een forum- en rechtskeuze.

Bij gebrek aan juridische initiatieven, zullen bedrijven en consumenten voorlopig genoegen moeten nemen met technische en organisatorische maatregelen. Partijen kunnen over en weer informatie uitwisselen omtrent woon- of vestigingsplaats en de inhoud van het toepasselijk recht, zodat zij tenminste een geïnformeerde keuze kunnen maken voor grensoverschrijdend contracteren. Ook kan het online aanbod uitdrukkelijk worden beperkt tot niet-consumenten of

---

[529] *Guidance Note. Cross Border Consumer Contractual Disputes: Guidance on the Rules on Jurisdiction and Applicable Law*, februari 2002, <http://www2.dti.gov.uk/CACP/ca/policy/jurisdiction/index.htm>.
[530] Overweging 1.16 van de *Guidance Note*.
[531] <http://www2.dti.gov.uk/CACP/ca/policy/jurisdiction/eustate.htm>.
[532] ABA 2000.

consumenten in bepaalde landen om het rechtsmachtrisico en het conflictenrechtelijke risico bij online consumentenovereenkomsten te beperken. In het geval van onrechtmatige daad zullen partijen naar verwachting echter weinig baat hebben bij technische en organisatorische oplossingen.

6. Conclusies

ICT-regulering beslaat een breed terrein. De zestien onderwerpen die voor dit rapport zijn onderzocht, hangen alle – direct of indirect – samen met elektronische handel, maar zijn van uiteenlopende aard. Ook de onderzochte landen, hoewel alle geïndustrialiseerd, zijn divers: er bestaan grote verschillen tussen Europa en de VS, zowel in cultuur als in beleidsopvattingen, en ook binnen de EU bestaat diversiteit aan rechtsstelsels (*common law* en *civil law*), culturele opvattingen en reguleringstradities. Japan verschilt op tal van punten van zowel de VS als van Europa. De diversiteit aan onderwerpen, maar vooral ook de diversiteit aan landen en rechtsstelsels, maken het moeilijk om uitspraken te doen over ICT-regulering in algemene zin. Het maken van vergelijkingen is slechts mogelijk als onderzoeksresultaten in verband worden gebracht met de verschillende rechtsstelsels – iets waarvoor in dit onderzoek geen ruimte was. Om deze redenen dient dit totaalbeeld te worden beschouwd als een indicatie van de belangrijkste bevindingen van het onderzoek, waarbij bevindingen tentatief met elkaar in verband worden gebracht.

6.1. Algemeen

internationale afstemming

Een belangrijk deel van ICT-regulering wordt internationaal voorbereid of aangestuurd. Dit betreft bijvoorbeeld onderwerpen met een sterke financieel-economische inslag, zoals auteursrecht en fiscale aspecten van e-handel, en onderwerpen waarbij het scheppen van rechtszekerheid voorop staat als noodzakelijke voorwaarde voor het ontstaan van grensoverschrijdende e-handel, zoals de juridische status van elektronische contracten en handtekeningen. Ook op andere, cultureel gevoeliger, punten vindt echter in belangrijke mate internationale afstemming plaats in verband met rechtshandhaving, zoals de bestrijding van computercriminaliteit en de export van cryptografie.

Over de brede linie blijkt echter op wereldwijde schaal slechts weinig overeenstemming te bereiken. Voor veel onderwerpen lopen de meningen en tradities te zeer uiteen, zodat overeenstemming slechts in kleiner verband valt te bereiken, bijvoorbeeld binnen de Europese Unie. In de EU zijn voor onderwerpen als privacy en spam, die in de VS volledig aan zelfregulering worden toevertrouwd, geharmoniseerde regelingen vastgesteld. Vrijwel alle onderwerpen uit deze studie worden in de EU op gemeenschapsniveau aangepakt; zelfs voor onderwerpen die niet tot de bevoegdheid van de EG behoren (zoals strafrecht) komen steeds meer gemeenschappelijke regelingen.

Dat neemt niet weg dat ook op EU-niveau harmonisatie in de praktijk niet overal wordt bereikt. Richtlijnen bevatten noodzakelijkerwijs herhaaldelijk compromissen die op nationaal niveau verschillend worden uitgelegd; soms ook wordt regeling bewust overgelaten aan de lidstaten. De implementatie van richtlijnen blijkt dan ook herhaaldelijk verschillend uit te pakken. Hoewel dit deels veroorzaakt zal worden door de verschillen in rechtsstelsels, ontstaat soms de indruk dat lidstaten – bewust of onbewust – kiezen voor materieel verschillende implementatie. De strafrechtelijke aansprakelijkheid van ISP's, het toezicht op niet-gekwalificeerde certificatieaanbieders en de inwisselplicht voor e-betaalsystemen zijn daar voorbeelden van. In grote lijnen wordt de regeling van de onderscheiden onderwerpen dan wel geharmoniseerd, maar op bepaalde details lijkt harmonisatie achterwege te blijven.

De internationale initiatieven zoals hier geschetst beogen grotendeels om nationale reguleringen op elkaar af te stemmen. Harmonisatie of approximatie van regulering maakt immers grensoverschrijdend handelsverkeer eenvoudiger. Een aspect dat echter minder voortvarend blijkt te kunnen worden aangepakt is het afstemmen van visies op rechtsmacht. Op strafrechtelijk niveau is de vraag wanneer een staat rechtsmacht kan uitoefenen (bijvoorbeeld als via het Internet 'elders' wordt opgespoord) niet beantwoord bij het Cybercrime-verdrag. Ook op civielrechtelijk niveau lijken de visies over de reikwijdte van rechtsmacht uiteen te lopen; binnen de Haagse Conferentie bleek over jurisdictie in relatie tot het Internet vooralsnog geen overeenstemming te bereiken.

zelf-, co- en overheidsregulering
Hoewel de meeste landen uit dit onderzoek een duidelijke voorkeur zeggen te hebben voor zelfregulering (Frankrijk is een uitzondering), valt op dat bij bijna alle onderwerpen overheidsregulering de boventoon voert. In de EU verschijnen grote hoeveelheden richtlijnen, maar ook in de VS en Canada bestaat op veel terreinen wetgeving. Deze wetgeving lijkt niet in eerste instantie het gevolg van een inzicht dat zelfregulering op de desbetreffende onderwerpen tekortschiet, maar eerder van een behoefte aan het scheppen van rechtszekerheid of het nationaal of federaal willen harmoniseren van regelgeving. Daardoor lijkt de bij wetgevers veelgehoorde voorkeur voor zelfregulering eerder een illusie dan een daadwerkelijke praktijk.
Soms wordt zelfregulering ingekaderd in overheidsregulering. Deze benadering wordt vaak aangeduid met de term 'co-regulering'. Het duidelijkste voorbeeld hiervan is de vorm van toezicht op Trusted Third Parties die Nederland en het Verenigd Koninkrijk hebben gekozen. In vergelijking met de situatie van twee jaar geleden, lijken er echter niet veel meer gevallen van co-regulering te zijn ontstaan, wanneer men co-regulering opvat als een vorm van regulering waarbij naleving kan worden afgedwongen.[533] Een andere vorm van co-regulering is het betrekken door overheden van 'de markt' bij het nader vormgeven of invullen van regelgeving; deze vorm lijkt wel vaker voor te komen. Bij het inrichten van de 'elektronische overheid', bijvoorbeeld in het faciliteren van elektronische communicatie met de overheid, blijkt een duidelijke rol te worden toebedeeld aan marktpartijen.

Ondanks de vrijwel alomtegenwoordige regelgevingsijver, blijft er tussen de onderzochte landen wel een verschil bestaan in de mate van zelfregulering die wordt toegestaan. Vooral in de VS worden enkele onderwerpen voor een belangrijk deel aan zelfregulering overgelaten die de EU heeft gereguleerd. Het gaat om onderwerpen als privacy en ongevraagde e-reclame (spam), waarbij de balans tussen vrije markt en rechtsbescherming in de VS grotendeels doorslaat naar het eerste en in de EU naar het tweede. Daar staat tegenover dat de VS op enkele andere punten (elektronisch contracteren door *agents* en de procedure om mogelijk onrechtmatig materiaal van het Internet te verwijderen) een bredere regeling kent dan de EU, wellicht omdat de praktijk hier in de VS een roep om rechtszekerheid kent die in de EU nog weinig wordt gehoord.
Overigens zijn ook binnen de EU duidelijke verschillen zichtbaar in de mate van zelfregulering: Frankrijk en in mindere mate Duitsland tenderen meer naar een primaire voorkeur voor overheidsregulering, terwijl het VK en Nederland (zeggen) een voorkeur (te) hebben voor zelfregulering. Bij de onderwerpen waarbij zelfregulering een rol kan spelen, heeft de VK in de praktijk wellicht nog iets meer een 'light touch'-benadering dan Nederland, bijvoorbeeld door het ongereguleerd laten van ongevraagde e-reclame.

Slechts op enkele punten lijken verschuivingen zichtbaar sinds twee jaar geleden. In de VS staat de onverkorte voorkeur voor zelfregulering bij privacy ter discussie, en in de EU is recentelijk het grotendeels overlaten aan de markt van spamregulering (via een opt-outsysteem) losgelaten ten behoeve van consumentenbescherming (via een verplicht opt-insysteem).
De verschuivingen op deze twee onderwerpen lijken zich vooral te laten verklaren door het inzicht in de (non-)effectiviteit van zelfregulering. Op het gebied van spam hebben de opt-outsystemen nauwelijks effect gehad om dit fenomeen te beteugelen. Ook de Safe Harbor Principles (die voor bedrijven in de VS een EU-rechtbestendige haven voor persoonsgegevens moeten creëren) lijken in de praktijk (nog) niet echt te werken. Er zijn evenwel geen aanwijzingen dat dergelijke bevindingen hebben geleid tot een veranderd inzicht in de algemene rol van zelfregulering.

Een ander aspect dat naar voren komt in het onderzoek is de rol die overheden spelen bij de actieve voorlichting aan burgers over ICT-regulering. Voor de effectiviteit van regulering die beoogt consumenten of burgers te beschermen is het van belang dat deze kennis en inzicht hebben in hun rechten en plichten. Op enkele terreinen blijken sommige overheden dan ook voorlichtingscampagnes te (willen gaan) voeren. Men ziet dit met name op het gebied van veilig

[533] Zoals gehanteerd in Landwell 2000, p. 8; dit rapport concludeerde reeds dat TTP's het onderwerp was waarbij co-regulering het dichtst benaderd werd.

Internetgebruik (Nederland, Canada, Duitsland, VS), elektronische handtekeningen (Canada, Japan) en privacy (Duitsland, Frankrijk, Nederland). Het gaat echter om enkele onderwerpen, die elk bovendien in lang niet alle landen worden opgepakt; over het algemeen lijken overheden zich niet actief in te spannen om via het Internet mensen bewust te maken van (de rechten en plichten van) ICT-regulering. De taak van voorlichting wordt voor een deel overgenomen door private instanties, zoals burgerrechtenorganisaties en brancheverenigingen. In het algemeen lijkt het erop dat overheden vooralsnog de publicatiemogelijkheden van nieuwe media niet aangrijpen om een actief voorlichtingsbeleid over de complexe ICT-regulering te voeren.

6.2. Positie van de diverse landen

Het globale beeld dat rijst uit het onderzoek is dat de stand van zaken in de vijf onderzochte EU-lidstaten over het algemeen onderling niet wezenlijk verschilt. ICT-regulering in de VS wijkt op diverse punten af van de situatie in Europa, terwijl Canada nu eens dichter bij de VS en dan weer dichter bij Europa staat. Japan kent voor een deel vergelijkbare regulering, maar voor een ander deel ook niet.

Meer in detail blijken binnen de EU wel verschillen te bestaan, niet alleen in de mate van zelf- of co-regulering (zie boven) maar ook in de aanpak van ICT-regulering. Nederland was het eerste land van de vijf onderzochte landen met een overkoepelende analyse van en visie op ICT-regulering (met de Nota WES uit 1998 en de nota IRIM uit 2000); meer recent heeft het VK iets soortgelijks, zij het minder uitgebreid, gedaan (de *E-Policy Principles* en de coördinatie door de e-Minister en e-Envoy), terwijl Frankrijk met het *Projet de loi sur la société de l'information* uit 2001 een poging heeft gedaan tot een meer overkoepelende regulering (die vooralsnog is gestrand door de verkiezingen). Nederland lijkt daarom meer dan de andere landen te hebben nagedacht over een integrale visie op ICT-regulering, hetgeen ook geldt in vergelijking met de VS, Canada en Japan. Daar staat tegenover dat de concrete regulering in Nederland vaak later tot stand komt dan in andere EU-lidstaten. Nederland loopt achter bij de implementatie van veel ICT-gerelateerde richtlijnen ten opzichte van de andere onderzochte landen (bescherming persoonsgegevens, elektronische handel, elektronische handtekeningen, elektronisch geld, auteursrecht in de informatiemaatschappij). Andere lidstaten (zoals het VK bij de e-handelrichtlijn) kiezen juist bewust voor snelle implementatie om tijdig rechtszekerheid te bieden en daarmee een aantrekkelijk klimaat voor nieuwe e-handelaars te scheppen.

Waar Nederland in de EU opvalt door een integrale visie en vaak trage wetgeving, valt verder vooral het VK op als de lidstaat waar een klimaat met een 'light regulatory touch' heerst; dit blijkt bijvoorbeeld uit het besluit de wettelijke bepalingen over toezicht op cryptografiedienstaanbieders vooralsnog niet van kracht te laten worden wegens het bestaan van een adequate zelfregulering. De lichte toets geldt evenwel met name voor direct e-handelgerelateerde regulering; op het punt van strafrechtelijke handhaving en terrorismebestrijding lijkt het VK juist repressiever dan de andere lidstaten (met uitzondering van Frankrijk).

De positie van de VS verschilt in twee opzichten van die van de EU, die mede samenhangen met het verschil in inzicht van beiden in de mogelijkheden van zelfregulering, maar ook in rechtsstelsels. Enerzijds laat de VS regulering op sommige terreinen (zoals privacy en spam) grotendeels over aan de markt, waar de EU rechtsbescherming laat prevaleren ten faveure van overheidsregulering; soms ook, zoals bij elektronische handtekeningen, kiest de VS voor een globale kaderregeling, waar de EU ten behoeve van rechtszekerheid ook een meer gedetailleerde regeling heeft. Anderzijds kent de VS op andere terreinen, vaak samenhangend met een behoefte bij het bedrijfsleven aan rechtszekerheid, juist een meer uitgewerkte of bredere regulering dan de EU; het reguleringskader voor elektronische contracten en e-betaalsystemen zijn daar voorbeelden van. Tevens lijkt de VS (vermoedelijk omdat de technologische ontwikkeling daar iets voorloopt op die in de EU) aandacht te hebben voor nieuwe ICT-ontwikkelingen (zoals *agents*) die in de EU-regulering nog niet zijn doorgedrongen; ook de aandacht voor nieuwe bedreigingen (zoals identiteitsfraude, de privacy van kinderen op het Internet en het toezicht op aftappen van Internetverkeer) lijkt in de VS groter dan in de EU. Al deze verschillen nemen overigens niet weg dat op bepaalde terreinen de aanpak van de VS en van de EU wel

overeenkomt, terwijl er ook wel wederzijdse pogingen worden ondernomen om dichter bij elkaar te komen.
De positie van Canada weerspiegelt de traditionele verbondenheid van dit land met zowel de VS als Europa. Op sommige terreinen overheerst de marktwerking en is de ICT-regulering vergelijkbaar met die in de VS (zoals e-handtekeningen en spam); op andere terreinen is evenwel de rechtsbescherming belangrijker en lijkt de regulering meer op die in de EU (zoals privacy).
De positie van Japan lijkt over het algemeen volgend te zijn. Op enkele terreinen voert Japan wetgeving door in navolging van internationale afspraken (zoals bij auteursrecht, cryptografie) of in verband met internationale ontwikkelingen (zoals aansprakelijkheid van Internetaanbieders, computercriminaliteit). Bepaalde onderwerpen, zoals regulering van elektronische overeenkomsten, e-betalen en cryptografie, lijken in Japan geen grote rol te spelen, en in het onderzoek zijn geen opvallende Japanse initiatieven of innovatieve standpunten op het gebied van ICT-regulering aangetroffen. De situatie van Japan is overigens vergelijkbaar met die van Zweden, waar evenmin opvallende initiatieven zijn aangetroffen. Hieraan kunnen evenwel geen scherpe conclusies worden verbonden, aangezien het onderzoek voor deze landen beperkt was tot vertaald materiaal.
Concluderend kan men stellen dat de positie van Nederland op ICT-reguleringsgebied internationaal gezien grotendeels vergelijkbaar is met die van de andere EU-lidstaten en op diverse vlakken afwijkt – soms meer, soms minder – van die van de VS. Nederland valt internationaal vooral op door het nadenken over een integrale visie en een vaak wat trage wetgeving. Enkele nieuwe onderwerpen (zoals *agents*, identiteitsfraude, privacy van kinderen op het Internet en toezicht op Internettaps) staan in andere landen wel maar in Nederland nog nauwelijks op de agenda.

Afkortingen

ABA	American Bar Association
ADR	alternatieve geschillenbeslechting (Alternative Dispute Resolution)
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
CA	certificatieaanbieder
C.F.R.	Code of Federal Regulations
CSP	certificatiedienstaanbieder (Certification Service Provider)
DMCA	Digital Millennium Copyright Act
DRM	Digital Rights Management
DTI	Department of Trade and Industry
ECP.NL	Electronic Commerce Platform Nederland
EEJ-Net	European Extra-Judicial Network
EER	Europese Economische Ruimte
EEX-Vo	Verordening EG/44/2001 van 22 december 2000 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken
EG	Europese Gemeenschap
EU	Europese Unie
FTC	Federal Trade Commission
ICANN	Internet Corporation for Assigned Names and Numbers
ipr	internationaal privaatrecht
ISP	Internetdienstaanbieder (Internet Service Provider)
ivd	inlichtingen- en veiligheidsdienst
JBZ	Justitie en Buitenlandse Zaken
NLIP	Brancheverenigingen van Nederlandse Internet Providers
ODR	online geschillenbeslechting (Online Dispute Regulation)
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
OJ	Official Journal
PbEG	Publicatieblad van de Europese Gemeenschappen
RIPA	Regulation of Investigatory Powers Act 2000
SHP	Safe Harbor Principles
Stb.	Staatsblad
TK	Tweede Kamer
Trb.	Tractatenblad
TTP	Trusted Third Party
UCITA	Uniform Computer Information Transactions Act
UDRP	Uniform Dispute Resolution Policy
UETA	Uniform Electronic Transactions Act
UNCITRAL	United Nations Commission on International Trade Law
VK	Verenigd Koninkrijk
VS	Verenigde Staten van Amerika
Wbp	Wet bescherming persoonsgegevens
WIPO	World Intellectual Property Organisation
Wiv	Wet op de inlichtingen- en veiligheidsdiensten 2002

Literatuur

Aalberts & Van der Hof 1999
B. Aalberts, S. van der Hof, *Digital Signature Blindness*, Deventer: Kluwer 1999.

ABA 2000
ABA Global Cyberspace Jurisdiction Project, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. London Meeting Draft*, <http://www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf>.

Ackerman e.a. 2001
R.E. Ackerman e.a., 'Tax Notes International', in: *Ernst & Young's Comments Regarding the OECD Discussion Draft on PEs and E-Commerce*, 2001, p. 1465-1484.

Baker & McKenzie 2000
Baker & McKenzie, *Internet Banking – Key Legal Considerations. Regional Overview – Japan*, 2000.

Baker & McKenzie 2001
Baker & Mckenzie, *Doing E-commerce in Europe*, 2001.

Böhle & Krueger 2001
K. Böhle & M. Krueger, *Payment Culture Matter, A comparative EU-US perspective on Internet payments*, Electronic Payment Systems Observatory (ePSO), Background Paper No. 4, augustus 2001, <http://epso.jrc.es/Docs/Backgrnd-4.pdf>.

Brenner 2001
Susan W. Brenner, 'State Cybercrime Legislation in the United States of America: A Survey', in: *The Richmand Journal of Law and Technology* Vol. 7, No. 28 (Winter 2001), <http://law.richmond.edu/jolt/v7i3/article2.html>.

Committee on Payment and Settlement Systems 2001
Committee on Payment and Settlement Systems, *Survey of electronic money developments*,, november 2001, p. 16, <http://www.bis.org/publ/cpss48.pdf>.

Doernberg e.a. 2001
R.L. Doernberg e.a., *Electronic Commerce and Multijurisdictional Taxation*, The Hague: Kluwer Law International 2001.

FSA 2001
Financial Services Authority, *Regulation of Electronic Money Issuers, CP117*, <http://www.fsa.gov.uk/pubs/cp/cp117.pdf>.

FSA 2002
Financial Services Authority, *Regulation of Electronic Money Issuers, feedback on CP117* , <http://www.fsa.gov.uk/pubs/policy/ps117.pdf>.

FTC 2000a
Federal Trade Commission, *Fair Information Practices in the Electronic Marketplace*, 22 mei 2000, <http://www.ftc.gov/os/2000/05/index.htm#22>.

FTC 2000b
FTC, *Online Profiling. A Report to Congress*, 2000, <http://www.ftc.gov/os/2000/07/onlineprofiling.htm>.

Le Goueff 2001
S. Le Goueff, 'Offering Financial Services on the Web: Experiencing the World Wide (Legal) Web', *World Internet Law Report* 2002/1.

HM Treasury 2001
HM Treasury, *Implementation of the Electronic Money Directive, a Consultation Document*, oktober 2001, <http://www.hm-treasury.gov.uk/mediastore/otherfiles/e_money.pdf>.

HM Treasury 2002
HM Treasury, *Implementation of the Electronic Money Directive, A Response to Comsultation*, 2002, <http://www.hm-treasury.gov.uk/mediastore/otherfiles/emoney_response.pdf>.

Internationale ICT-toets 2000
Ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijkrelaties, Financiën, Justitie, Onderwijs, Cultuur en Wetenschappen en Verkeer en Waterstaat, *Internationale ICT-toets 2000*, Den Haag 2000.

Käbisch & Unruh 2000
V. Käbisch & M. M. Unruh, ITM, *Law & Technology Convergence – Tax*, ESPRIT Project 27028, Electronic Commerce Legal Issues Platform 2000.

Kaspersen 2002
R. Kaspersen, 'Het Cybercrime-Verdrag van de Raad van Europa', in: J.E.J. Prins e.a. (red.), *Recht & Informatietechnologie*, Den Haag: Sdu (losdelig), par. 9.5.

Kemmeren 2001
E.C.C.M. Kemmeren, *Principle of Origin in Tax Conventions, A Rethinking of Models* (diss. Tilburg), 2001.

Koops e.a. 2000
B.J. Koops e.a. (eds.), *ICT Law and Internationalisation. A Survey of Government Views,* The Hague: Kluwer Law International 2000.

Koops 2000
B.J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000.

Koops 2002
B.J.Koops, *Crypto Law Survey*, <http://rechten.kub.nl/koops/cryptolaw/index.htm>, versie 20.0, maart 2002.

Krueger 2001
M. Krueger, *Innovation and Regulation, The Case of E-Money Regulation in the EU*, Electronic Payment Systems Observatory (ePSO), Background Paper No. 5, augustus 2001, p. 19, <http://epso.jrc.es/Docs/Backgrnd-5.pdf>.

Kuypers 2002
Pieter Kuypers, 'Internationaal privaatrecht', in: J.E.J. Prins e.a. (red.), *Recht & Informatietechnologie*, Den Haag: Sdu (losdelig), par. 7.5.

Landwell 2000
Landwell B.V. Advocaten en Notarissen, *Beleidsinitiatieven en ICT – een overzicht van initiatieven op het geibed van wetgeving en zelfregulering in Duitsland, Finland, Frankrijk, Nederland, het Verenigd Koninkrijk, de Verenigde Staten, Zweden en Japan, in opdracht van het ministerie van EZ*, oktober 2000, <http://www.ez.nl/publicaties/pdfs/05R115.pdf>.

Lelieveldt 2001

S. Lelieveldt, 'Why is the electronic Money-Directive Significant?', *Electronic Payment Systems Observatory Newsletter* 2001/7, <http://epso.jrc.es/>.

Lodder & Bergfeld 2002
A.R. Lodder & J.P.R. Bergfeld, 'De moeizame strijd tegen spam', *NJB* 2002/22, p. 1050-1057.

Menais 2001
A. Menais, *Decree n°2001-272 of 30 March 2001 taken for the application of article 1316-4 of the French Civil Code and relating to electronic signatures*,
<http://www.juriscom.net/en/pro/1/ec20010720.pdf> (laatst bezocht 13 mei 2002).

Le Menestrel, Hunter & De Bettignies 2001
Marc Le Menestrel, Mark Hunter & Henri-Claude de Bettignies, *Internet e-ethics in Confrontation with an Activists' Agenda: Yahoo! on Trial*,
<http://www.econ.upf.es/deehome/what/wpapers/postscripts/577.pdf>.

OECD 2001a
OECD, *Taxation and Electronic Commerce, Implementing the Ottawa Taxation Framework Conditions*, Parijs: OECD 2001.

OECD 2001b
OECD, *Draft Contents of the 2002 update to the Model Tax Convention*, Parijs: OECD 2 oktober 2001, p. 19-22.

Palme 2000
J. Palme, *Freedom of Speech, The EU Data Protection Directive and the Swedisch Personal Data Act*,
<http://dsv.su.se/jpalme/society/eu-data-directive-freedom.html>, laatst gewijzigd: 9 juni 2000.

Prins 2002
J.E.J. Prins (ed.), *E-Government and its implications for administrative law. Regulatory initiatives in France, Germany, Norway and the United States*, The Hague: TMC Asser Press 2002.

Registratiekamer 2000
Registratiekamer, 'Klant in het web' (Achtergrondstudies en verkenningen 17, juni 2000,
<www.cbpweb.nl>.

A. Rossnagel, A. Pfitzmann & H. Garstka, *Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern*, 12 november 2001, p. 153-168.
<http://www.bmi.bund.de/Annex/de_11659/Download.pdf>.

Schudelaro 2002
Ton Schudelaro, 'Elektronisch geld in de Wet Toezicht Kredietwezen: Gegoochel met definities', te verschijnen in *Nederlands Juristenblad* 2002.

Sieber 2002
U. Sieber, 'Responsibility of Internet Providers: Comparative Analysis of a Basic Question of Information Law', in: E. Lederman & R. Shapira (eds.), *Law, Information and Information Technology,* The Hague: Kluwer Law International 2002, p. 231-292.

Sprague & Boyle 2001
G.D. Sprague & M.P. Boyle, 'General Report', in: *International Fiscal Association, Taxation of Income Derived from Electronic Commerce, Cahiers de Droit Fiscal International*, Volume LXXXVIa, Deventer: Kluwer 2001, p. 21-63,

Strunk 2000

G. Strunk, 'Possible Solutions for Basic Problems. A German View', *Tax Planning International E-Commerce* 2000/2, p. 9-17.

Taft 2000
J. Taft, *Uniform Money Services Act Covers Stored Value and Other Internet-Based Payments*, augustus/september 2000, <http://www.securitization.net/knowledge/legal/uniform.asp>.

Tassé, Faille & Henderson 2001
R. Tassé, M. Faille & G.L. Henderson, 'Online Consumer Protection: a Study on Regulatory Jurisdiction in Canada, prepared for the Office of Consumer Affairs', Industry Canada: juli 2001.

Truche 2002
Pierre Truche, Jean-Paul Faugère & Patrice Flichy, *Livre blanc sur l'administration électronique et la protection des données personnelles*, Paris: Ministère de la fonction publique 26 februari 2002, <www.fonction-publique.gouv.fr/communications/rapports/rapports_index.htm>.

Van der Hof 2001
Simone van der Hof, 'Regulering van elektronische handtekeningen', in: D.D. Dielissen-Breukers e.a. (red.), *JUVAT-dag 2001, Bundeling van lezingen gehouden op 26 april 2001*, WLP Tilburg 2001, p. 35-44.

Van der Hof 2002
Simone van der Hof, *Digital Signature Law Survey*, 2002 <http://rechten.kub.nl/simone/ds-lawsu.htm>.

Zila 2000
J. Zila, 'Zweden', in: P.J.P.Tak (red.), *Heimelijke opsporing in de Europese Unie. De normering van bijzondere opsporingsmethoden in de landen van de Europese Unie*, Antwerpen/Groningen: Intersentia rechtswetenschappen 2000, p. 761-814.

Auteurs

Het onderzoek is uitgevoerd door het Centrum voor Recht, Bestuur en Informatisering (CRBI) van de Katholieke Universiteit Brabant (KUB, vanaf 1 september 2002 Universiteit van Tilburg geheten), met medewerking van het Fiscaal Instituut Tilburg van de KUB en het Instituut voor Informatierecht van de Universiteit van Amsterdam.

Ot van Daalen is student informatierecht aan de Universiteit van Amsterdam. Hij onderzoekt vooral de verhouding van het mededingingsrecht en de intellectuele eigendom in de informatiemaatschappij. Daarnaast is hij freelance computerprogrammeur.

Mr. Marcel Dellebeke is onderzoeker bij het CRBI van de KUB. Hij onderzoekt de mogelijkheden en kaders voor regulering van commerciële communicatie via nieuwe media.

Mr. Mireille van Eechoud is onderzoeker aan het Instituut voor Informatierecht, met bijzondere aandacht voor intellectuele eigendom en internationaal privaatrecht, en toegang tot overheidsinformatie.

Mr. Bastiaan Garnier is toegevoegd onderzoeker bij het CRBI van de KUB en specialiseert zich in auteursrecht en elektronische media.

Mr. Simone van der Hof is onderzoeker bij het CRBI van de KUB. Zij onderzoekt onder andere internationaal privaatrecht bij online overeenkomsten, elektronische handtekeningen en openbaarheidsvraagstukken.

Prof.mr. Eric Kemmeren is hoogleraar internationaal belastingrecht (met bijzondere aandacht voor ICT-aspecten) aan het Fiscaal Instituut Tilburg van de KUB en is tevens wetenschappelijk adviseur van Ernst & Young Belastingadviseurs.

Dr. Bert-Jaap Koops is universitair hoofddocent bij het CRBI van de KUB. Hij onderzoekt vooral computercriminaliteit, opsporing & privacy, digitale grondrechten, cryptografie, elektronische handtekeningen en ICT-reguleringsvraagstukken.

Dr. Chris Nicoll is *senior lecturer* bij de afdeling Commercial Law van de Universiteit van Auckland, Nieuw-Zeeland. Hij specialiseert zich in verzekeringsrecht en maritiem recht, toegepast op juridische vraagstukken rond elektronische handel.

Mr. Gert-Jan van Norden is onderzoeker en docent bij het Fiscaal Instituut Tilburg van de KUB, alsmede deeltijd-belastingadviseur bij KPMG Meijburg & Co. te Rotterdam. Hij is gespecialiseerd in omzetbelasting.

Mr.dr. Sjaak Nouwt is universitair docent bij het CRBI van de KUB. Zijn onderzoeksactiviteiten liggen vooral op het terrein van het privacyrecht, waaronder privacy op het Internet en privacy in de gezondheidszorg.

Prof.mr. Corien Prins is hoogleraar recht en informatisering bij het CRBI van de KUB. In haar onderzoek richt zij zich momenteel op internationale regulering van ICT, de elektronische overheid en vraagstukken rondom identiteit en anonimiteit in een elektronische omgeving.

Dr. Maurice Schellekens is postdoc bij het CRBI van de KUB. Hij onderzoekt vooral aansprakelijkheidsvraagstukken, intellectuele eigendom en reguleringsvraagstukken.

ir. Ton Schudelaro is assistent in opleiding bij het CRBI van de KUB. Zijn promotieonderzoek richt zich op elektronische betaalsystemen en witwassen.

Mr. Arno Smits is assistent in opleiding bij het CRBI en de vakgroep strafrecht van de KUB. Zijn promotieonderzoek richt zich op aftappen in Nederland.

Berend de Vries is junior-medewerker bij het CRBI van de KUB. Hij houdt zich onder andere bezig met domeinnaamrecht en online geschillenbeslechting.