

Marike Vermeer en Tina van der Linden: Internetrecht.

In: F.W. Grosheide (red.), Hoofdstukken Communicatie- en mediarecht, 2e druk, najaar 2006.

6. Grenzen aan de communicatievrijheid op het Internet

6.1 Regelgeving voor het Internet?

Wat betreft de vraag of het Internet gereguleerd dient te worden, en zo ja hoe, lopen de meningen zeer uiteen. Aan de ene kant wordt betoogd dat het Internet in het geheel niet gereguleerd dient te worden. De grondgedachte van de Internetpioniers was dat informatie vrij moest kunnen stromen zonder gehinderd te worden door allerlei regels van overheidswege.¹ Variant op deze grondgedachte is de opvatting dat het Internet weliswaar regels behoeft maar dat dat in de vorm van zelfregulering in plaats van overheidsregulering dient plaats te vinden.² Anderen zien zelfregulering juist weer helemaal níet zitten.³

De algemene opvatting is echter dat het Internet beslist geen “rechtsvrije ruimte” is en wel (enige mate van) regulering behoeft,⁴ al was het alleen maar om maatschappelijk ongewenste verschijnselen, zoals het verspreiden van kinderporno, aan banden te kunnen leggen. De vraag is alleen *hoe* het Internet gereguleerd dient te worden. Hier kunnen drie niveaus van regelgeving worden onderscheiden, nl. supranationale en nationale regelgeving en zelfregulering.

Eerste niveau van regelgeving voor het Internet is die van supranationale regelgeving in de vorm van een verdrag of andere internationale afspraken. Een internationaal verdrag over de aspecten van het gebruik van het Internet zou in beginsel de ideale regulering van het Internet betekenen. Echter, normen en waarden en rechtsopvattingen over bepaalde zaken, bijvoorbeeld over de grenzen aan de vrijheid van meningsuiting,⁵ lopen in de wereld nogal uiteen en zullen nooit met elkaar te verenigen zijn. Het is daarom niet realistisch te verwachten dat er een dergelijk wereldwijd “Internet-verdrag” opgesteld zal gaan worden.

Tweede niveau van regulering is die van de nationale regelgeving. Deze kan weer onderscheiden worden in de toepassing van bestaande regelgeving op het Internet en het opstellen van nieuwe nationale specifieke Internet regelgeving. Het opstellen van specifieke Internet-regels wordt niet door een ieder noodzakelijk geacht. Door sommigen wordt betoogd dat het Internet niet wezenlijk anders is dan andere mediavormen en dat de bestaande nationale wetgeving daarom voldoende bescherming biedt.⁶ Anderen zijn van mening dat het Internet wél wezenlijk verschilt van andere mediavormen, en

¹ Het meest expliciet is wel “A Declaration of the Independence of Cyberspace” van John Perry Barlow, te vinden op <http://homes.eff.org/~barlow/Declaration-Final.html>.

² Johnson en Post, (1996), pp. 1367-1411. Johnson en Post betogen dat Cyberspace een “ruimte begrensd door computerschermen en paswoorden” is en dat deze zijn eigen regels, anders dan die van de “fysieke wereld” verdient. De gebruikers zelf zouden de enigen moeten zijn die regels kunnen opstellen.

³ Zie bv. Katherine C. Sheehan, Predicting the future: personal jurisdiction for the twenty-first century, University of Cincinnati, 1998. 66 U. Cin. Law Review 385, te vinden op <http://cyber.law.harvard.edu/property00/jurisdiction/sheehan.html>: “*The internet is not a community that can and should be trusted to govern itself. It is not a community at all, separate from the real world communities to which it users belong. First of all, the internet was constructed by, and remains dominated by, a small class of financially, intellectually, ethnically, and racially elite American users who are disproportionately young males with access to expensive computer equipment and the time to use it. At best allowing these persons to make the rules for cyberspace would be like allowing the guys with the coolest cars to make the rules for the highway.*”

⁴ Zie Lucas, (1998), pp 15, “.. *the question is obviously futile to those who talk about cyberspace without sovereignty, seen as a “lawless” zone to be regulated by ethics alone. However this view, which reflects the myth of the pioneers of the Internet, is too naïve to be convincing.*”

⁵ Zelfs tussen twee westerse landen als Frankrijk en Amerika bestaat hierover al een fundamenteel verschil van mening, getuige de Yahoo-zaak: TGI Paris, Ordonnance de référé du 20 nov. 2000 <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm>, versus het oordeel van de Amerikaanse rechter: Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme, F.Supp.2d, 2001 WL 1381157 (N.D.Cal. Nov. 7, 2001) te vinden op <http://cyber.law.harvard.edu/stjohns/Yahoo.html>, zie ook <http://www.cdt.org/jurisdiction/011107judgement.pdf>.

⁶ Zie hiervoor Jack L. Goldsmith, Against Cyberanarchy, in: Adam Thierer and Clyde Wayne Crews Jr. (eds.), Who Rules the Net? Internet Governance and Jurisdiction, CATO Institute, Washington D.C. 2003, pp. 31-70.

dat bestaande rechtsregels geen oplossing bieden voor met name grensoverschrijdende problemen.⁷ Het probleem doet zich vooral voor als het oordeel over wat wel en wat niet door de beugel kan, van land tot land verschilt, zowel strafrechtelijk (bv. discriminatie) als privaatrechtelijk (bv. auteursrechtinbreuk, belediging). Welke staat heeft dan rechtsmacht? De staat waar de server staat waar de gewraakte uiting op gepubliceerd wordt? De staat wiens nationaliteit de uploader heeft? Of de staat waar de gewraakte uiting gelezen wordt, dan wel te lezen is?

Dat laatste zou betekenen dat het recht van iedere staat eigenlijk van toepassing is – publicaties op Internet zijn immers in theorie overal ter wereld te lezen. Dat zou betekenen dat je dus eigenlijk alleen iets op Internet kunt publiceren, als je er zeker van bent dat 't nergens ter wereld verboden is of zou kunnen zijn. En dat komt feitelijk neer op het einde van de vrijheid van meningsuiting – en de democratische rechtsstaat, en Internet. Toch claimen staten graag rechtsmacht over uitingen (al dan niet via Internet) die vanaf hun grondgebied toegankelijk zijn. Ook de Nederlandse rechter doet dat in de diverse internet-gokzaken.⁸

Maar kies je voor het recht van de staat waar de informatie vandaan komt, dan leidt dat onherroepelijk tot “Internet-vrijhavens”,⁹ staten die weinig of geen regulering hebben. En dat komt feitelijk neer op het einde aan normen en waarden – en de democratische rechtsstaat, en Internet.

Boven wetgeving wordt echter zoveel mogelijk de voorkeur gegeven aan zelfregulering, het derde niveau van regulering. Zelfregulering is echter geen oplossing voor zover het gaat om fundamentele normen en waarden van de democratische rechtsstaat, zoals de bescherming van grondrechten.

Voordeel is wel dat zelfregulering niet gebonden is aan de territoriale grenzen van staten.

Zelfregulering dient overigens wel aan een aantal elementaire voorwaarden te voldoen. Eerste voorwaarde is dat de doelgroepen die in het geding zijn voldoende georganiseerd dienen te zijn.

Daarnaast dient er een gelijkwaardige behartiging van de maatschappelijke belangen plaats te vinden en dient de handhaving van de afspraken voldoende verzekerd te zijn. Tenslotte mogen zelf opgestelde regels natuurlijk niet in strijd zijn met dwingend recht, bv. met betrekking tot consumentenbescherming.

Ook de Europese Commissie heeft laten blijken de oplossing van zelfregulering te omarmen.¹⁰ In Nederland heeft het Electronic Commerce Platform Nederland (ECP.nl), in samenwerking met het Ministerie van Economische Zaken, een aantal jaren geleden de “Modelgedragscode voor Elektronisch Zakendoen” vastgesteld.

Maar ook als uitgegaan wordt van regulering door een nationale overheid, blijven er genoeg problemen over. We noemen er twee: de "ongrijpbare" techniek en het hiervoor bij nationale regelgeving al aangeduide grensoverschrijdende aspect.

Internettelefonie ofwel Voice over IP (hierna: VoIP) noemen we als voorbeeld van een voor regelgeving ongrijpbare techniek. De vorm van VoIP die we hier op 't oog hebben is die tussen computers, zonder dat er een vaste telefoon aan te pas komt.¹¹ In feite is VoIP een peer-to-peer toepassing zoals MSN of Kazaa; hetgeen volgens het principe van packet-switching uitgewisseld wordt zijn pakketjes spraak, eventueel aangevuld met beeld van een webcam (videoconferencing). Deze vorm van VoIP, bijvoorbeeld met behulp van een programma zoals Skype, maakt alleen maar gebruik van het Internet zoals het er ligt. Het enige dat gebruikers nodig hebben is, behalve hardware

Het artikel is ook online verkrijgbaar op <http://swissnet.ai.mit.edu/6805/articles/goldsmith-against-cyberanarchy.html>.

⁷ Zie het volgende artikel van het in de vorige noot genoemde boek: David G. Post, *Against 'Against Cyberanarchy'*, in: Adam Thierer and Clyde Wayne Crews Jr. (eds.), *Who Rules the Net? Internet Governance and Jurisdiction*, CATO Institute, Washington D.C. 2003, pp. 71-89. Het artikel is ook online verkrijgbaar op <http://www.law.berkeley.edu/journals/btlj/articles/vol17/Post.stripped.pdf>.

⁸ zie o.a. HR 18 februari 2005, NJ 2005, 404 (*Ladbroke's*) en Hoge Raad 21 april 2006, LJN-nummer AV0641 (*Betfair*)

⁹ En dat hoeven niet eens exotische eilanden als Tokelau (www.dot.tk) te zijn. Een bijna letterlijke “vrijhaven” is Sealand, een verlaten kunstmatig eiland pal voor de Engelse kust, waar het bedrijf Havenco internetdiensten aanbiedt. Zie <http://www.sealandgov.com/index.html>.

¹⁰ Zie Artikel 16 richtlijn inzake elektronische handel, PbEG 2000 L 178/1

¹¹ Er bestaan ook varianten waarbij internettelefonie met aan één of beide kanten van de lijn een vaste telefoon - die blijven hier buiten beschouwing.

als een microfoon en een koptelefoon (of een headset) of boxen, een gebruiksrecht op de software. Maar functioneel gezien komt VoIP neer op telefoneren.

Telefonie valt onder de Telecommunicatiewet, en voor een aanbieder van een openbare telecommunicatiedienst gelden allerlei regels, zoals de verplichting tot aftapbaarheid, toezicht door de OPTA, en bereikbaarheid van alarmnummers.¹² Zelfs al zou de overheid besluiten VoIP te willen reguleren, dan is moeilijk in te zien wie of wat het aanknopingspunt van die regulering zou moeten zijn. De producent van de software? Die brengt geen signalen over. De ISP bij wie de gebruiker is aangesloten? Maar die heeft niets te maken met de software die zijn abonnee gebruikt.

Het grensoverschrijdende aspect van internetregulering laat zich goed illustreren aan de hand van de jurisprudentie over gokken op internet. Kort gezegd: de Wet op de Kansspelen (WoK) bepaalt dat het aanbieden van een kansspel gebonden is aan een vergunning.¹³ Op Internet is een breed scala aan sites die gelegenheid geven tot gokken, zonder de volgens de WoK benodigde vergunning. Is de WoK in een online omgeving wel te handhaven?

Afgezien van allerlei andere vragen die in dit verband spelen (zoals: of de Nederlandse vergunninghouders wel een beroep op de WoK kunnen doen om buitenlandse concurrenten van de Nederlandse markt te weren,¹⁴ en of het Nederlandse kansspelbeleid op basis van de WoK wel in overeenstemming is met het EG-mededingingsrecht)¹⁵ is de Nederlandse rechter van oordeel dat aan buitenlandse sites een verbod opgelegd kan worden om kansspelen in Nederland aan te bieden.¹⁶ Het moge duidelijk zijn dat het fenomeen gokken op Internet hiermee geenszins verdwenen is (ook niet uit Nederland).

6.2 Grondrechten

6.2.1 Algemeen

Het gebruik van het Internet, de daarbijbehorende communicatievrijheid en de eerder genoemde *free flow of information*, en de uitoefening en bescherming van een aantal grondrechten kunnen tot spanningen leiden. Het Internet heeft direct gevolgen voor grondrechten zoals de vrijheid van meningsuiting (artikel 10 EVRM en artikel 7 Grondwet) en het recht op bescherming van de persoonlijke levenssfeer (artikel 8 EVRM en artikel 10 Grondwet). Het doen van beledigende of racistische uitlatingen in nieuwsgroepen of chatrooms, websites die oproepen tot de jihad of de verspreiding van kinderporno zijn hier de meest sprekende voorbeelden van. Daarnaast kunnen ook andere grondrechten zoals de vrijheid van godsdienst (artikel 9 EVRM en artikel 6 Grondwet), het recht tot vereniging, vergadering en betoging (artikel 11 EVRM en artikel 9 Grondwet) of het brief-, telefoon en telegraafgeheim (artikel 13 Grondwet) door het Internet in het gedrang komen. Denk hierbij aan het feit dat door godsdienstige of levensbeschouwelijke overtuigingen op het Internet te plaatsen dit ook wereldwijde publicatie inhoudt, ook in die landen waar vrijheid van godsdienst niet zo vanzelfsprekend is.¹⁷ Bij de vrijheid van vergadering en betoging kan er gedacht worden aan mailinglijsten en abonnee websites.

In tegenstelling tot artikel 10 EVRM is artikel 7 van de Nederlandse Grondwet (vrijheid van meningsuiting) techniek-afhankelijk geformuleerd. Dit geldt eveneens voor artikel 13 Grondwet (brief-, telefoon- en telegraafgeheim). Na de grondwetwijziging van 1983 zijn er nieuwe informatie-

¹² Resp. de artt. 13.1 e.v., 2.1 en 11.10 Tw.

¹³ art. 1 WoK.

¹⁴ een vraag die overigens door de rechter met een beroep op de zgn. correctie Langemeijer positief beantwoord wordt, zie onder meer Vz. Arnhem 27 januari 2003 (Toto vs. Ladbroses) LJN-nummer AF3374 en Voorzieningenrechter Utrecht 31 juli 2003 (Holland Casino vs. Peak) LJN-nummer AI0977.

¹⁵ Europees Hof van Justitie 6 november 2003 (Gambelli).

¹⁶ HR 18 februari 2005 (Ladbroses), NJ 2005, 404, en recentelijk HR 21 april 2006, Betfair en Interwetten Cyprus vs. Nationale Sporttotalisator, LJN AV0641

¹⁷ A. Koekkoek e.a., "Vergelijking van grondrechten inzake informatie en privacy. Een oriënterend onderzoek." Centrum voor wetgevingsvraagstukken, Centrum voor recht bestuur en informatisering, KUB, Tilburg, juni 1999, p. 8. In dit onderzoek wordt de situatie met betrekking to problematiek van grondrechten en informatisering in Frankrijk, Duitsland, Zweden, Engeland, de Verenigde Staten, Canada en Zuid-Afrika onderzocht en met elkaar vergeleken.

en communicatietechnologieën, waaronder het Internet, ontstaan die niet meer onder het bereik van deze artikelen zijn te brengen. Gevolg is dat er onduidelijkheid is ontstaan of dergelijke grondrechten nog wel uitgeoefend c.q. beschermd kunnen worden wanneer er gebruik gemaakt wordt van de nieuwe communicatie-technologieën. Hoewel er wel veel nagedacht en geschreven is over “Grondrechten in het digitale tijdperk”¹⁸ zijn er nog geen wetsvoorstellen ingediend.¹⁹

6.2.2 Vrijheid van meningsuiting

Met betrekking tot de vrijheid van meningsuiting bepaalt art. 7 lid 3 Gw. dat voor het openbaren van gedachten of gevoelens door andere dan in de voorgaande leden genoemde middelen (drukkers lid 1, en radio en televisie lid 2) niemand voorafgaand verlot nodig heeft wegens de inhoud daarvan, behoudens ieders verantwoordelijkheid volgens de wet.

Het ligt voor de hand om het Internet te scharen onder “andere middelen” zoals bedoeld in dit lid. Relevant hierbij is het onderscheid tussen openbare en besloten communicatie omdat de vrijheid van meningsuiting in artikel 7 Grondwet alleen openbare uitlatingen betreft. Besloten uitlatingen worden beschermd door het recht op bescherming van de persoonlijke levenssfeer (art. 10 Grondwet). De vraag is dus wat precies openbaar en wat besloten is bij het gebruik van het Internet. Op het eerste gezicht lijkt de scheiding te vallen bij het onderscheid tussen het WWW, nieuwsgroepen, fora en openbare chatrooms als openbare vormen van communicatie en e-mail en privé-chat als besloten vormen.²⁰ De eerste groep is in beginsel voor een ieder toegankelijk terwijl communicatie per e-mail en privé-chat zich in beginsel tussen twee of een beperkte groep personen voltrekt. Maar die grens is ook weer niet in alle gevallen zo scherp te trekken gezien bijvoorbeeld de mogelijkheden van websites waar je op in moet loggen en mailinglijsten waar iedereen zich voor aan kan melden.

Waar het hier om gaat is dat de vrijheid van meningsuiting kan worden ingeperkt wanneer het in botsing komt met andere grondrechten, zoals bescherming van de persoonlijk levenssfeer e.d. Dit betekent een directe aantasting van het oorspronkelijke Internet beginsel, nl. “de free flow of information”.

Ook op Europees niveau wordt de behoefte gevoeld om illegale en schadelijke informatie op het Internet te kunnen bestrijden en aldus de communicatievrijheid noodzakelijkerwijs aan banden te leggen. Hierbij wordt dan met name gedoeld op informatie zoals kinderporno of informatie die aanzet tot haat op grond van ras, geslacht godsdienst, nationaliteit of etnische oorsprong. Het “Actieplan voor het veiliger gebruik van het Internet”²¹ uit 1999 is in 2003 verlengd.²² Marktpartijen (industrie, gebruikersorganisaties) worden gestimuleerd om doeltreffende zelf-reguleringsystemen te ontwikkelen en in te voeren.

Ook via de strafrechtelijke weg wordt dergelijke illegale en schadelijke informatie op het Internet aangepakt. Op Europees niveau is de Convention on Cybercrime²³ in dit verband van belang. In Nederland is de Safe Internet Foundation actief, de belangenbehartiger voor de eindgebruiker van de

¹⁸ Zie <http://www.ivir.nl/dossier/grondrechten/grondrechten.html> voor een overzicht.

¹⁹ en wordt er inmiddels weer aan nieuwe voorstellen gewerkt, waarbij nieuwe internationale ontwikkelingen op het gebied van de toepassing van mensenrechten in de informatiesamenleving betrokken (<http://www.minaz.nl/data/1099053965.pdf>).

²⁰ Ook de Minister van Binnenlandse Zaken lijkt daarvan uit te gaan, gezien de Nota van toelichting bij het Instellingsbesluit van de Commissie “Grondrechten in het digitale tijdperk. In de inleiding wordt bepaald “..Bij nieuwe technieken valt hierbij in het kader van artikel 7 Grondwet te denken aan Internet, terwijl in het licht van artikel 13 Grondwet valt te denken aan e-mail.” Opmerking verdient hierbij dat de terminologie niet helemaal juist is gehanteerd. E-mail is een toepassing die gebruik maakt van de infrastructuur Internet. Met het Internet zal waarschijnlijk het WorldWide Web bedoeld zijn.

²¹ Beschikking Nr. 276/1999/EC van het Europees Parlement en de Raad van 25 januari 1999 tot vaststelling van een communautair meerjaren actieplan ter bevordering van een veiliger gebruik van het Internet door het bestrijden van illegale schadelijke inhoud op mondiale netwerken, PbEG 1999, L33/1. Ook gepubliceerd op www2.echo.lu/iap/decision.

²² Beschikking Nr. 1151/2003/EG van het Europees Parlement en de Raad van 16 juni 2003 tot wijziging van Beschikking nr. 276/1999/EG tot vaststelling van een communautair meerjarenactieplan ter bevordering van een veiliger gebruik van internet door het bestrijden van illegale en schadelijke inhoud op mondiale netwerken

²³ Convention on Cybercrime ETS No.: 185 (Raad van Europa), te vinden op <http://conventions.coe.int>. In art. 9 wordt verdragspartijen de verplichting opgelegd om kinderpornografie strafbaar te stellen.

elektronische snelweg. SIF onderzoekt, publiceert, voert projecten uit en zoekt de publiciteit om de kwaliteit en vooral veiligheid van het internet te verbeteren.²⁴ Strafrechtelijk zijn in Nederland de reguliere artikelen uit het Wetboek van Strafrecht van toepassing, het gaat dan met name om art. 240b Sr. voor kinderporno, en artt. 137c e.v. Sr. voor belediging en aanzetting tot haat etc.

Het blijkt in de praktijk erg moeilijk te zijn om schadelijke uitingen op het Internet tegen te gaan, zowel strafrechtelijk als privaatrechtelijk. In sommige gevallen is het moeilijk de content provider te achterhalen - vaak is de medewerking van de ISP nodig om de NAW-gegevens van de inbreukmaker boven tafel te krijgen (zie hierna). Vervolgens is er de internationale dimensie: hoewel de Nederlandse rechter zich op het standpunt stelt dat uitingen via Internet die in Nederland te lezen zijn onder de Nederlandse jurisdictie vallen, is het tenuitvoerleggen van een eventuele uitspraak tegen een veroordeelde die zich in het buitenland bevindt vaak bijzonder lastig. En tenslotte zijn met één veroordeling uitingen niet van het Internet verdwenen. Juist controversiële uitingen hebben de neiging voortdurend op allerlei plaatsen weer op te duiken.

Vrijheid van meningsuiting is een groot goed, ook op Internet. Via Internet kunnen mensen, met eenzelfde belangstelling of met dezelfde beperkingen met elkaar in contact komen. Maar dat geldt niet alleen voor alleenstaande moeders en reumapatiënten, maar ook voor liefhebbers van kinderporno en sympathisanten van terroristische organisaties.²⁵ En omdat op Internet letterlijk iedereen alles kan publiceren, worden er dingen wereldkundig gemaakt waar de traditionele media niet aan willen of durven beginnen, zoals videobeelden van allerlei gruwelijkheden.

Iedereen die dat wil kan wat hij of zij maar wil, op Internet publiceren. Bekend zijn tegenwoordig de weblogs (kortweg Blogs), websites als een soort dagboeken, met links en commentaar van de maker, zowel persoonlijk (bijv. van een "gewone" burger, of van een minister) als met betrekking tot een vastomlijnd onderwerp (bijv. van een advocatenkantoor met betrekking tot een gespecialiseerd rechtsgebied).

Een ander fenomeen dat in dit verband genoemd moet worden zijn de zogenaamde klaagsites; sites die gewijd zijn aan het aan de kaak stellen van c.q. kritiek leveren op anderen. Ook daarbij worden de grenzen van de maatschappelijke betamelijkheid soms overschreden.²⁶

Ook al blijft men binnen de grenzen van wat naar Nederlands recht aanvaardbaar wordt geacht, dan nog bestaat de kans om in het buitenland voor de rechter gesleept te worden. Rechter in Australië, de VS en Engeland bijvoorbeeld aarzelen niet om, in voorkomende gevallen, een buitenlander wegens een internetpublicatie voor belediging, smaad of laster te veroordelen.²⁷ De dreiging die daarvan uitgaat voor de vrijheid van meningsuiting op het Internet wordt wel het "chilling effect" genoemd.²⁸ Er zijn ook nationale overheden die met betrekking tot het Internet zeer vergaande regelgeving voor inhoudscontrole van overheidswege opstellen. Voorbeeld hiervan is China, waar internetgebruikers zich moeten melden bij de autoriteiten en waar websites lukraak door de overheid worden geblokkeerd. Onlangs kwam Google nog in het nieuws bij de lancering van zijn Chinese site waarbij zoekresultaten over gevoelige onderwerpen – bijvoorbeeld over mensenrechten, Tibet of de Falun

²⁴ Zie www.veiligophetweb.nl. Een vergelijkbaar initiatief is www.surfopsafe.nl.

²⁵ Volgens het AIVD-rapport Van dawa tot jihad, De diverse dreigingen van de radicale islam tegen de democratische rechtsorde, 22 december 2004 (te vinden op <http://www.aivd.nl/contents/pages/10835/notavandawatotjihad.pdf>) speelt het Internet in toenemende mate een rol bij de radicalisering van islamitische jongeren in Nederland, niet alleen via websites maar vooral via chatrooms. (rapport, p. 43).

²⁶ Zie onder meer Gerechtshof Arnhem 12 maart 2002 (Stichting Jeugd en Gezin) LJN-nummer AE1664, Rb. Alkmaar 13 augustus 2003 (campingmaffia) LJN-nummer AI1806, Voorzieningenrechter Almelo 24 februari 2004 (CAD-telewerk lastercampagne), LJN-nummer AO4874, Voorzieningenrechter Groningen 25 mei 2004 (biostabiel sucks), LJN-nummer AO9943.

²⁷ Zie bijvoorbeeld High Court of Australia, *Dow Jones & Company, Inc v Gutnick* M3/2002 (28 May 2002), uitspraak te vinden op http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html; *Batzel vs. Cremers* CV-00-09590-SVW (9th Cir. Jun. 24, 2003), uitspraak te vinden op <http://caselaw.lp.findlaw.com/data2/circs/9th/0156380pv2.pdf>; en *Richardson v. Schwarzenegger & Others* [2004] EWHC 2422 (QB), <http://portal.nasstar.com/75/files/Richardson-v-Schwarzenegger%20QBD%2029%20Oct%202004.pdf>.

²⁸ www.chillingeffects.org.

Gong-sekte – niet worden doorgegeven.²⁹ Dergelijke regelgeving betekent simpelweg censuur van overheidswege, welke een ernstige inbreuk op de vrijheid van meningsuiting oplevert.

6.2.3 Recht op bescherming van de persoonlijke levenssfeer

Privacy, “the right to be let alone”,³⁰ is een tweede grondrecht dat door de komst van nieuwe technieken in een ander daglicht gesteld wordt. Het recht op bescherming van de persoonlijke levenssfeer, neergelegd in artt. 10 Gw, 17 B.U.P.O. en 8 E.V.R.M., omvat in ieder geval een ruimtelijke en een informationele dimensie. De door art. 10 lid 2 Gw. genoemde wet die regels stelt “ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens” is de sinds september 2001 geldende Wet bescherming persoonsgegevens (Wbp). De Wbp regelt tevens “de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op de verbetering van zodanige gegevens” (art. 10 lid 3 Gw.).

Kernbegrippen in de Wbp zijn “persoonsgegevens” en “verwerking”. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.³¹ Hier is meteen al de eerste onduidelijkheid bij toepassing van deze definitie op het Internet: een emailadres kan een persoonsgegeven zijn (bv. bij een adres als Pietje.Puck@commercieelbedrijf.nl – zodat we weten dat Pietje Puck bij commercieelbedrijf werkt), maar dat hoeft niet: bink14@hotmail.com is duidelijk geen persoonsgegeven. Een emailadres kan zelfs een gevoelig persoonsgegeven³² zijn, als het emailadres de naam van, bijvoorbeeld, een organisatie voor homoseksuelen, of een patiëntenvereniging bevat. Alles, maar dan ook alles wat met persoonsgegevens gedaan kan worden, valt onder “verwerken”.³³ Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld, en mogen slechts in een limitatief opgesomd aantal gevallen worden verwerkt, nl. met toestemming van de betrokkene,³⁴ voor zover noodzakelijk voor de uitvoering van een overeenkomst of van een wettelijke plicht, ter vrijwaring van een vitaal belang van de betrokkene, voor de vervulling van een publiekrechtelijke taak, of, tenslotte, voor zover “de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.”³⁵ Het College bescherming persoonsgegevens (CBP)³⁶ houdt toezicht op de naleving van de Wbp.

Gebruik van het Internet brengt met zich mee dat persoonsgegevens verzameld (kunnen) worden, zowel met medeweten van de betrokken gebruiker als zonder. Zonder medeweten van de gebruiker kunnen gegevens verzameld worden door middel van cookies en spyware:

²⁹ Zie hiervoor bijv. www.geledraak.nl waar het volgende berichtje staat: “De directeur van het Chinese centrale Bureau Internetzaken gaf in februari 2006 een persconferentie over internet en verboden websites. Dit mede na de ophef over oa zoekmachine Google die zich in China zal houden aan de daar geldende censuur. De tekst van de gehele persconferentie is door Xinhua [online geplaatst](#). O.a. zei hij: ‘Chinese can access the Web freely, except when blocked from a very few websites whose contents mostly involve pornography or terrorism’. In de praktijk echter worden ook tal van andere sites geblokkeerd, met de regering onwettige inhoud, zoals weblogs.” Voor een kritisch geluid over Google, zie Chr. Alberdingk Thijm, Google Stop, BNR, 28 februari 2006 (www.Solv.nl/pub_docs/111BNR_Google.pdf).

³⁰ Zowel de term “privacy” als “the right to be let alone” zijn afkomstig uit een artikel van S. Warren en L.D. Brandeis in de Harvard Law Review van 1891, (nr. 5, pp. 193-220), online te vinden op http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html.

³¹ Art. 1 sub a Wbp.

³² Art. 16 Wbp.

³³ Art. 1 sub b Wbp: “elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raddplegen, gebruiken, verstrekken door middel van rondzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.”

³⁴ De “betrokkene” is degene op wie de persoonsgegevens betrekking hebben, art. 1 sub f Wbp.

³⁵ Art. 8 Wbp.

³⁶ Zie www.cbppweb.nl.

dit zijn, kort gezegd, stukjes software die bij het bezoeken van een bepaalde website meegestuurd worden naar de computer van de gebruiker en daar worden geplaatst. Via deze software is het mogelijk om de gangen van de gebruiker op het Internet te volgen, en zelfs te registreren wat er allemaal via het toetsenbord ingetypt wordt. Voor zover de gebruiker geen toestemming heeft gegeven voor het plaatsen van dit soort software (bijvoorbeeld door in de opties van de browser aan te geven dat geen cookies zonder toestemming geaccepteerd mogen worden) zou betoogd kunnen worden dat dit strafbaar is.³⁷ Het is alleen praktisch gesproken meestal onmogelijk om de dader te achterhalen. Voor zover de informatie die op deze manier verzameld wordt niet herleidbaar is tot een individueel natuurlijk persoon, is er strikt gesproken geen sprake van schending van de Wbp. Toch wordt ook het anoniem verzamelen van gegevens door sommigen ervaren als een inbreuk op hun persoonlijke levenssfeer.³⁸

Een gebruiker laat zelf ook vaak een digitaal spoor van persoonlijke gegevens achter. Dit kan gebeuren bij het versturen van een e-mail, bij deelname aan een discussie op een forum, het invullen van een enquête of het doen van een aankoop via het Internet. Activiteiten zoals bijv. het aanschaffen van een boek of CD, het boeken van een reis of het afnemen van een entertainment dienst, vereisen in het algemeen het afgeven van gegevens als naam, adres en credit card nummer. In verband met de "toestemming" van art. 8 sub a Wbp, is het van belang om, alvorens aangevinkt wordt dat men accoord gaat met de privacy policy en/of de algemene voorwaarden, even te kijken waar met betrekking tot de verstrekte persoonsgegevens toestemming voor gegeven wordt. Vaak staat er dat gegevens gebruikt kunnen worden voor marketing doeleinden, door het bedrijf zelf en haar zakenpartners. Dat laatste komt er dus op neer dat persoonsgegevens doorgegeven c.q. verkocht worden aan derden.

En dan is er nog het probleem van het grensoverschrijdende karakter van het Internet. Nederlandse bedrijven zijn uiteraard gebonden aan de Wbp, en omdat de Wbp een uitvloeisel is van een Europese richtlijn³⁹ mag een consument verwachten dat bedrijven uit andere EU-lidstaten zich ook netjes gedragen. Maar voor zover gegevens buiten Europa verzameld en verwerkt worden, is er voor betrokkenen geen enkele waarborg meer.

Het probleem met betrekking tot het verwerken van persoonsgegevens is nou juist, dat de betrokkenen er totaal geen zicht op hebben: niet op welke gegevens (al dan niet juist) over hem of haar bekend zijn, en bij wie. Het wordt natuurlijk nog interessanter op het moment dat allerlei gegevens met elkaar in verband gebracht worden. Zo bestaan er "groepsprofielen", opgesteld met behulp van technieken als datamining en datawarehousing, op basis waarvan een gebruiker kan worden gekwalificeerd als bv. student, alleenstaande vader of iets dergelijks. Het gevaar van dergelijke profielen is dat ze gaan werken als een soort onzichtbare, geautomatiseerde vooroordelen: het is niet ondenkbaar dat op basis van zo'n groepsprofiel iemand bijvoorbeeld geen kredietfaciliteiten krijgt aangeboden,⁴⁰ of alleen tegen strengere voorwaarden een verzekering af kan sluiten.⁴¹ Het probleem is dat de betrokkene geen idee heeft dat hij of zij op basis van een dergelijk groepsprofiel behandeld wordt, en dus ook niet de mogelijkheid heeft om de bij het profiel behorende veronderstellingen te ontcrachten.⁴²

Ook worden persoonsgegevens veel gebruikt voor reclame-doeleinden: om een gebruiker de "juiste" banners te kunnen laten zien als hij of zij een website bezoekt, om hem of haar "speciale aanbiedingen" via de gewone post of via e-mail te kunnen sturen. Dit laatste wordt ook wel "spam" genoemd, en is misschien eerder een probleem van overlast dan van privacy.⁴³

³⁷ Zie bv. art. 350a lid 1 Sr.

³⁸ Zie voor een vlamvend betoog hierover: Steve Gibson, The Ethics of Anonymous Surveillance for Profit, <http://grc.com/oo/ethics.htm>.

³⁹ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (EUR-Lex (Publikatieblad nr L 281 van 23/11/1995 pp. 31-50).

⁴⁰ Bijvoorbeeld: als op basis van een postcode geoordeeld wordt dat iemand waarschijnlijk niet kredietwaardig is.

⁴¹ Bijvoorbeeld: als op basis van een groepsprofiel geconcludeerd wordt dat iemand in een risicogroep met betrekking tot een bepaalde ziekte zit.

⁴² Hoewel de genoemde handelswijze wel verboden wordt door art. 42 Wbp.

⁴³ Hoewel, zeker als er op basis van een profiel gespamd wordt, er duidelijk ook een privacy-aspect aan zit. Zie ook: Christiaan Alberdingk Thijm, Het nieuwe informatierecht, Nieuwe regels voor het internet, p. 54.

Nog een ander aspect met betrekking tot informatiele privacy op het Internet betreft het publiceren van persoonsgegevens op het Internet, bv. in de vorm van een website over een bedrijf of organisatie, een ledenlijst van een sportvereniging, een fanpagina, etc. Voor zover expliciete, voorafgaande toestemming van betrokkenen ontbreekt, kan geoordeeld worden dat er sprake is van strijd met de Wbp.⁴⁴ Er zijn op Internet heel veel persoonsgegevens te vinden – terwijl lang niet altijd duidelijk is dat het wel in het belang van de betrokkene is dat iedereen die even de moeite neemt om te zoeken, die informatie ook kan vinden.⁴⁵

6.2.4 Brief-/telefoon-/telegraafgeheim

De huidige bescherming van het brief-, telefoon- en telegraaf geheim is opgenomen in artikel 13 Grondwet. Doordat dit artikel techniek afhankelijk is geformuleerd (het noemt brief, telefoon en telegraaf expliciet!) dient het te worden aangepast. Ook hierover is veel nagedacht en geschreven, vooral in termen van een techniek-onafhankelijk recht op vertrouwelijke communicatie,⁴⁶ maar een concreet wijzigingsvoorstel is nog niet ingediend.⁴⁷ Overigens zijn activiteiten als het “afluisteren” van chat en het onderscheppen van email in verband met opsporing wel wettelijk geregeld.⁴⁸

6.3 Elektronische handel

6.3.1. Begripsbepaling

Het begrip "e-commerce" is geen juridisch begrip. Het is een paraplubegrip voor sterk uiteenlopende vormen van handel die gemeenschappelijk hebben dat zij op elektronische wijze worden verricht.⁴⁹ Lodder definieert het begrip e-commerce als het volgt: *Any business transaction concerning goods and services, including relating commercial activities, where participants are not at the same physical location and communicate through electronic means.*⁵⁰

Er kan een onderscheid worden gemaakt tussen directe en indirecte elektronische handel. Bij de directe elektronische handel neemt een partij direct op internet diensten af.⁵¹ Bij de indirecte elektronische handel bestelt een partij via Internet, en wordt het goed vervolgens via de ‘traditionele’ manier (bijv. de post) geleverd.

6.3.2. Regelgeving met betrekking tot elektronische handel

⁴⁴ Een Zweedse mevrouw had in haar vrije tijd een website gemaakt voor nieuwe leden van het plaatselijke kerkgenootschap, waarin ze in licht humoristische bewoordingen wat vertelde over de mensen die aan die kerk verbonden waren. Het Europese Hof van Justitie oordeelde dat zij daarmee de Zweedse equivalent van de Wbp had geschonden: Europees Hof van Justitie 6 november 2003 (Lindqvist), van zaak C101/01.

⁴⁵ Bijvoorbeeld “jeugdzonden” waarvan nog steeds de sporen op het internet te vinden zijn. Gewoon via Google, of via gespecialiseerde sites zoals voelspriet.nl is verrassend veel te vinden.

⁴⁶ Zie onder meer TK 1996-1997 25 443: Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepalingen inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim; TK 1997-1998 25 443, nr.5: nota naar aanleiding van het verslag, 18 november 1997; EK 1997-1998, 25 443, nr 232, gewijzigd voorstel van wet van 21 januari 1998.

⁴⁷ <http://www.minaz.nl/data/1099053965.pdf>

⁴⁸ Zie bv. art. 125i e.v. Sv., 126m e.v. Sv., 13.1 e.v. Tw.

⁴⁹ C. Stuurman, E-commerce: what’s new? Enkele recente ontwikkelingen op het terrein van reguleringsinitiatieven voor de elektronische handel, Computerrecht 1999, nr. 3, p. 99

⁵⁰ A.R. Lodder en H.W.K. Kaspersen, eDirectives: Guide to European Union Law on E-commerce, Kluwer Law International 2002, p. 3

⁵¹ De levering geschiedt ook via internet. Denk aan het downloaden van muziek of software, of dienstverlening van een therapeut door middel van chatsessies.

In juni 2000 is de Richtlijn betreffende bepaalde aspecten van de elektronische handel (E-commerce Richtlijn) door de Europese Unie aangenomen.⁵² Deze richtlijn heeft het over "diensten van de informatiemaatschappij", die omschreven worden als "elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn. Een dienst wordt langs elektronische weg verricht indien deze geheel per draad, per radio, of door middel van optische of andere elektromagnetische middelen wordt verzonden, doorgeleid en ontvangen met behulp van elektronische apparatuur voor de verwerking, met inbegrip van digitale compressie, en de opslag van gegevens."⁵³

De bepalingen van de E-commerce Richtlijn zijn in de Nederlandse wetgeving op diverse plekken opgenomen. In de eerste plaats is een aantal bepalingen van zeer algemene strekking opgenomen in Afdeling 1A van Titel 1 van Boek 3, getiteld "Elektronisch vermogensrechtelijk rechtsverkeer". Daarnaast wordt in een eveneens door de Aanpassingswet gecreëerde nieuwe afdeling 4A van Titel 3 van Boek 6 van het Burgerlijk Wetboek, getiteld "Aansprakelijkheid bij elektronisch rechtsverkeer" de regeling vastgelegd betreffende de aansprakelijkheid van dienstverleners die als tussenpersoon optreden. Tenslotte zijn in afdeling 2 van Titel 5 van Boek 6 (Het tot stand komen van overeenkomsten) een drietal nieuwe artikelen opgenomen ter uitvoering van het in de richtlijn omtrent de totstandkoming van overeenkomsten langs elektronische weg bepaalde. Daarnaast zijn het Wetboek van Strafrecht en de Wet op de economische delicten aan de richtlijn aangepast.⁵⁴

De E-commerce Richtlijn geeft onder andere regels voor de algemene informatie die aanbieders van elektronische diensten moeten verschaffen. Dergelijke informatie betreft onder meer de naam en het adres van de dienstverlener, handelsregistergegevens, gegevens over vergunningen en de adresgegevens "die een snel contact en een rechtstreekse en effectieve communicatie met de dienstverlener mogelijk maken, met inbegrip van diens e-mailadres". Deze informatieverplichtingen zijn thans als artikel 15 d t/m 15f in boek 3 van het Burgerlijk Wetboek opgenomen. Naast regels voor informatieverschaffing bevat de E-commerce Richtlijn bepalingen over het totstandkomen van online overeenkomsten (artt. 9-11; in de Nederlandse wetgeving opgenomen als art. 6:227 a-c BW), de vestiging van informatie aanbieders (artt. 4-5), commerciële communicatie (artt. 6-8), aansprakelijkheid van tussenpersonen (artt. 12-15; in de Nederlandse wetgeving opgenomen als art. 6:196c BW), gedragscodes (art. 16), buitengerechtelijke geschillenregelingen (art. 17) en samenwerking tussen nationale autoriteiten (art. 19). Met deze richtlijn beoogt de Europese wetgever een Europees geharmoniseerd wettelijk kader te scheppen voor de elektronische handel.

In de late jaren negentig ontwikkelden een aantal internationale organisaties, gouvernementele en niet-gouvernementele zoals UNCITRAL,⁵⁵ de OESO en de Internationale Kamer van Koophandel (ICC),⁵⁶ initiatieven tot regelgeving op het gebied van de elektronische handel in de vorm van modelwetten, richtlijnen of gedragscodes. Naast de update in 2001 van de ICC richtlijnen voor veilig internetgebruik, is er sinds 2005 bij dergelijke instanties de vaart er een beetje uit. Er komen niet veel internationale initiatieven meer van de grond.

⁵² Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt. PbEG 17.7.2000, L178.

⁵³ Art. 3:15d lid 3 BW.

⁵⁴ MvT Wetsvoorstel Aanpassingswet, TK 2001-2002 28197.

⁵⁵ In 1996 heeft UNCITRAL, als een van de eerste internationale organisaties, de "Model law on Electronic Commerce" uitgevaardigd. Deze Model Law was indertijd bedoeld als een richtsnoer voor staten in de modernisering van hun nationale wetgevingen op het gebied van e-commerce. Deze Model Law is inmiddels alweer door de tijd achterhaald.

⁵⁶ In 1997 heeft de internationale Kamer van Koophandel (ICC) de "General Usage for International Digitally Ensured Commerce" (GUIDEC)⁵⁶ opgesteld en deze is in 2001 herzien (GUIDEC II). Deze richtlijnen beogen een set van algemene definities en algemene gebruiken in de elektronische handel vast te leggen. GUIDEC betreft geen gedragscode, maar geeft veeleer een overzicht van probleempunten, *best practices* en certificatieprocessen die zich in de elektronische handel voordoen.

Zoals eerder gezegd geven nationale overheden de ruimte voor het ontwikkelen van zelfregulering. Zie hiervoor de eerder genoemde Gedragscode voor elektronisch zakendoen van ECP.nl. Het is onduidelijk of van deze gedragscode in de praktijk veel gebruik is gemaakt. Het is inmiddels een stille dood gestorven.⁵⁷ Veeleer is ECP.nl in de loop der jaren een informatieplatform voor internetondernemers geworden.

Vóór de E-commerce Richtlijn was er al de Richtlijn Verkoop op Afstand,⁵⁸ die geïmplementeerd is in de Wet Koop op Afstand:⁵⁹ art. 7:7 lid 2 BW en afdeling 9A (artt. 46a t/m 46j) van boek 7 BW. Een overeenkomst op afstand wordt door art. 7:46a sub a BW omschreven als *“de overeenkomst waarbij, in het kader van een door de verkoper of dienstverlener georganiseerd systeem voor verkoop of dienstverlening op afstand, tot en met het sluiten van de overeenkomst uitsluitend gebruik wordt gemaakt van één of meer technieken voor communicatie op afstand”*. Koop op afstand wordt door art. 7:46a sub b BW gedefinieerd als een overeenkomst op afstand die een consumentenkoop⁶⁰ is. En tenslotte omschrijft 7:46a sub c BW een overeenkomst op afstand tot het verrichten van diensten als: *“de tot het verrichten van diensten strekkende overeenkomst op afstand tussen een dienstverlener die handelt in de uitoefening van een beroep of bedrijf en een wederpartij, natuurlijk persoon, die niet handelt in de uitoefening van een beroep of bedrijf”*. Tenslotte verdient in dit verband vermelding de Richtlijn Elektronische Handtekeningen,⁶¹ onder meer geïmplementeerd in artt. 3:15a-c BW en 6:196b BW,⁶² die hierna kort aan de orde zullen komen.

6.3.3. Overeenkomsten via Internet.

Hoe gaat e-commerce nou in de praktijk in z'n werk? Hieronder zal kort besproken worden welke regels gelden voor een webwinkelier die zaken wil doen met consumenten, de zogenaamde B2C (business-to-consumer) e-commerce. B2B (business-to-business) en C2C (consumer-to-consumer, zoals bijv. via eBay of marktplaats) e-commerce worden hier niet afzonderlijk besproken. Zoals gebruikelijk kan er een onderscheid gemaakt worden tussen de pre-contractuele fase, het sluiten van de overeenkomst en nakoming.

Voordat een overeenkomst gesloten wordt, moet een webwinkelier vooral informatie verschaffen, om het ontbreken van fysiek contact enigszins te compenseren. Het gaat daarbij om:

- de identiteit van de verkoper (en als er iets vooruit betaald moet worden ook zijn adres);
- de belangrijkste kenmerken van de aangeboden zaak;
- de prijs, inclusief BTW;
- de kosten van aflevering;
- de wijze van betaling.

Deze informatie moet *“met alle aan de gebruikte techniek voor communicatie op afstand aangepaste middelen en op duidelijke en begrijpelijke wijze ... worden verstrekt”*, waarbij ook *“het commerciële oogmerk ondubbelzinnig moet blijken”*.⁶³

⁵⁷ Die conclusie kan getrokken worden omdat deze gedragscode inmiddels niet meer is terug te vinden op de website van ECP.nl.

⁵⁸ Richtlijn 97/7/EG van het Europees Parlement en de Raad van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (EUR-Lex - Publicatieblad Nr. L 144 van 04/06/1997 blz. 19-27).

⁵⁹ Officieel de Wet Bescherming van de consument bij op afstand gesloten overeenkomsten (wetsvoorstel 26 861).

⁶⁰ Consumentenkoop: *“de koop met betrekking tot een roerende zaak, die wordt gesloten door een verkoper die handelt in de uitoefening van een beroep of bedrijf, en een koper, natuurlijk persoon, die niet handelt in de uitoefening van een beroep of bedrijf.”* (art. 7:5 lid 1 BW).

⁶¹ Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (EUR-Lex - Publicatieblad Nr. L 013 van 19/01/2000 blz. 0012 - 0020)

⁶² Daarnaast zijn er nog meer Richtlijnen die (mede) van toepassing zijn op e-commerce. Zie www.ecp.nl onder “dossier wet- en regelgeving” voor een compleet overzicht.

⁶³ Art. 7:46c lid 1 BW. Zie ook de informatieplichten voorkomend uit de e-commerce richtlijn: art. 3:15d en 3:15e BW.

In de praktijk wordt veel van deze informatie (met uitzondering van de belangrijkste kenmerken van de aangeboden zaak) verwerkt in algemene voorwaarden.⁶⁴ Om vernietigbaarheid van algemene voorwaarden te voorkomen moet de webwinkelier ervoor zorgen dat de consument een redelijke mogelijkheid heeft gehad om van die algemene voorwaarden kennis te nemen.⁶⁵ Ten aanzien van elektronische algemene voorwaarden is daaraan voldaan als de webwinkelier de voorwaarden op een zodanige wijze ter beschikking stelt dat ze door de consument kunnen worden opgeslagen en voor hem toegankelijk zijn ten behoeve van latere kennisneming.⁶⁶ Onduidelijk is voorts of de opslagmogelijkheid via de rechtermuisknop in Windows hiervoor voldoende is, of dat er een aparte voorziening op de website voor moet bestaan. De toegankelijkheid voor latere kennisneming is uiteraard van belang in het geval de algemene voorwaarden gewijzigd worden.⁶⁷ Net als iedere andere overeenkomst komt ook een overeenkomst via Internet tot stand door een aanbod en de aanvaarding daarvan.⁶⁸ Aanbod en aanvaarding zijn wilsverklaringen, en volgens art. 3:37 BW kunnen die (tenzij anders is bepaald) in iedere vorm geschieden, of in een of meer gedragingen besloten liggen. Dat betekent dat het aanklikken van een button in principe een wilsverklaring kan zijn. Voor "gewone" overeenkomsten geldt de ontvangsttheorie.⁶⁹ Omdat elektronische communicatie, en zeker communicatie via Internet niet zo voorspelbaar verloopt als traditionele communicatie, is voor e-commerce gekozen voor een extra stap: art. 6:227c lid 2 BW bepaalt dat de consument de overeenkomst kan ontbinden zolang de aanvaarding niet door de webwinkelier is bevestigd. Heel vaak zal die bevestiging door middel van een autoreply email verstuurd worden, waarin de door de consument opgegeven gegevens herhaald (en daarmee bevestigd) worden. Als het om grote belangen gaat is soms de extra zekerheid van een elektronische handtekening gewenst. Met behulp van een elektronische handtekening kan de identiteit van partijen vastgesteld worden, wordt de authenticiteit van de uitgewisselde berichten gegarandeerd, en kan een partij niet ontkennen een bericht met een bepaalde inhoud verzonden te hebben (non-repudiation). Bij elektronische handtekeningen wordt gebruik gemaakt van asymmetrische encryptie: versleuteling van berichten met behulp van twee verschillende sleutels die, hoewel ze uiteraard aan elkaar verwant zijn, niet uit elkaar te herleiden zijn. De private sleutel berust alleen bij de persoon zelf en is geheim. De publieke sleutel is openbaar en kan bijvoorbeeld in een keybase (database met publieke sleutels) van een zogenaamde "trusted third party" (TTP, zie hierna) gevonden worden. De afzender versleutelt een bericht met zijn private sleutel en stuurt 't naar de ontvanger. De ontvanger haalt de publieke sleutel van de afzender uit de keybase en ontsleutelt het bericht daarmee. Als dat een leesbaar bericht oplevert, weet de ontvanger zeker dat 't van de afzender afkomstig is (authenticiteit) en dat er onderweg niet mee geknoeid is (integriteit). Voorts kan de afzender vervolgens niet meer ontkennen dat bericht verstuurd te hebben. Wil een afzender een bericht versturen dat uitsluitend door de beoogde ontvanger gelezen kan worden, dan kan de afzender de publieke sleutel van de ontvanger gebruiken om het bericht te versleutelen. Omdat alleen de ontvanger over de sleutel beschikt waarmee dat bericht ontsleuteld kan worden kan de vertrouwelijkheid van dat bericht gegarandeerd worden. De TTP, een "vertrouwenwekkende onafhankelijke derde" of certificatieinstantie in termen van de wet, staat dus garant voor de identiteit van de persoon achter de handtekening. Hij is aansprakelijk als wederpartijen op basis van een onjuist certificaat hebben gehandeld - waarbij tegenbewijs (nl. dat de TTP niet onzorgvuldig gehandeld heeft) is toegestaan. Ook is het mogelijk voor een TTP om zijn aansprakelijkheid te beperken, bijvoorbeeld tot bepaalde soorten transacties of tot een bepaalde geldswaarde.⁷⁰

⁶⁴ Art. 6:231 e.v. BW.

⁶⁵ Art. 6:233 sub b BW.

⁶⁶ Art. 6:234 lid 1 sub c BW.

⁶⁷ Voor zgn. m-commerce (e-commerce via bijvoorbeeld een mobiele telefoon) geldt dat de consument moet weten waar de algemene voorwaarden staan, en dat zij op verzoek elektronisch of anderszins zullen worden toegezonden, art. 6:234 lid 1 sub c BW.

⁶⁸ Art. 6:217 BW.

⁶⁹ Artt. 3:37 lid 3 en 6:224 BW.

⁷⁰ Art. 6:196b BW.

Art. 3:15a BW stelt een elektronische handtekening gelijk aan een handgeschreven handtekening, indien hij, kort gezegd, voldoende betrouwbaar is. En voldoende betrouwbaarheid wordt verondersteld indien de elektronische handtekening

- op unieke wijze aan de ondertekenaar verbonden is;
- het mogelijk maakt de ondertekenaar te identificeren;
- tot stand komt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
- op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft is verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
- gebaseerd is op een gekwalificeerd certificaat;⁷¹ én
- gegenereerd is met een veilig middel.⁷²

Dan, als de overeenkomst eenmaal tot stand gekomen is, moeten beide partijen nakomen. In principe moet de verkoper binnen 30 dagen nakomen.⁷³ En wat de betaling door de consument betreft: bij fraude met betaalkaarten is de consument niet verplicht tot betaling, tenzij het frauduleus gebruik een gevolg is van een omstandigheid die aan hem kan worden toegerekend.⁷⁴

Bij de nakoming gelden opnieuw een aantal informatieplichten voor de verkoper.⁷⁵

- de eerdere gegevens (bij totstandkoming) - behalve voor zover die toen al verstrekt waren;
- het ontbindingsrecht van de consument;
- een bezoekadres van de verkoper, waar de koper een klacht kan indienen;
- gegevens omtrent garantie;
- bij duurovereenkomsten: de vereisten voor opzegging.

Bij dat ontbindingsrecht zit een flinke adder onder het gras. Art. 7:46d lid 1 BW bepaalt dat de koper, gedurende zeven werkdagen na de ontvangst van de zaak het recht heeft de koop op afstand zonder opgave van redenen te ontbinden. Dit geldt uiteraard niet voor alle zaken: art. 7:46d lid 4 BW noemt de zaken waarvoor het ontbindingsrecht niet geldt. Maar, indien niet aan alle informatieplichten bij de nakoming zoals hierboven genoemd, voldaan is, geldt als "straf" dat de consument een termijn van drie maanden heeft om de overeenkomst zonder opgave van redenen te ontbinden.

Dat ontbindingsrecht wordt door veel webwinkels niet vermeld. Vaak staat er in de algemene voorwaarden dat de consument, "op straffe van verval van alle rechten", de ontvangen goederen meteen moet controleren en eventuele klachten binnen 24 uur moet melden, of iets van vergelijkbare strekking. Veel consumenten zullen zich hierdoor af laten schrikken, en als ze pas na een paar dagen zien dat er iets niet klopt of dat het artikel om één of andere reden niet aan de verwachtingen voldoet, er ten onrechte van uitgaan dat ze hun recht om de zaak terug te sturen, verspeeld hebben.

En als er dan toch nog iets misgaat, en er een geschil tussen koper en verkoper ontstaat, dan is het voor beide partijen wenselijk als er een vorm van online dispute resolution (ODR), alternatieve geschillenbeslechting online, beschikbaar is. Hoewel ODR nog in de kinderschoenen staat zijn er wel een aantal hoopvolle initiatieven: arbitrage (werkt bijvoorbeeld goed bij geschillen rond domeinnamen), mediation en online geschillencommissies.⁷⁶

Er liggen op het gebied van e-commerce nog wel wat problemen en uitdagingen. Zo is bij grensoverschrijdende e-commerce in veel gevallen en voor veel partijen niet duidelijk welk recht van toepassing is, en welke rechter bevoegd is. Dat kan voor webwinkels een reden zijn om dan maar niet naar het buitenland te leveren, uit angst om in een onbekend buitenland voor de rechter gesleept te worden. Zelfs binnen de EU, waar door de E-Commerce Richtlijn toch sprake zou moeten zijn van harmonisatie van regelgeving, speelt dit probleem. En Europese webwinkeliers durven vaak niet aan

⁷¹ bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet.

⁷² als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet.

⁷³ Art. 7:46f lid 1 BW.

⁷⁴ Art. 7:46g BW.

⁷⁵ Art. 7:46c lid 2 BW.

⁷⁶ Zie het Dossier online geschillenoplossing van Arno Lodder op <http://appia.rechten.vu.nl/~lodder/crodr/index.html> voor een overzicht. Zie <http://www.onlineresolution.com/index-om.cfm>, en www.mediate.com voor werkende voorbeelden van online mediation. En zie tenslotte Gijsbert Brunt, Peter van Schelven, Leo van der Wees (red.), 'Loshetzelfop.nl', ADR in digitale context, Elsevier Juridisch, 2004.

de VS te leveren, uit angst voor productenaansprakelijkheid. Het moge duidelijk zijn dat deze rechtsonzekerheid de internationale handel niet ten goede komt.

Sowieso is de juridische wirwar van regels voor (potentiële) webwinkeliers een probleem. Ze worden met allerlei regels geconfronteerd op het gebied van domeinnamen, auteursrecht (wat mag wel en wat mag niet open een website staan), privacy (welke gegevens van klanten mogen verzameld worden, en wat mag wel en niet met die gegevens gedaan worden), consumentenrecht etc. Er zijn wel initiatieven om een en ander, bijvoorbeeld voor het MKB, wat inzichtelijker te maken.⁷⁷

Tenslotte zijn er ook nog allerlei technische problemen en beveiligingsrisico's. Zo is er pas sinds kort een geaccepteerde en veilige manier om via Internet te betalen, en ook verhalen over frauduleuze praktijken als identity theft en phishing⁷⁸ doen het benodigde vertrouwen om aan e-commerce te beginnen (zoals voor de aanbieder als de consument) geen goed.

6.3.4 Online marketing en reclame

6.3.4.1 Reclame en marketing via het WWW

Belangrijk onderdeel van de elektronische handel betreft de online marketing en reclame.

Dit is een zeer snel groeiende markt, waar ook zeer veel geld in omgaat. Reclame gebeurt met name via web sites, welke niet alleen kan dienen als een passieve advertentie of als een product catalogus maar ook als een interactieve manier om (potentiële) klanten direct te kunnen laten communiceren met de aanbieder om bijv. de order te plaatsen of de dienst direct af te nemen. Naast het adverteren op de eigen site is het ook mogelijk om te adverteren op de sites van anderen. Dit gebeurt meestal in de vorm van een *banner*, een klein balkje met de naam van het bedrijf en een hyperlink naar de website van diens bedrijf.

Wat bij online reclame belangrijk is, is het feit om hoog in de resultatenlijst van de zoekmachines, en met name Google, te komen. Zoals eerder vermeld, zijn de relevante zoektermen van essentieel belang voor een website om gevonden te kunnen worden door de betreffende zoekmachines. Vaak worden de zoekresultaten in de zoekmachines gemanipuleerd door het invoeren van zoektermen die populair zijn of niets met de aangeboden producten of diensten te maken hebben. Hiervoor bestaan zelfs speciale bedrijven met tekstschrijvers die ingehuurd kunnen worden, ook wel zoekmachinemarketing genoemd. De technieken om de zoekmachines te manipuleren worden steeds geavanceerder. Hieronder bij de bespreking van het merkenrecht zal de manipulatie van zoekmachines verder worden besproken.⁷⁹

De algemene regels betreffende misleidende reclame (artt. 6:194-196 BW) zijn onverkort van toepassing op online reclame. Naast misleidende uitingen op een website kan online reclame en marketing ook anderszinds onrechtmatig zijn. Dit kan bijvoorbeeld het geval zijn bij het gebruik van hyperlinks. Door een hyperlink wordt gebruik gemaakt van de informatie op de website waarnaar verwezen wordt. In principe hoeft er geen voorafgaande toestemming aan de site houder gevraagd hoeft te worden om een hyperlink naar diens site aan te leggen. Uit de jurisprudentie⁸⁰ blijkt dat het aanbrengen van een hyperlink naar elders rechtmatig openbaar gemaakt materiaal in het algemeen toelaatbaar wordt geacht, in elk geval zolang de rechthebbende geen adequate technische beschermingsmaatregelen heeft getroffen.⁸¹

De sitehouder kan in principe wel technisch wel wat doen om hyperlinken naar zijn site te verhinderen, maar juridisch niets, tenzij er op een onrechtmatige manier gebruik wordt gemaakt van de informatie op zijn website. Indien door middel van een hyperlink op een onbetamelijke wijze gebruik wordt gemaakt van de inhoud van een andere website, of als er door een hyperlink de indruk wordt

⁷⁷ Bijvoorbeeld door Syntens met het boekje "Nederland gaat digitaal, netjes volgens het boekje", www.innovatienet.nl en vergelijkbare initiatieven.

⁷⁸ Oplichting op internet, zie <http://www.xs4all.nl/veiligheid/phishing/>.

⁷⁹ Zie ook N. van Eijk, *Zoekmachines; zoekt en gij zult vinden?*, Inaugurale rede 17 juni 2005, Amsterdam: Otto Cramwinckel (2005).

⁸⁰ Pres. Rb. Rotterdam 22 augustus 2000, *Informatierecht/AMI* 2000-10, p. 207-210, m.nt K.J. Koelman (*Kranten.com*); HR 22 maart 2002, *Computerrecht* 2002-3 (*NVM/Telegraaf*); Vzr. Rb Leeuwarden, 30 oktober 2003, *IER* 2004/25, (*Vriend/Batavus*); anders: Hof Amsterdam, 15 juni 2006, LJN: AX7579, (*Zoek MP3*)

⁸¹ R. Chavannes en W. Steenbruggen, Paperboy, noot onder Bundesgerichtshof 17 juli 2003, I ZR 259/00 (*Paperboy*), *JAVI* 2003/6

gewekt dat er een economische of administratieve band bestaat tussen de houders van de twee sites kan dit onder omstandigheden als ongeoorloofde mededinging beschouwd worden.⁸² Dit werd bijvoorbeeld aangenomen in de Batavus zaak.⁸³ Hier ging het om een specifieke manier van hyperlinken, nl. het zgn. *framing*. Dit wil zeggen dat de website waarnaar verwezen wordt door middel van de hyperlink in het beeld (het *frame*) van de verwijzende partij verschijnt.⁸⁴ De rechter was in dit geval van oordeel dat het hyperlinken op zichzelf weliswaar geen auteursrechtelijke verveelvoudiging oplevert, maar dat het in een kader van de eigen site weergeven van pagina's van Batavus toch onrechtmatig is en het auteursrecht schendt, omdat de indruk wordt gewekt dat het *geframede* gedeelte eigen materiaal van Vriend betreft. In welke gevallen door een hyperlink inbreuk op auteursrecht gemaakt wordt komt hierna (paragraaf 6.4.2) verder aan de orde.

In het verband van online reclame en marketing verdient art. 3:15e BW eveneens bespreking. Dit artikel, zijnde de implementatie van art. 2 sub f en art. 6 van de Richtlijn elektronische handel, bevat een regeling voor commerciële communicatie in het algemeen. Hieronder wordt verstaan “*elke vorm van communicatie bestemd voor het aanprijzen van de goederen, diensten of het imago van een onderneming, instelling of persoon die een commerciële, industriële of ambachtelijke activiteit of een gereguleerde beroep uitoefent, met uitzondering van informatie die rechtstreeks toegang geeft tot de activiteit van de onderneming, instelling of persoon, in het bijzonder een domeinnaam of een elektronisch postadres. Mededelingen over goederen of diensten of het imago van een onderneming, instelling of persoon die onafhankelijk van deze en in het bijzonder zonder financiële tegenprestatie zijn samengesteld, zijn geen commerciële communicatie.*”⁸⁵ Degene die de commerciële communicatie doet uitgaan dient er voor te zorgen dat (i) deze duidelijk als zodanig herkenbaar is; (ii) hij zijn identiteit vermeldt; en (iii) dat de commerciële communicatie, indien deze verkoopbevorderende aanbiedingen, wedstrijden of spelen omvat, een duidelijke en ondubbelzinnige vermelding bevat van de aard en de voorwaarden van de aanbieding of de deelneming.

6.3.4.2 Marketing en reclame via e-mail (spamming)

Lid 4 van het bovenbesproken art. 3:15e BW bevat tevens de plicht om zich “duidelijk en ondubbelzinnig als zodanig herkenbaar te maken” voor degene die ongevraagd per e-mail reclame verstuurt. Het ongevraagd toezenden van e-mails met commerciële inhoud wordt ook wel *spamming* genoemd.⁸⁶ Op grond van art. 11.7 van de Telecommunicatiewet is sinds mei 2004 het versturen van spam in of vanuit Nederland is niet toegestaan, tenzij de ontvanger voorafgaande toestemming heeft gegeven (de zogenaamde *opt in*). Het verbod heeft betrekking op alle verstuurde spam (bulk)mail en ongeacht of de inhoud nu commercieel of politiek is. Niet alleen ongevraagde e-mails maar bijvoorbeeld ook ongevraagde SMS'jes en faxen zijn spam. De regel dat voorafgaande toestemming van de ontvanger is vereist, geldt alleen voor abonnees die natuurlijke personen zijn, meestal particulieren. Rechtspersonen, meestal ondernemingen, vallen (nog) niet onder het verbod op spam.⁸⁷

⁸² De Cock Buning en Vermeer, (1999), pp. 166-173.

⁸³ V.zr. Rb Leeuwarden, 30 oktober 2003, *IER* 2004/25 (Vriend/Batavus)

⁸⁴ Er zijn nog meerdere varianten van hyperlinken mogelijk, zoals *surface links*, *deep links*, *inline links* en *framed links*. Zie Deborah Lakerveld en Tina van der Linden-Smith, ‘Verboden links’, *NJB* 22 augustus 2003, p. 1490 - 1496.

⁸⁵ Het is overigens twijfelachtig of bijvoorbeeld een “hyperlink” onder het begrip commerciële communicatie valt. Zie hiervoor M. Vermeer, IPR-kluwen van elektronische ongeoorloofde mededinging; de warboel na de implementatie van de E-commerce richtlijn, *JAVI* 2002/1, pp. 16-23

⁸⁶ Over spam zie A. Lodder, H.W.K. Kaspersen e.a. Spam, Spammer,... Sdu Uitgevers Den Haag, 2004, p. 157 e.v. Zij definiëren spam als: "E-mail die als communicatie ongevraagd is en een niet-gewenste inhoud heeft."

⁸⁷ Recentelijk (maart 2006) heeft de ministerraad op voorstel van minister Brinkhorst van Economische Zaken ingestemd met een aantal wijzigingen van de Telecommunicatiewet. Een daarvan betreft een verbod voor ongevraagde spam, sms'jes, faxen en andere soorten elektronische communicatie zonder voorafgaande toestemming van bedrijven. Ongevraagde elektronische berichten voor marketingdoeleinden zijn al bij wet verboden als het gaat om berichten naar burgers (natuurlijke personen). De nieuwe wijziging zorgt ervoor dat deze regeling ook geldt voor ongevraagde berichten tussen bedrijven (rechtspersonen).

De verzenders van de berichten moeten kunnen aantonen dat de ontvanger van de berichten toestemming heeft gegeven om de mail te ontvangen. Daarnaast moet bij elke e-mail een duidelijke en makkelijke opt-out mogelijkheid aanwezig zijn, zodat mensen zich kunnen uitschrijven en moet de afzender zich duidelijk kunnen identificeren.⁸⁸

De OPTA, de toezichthouder op de Nederlandse post- en telecommunicatiemarkt, handhaaft het verbod. Bij de OPTA kunnen er klachten ingediend worden over spam⁸⁹ indien: (a) die is verzonden aan een adres of nummer dat bij een particulier in gebruik is; (b) die een commercieel, ideëel of charitatief karakter heeft; en (c) waarvan de verzender (degene die op de verzendknop drukt, of degene die opdracht geeft tot de verzending) zich in Nederland bevindt. OPTA kan dus niet optreden tegen buitenlandse spam. Als blijkt dat er sprake is van een overtreding, kan OPTA besluiten een boete op te leggen of een waarschuwing uit te delen.

Ook in de jurisprudentie is het spammen al meerdere keren aan bod gekomen.⁹⁰ De meeste bekende uitspraak is die van de Hoge Raad in de zaak van XS4ALL v. AbFab,⁹¹ die overigens gedaan is vóórdat het huidige art. 11.7 Tw. van kracht werd. XS4all wil Ab.Fab verbieden om commerciële e-mail berichten te (doen) verzenden, al dan niet namens derden, naar (e-mail adressen van) gebruikers en/of klanten en/of abonnees van XS4ALL, voor zover deze niet expliciet en per geval aantoonbaar hebben ingestemd met het ontvangen van dergelijke berichten. De Hoge Raad oordeelt dat “*indien iemand zonder daartoe gerechtigd te zijn gebruik maakt van een goed waarop een ander een exclusief recht heeft, en hij daardoor - zoals in de regel het geval zal zijn - inbreuk maakt op dat exclusieve recht, hij onrechtmatig handelt tegenover die rechthebbende, behoudens de aanwezigheid van een rechtvaardigingsgrond.*”⁹² Het versturen van spam kan dus onrechtmatig zijn jegens de provider. Echter, in de praktijk blijkt dat het wettelijke spamverbod geen daadwerkelijke oplossing biedt voor de grote hoeveelheid commerciële e-mail die dagelijks in de mailboxen verschijnt. Door gebruikmaking van allerlei technieken kunnen degenen die dergelijke mailtjes versturen anoniem en onzichtbaar blijven. Slechts een klein deel van hen kan daadwerkelijk worden achterhaald. In Nederland heeft de OPTA in de laatste twee jaar slechts twaalf boetes aan spammers opgelegd.⁹³ Daarbij komt dat de meeste spam uit het buitenland komt, en dan is handhaving van het spamverbod feitelijk zo goed als onmogelijk. Waarschijnlijk is het technisch weren van spam door middel van het gebruik van spamfilters nog het meest effectief.

6.4 Bescherming van intellectuele eigendomsrechten

6.4.1 Merkenrecht

6.4.1.1 Domeinnamen

⁸⁸ Er bestaan ook zgn. opt-out registers: consumenten die zich gemeld hebben bij infofilter.nl zouden verstoken moeten blijven van alle aangegeven vormen van spam. Of dit soort registers ook echt werken is onduidelijk, in ieder geval “gelden” ze alleen voor bedrijven en organisaties die zich bij zo’n register aangesloten hebben.

⁸⁹ www.spamklacht.nl

⁹⁰ Zie oa. V.zr. Rotterdam 5 december 2002, *Computerrecht* 2003-2, p. 209-212 (Netwise/NTS) m.nt. Lodder, Hof Arnhem, 4 februari 2003, *NJ* 2004/54 (Dr Rath/Staat der Nederlanden), Interessant is ook de uitspraak van de Rb Breda in een “omgekeerde” spamactie, nl het verzenden van een heleboel mailtjes aan één persoon (ipv het gebruikelijke spammen, één mailtje naar een heleboel personen) Rb. Breda 10 november 2005 (spamwraakactie), L.J.N. AU6703 m.nt. A.R. Lodder, *Privacy & Informatie*, (2), 2006.

⁹¹ HR 12 maart 2004, L.J.N.-nummer AN8483.

⁹² Dezelfde redenering (inbreuk op eigendomsrecht) is later, nog discutabeler, toegepast in Voorzieningenrechter 's-Gravenhage 21 juli 2004 (nationalevacaturebank.nl vs. CVBank), met noot door J.J.C. Kabel te vinden op http://www.ivir.nl/publicaties/kabel/IER2004_6vacaturebank.html. Andere uitspraken over spam zijn o.a. Rb Amsterdam, 15 juli 2004, L.J.N.-nummer AQ1745 (*Nigeriaanse Advance Fee Fraude*) en Rb Amsterdam, 12 februari 2004, L.J.N.-nummer AO3649 (*Van Dusseldorp-Broadcast Press*) en Rechtbank Breda 10 november 2005 (spamwraakactie), L.J.N.-nummer AU6703

⁹³ Zie de berichtgeving over het eerste EU Spam symposium op 15 juni 2006 (www.spamsymposium.org), E. Feldmann, *Spamwetgeving blijkt weinig effectief*, Webwereld, 16 juni 2006. Zie ook H. de Vries en N. Wolters Ruckert, De eerste boetes voor Nederlandse spammers, *JutD* nr. 2, 3 febr. 2005 blz. 16-19

Een keerzijde van de commerciële mogelijkheden van het Internet is dat het óók inbreuken mogelijk maakt. Er zijn verschillende manieren waarop bijvoorbeeld inbreuk op een merkrecht gemaakt kan worden.

Een merk is een teken dat dient om de waren van een onderneming te onderscheiden.⁹⁴ Een merkhouder verkrijgt een uitsluitend recht op een merk door een depot conform art. 3 BMW.

Omdat domeinnaam registraties in principe op een “wie-het-eerst-komt-wie-het-eerst-maakt” basis worden behandeld, werden in het verleden vaak de merken van bekende of minder bekende bedrijven als domeinnaam geregistreerd door personen die niet de rechthebbende waren. Het komt voor dat een dergelijk geregistreerde domeinnaam vervolgens aan de merkhouder worden aangeboden voor een prijs die veel hoger ligt dan de registratielasten. Dergelijke acties worden “domain name grabbing” of “cybersquatting” genoemd. Indien de geregistreerde domeinnaam niet aan de merkhouder wordt aangeboden maar door de registrant zelf wordt gebruikt wordt er gesproken van “not quite domain name grabbing”. Van een onschuldige registratie is sprake als de registrant logischerwijze zelf ook reden heeft om die betreffende domeinnaam te doen registreren.⁹⁵

Normaliter kunnen twee of meer merken naast elkaar bestaan zolang ze maar geen verwarring wekken.⁹⁶ Het is echter technisch onmogelijk om twee dezelfde domeinnamen naast elkaar te laten bestaan omdat zij beide verwijzen naar het hetzelfde IP-adres. Het registreren van andermans merknaam als domeinnaam wordt in de regel bestreden op basis van de het merkrecht. Een merkhouder kan zich op grond van art. 13A lid 1 BWM verzetten tegen gebruik van een teken door anderen:

- a. *“wanneer dat teken gelijk is aan het merk en in het economisch verkeer gebruikt wordt voor dezelfde waren als die waarvoor het merk is ingeschreven;”*
Het moet dus gaan om een gebruik van precies hetzelfde teken voor precies dezelfde waren. Een voorbeeld hiervan is te vinden in Pittway-Blom.⁹⁷ Pittway brengt koolmonoxidemelders op de markt onder de gedeponeerde merknaam “first alert” en is houder van de domeinnaam firstalert.com. Blom verkoopt de melders in Nederland, en registreert de domeinnaam firstalert.nl bij de SIDN. De rechter oordeelt dat door het gereserveerd houden van de domeinnaam firstalert.nl sprake is van gebruik voor de waren waarvoor het merk “first alert” is ingeschreven en daarmee van inbreuk op het merk “first alert”.
- b. *“Wanneer dat teken gelijk is aan of overeenstemt met het merk en in het economisch verkeer gebruikt wordt voor dezelfde of soortgelijke waren, indien daardoor bij het publiek verwarring kan ontstaan, inhoudende het gevaar van associatie met het merk;”*
Factoren die een rol spelen bij de vraag of er sprake is van verwarringsgevaar zijn: de overeenstemming van het merk met het teken, de onderscheidingskracht van het merk en de soortgelijkheid van waren. En het gaat daarbij om de indruk van de gemiddelde internetgebruiker. Een voorbeeld is de zaak I do! I do!⁹⁸ Eiser in deze zaak, I do! I do! is een detailhandel in bruidsen gelegenhedskleding, die het woordmerk “I do! I do!” gedeponeerd heeft. De gedaagde is uitgever van een huwelijkskrant, die de domeinnaam “ido.nl” geregistreerd heeft. De rechter oordeelt dat de domeinnaam inbreuk maakt op het merkrecht van eiser. En met betrekking tot de domeinnaam: *“Gelet op de vastgestelde merkinbreuk, geldt ook dat sprake is van merkinbreuk bij het gebruik door [gedaagde] c.s. van de domeinnamen IDO.NL (...). Immers de kans bestaat dat de raadpleger van de website van [gedaagde] ten onrechte meent dat de informatie van [eiseres] afkomstig is. Voorts ontnemt het gebruik van de domeinnaam IDO.NL, [eiseres] de mogelijkheid om zelf een website onder die naam te openen. Het gebruik van domeinnamen die aanvangen met IDO en in verband worden gebracht met bruidsartikelen, wekken de suggestie dat deze betrekking hebben op websites van [eiseres].”*
- c. *“wanneer dat teken gelijk is aan of overeenstemt met het merk en in het economisch verkeer gebruikt wordt voor waren, die niet soortgelijk zijn aan die waarvoor het merk is ingeschreven,*

⁹⁴ Zie de definitie in art. 1 BMW. Daarnaast zijn er ook nog zgn. collectieve merken, art. 19 BMW.

⁹⁵ Zoals naar het oordeel van de rechter het geval was in ariel.nl, Pres. Rb. Amsterdam 24 februari 2000, LJN-nummer AA4931.

⁹⁶ Zoals bijv. “Ajax” voor een voetbalclub, een schoonmaakmiddel en brandblusapparatuur.

⁹⁷ Pres. Rb. 's-Gravenhage 11 augustus 1999, DomJur 2001-49 (te vinden op www.domjur.nl).

⁹⁸ Pres. Rb. Amsterdam 13 april 2000, DomJur 2000-32.

indien dit merk bekend is binnen het Benelux-gebied en door het gebruik, zonder geldige reden, van dat teken ongerechtvaardigd voordeel wordt getrokken uit of afbreuk wordt gedaan aan het onderscheidend vermogen of de reputatie van het merk;”

Vaak wordt een beroep hierop gedaan in combinatie met een beroep op art. 13A lid 1 sub d BMW (zie hierna). Een voorbeeld is de zaak ID-NL.⁹⁹ Het bedrijf ID-NL (houder van het woordmerk ID-NL) is een innovatiecentrum voor uitvindingen. Gedaagde voert een onderneming onder de naam ID Nederland Multi Media en maakt gebruik van de domeinnaam IDNL.NET. De President stelt vast dat voor een merkinbreuk ex art. 13A lid 1 sub c het niet nodig is dat de gebruikte domeinnaam precies identiek is aan de merknaam (i.c. ID-NL). Voldoende is dat er sprake is van zodanige visuele en auditieve gelijkenissen, dat er gevaar is voor verwarring. Bovendien ‘lift’ de gedaagde mee op de bekendheid en reputatie van eiseres, wat kan leiden tot ongerechtvaardigd voordeel trekken uit of afbreuk doen aan de reputatie van eiseres.

- d. *“wanneer dat teken gebruikt wordt anders dan ter onderscheiding van waren, indien door gebruik, zonder geldige reden, van dat teken ongerechtvaardigd voordeel wordt getrokken uit of afbreuk wordt gedaan aan het onderscheidend vermogen of de reputatie van het merk.”*

Deze bepaling dient vaak als vangnet, voor het geval een beroep op 13A lid 1 sub c BMW (zie hierboven) niet lukt. Er is dan ook veel jurisprudentie op deze bepaling. Een bekend voorbeeld is klm-alitalia.com,¹⁰⁰ waarin een juwelier meteen na het bekendworden van samenwerkingsplannen tussen KLM en Alitalia de domeinnaam klm-alitalia.com registreerde en daarmee afbreuk deed aan het onderscheidend vermogen van de merken KLM en Alitalia.

Overigens kunnen domeinnamen ook inbreuk maken op een handelsnaamrecht of een “gewone” onrechtmatige daad opleveren. Een voorbeeld van een handelsnaamrechtzaak is Eendengarage.nl¹⁰¹ (twee garagebedrijven gespecialiseerd in deux-chevaux, die zich allebei eendengarage noemden, en waarvan eentje de domeinnaam eendengarage.nl geregistreerd had), waarin overigens werd geoordeeld dat er in casu géén sprake van was inbreuk op een handelsnaam. En in alle andere gevallen waarin een eiser niet blij is met een domeinnaam, maar hij geen merkrecht of handelsnaam heeft, moet art. 6:162 BW soelaas bieden. Voorbeelden zijn conflicten waarbij een overheidsdomeinnaam of iets wat daarop lijkt betrokken is (zoals ministers.nl en betuweroute.nl),¹⁰² of waarbij het gaat om een eigenaam (zoals janpeterbalkenende.nl).¹⁰³

Sinds januari 2003 kunnen geschillen over na die datum geregistreerde domeinnamen door middel van arbitrage beslecht worden. Indien een houder van een merk of een handelsnaam van mening is dat een bepaalde .nl-domeinnaam inbreuk maakt op zijn rechten heeft de keuze om een arbitrageprocedure te starten bij het arbitrage-instituut voor .nl-domeinnamen, of een gerechtelijke procedure te starten.¹⁰⁴ Dit arbitrage instituut is het WIPO Arbitration and Mediation Center. Dit instituut past in geschillen in het .nl domein de bestaande SIDN arbitrageregeling¹⁰⁵ toe. Echter deze arbitrageregeling voldoet niet helemaal. Sinds 2003 slechts een negental uitspraken gedaan onder de .nl arbitrage regeling tegenover meer dan 50 “gewone” gerechtelijke procedures. Volgens het Rapport Domeinnaamdebat 2006¹⁰⁶ is de arbitrage regeling niet laagdrempelig, en te duur. De SIDN beraadt zich thans over een alternatieve geschillenregeling. Eén van de opties is een administratieve procedure gebaseerd op de internationale Uniform Domain-Name Dispute-Resolution Policy (UDRP).¹⁰⁷ In deze procedure dient o.a. een domeinnaam door een registrant overgedragen te worden indien

⁹⁹ Pres. Rb. Almelo 3 mei 2000, DumJur 2000-16.

¹⁰⁰ Pres. Rb. Arnhem 25 oktober 1999, DomJur 2000-6.

¹⁰¹ Rb. Haarlem, Sector Kanton Locatie Zaanstad 3 oktober 2002 (Eendengarage), LJN-nummer AE7409.

¹⁰² Pres. Rb. Utrecht 11 januari 2001, LJN-nummer AA9488 resp. Hof Amsterdam 15 november 2001, DomJur 2001-116. Zie ook de noot van P.B. Hugenholtz op <http://www.ivir.nl/publicaties/hugenholtz/noot-ministers.nl.html>.

¹⁰³ Voorzieningenrechter Arnhem 3 december 2002, LJN-nummer AF1373

¹⁰⁴ www.sidn.nl onder “domeinnaam kaping”. Alle houders van na 29 januari 2003 aangevraagde, verhuisde of gewijzigde .nl-domeinnamen hebben zich door het tekenen van het registratiecontract onderworpen aan deze arbitrage.

¹⁰⁵ Regeling voor .nl-domeinnaamarbitrage, SIDN, 2003

¹⁰⁶ Rapport Domeinnaamdebat 2006, www.domeinnaamdebat206.nl

¹⁰⁷ Deze procedure is opgesteld door de ICANN, zie hiervoor www.icann.org/udrp/udrp-policy-24oct99.htm

- de domeinnaam identiek is aan een ouder merk;
- de domeinnaamhouder geen rechten of legitieme belangen met betrekking tot de domeinnaam heeft; en
- de domeinnaam te kwader trouw is geregistreerd en gebruikt.¹⁰⁸

Het aantal rechtszaken over domeinnamen is de laatste jaren spectaculair gedaald. Een belangrijke oorzaak hiervan is dat de problematiek hierover (wel of geen merkinbreuk) min of meer is uitgekristalliseerd. Daarnaast zijn de mogelijkheden voor domeinnaamkapers zo beperkt geworden zodat er niet veel geld meer aan te verdienen is en er dus ook veel minder geschillen zijn. Als derde reden wordt nog aangevoerd dat in dit rechtsgebied veel geschillen worden geschikt. Bij een mogelijk inbreukmakende domeinnaam is een brief van een advocaat vaak al voldoende om de domeinnaam over te dragen.¹⁰⁹

6.4.1.2 Zoekmachines

Ook het gebruik van de sleutelwoorden in de onderliggende HTML codes, de metatags, kan aan merkenrechtelijke beperkingen onderhevig zijn.¹¹⁰ Op grond van het merkenrecht kan het gebruik van bekende merken in de metatags van websites worden bestreden. In de eerste Nederlandse uitspraak over metatags¹¹¹ oordeelde de rechtbank dat het gebruiken van eens anders merknaam in de metatags van een website merkinbreuk in de zin van artikel 13A lid 1 sub d BMW kan opleveren. In de daaropvolgende uitspraak inzake VNU/MonsterBoard¹¹² bepaalde de rechtbank dat het gebruik van het woord "Intermediair" als magneetwoord door een concurrent van de rechthebbende is te beschouwen als gebruik van dat merk in de zin van artikel 13A lid 1 sub a BMW.¹¹³

Behalve een lijst met sites waarop het gevonden woord voorkomt, presenteert zoekmachine Google ook advertenties die mogelijk relevant zijn voor de gebruiker die op dát woord zoekt. Zo kan een bedrijf de merknaam van een concurrent als zgn. "Adword" opgeven, waardoor zijn advertentie getriggerd wordt op het moment dat een gebruiker via Google zoekt naar de site van de concurrent. Ook dit kan merkinbreuk opleveren, zo oordeelde de rechter in een conflict tussen twee carrier-preselect bedrijven Pretium en Yiggers.¹¹⁴

6.4.2. Auteursrecht

Een tweede intellectueel eigendomsrecht waarop via Internet gemakkelijk inbreuk kan worden gemaakt, is auteursrecht. Het auteursrecht is, volgens art. 1 Aw: *"het uitsluitend recht van den maker van een werk van letterkunde, wetenschap of kunst, of van diens rechtverkrijgenden, om dit openbaar te maken en te verveelvoudigen, behoudens de beperkingen, bij de wet gesteld."* Cruciale termen in deze definitie zijn "openbaar maken" en "verveelvoudigen", en ook de wettelijke beperkingen van het uitsluitende recht van de rechthebbenden spelen in een internetcontext een belangrijke rol. We zullen een aantal veelvoorkomende handelingen op het Internet bespreken, om te bezien of en in hoeverre er sprake is of kan zijn van inbreuk op auteursrecht. Achtereenvolgens zullen aan de orde komen: browsen, linken, uploaden (of beschikbaar stellen), downloaden, en tenslotte het aanbieden van programmatuur om het delen van bestanden mogelijk te maken. Vervolgens zal bekeken worden welke mogelijkheden er voor auteursrechthebbenden zijn om hun belangen veilig te stellen.

¹⁰⁸ Zie <http://arbiter.wipo.int/domains>

¹⁰⁹ Rapport Domeinnaamdebat 2006, p. 41

¹¹⁰ Zie uitgebreid T. Oudejans, *Electronic Highway of Electronic Subway?*, IteR uitagve nr. 23, Kluwer, Deventer, 1999.

¹¹¹ Pres. Rb. Dordrecht 9 februari 1999, BIE 1999/5, p. 171-174 (Deutz/ADT).

¹¹² Pres. Rb. 's Gravenhage, 29 juni 1999, IER 1999/5 (VNU/The Monsterboard) (met nt JK), p. 219.

¹¹³ Overigens oordeelde het Hof in hoger beroep dat "Intermediair" een generieke term is en dus geen bescherming als merk geniet, Hof 's-Gravenhage 8 maart 2001 (VNU-Monsterboard), te vinden op www.internetrechtspraak.nl.

¹¹⁴ Voorzieningenrechter 's Gravenhage 12 november 2004. Zie voor een overzicht van de internationale jurisprudentie op dit punt: Tina van der Linden: Google: zoekresultaten in een juridische context, Javi nr 4, augustus 2004, pp. 143-148.

Tekst, plaatjes, foto's, bewegende beelden of muziek kunnen gedigitaliseerd worden en via het Internet verspreid. De techniek van het Internet brengt met zich mee dat talloze elektronische kopieën van data, dus ook van auteursrechtelijke beschermde werken, gemaakt worden. Ten eerste bij het "uploaden" van het betreffende werk op het Internet, daarnaast bij het "downloaden" of het uitprinten ervan. Vervolgens worden ook tijdens de transmissie van de data van de een naar de andere computer ook (tijdelijke) kopieën gemaakt op de routers, de computers die voor de verzending via het Internet zorgdragen.

Ieder auteursrechtelijk beschermd werk kan in feite worden verzonden via het Internet aan een of meerdere ontvangers. Die ontvangers kunnen het op hun beurt weer aan een of meerdere personen doorsturen. Op die manier kan een auteursrechtelijke beschermd werk talloze malen gekopieerd worden zonder dat er verlies in de kwaliteit van het werk optreedt. Omdat het werk in digitale vorm is opgeslagen kunnen er tevens gemakkelijk veranderingen in worden aangebracht, en in gewijzigde vorm weer verder worden verspreid. Een andere aan de techniek inherente bijkomstigheid is dat er geen substantiële kosten zijn verbonden aan de verspreiding op grote schaal van een auteursrechtelijk beschermd werk.

Het in december 1996 totstandgekomen Auteursrechtverdrag van de WIPO bepaalt in artikel 8 dat de beschikbaarstelling van werken via het Internet in beginsel onder het auteursrecht valt: "*.. authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.*"

Dit betekent dat in beginsel voor iedere openbaarmaking en verveelvoudiging van een auteursrechtelijk beschermd werk de rechthebbende toestemming moet hebben gegeven. Echter, een probleem vormen de tijdelijke kopieën die tijdens de transmissie gemaakt worden op de *routers* wanneer data van de een naar de andere computer worden gestuurd. Een hier mee verwant probleem is ook het zogenoemde *browsen*, ook wel het "surfen" genaamd, wat inhoudt dat de gebruiker websites even bekijkt om vervolgens weer door te klikken naar andere sites. Wanneer bij het browsen een gebruiker het adres van een website intypt of een hyperlink activeert, doet de gebruiker als het ware een verzoek aan de computer waar de data van die website opgeslagen liggen om een kopie naar zijn computer te sturen. De kopie van de data van de betreffende website worden dan, zo lang de gebruiker de site bekijkt, tijdelijk opgeslagen in het geheugen van zijn computer. Hiermee is verwant is het zgn. *caching*. Dit houdt in dat de kopieën van veelvuldig of recent opgevraagde web pagina's op de server van de service provider worden opgeslagen, om het wachten voor het opvragen van een website te bekorten.¹¹⁵

Het is een belangrijke vraag of dergelijke vormen van tijdelijke verveelvoudiging een auteursrechtelijke inbreuk vormen. Zo ja, dan zou voor iedere tijdelijke kopie voorafgaand toestemming gevraagd moeten worden aan de auteursrechthebbende. Dit zou de werking van het Internet in het algemeen en van het WWW in het bijzonder, niet ten goede komen, om niet te zeggen onmogelijk maken. Tijdens de onderhandelingen van het WIPO Auteursrechtverdrag in 1996 kon er over dit punt geen overeenstemming worden bereikt.¹¹⁶ De WIPO verdragen bevatten hier dan ook geen regeling over. De Europese Auteursrechtlijn¹¹⁷ daarentegen bevat wel duidelijke regels over de digitale reproductiehandeling. Volgens art. 2 van de Richtlijn zijn ook de indirecte, tijdelijke en gedeeltelijke verveelvoudigingen aan toestemming van de rechthebbende onderhevig. Een uitzondering hierop is geformuleerd in artikel 5 lid 1 waarin het volgende wordt bepaald:

"Tijdelijke reproductiehandelingen, als bedoeld in artikel 2, die van voorbijgaande of incidentele aard zijn, en die een integraal en essentieel onderdeel vormen van een technisch procédé en die worden toegepast met als enig doel

a) de doorgifte in een netwerk tussen derden door een tussenpersoon of

¹¹⁵ Zie uitgebreid over het auteursrecht en het Internet, Hugenholtz, Handelingen NJV 1998-I, pp. 198-260, en, recenter, Bart Schermer, Rapport Auteursrecht en Informatiemaatschappij, een kort overzicht, te vinden op http://www.ecp.nl/publications/Rapport_Auteursrecht_en_Informatiemaatschappij.pdf

¹¹⁶ Lucas, (1998), p. 207.

¹¹⁷ Richtlijn 2001/29/EG ter harmonisering van bepaalde aspecten van auteursrecht en de naburige rechten in de informatiemaatschappij, 22 mei 2001, PB EG L 167.

b) een rechtmatig gebruik van een werk of ander materiaal mogelijk te maken, en die geen zelfstandige economische waarde bezitten, zijn van het in artikel 2 bedoelde reproductierecht uitgezonderd."

Vooralsnog gaan we ervan uit dat browsen en het opslaan van cache-kopieën geen auteursrechtinbreuk opleveren, omdat anders het hele Internet wel opgedoekt kan worden.

Vervolgens komt de vraag aan de orde of door middel van het leggen van een hyperlink van de ene webpagina naar de andere auteursrechtinbreuk gemaakt kan worden. Voor zogenaamde deeplinks (zie hiervoor) heeft de rechter beslist, dat het aanleggen daarvan niet is aan te merken als een (auteursrechtelijke relevante) verveelvoudiging.¹¹⁸ Kortom: deeplinken mag. Voor framed links kan dat anders liggen; als door middel van een framed link de indruk gewekt wordt dat het materiaal van de eigen site afkomstig is, terwijl het in feite ergens anders vandaan gehaald wordt, kan er sprake zijn van "pronken met andermans veren" en daarmee van inbreuk op auteursrecht. De rechter oordeelde dat dit het geval was in de hiervoor ook al genoemde Batavus-zaak.¹¹⁹

Datzelfde geldt waarschijnlijk voor zgn. inline links, waarbij een plaatje of een object uit een andere website wordt gekopieerd en (dynamisch) in de eigen website geplakt, zonder dat de browsende gebruiker zich hier noodzakelijkerwijs van bewust is. Over inline links is in Nederland nog geen uitspraak gedaan.¹²⁰

Als materiaal waar iemand anders auteursrecht op heeft, via Internet beschikbaar wordt gemaakt, is er wèl sprake van openbaarmaking, en daarmee van inbreuk op auteursrecht. Dat kan bijvoorbeeld zijn knippen van andermans materiaal en het vervolgens plakken in een eigen omgeving, of het beschikbaar stellen van bestanden, door ze te uploaden op een webpagina, of door ze bij een peer-to-peer programma ter download aan te bieden in bijvoorbeeld een shared files folder op de eigen harde schijf.

Aan de andere kant is downloaden, zolang het maar voor eigen gebruik is, geen inbreuk op auteursrecht, omdat het valt onder de regeling van de privé-kopie van art. 16b Aw.¹²¹ Daarbij mogen de gemaakte privé-kopieën niet aan derden afgegeven worden,¹²² en is ook belangrijk om op te merken dat deze uitzondering niet geldt voor programmatuur,¹²³ waaronder games.

Tenslotte heeft het Hof Amsterdam beslist, dat ook het aanbieden van programmatuur waarmee filesharing mogelijk is (zgn. peer-to-peer programmatuur) niet aan te merken is als inbreuk op auteursrecht,¹²⁴ dit omdat het voor het programma niet mogelijk is om auteursrechtelijk beschermde bestanden van andere bestanden te onderscheiden.¹²⁵ De HR heeft deze beslissing in stand gelaten.¹²⁶

¹¹⁸ Pres. Rb. Rotterdam 22 augustus 2000 (Kranten.com) LJN-nummer AA6826

¹¹⁹ Voorzieningenrechter Leeuwarden 30 oktober 2003 (Batavus), LJN-nummer AN4570: "*In vergelijking tot de "papieren-wereld" komt het er op neer dat [V.] een brochure van Batavus aan het publiek verstrekt, waarbij de naam van de fabrikant (Batavus) is vervangen door een etiket met de handelsnaam van [V.], aldus Batavus. De rechter is met Batavus van oordeel dat deze handelwijze onrechtmatig is en tevens in strijd is met het auteursrecht van Batavus. Op deze manier wordt immers de indruk gewekt dat de informatie van de website van Batavus eigen materiaal van [V.] betreft.*"

¹²⁰ In de VS wel: Kelly vs. Arriba Soft, U.S. Court of Appeals for the 9th Circuit Court, decision 280 F.3d 934, 6 februari 2002. Zie hierover C. Alberdingk Thijm, "Kelly, Playboy en het ondeugende hyperlinkje", Emerce, 2 mei 2002. Ook de Duitse rechter oordeelde dat de inline links die de afbeeldingen-zoeker van Google als resultaat oplevert, in strijd zijn met het auteursrecht: zie www.jurpc.de/rechtspr/20040146.pdf.

¹²¹ Art. 16b lid 1 Aw: "*Als inbreuk op het auteursrecht op een werk van letterkunde, wetenschap of kunst wordt niet beschouwd de verveelvoudiging welke beperkt blijft tot enkele exemplaren en welke uitsluitend dient tot eigen oefening, studie of gebruik van de natuurlijke persoon die zonder direct of indirect commercieel oogmerk de verveelvoudiging vervaardigt of tot het verveelvoudigen uitsluitend ten behoeve van zichzelf opdracht geeft.*"

¹²² Art. 16b lid 4 Aw.

¹²³ Art. 45n Aw, jo. art. 10 lid 1 onder 12 Aw.

¹²⁴ Hof Amsterdam 28 maart 2002 (Kazaa) LJN-nummer AE0805.

¹²⁵ De voorloper van de huidige generatie peer-to-peer programmatuur, Napster, hield een centrale database bij, waardoor het voor de makers van het programma eenvoudig was auteursrechtelijk beschermde bestanden uit die centrale index te halen. De Amerikaanse rechter oordeelde dan ook dat Napster zich wel mede schuldig maakte aan auteursrechtinbreuk: A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001). Alles over de Napster-zaak is te vinden op <http://www.gseis.ucla.edu/iclp/napster.htm>.

¹²⁶ HR 19-12-2003 (Kazaa) LJN-nummer AN7253.

In de uitspraak van het Hof Amsterdam over de zoekmachine voor mp3 bestanden, Zoek MP3,¹²⁷ waarbij auteursrechtelijke aspecten een grote rol speelden, werd er, opmerkelijk genoeg, geen uitspraak gedaan over auteursrechtinbreuk. Het ging hier over een website die het zoeken van mp3-muziekbestanden op het WWW faciliteert. Zij levert na ontvangst van een zoekopdracht van een bezoeker van haar website hyperlinks/deeplinks naar het door hem of haar gewenste mp3-muziekbestand op het WWW. Als haar bezoeker die link aanklikt, maakt zijn computer contact met de server waarop het gevonden bestand staat en wordt het bestand direct gedownload naar de computer van de bezoeker. Het Hof zegt over het beschikbaar stellen via internet van mp3-muziekbestanden dat het *“ophalen van die muziekbestanden noodzakelijkerwijs een auteursrechtelijk of nabuurrechtelijk relevante openbaarmaking voorafgaat. Indien die openbaarmaking geschiedt zonder toestemming van de rechthebbenden, maakt de openbaarmaker inbreuk op de auteurs- en/of nabuurrechten van de rechthebbenden. Aan het ophalen van ongeautoriseerde muziekbestanden gaat dus noodzakelijkerwijs een inbreuk op de auteurs- en/of nabuurrechten van de rechthebbenden vooraf.”* De exploitant van de betreffende website wordt niet veroordeeld voor auteursrechtinbreuk, maar voor onrechtmatig handelen vanwege het feit dat zij bij gebruik maken van de beschikbaarheid op het World Wide Web van ongeautoriseerde MP3-bestanden geen rekening hield met de belangen van de auteurs- en nabuurrechthebbenden. Dit achtte het Hof in strijd met de zorgvuldigheid die de exploitant in het maatschappelijk verkeer betaamt.

De entertainment industrie zegt ondertussen door file-sharing van muziek- en filmbestanden heel veel inkomsten mis te lopen. Er zijn allerlei initiatieven om file-sharing te ontmoedigen, zoals het (dreigen met het) juridisch aanpakken van individuele aanbieders,¹²⁸ en het creëren van "legale", betaalde alternatieven. Daarnaast wordt ook hard gewerkt aan allerlei vormen van beveiliging en "Digital Rights Management" (DRM). DRM kan worden omschreven als: *"elektronische systemen van ter beschikkingstellen en gebruik van creatief materiaal in digitale vorm waarmee beveiliging tegen illegaal gebruik mogelijk is en waarmee legaal gebruik kan worden gemonitord en afgerekend."*¹²⁹ Ook de plannen van de Trusted Computing Group kunnen in dit licht gezien worden.¹³⁰ Het is de vraag of in de belangenafweging tussen auteursrechthebbenden en consument/gebruiker het evenwicht niet teveel verstoord wordt ten gunste van de rechthebbenden.¹³¹ Een tegenbeweging tegen het uitdijende auteursrecht wordt gevormd door de "Creative Commons",¹³² mede geïnspireerd op de ideeën van de Amerikaanse rechtsgeleerde Lawrence Lessig.¹³³

6.4.3. Databankenrecht

Het Internet is een verzameling van computers waarop een onmetelijke verzameling informatie is opgeslagen. Zo bekeken zou men zich kunnen afvragen of het Internet *an sich*, of delen daarvan, een databank is (of zijn) en hoe het zgn. "databankenrecht" daarop van toepassing kan zijn. Het databankenrecht wordt in Nederland geregeld in de Databankenwet (Dw). Deze wet is de implementatie van de Europese Databankenrichtlijn.¹³⁴ Hierin is de bescherming van databanken

¹²⁷ Hof Amsterdam, 15 juni 2006, LJN: AX7579, (Zoek MP3)

¹²⁸ Hetgeen nog niet zo eenvoudig is omdat voor het achterhalen van iemand's identiteit de medewerking van de provider nodig is, zie hierna.

¹²⁹ "Auteursrecht in de informatiemaatschappij – Bouwstenen voor een justitiestrategie" (TK 2001-2002, 26 538, nr. 6).

¹³⁰ Al eerder genoemd. Zie <https://www.trustedcomputinggroup.org/home>. Heel kritisch hierover is Ross Anderson in zijn Trusted Computer FAQ 1.1 te vinden op <http://home.wanadoo.nl/squell/tpca-faq.html>.

¹³¹ Zie over dit dilemma al eerder Chr.A. Alberdingk Thijm, Privacy vs. auteursrecht in een digitale omgeving ITeR-rapport, digitaal beschikbaar op http://www.ivir.nl/publicaties/overig/alberdingk_thijm/ITeR-privacy-v-auteursrecht.html.

¹³² <http://creativecommons.org/>, naar eigen zeggen: *"Creative Commons offers a flexible range of protections and freedoms for authors and artists. We have built upon the "all rights reserved" of traditional copyright to create a voluntary "some rights reserved" copyright."* Een Nederlandse versie van de Creative Commons publieke licentie is verkrijgbaar op <http://creativecommons.org/worldwide/nl/translated-license>.

¹³³ Zie <http://www.lessig.org/>. Vooral zijn boek "Free Culture, How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity" (online verkrijgbaar op <http://www.free-culture.cc/freecontent/>) is een zeer leesbare aanklacht tegen de almaar groter wordende greep van rechthebbenden op hun werk.

opgenomen. Art. 1 sub a omschrijft een databank als "een verzameling van werken, gegevens of andere zelfstandige elementen die systematisch of methodisch geordend en afzonderlijk met elektronische middelen of anderszins toegankelijk zijn en waarvan de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering". Volgens overweging 17 van de Databankenrichtlijn moet onder de term databank worden verstaan: "iedere verzameling van literaire, artistieke, muzikale of andersoortige werken, of van enig ander materiaal, zoals tekst, geluid, beeld, cijfers, feiten, gegevens." Het moet dus gaan om verzamelingen van werken, gegevens of andere zelfstandige elementen, systematisch of methodisch geordend en afzonderlijk toegankelijk. Hier kunnen we dus al concluderen dat het Internet als zodanig niet voor bescherming onder de Databankenwet in aanmerking komt. De informatie opgeslagen op het Internet is namelijk bepaald niet systematisch of methodisch geordend.

Met name over de betekenis van het woord "substantieel", dat in verschillend verband op diverse plaatsen in de wet wordt gebruikt en uit de Richtlijn is overgenomen, is in de afgelopen paar jaar al heel wat te doen geweest. Want wanneer is een investering nu aan te merken als "substantieel"?¹³⁵ Moeten er bijvoorbeeld grote investeringen gedaan zijn om de gegevens met het oog op het creëren van een databank bij elkaar te brengen? Noch de Richtlijn noch de Databankenwet geeft hierop antwoord. Het enige wat de Richtlijn hierover meldt is dat deze (substantiële) "investering een kwestie kan zijn van geld en/of tijd, moeite en energie."¹³⁶ Maar met het antwoord op deze essentiële vraag staat of valt bescherming van een databank. In een reeks van uitspraken in deze vraag aan de orde geweest.¹³⁷ Daaruit kwam echter geen eenduidig antwoord op de vraag wat nu precies een substantiële investering is.

Bekende uitspraak van de Hoge Raad in dit verband is de zaak van NVM/Telegraaf. Belangrijk punt in deze zaak was of de Hoge Raad de zogenoemde "spin-off" theorie zou aannemen of niet. Deze theorie houdt in dat databanken die ontstaan zijn als een soort bij-product van een andere activiteit, waarop dus de inspanningen van de maker niet zijn gericht, ook beschermd moeten worden onder de Databankenwet. Denk hierbij aan bijvoorbeeld een programmeergegevens van de omroep of aan voetbaluitslagen.¹³⁸ In de NVM/Telegraaf zaak ging het om Funda, de web site van de Nederlandse Vereniging voor Makelaars met woningen die via de bij de NVM aangesloten makelaars te koop worden aangeboden. Via een hyperlink kan er per woning doorgelinkt worden naar een vervolgpagina met foto's en verdere details. Maar wie op zoek was naar een huis kon ook terecht bij de zoekmachine El Cheapo, een dienst van De Telegraaf. Deze zoekmachine doorzocht hierbij diverse woningenbestanden op het Internet, waaronder ook het bestand van de NVM. De gegevens van de aldus gevonden woningen werden op de server van El Cheapo gekopieerd en gecombineerd tot één lijst. Bij ieder woning in die lijst staat een hyperlink. Als het gaat het om een huis dat uit het NVM bestand afkomstig is, dan verscheen bij het aanklikken daarvan de betreffende vervolgpagina die bij een zoeksessie op de website van NVM kon worden verkregen. De NVM beriep zich hierbij op haar databankenrecht en stelde dat haar databank in feite bestaat uit een verzameling kleinere databanken van de verschillende steden en dorpen en dat slechts de afzonderlijke databanken zijn te raadplegen. De vraag die hierbij werd opgeworpen was of delen van een databank zelf ook als afzonderlijke databanken kunnen worden aangemerkt. De Hoge Raad antwoordde hierop dat "noch de Richtlijn noch de tekst van art. 1 onder a Databankenwet een aanknopingspunt biedt voor de zienswijze dat, ingeval een databank voor meer doelen wordt gebruikt, voor elk van die doelen afzonderlijk een substantiële investering moet zijn aan te wijzen."

¹³⁴ Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken (Publicatieblad Nr. L 077 van 27/03/1996, pp. 20-28)

¹³⁵ P.B. Hugenholtz, Het Europese Databankenrecht. Acht jaar later – en nu?, *Auteurs & Media*, 2004- 5/6

¹³⁶ Overweging 40 in Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken (Publicatieblad Nr. L 077 van 27/03/1996, pp. 20-28)

¹³⁷ Pres. Rb Den Haag 14 jan. 2000, *AMI* 2000, p. 71 (KPN/XSO), Hof Arnhem 15 april 1997 *BIE* 1999/119 (KPN/Denda), Pres. Rb. Rotterdam 22 augustus 2000, *Informatierecht/AMI* 2000-10, p. 207-210, m.nt K.J. Koelman (*Kranten.com*), HR 22 maart 2002, *RdW* 2002, 61 (NVM/Telegraaf; El Cheapo), Rb Amsterdam 4 september 2002, *IER* 2003/1, p. 21 (Knipseldiensten), Hof Leeuwarden, 27 november 2002, *IER* 2003/1, p. 25 (PCM-Wegener/Hunter Select)(Nationale Vacaturebank.nl)

¹³⁸ P.B. Hugenholtz, Het Europese Databankenrecht. Acht jaar later – en nu?, *Auteurs & Media*, 2004- 5/6

Het Europese Hof van Justitie heeft in een viertal uitspraken vereiste van de substantiële investering nader uitgelegd.¹³⁹ De vier arresten hebben allen betrekking op de databankrechtelijke bescherming van gegevens over sportwedstrijden die door ondernemingen zoals The British Horseracing Board Ltd (BHB) zijn gegenereerd, verzameld en opgeslagen in elektronische databanken. De meest besproken uitspraak is die in de zaak tussen de British Horse Racing Board (BHB) en William Hill. Ook hier ging het om een zgn. spin-off. BHB organiseert paardenrennen in het Verenigd Koninkrijk en beheert een databank met een enorme hoeveelheid informatie over de paardenraces en over de paarden zelf. Deze gegevens zijn niet alleen essentieel voor degenen die direct te maken hebben met de paardenrennen, maar ook voor de radio- en televisieomroeporganisaties en voor wedkantoren en hun cliënten. Deze databank is on-line toegankelijk via de website van BHB. William Hill Organisation (Hill) organiseert weddenschappen over paardenrennen, een zogenaamde *bookmaker*. Informatie over paardenrennen wordt door Hill o.a. aangeboden via haar eigen web site. De informatie die Hill op haar website publiceert, komt voor een klein deel uit de databank van BHB.¹⁴⁰ De vraag was of William Hill hiermee inbreuk maakt op de databankrechten van BHB door zonder toestemming delen van de databank van BHB aan het publiek ter beschikking te stellen. Het Hof van Justitie oordeelt van niet. Kort gezegd bepaalde het Hof dat gegevensverzamelingen die een spin-off zijn van de normale bedrijfsactiviteiten van een bedrijf, niet door middel van een databankrecht beschermd worden.¹⁴¹ Investerings die zijn gedaan in het creëren van de gegevens voor de databank (in dit geval het verzamelen en actualiseren van alle gegevens die nodig zijn voor de organisatie van paardenrennen) mogen niet meetellen bij de beantwoording van de vraag of er substantieel geïnvesteerd is in de databank.¹⁴²

De gevolgen van de uitspraken van het HvJ zijn inmiddels ook in Nederland merkbaar. Conclusie is dat gebruikmaking van spin-off gegevens niet verboden is op grond van de Databankenwet.¹⁴³ De eerste Nederlandse uitspraak waar de William Hill uitspraak van het Hof van Justitie is toegepast is de uitspraak in Zoekallehuizen.nl.¹⁴⁴ Hier komen we de (databankrechtelijk) veelgeplaagde Nederlandse Vereniging van Makelaars weer tegen.

De makelaars hebben het dit keer aan de stok met de exploitant van de zoekmachine “zoekallehuizen.nl”(ZAH). De zoekmachine van ZAH doorzoekt het Internet en indexeert de websites van de individuele sites van (NVM) makelaars. Zij neemt van de websites van de makelaars de foto, de adresgegevens, de vraagprijs en een beperkte tekst over het huis over en plaatst deze op haar eigen website. Door middel van deeplinks wordt een potentiële koper geleid naar de website van de makelaars. De rechtbank oordeelde dat de gegevensverzamelingen bij de NVM-makelaars geen beschermde databank in de zin van de Databankenwet vormen. In dit kort geding is niet komen vast te staan dat de aanleg van deze gegevensverzamelingen in kwalitatief of kwantitatief een substantiële investering van de NVM-makelaars vergt. Daarom hebben de NVM-makelaars niet de bescherming tegen opvragen en hergebruiken van gegevens in een databank die is neergelegd in art. 2 Databankenwet. Deze zaak is vergelijkbaar met Kranten.com. Het deeplinken naar sites waarvan de exploitant dat niet wil mag dus van de rechter.

6.5 Positie van providers

5.1.1 Aansprakelijkheid

De Internet service providers (ISP's) zijn hiervoor al een aantal keren ter sprake gekomen. Zij zijn een onmisbare schakel tussen het Internet en de gebruikers. ISP's verlenen de gebruikers namelijk

¹³⁹ HvJ EG in de zaken C-46/02, C-203/02, C-338/02 en C-444/02 (Fixtures Marketing Ltd./Oy Veikkaus Ab, The British Horseracing Board Ltd/ William Hill Organization Ltd, Fixtures Marketing Ltd./Svenska Spel AB, Fixtures Marketing Ltd./Organismos prognostikon agonon podosfairou AE (OPAP), 9 november 2004

¹⁴⁰ F.W. Grosheide, noot bij uitspraak Hof van Justitie EG 9 november 2004, Zaak C-203/02, IER 2005/5

¹⁴¹ AKD Prinsen van Wijmen., Europees Hof beperkt databankenrecht, www.akd.nl/index.html?veelzijdige_expertise/40_1432.html

¹⁴² Th. Bosboom, Column Databankenrecht, Nieuwsbrief december 2004, www.checkit.nl/newsitem_313.html

¹⁴³ R. Davidse, Hof van Justitie doet belangrijke uitspraak voor het databankenrecht, 31 december 2004, www.ujg.nl

¹⁴⁴ Vzr Rb Arnhem, 16 maart 2006, AMI 2006/3 (Zoekallehuizen.nl) m nt. Ch. Alberdingk Thijm

allereerst toegang tot het Internet. Vroeger waren er providers die louter toegang verleenden, de zogenoemde *access providers*. Tegenwoordig komen die nauwelijks meer voor. Naast toegang tot het Internet¹⁴⁵ verlenen de ISP's ook andere diensten, zoals onder andere e-mail, het zgn *hosting*¹⁴⁶ en *caching*¹⁴⁷ en, in de voortschrijdende convergentie, behoren ook het aanbieden televisie-, en telefoondiensten tot de mogelijkheden.¹⁴⁸

Het begrip "Internet Service Provider" als zodanig komt echter niet voor in de Nederlandse wet.¹⁴⁹ Er wordt in art. 6:196c BW gesproken over "*degene die diensten van de informatiemaatschappij verricht (...) bestaande uit het doorgeven van van een ander afkomstige informatie of het verschaffen van toegang tot een communicatienetwerk.*"

Het feit dat ISP's informatie van anderen doorgeven maakt hen tot een tussenpersoon. Hier ligt ook een aansprakelijkheidsvraag. Aansprakelijkheid voor onrechtmatige informatie ligt natuurlijk primair bij degene van wie die betreffende informatie afkomstig is. Maar ook een tussenpersoon heeft hier een zekere aansprakelijkheid. Nu verschilt de aansprakelijkheid al naar gelang het "type" tussenpersoon. In het verleden zijn er uitspraken gedaan over diverse soorten tussenpersonen.¹⁵⁰ ISP's vervullen in dit opzicht een bijzondere rol als tussenpersoon. De vraag die in dit verband gesteld werd was de volgende: Zijn ISP's slechts een doorgeefluik van informatie waar zij geen enkele controle op hebben (het zogenaamde *mere conduit*) of dienen zij vooraf de door hen door te geven informatie te screenen op de inhoud? Het laatste is gezien de enorme hoeveelheid informatie die ISP's dagelijks doorgeven een onmogelijke opgave (en zou bovendien neerkomen op censuur), maar het eerste ontslaat hen van iedere verantwoordelijkheid. In 1996 werd er voor het eerst een uitspraak gedaan over de aansprakelijkheid van ISP's in de bekende Scientology zaak.¹⁵¹ Toen werd er door de rechtbank (in kort geding) geoordeeld dat een ISP niets meer is dan een doorgeefluik omdat zij slechts de gelegenheid geven tot openbaarmaking, en dus niet aansprakelijk zijn. Dit is anders als het onmiskenbaar duidelijk is dat er sprake is van onrechtmatige informatie. In 1999 wordt er in de bodemprocedure geoordeeld dat een ISP aansprakelijk kan zijn voor onrechtmatige informatie indien hij hiervan op de hoogte is en vervolgens niets heeft ondernomen om de doorgifte van deze onrechtmatige informatie te verhinderen, de zogenaamde "notice-and-take-down-procedure."¹⁵² Hier werd geoordeeld dat de ISP een zekere mate van zorg heeft. In de tussentijd werd de Europese Richtlijn Elektronische handel voorbereid, waarin een soortgelijk aansprakelijkheidsregime voor ISP's was opgenomen. In 2000 werd deze richtlijn aangenomen en werd in 2004 in de Nederlandse wetgeving geïmplementeerd. Het aansprakelijkheidsregime werd opgenomen in art. 6:196c BW, waar in lid 1 wordt bepaald dat voor het enkel doorgeven van informatie (*mere conduit*) de ISP in beginsel niet aansprakelijk is. In lid 4 wordt de aansprakelijkheid voor hosting diensten geregeld. Hier zien we de eerder genoemde "notice-and-take-down-procedure" in gecodificeerde vorm terug, namelijk geen aansprakelijkheid voor de ISP voor het opslaan (en doorgeven) van informatie van anderen op zijn servers, "*indien hij:*

a. niet weet van de activiteit of informatie met een onrechtmatig karakter en, in geval van een schadevergoedingsvordering, niet redelijkerwijs behoort te weten van de activiteit of informatie met een onrechtmatig karakter, dan wel

¹⁴⁵ Zie Rb Den Haag in 22 maart 2006, (nl.tree en Easynet vs. KPN), LJN AV6314, waarbij geoordeeld werd dat KPN geen machtspositie had op de "markt voor internettoegang". De Rb baseert bij het vaststellen van de relevante markt op marktanalyses van de OPTA en de NMa

¹⁴⁶ Hosting is het bieden van de mogelijkheid om informatie van abonnees (veelal in de vorm van een homepage) op te slaan op de servers van de ISP.

¹⁴⁷ Caching is het tijdelijk opslaan van informatie van (veelvuldig) opgevraagde web sites op de server van de ISP om op die manier het Internet verkeer te versnellen.

¹⁴⁸ Zie voor problemen voor ISP's om toegang tot de televisiemarkt te krijgen, Chr. Alberdingk Thijm, Rechtenjungle, *Emerce* 2005/53.

¹⁴⁹ L. Siemerink, Elektronische gedragscodes; een voorbeeld uit de praktijk, *Mediaforum*, 2003/10, pp.318-323.

¹⁵⁰ Onder tussenpersonen worden o.a. telecommunicatie aanbieders, drukkers, uitgever, handelaren in gepirateerde producten en kabelexploitanten gedaan. Zie voor de laatste groep HR 14 januari 1983, *NJ* 1984, 696 (*KTA/Columbia*)

¹⁵¹ Rb Den Haag 9 juni 1999, tot aan de HR [...]

¹⁵² Zie hierover uitgebreid het dossier aansprakelijkheid van internetproviders op eJure.nl: http://www.ejure.nl/dossier_id=261/f_dossier/dossier.html

b. zodra hij dat weet of redelijkerwijs behoort te weten, prompt de informatie verwijdert of de toegang daartoe onmogelijk maakt.”

5.1.2 Afgifte van NAW gegevens

Naast aansprakelijkheid voor de informatie van anderen kunnen ISP's ook te maken krijgen met derden die afgifte van de NAW gegevens van haar abonnees vorderen. De rechtspraak laat hier een gevarieerd beeld zien.¹⁵³ Recent is de uitspraak van de Hoge Raad¹⁵⁴ in een kort geding over de vraag of Lycos als hosting internetprovider aan Pessers de naam en het adres bekend moet maken van de websitehouder, die in een website op <http://members.lycos.nl> anoniem Pessers had beschuldigd van oplichting bij de verkoop van postzegels via de veiling op de website www.ebay.com. Lycos voerde aan dat zij de NAW-gegevens aan een benadeelde alleen hoefde te af te geven als er sprake is van evident onrechtmatige uitlatingen of als het gaat om strafbare feiten en politie en justitie de gegevens opvragen. Het Hof Amsterdam oordeelde echter anders. Weliswaar was het voor Lycos niet onmiskenbaar dat de bewuste informatie op die website in dit geval onrechtmatig was, maar het hof vond het aannemelijk dat de mogelijkheid bestaat dat die informatie onrechtmatig en voor Pessers schadelijk is. Volgens het hof heeft Pessers een reëel belang bij die NAW-gegevens en is er geen minder ingrijpende manier om ze te verkrijgen. Het hof was van oordeel dat Lycos bij afweging van de belangen van de hosting provider, de betrokken websitehouder en Pessers in dit concrete geval onzorgvuldig handelt door de naam en het adres van die websitehouder niet aan Pessers bekend te maken. De Hoge Raad heeft alle bezwaren van Lycos tegen de uitspraak van het hof verworpen. Dat betekent dat het bevel aan Lycos om de NAW-gegevens aan Pessers bekend te maken in stand is gebleven. Aldus worden providers feitelijk opgezadeld met de taak om een lastige belangenafweging te maken, waarbij ze ook nog aansprakelijk zijn (ofwel tegenover de derde, ofwel tegenover hun abonnee wegens contractbreuk) als ze die belangenafweging verkeerd maken.

6.5.3 Kwalificatie

Gelden de regels voor ISP's ook voor beheerders van virtuele marktplaatsen, zoals Marktplaats.nl? Dit zijn geen ISP's in de strikte zin van het woord (ze bieden nl. geen toegang tot het internet), maar zij slaan wel informatie van derden op hun servers/web site op. Kunnen zij ook aansprakelijk worden gehouden voor hetgeen via hun web sites aangeboden wordt? In de zaak Stokke/Marktplaats.nl¹⁵⁵ werd Stokke, producent van de bekende Tripp Trapp kinderstoel, geconfronteerd met advertenties op marktplaats.nl die inbreuk maakten op haar merkrechten. Zij vorderde van Marktplaats.nl de afgifte van de NAW gegevens van de adverteerders en voorts dat marktplaats.nl de betreffende advertenties van haar site zou verwijderen. De vraag was of Marktplaats.nl wel of niet hosting activiteiten aanbiedt en daardoor ofwel onder het aansprakelijkheidsregime voor ISP's ofwel onder het gewone onrechtmatige daadsrecht zou vallen. Marktplaats stelde hierbij dat zij zich aan de voorwaarden van art. 6:196c BW houdt en daarom gevrijwaard is van aanspraken onder art. 6:162 BW. In de beantwoording van deze vraag hield de rechtbank art. 6:196c BW tegen het licht van de Richtlijn elektronische handel. De Rechtbank overweegt *“..dat de Richtlijn er niet aan in de weg staat dat de internetdienstverlener die zich op de beperkte aansprakelijkheid kan beroepen op grond van de wetgeving van de lidstaat toch kan worden bevolen maatregelen te nemen ter voorkoming of*

¹⁵³ In de bodemprocedure van de beruchte Scientology zaak (Rb. Den Haag 9 juni 1999, LJN-nummer AA1039) oordeelt de Rechtbank dat inderdaad de NAW-gegevens van de content-providers aan eiseres verstrekt moeten worden. Tot eenzelfde oordeel komt de Voorzieningenrechter in Deutsche Bahn vs. XS4ALL (Hof Amsterdam 7 november 2002, LJN-nummer AF0091) Maar de Voorzieningenrechter in de Teleatlas-zaak (Voorzieningenrechter Utrecht 9 juli 2002, LJN-nummer AE5537) vindt dat eiseres eerst maar op een andere manier moet proberen om aan de de NAW-gegevens van de vermeende auteursrecht-inbreukmaker te komen. In onfriesepaard.nl (Rb. Leeuwarden 26 maart 2004, LJN-nummer AO7028) werd beslist dat de omweg via 187 Rv. door een webmaster als getuige op te roepen als getuige in een voorlopig getuigenverhoor daar niet voor bedoeld is. In Stokke/ Marktplaats.nl, Rb Zwolle, 3 mei 2006, LJN AW6288 (zie hieronder) het afgeven van NAW gegevens van adverteerders op Marktplaats.nl aan de orde.

¹⁵⁴ HR 25 november 2005, IER 2006/2, (Lycos/Pessers)

¹⁵⁵ Rb Zwolle, 3 mei 2006, (Stokke c.s. vs. Marktplaats), LJN AW6288

beëindiging van inbreukmakende handelingen.” Geconcludeerd wordt dat, ongeacht of Marktplaats nu wel of geen hosting activiteiten aanbiedt en voldoet aan de voorwaarden van art. 6:196c BW, dat haar handelen wel degelijk aan de zorgvuldigheidsnorm van art. 6:162 BW getoetst kan worden. Daardoor heeft de rechtbank zich niet uitgesproken of Marktplaats hosting activiteiten aanbiedt en dus onder het aansprakelijkheidsregime voor ISP's valt.¹⁵⁶

De exploitant van een website die het zoeken van mp3 bestanden faciliteert, het al eerder genoemde Zoek MP3,¹⁵⁷ is volgens het Hof Amsterdam echter niet als een ISP te kwalificeren. De handelwijze van de website exploitant “...strekt aanzienlijk verder dan die van een ISP. Daarom komt haar niet dezelfde bescherming toe als een ISP - gelet op haar maatschappelijke betekenis - toekomt. Voor een ISP geldt in de bewoordingen van het ‘Agreed Statement’ bij artikel 8 van het WIPO-Auteursrechtverdrag:

“It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11 bis (2).”

Tot het passieve gedrag dat in artikel 8 tot uitdrukking is gebracht is de handelwijze van Techno Design bepaald niet beperkt gebleven. Techno Design heeft immers niet alleen haar muziekminnende bezoekers tot communicatie met andere muziekliefhebbers in staat gesteld, maar zij heeft ook de door haar verzamelde data zodanig bewerkt dat zij het zoeken van mp3-muziekbestanden voor bezoekers van haar website zeer aanzienlijk heeft vergemakkelijkt. Bovendien verschaft zij haar bezoekers bij die muziekbestanden de nodige voor die bezoekers terzake dienende informatie.”

7 Slotopmerkingen

Het Internet is een medium dat een zeer snelle ontwikkeling doormaakt. Zoals in de inleiding al opgemerkt kunnen de technieken van vandaag, morgen al weer achterhaald zijn. Dat maakt niet alleen het reguleringsvraagstuk voor het Internet tot een complexe aangelegenheid, maar ook het beschrijven van het medium zelf en de regelgeving daaromtrent. Dit hoofdstuk is daarom slechts een momentopname van de stand van zaken zoals die er voor staat anno 2006.

Het is te verwachten dat kwesties waar nu veel over te doen is, over een paar jaar compleet achterhaalde problemen zijn. Wie weet is het over een paar jaar normaal om bijna continu draadloos met Internet verbonden te zijn. Als allerlei content dan, al dan niet tegen betaling, streaming aangeboden wordt, speelt het hele file-sharing en download-probleem wellicht niet meer. Of als de al eerder genoemde plannen met betrekking tot Trusted Computing bewaarheid worden. We kunnen niet in de toekomst kijken - maar waarschijnlijk kunnen we over een paar jaar hard lachen om veel van de kwesties die in dit hoofdstuk aan de orde zijn geweest.

¹⁵⁶ Ten aanzien van de vraag of Marktplaats aan merkrechtgebende NAW-gegevens van adverteerders dient af te geven worden partijen in de gelegenheid gesteld de rechtbank nog voor te lichten. De rechtbank stelt hierbij voorop dat Marktplaats in geen geval jegens Stokke c.s. verplicht is om de gegevens van al haar adverteerders te registreren. Als Marktplaats al jegens Stokke c.s. gehouden zou zijn tot registratie van enige gegevens van haar adverteerders, is deze verplichting beperkt tot de gegevens van adverteerders die een advertentie met de aanduiding STOKKE of TRIPP TRAPP (of een vergelijkbare aanduiding) gebruiken.

¹⁵⁷ Hof Amsterdam, 15 juni 2006, LJN: AX7579, (Zoek MP3)

Aanbevolen literatuur

Alberdingk Thijm, Christiaan, Het nieuwe informatierecht, Nieuwe regels voor het internet, Academic Service, Den Haag, 2004.
Boele-Woelki, K. en Kessedjian, C. (red.), Internet Which Court Decides? Which Law Applies?, Kluwer Law International, Den Haag 1998
Lawrence Lessig, Free Culture, How big media uses technology and the law to lock down culture and control creativity, The Penguin Press, New York, 2004.
M. van der Linden-Smith en A.R. Lodder(red.),. Jurisprudentie Internetrecht, Annotaties, Kluwer, Deventer, 2006.
M. van der Linden-Smith en A.R. Lodder(red.),. Jurisprudentie Internetrecht, Uitspraken, Kluwer, Deventer, 2006.
Lokke Moerel, On-line reclame, Kluwer, Deventer, 2002.
Adam Thierer and Clyde Wayne Crews Jr., Who Rules the Net? Internet governance and jurisdiction, CATO Institute, Washington D.C., 2003.

Aanbevolen websites

www.cier.nl
www.itrecht.nl
www.internetrechtspraak.nl
www.javisite.nl
www.netkwesties.nl
www.recht.nl
www.solv.nl