
HANDELINGEN
NEDERLANDSE JURISTEN-VERENIGING

128e JAARGANG/1998-I

Recht en Internet

*Verkenningen op het gebied van het Internationaal Privaatrecht, het
Strafrecht en het Auteursrecht*

Preadviezen van

Prof. dr. A.W. Koers

Prof. mr. M.V. Polak

Prof. mr. Y. Buruma

Mr. P.B. Hugenholtz

1998
W.E.J. Tjeenk Willink
Deventer

Lay-out en omslag Evelien de Vries Robbé

ISBN: 90 271 4854 6

NUGI: 691

© 1998 A.W. Koers, M.V. Polak, Y. Buruma, P.B. Hugenholtz.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van uitgeverij W.F.J. Tjeenk Willink te Zwolle.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van art. 16b Auteurswet 1912 jo. het Besluit van 20 juni 1974, Stb. 351, zoals gewijzigd bij Besluit van 23 aug. 1985, Stb. 471, en art. 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 882, 1180 AW Amstelveen). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (art. 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without written permission from the publisher.

ALGEMENE INHOUD

Preadviczen over het onderwerp:

Recht en Internet

Verkenningen op het gebied van het Internationaal
Privaatrecht, het Strafrecht en het Auteursrecht

PREADVIES PROF. DR. A.W. KOERS

Internet in kort bestek, 1

PREADVIES PROF. MR. M.V. POLAK

Internationaal privaatrecht: vangnet voor het Internet, 59

PREADVIES PROF. MR. Y. BURUMA

Internet en strafrecht, 119

PREADVIES MR. P.B. HUGENHOLZ

Het Internet: het auteursrecht voorbij, 197

DEEL I

INTERNET IN KORT BESTEK

VAN TECHNISCH TOT SOCIAAL

SYSTEEM

preadvies prof. dr. A.W. Koers

INHOUD DEEL I

	INLEIDING	5
1	INTERNET ALS TECHNISCH SYSTEEM	8
	1.1 Historie	8
	1.2 Techniek	11
	1.3 Organisatie	20
	1.4 Functies	24
2	INTERNET ALS SOCIAAL SYSTEEM	30
	2.1 Perspectief	30
	2.2 Betekenis(sen)	34
	2.3 Voor het recht	40
	2.4 Voor juristen	47
	UITLEIDING	55

Deel I

INLEIDING

Wat hierna volgt is eigenlijk geen preadvies maar een prelude: een introductie op de preadviezen van mijn mede-rapporteurs. Doel van mijn bijdrage is niet u te confronteren met de veelheid aan juridisch-inhoudelijke vragen die Internet oproept, noch met de mogelijke antwoorden op al die vragen. Mijn opdracht is u een beeld aan te reiken van het verschijnsel Internet. Dit vanuit de veronderstelling dat er nog heel wat juristen zijn – zelfs als ze Internet gebruiken – die weinig of geen kennis hebben van de achtergronden en de werking van Internet.

Omdat een dergelijke verhandeling over Internet weliswaar nuttig is, maar niet bijzonder origineel,¹ heb ik mijzelf daarnaast een tweede doel gesteld: iets te zeggen over de (mogelijke) maatschappelijke implicaties van Internet. Ook dat kan worden opgevat als een introductie tot de preadviezen van mijn collega's omdat het een breder kader neerzet, zowel voor die preadviezen zelf als voor de discussie daarover. In die zin is deze verhandeling dus eveneens een 'postlude': een blik voorbij de discussie over de problemen van dit moment.²

Elke keer dat er iets wordt opgeschreven (of geautomatiseerd), wordt er iets vastgelegd dat zich in werkelijkheid verder blijft ontwikkelen en dat er dus al weer snel anders uitziet dan het beeld dat op papier werd gezet. Dit geldt in het bijzonder voor Internet

1. Zie bijvoorbeeld J.G.L. van Wees en W.G. Renden, *Internet voor juristen*, Kluwer, Deventer 1997, dat niet alleen schetst hoe Internet in elkaar zit, maar dat ook een schat aan informatie bevat over de concrete mogelijkheden van Internet voor de juridische beroepspraktijk.
2. Deze opzet verklaart tevens waarom het aantal literatuurverwijzingen zeer gering zal zijn: in de prelude is daarvoor weinig *reden* vanwege de sterk descriptieve aard en in de postlude is daarvoor weinig *mogelijkheid* vanwege de overwegend prospectieve invalshoek van mijn verhaal.

want Internet maakt juist op dit moment een zeer snelle ontwikkeling door. Globaal zal er ruim een half jaar verlopen tussen het moment dat ik dit schrijf en het moment dat u, de lezer, deze verhandeling onder ogen krijgt. In die periode zal er, zo vermoed ik, heel wat veranderen als het gaat om Internet en het gebruik daarvan. Dat is dus één *caveat* die ik maar direct wil agenderen: ik sta er niet voor in dat alles wat ik nu schrijf nog klopt als u het leest.

Een tweede *caveat* betreft een risico dat inherent is aan de twee doelen die ik mij stel. Ik *moet* iets zeggen over de technische kant van Internet en ik *wil* iets zeggen over de mogelijke maatschappelijke betekenis van Internet. De conclusie ligt dan voor de hand: maatschappelijke betekenis wordt bepaald door technologie. Dit nu is een gedachte die ik op voorhand in de kiem wil smoren en die in elk geval niet aan mij mag worden toegeschreven. Mijn opvatting is juist dat er geen sprake is van technologisch determinisme: niet de technologie bepaalt de maatschappelijke betekenis van de technologie, maar bepalend is het gebruik dat mensen en organisaties maken van die technologie. En daarnaast is er ook nog eens sprake van een wisselwerking: de maatschappelijke implicaties van een technologie zijn weer van invloed op het gebruik van die technologie. Gelukkig maar want anders waren de hiernavolgende preadviezen overbodig: het recht zou dan immers geen enkele invloed hebben op de loop der 'Internetse' dingen.

Tot nu toe heb ik steeds gesproken van Internet en dat zal ik hierna consequent blijven doen. Termen als 'de elektronische snelweg' of 'de digitale snelweg' zult u hier dus niet tegenkomen. Reden is dat deze laatste termen weliswaar aansprekende metaforen zijn, maar dat zij ook al direct associaties en beelden oproepen die in hoge mate misleidend kunnen zijn.³ Wie denkt er – zoals precies de bedoeling was bij het introduceren van de metafoor – bij het woord 'snelweg' niet aan snelheid, drukte en economisch belang? Maar wie denkt bij diezelfde term 'snelweg' ook niet direct aan gevaren en risico's, verkeersregels en aan aanleg door de overheid? Hetgeen de discussie over de rol van de overheid en over de

3. Zie ook mijn bijdrage in de Automatisering Gids van 3 oktober 1997, p. 15. Zie ook paragraaf 2.2.

behoefte aan wet- en regelgeving al direct een kleur geeft die wel past bij de metafoor maar die helemaal niets zegt over het onderliggende verschijnsel: Internet. Juist om die valse kleur uit het debat te halen, geef ik dus de voorkeur aan de term 'Internet'.⁴ Daarbij vermijd ik zoveel mogelijk het lidwoord want de uitdrukking 'het' Internet wekt de suggestie dat het om een bepaald systeem gaat terwijl het mij om het concept gaat.

Er zit in de discussies over Internet en over informatietechnologie in het algemeen nog een valse kleur. In het spraakgebruik wordt Internet altijd geassocieerd met informatie: je zoekt er naar informatie, vindt er (meestal na enig zoekwerk) informatie en je kunt er zelf informatie aanbieden. Echter, in wezen heeft Internet helemaal niets van doen met informatie: het bevat 'alleen maar' in bits en bytes gecodeerde gegevens. En die gegevens zijn pas informatie als zij bij de gebruiker van Internet een vraag beantwoorden of een onzekerheid wegnemen. Dit is meer dan een semantische discussie want er is een wezenlijk verschil tussen de uitspraak 'Internet zit vol met informatie' en 'Internet zit vol met gegevens'. In het eerste geval verwacht ik een pasklaar antwoord van Internet op al mijn vragen – in het tweede geval realiseer ik mij dat ik slechts bouwstenen van een antwoord aangeleefd krijg. En, net als alle andere zogenaamde 'informatiesystemen', Internet doet wel het laatste, maar zeker niet het eerste. Dit gezegd hebbend, conformeer ik mij hierna aan het algemeen gangbare spraakgebruik en zal ik dus de termen 'informatie' en 'gegevens' toch maar door elkaar gebruiken.⁵

Genoeg 'ingeleid' – wat komt hierna aan de orde?

– In deel 1 van deze verhandeling gaat het om Internet als technisch systeem: paragraaf 1.1 zegt iets over de historie van Internet, paragraaf 1.2 handelt over de techniek en paragraaf

4. En als u niet gelooft dat het gebruik van een term als 'elektronische snelweg' uw denken beïnvloedt, vervang die metafoor dan eens door een andere – bijvoorbeeld: 'elektronische markt' – en ga bij u zelf na welke associaties die laatste term oproept als het gaat om de rol van de overheid en het recht.
5. Het komt de leesbaarheid niet ten goede, noch de vergelijkbaarheid met de andere preadviseurs, als ik het steeds zou hebben over 'gegevenssystemen', 'gegevensverwerking', 'gegevensleverancier', 'gegevensmacht', etc. waar de rest van de wereld het heeft over 'informatiesystemen', etc.

1.3 en 1.4 gaan, respectievelijk, over de organisatie van Internet en over de soorten functies die het heeft.

– Deel 2 handelt over Internet als sociaal systeem. Paragraaf 2.1 zegt iets over de vraag hoe naar technologie gekeken kan worden en op die basis verkent paragraaf 2.2 de maatschappelijke betekenis van Internet. In de paragrafen 2.3 en 2.4 wordt de discussie toegespitst op het recht en juristen.

Vooraf in deel 1 beperk ik mij tot het absolute minimum dat nodig is voor een jurist die mee wil denken en praten over de juridische vragen die Internet oproept. Technici en andere deskundigen zullen dus vereenvoudigingen tegenkomen die hen de adem zal benemen. Maar dit verhaal is dan ook niet voor hen bestemd.

1 INTERNET ALS TECHNISCH SYSTEEM

1.1 Historie

Internet in beperkte kring

De oorsprong van Internet ligt in de Koude Oorlog. In de jaren '60 kreeg het Advanced Research Project Agency (ARPA) opdracht van het Amerikaanse Ministerie van Defensie om een netwerk te ontwikkelen tussen een aantal belangrijke computercentra dat een Russische atoomaanval zou kunnen doorstaan. Het idee was dat als een bepaald computercentrum uitgeschakeld zou worden, het netwerk in staat moest zijn het gegevensverkeer om te leiden via andere centra. In het begin van de jaren '70 was het ARPA-net een feit en was een beperkt aantal grote Amerikaanse computercentra zodanig aan elkaar gekoppeld dat bij uitval van een bepaald centrum het gegevensverkeer omgeleid kon worden via andere centra. Om te voorkomen dat dit netwerk alleen maar kon werken met één type computer en één type fysieke verbinding werd er vervolgens door ARPA een set afspraken opgesteld voor het uitwisselen van berichten⁶ binnen het

6. Deze term ziet in deze verhandeling niet alleen op tekstboodschappen, maar op alle vormen van gegevensverkeer, ongeacht of het daarbij gaat om tekst, beeld, geluid, programmatuur of nog weer wat anders.

ARPA-net. Dit was het TCP/IP protocol: het Transmission Control Protocol/Internet Protocol.⁷

Hocwel het ARPA-net en het TCP/IP protocol dus een militaire achtergrond hadden, werden ze niet als staatsgeheim behandeld. Integendeel, tot verbazing van velen werd in 1973 het TCP/IP protocol volledig – en gratis – vrijgegeven door de Amerikaanse overheid. Met dat besluit werd in feite de basis gelegd voor de verdere, niet-militaire uitbouw van het ARPA-net: andere computers konden aanhaken als zij maar voldeden aan het TCP/IP protocol. Daarbij kon het gaan om een enkele computer, maar het kon ook gaan om een eigen netwerk dat aan het ARPA-net werd gekoppeld via een bepaalde computer in dat eigen netwerk. De (achteraf gezien) cruciale beslissing om het TCP/IP protocol vrij te geven, was dus de reden dat het ARPA-net kon uitgroeien tot het netwerk van de netwerken: Internet dus.

Het eerste netwerk dat zo aan ARPA-net werd gekoppeld was het Computer Science Research Network (CS-net) – en daarmee was dus het eerste ‘inter-net’ verkeer op basis van het TCP/IP protocol een feit. In de jaren daarna – vooral tussen 1975 en 1985 – volgden zo tal van andere netwerken. Een bijzondere plaats daarbij werd ingenomen door het NSF-net, het netwerk van de Amerikaanse National Science Foundation (NSF) dat vooral was bestemd voor onderwijs- en onderzoekinstellingen. NSF-net was meer dan een netwerk dat aan het ARPA-net werd aangehaakt. Omdat het NSF-net bestond uit snelle verbindingen tussen grote computercentra werd het een backbone van het gehele systeem, dat wil zeggen: een netwerk dat, tezamen met de andere backbones, het overgrote deel van het gegevensverkeer voor zijn rekening neemt. Daarmee vervaagde de grens tussen het oorspronkelijke ARPA-net en de daarop aangesloten netwerken: Internet werd uiteindelijk één geheel waarbij een gebruiker niet weet, en ook niet hoeft te weten, via welk specifiek deel-netwerk het gegevensverkeer wordt afgewikkeld.

Vanwege het belang van het NSF-net had de NSF een belangrijke rol bij het bepalen van de verdere ontwikkeling van Internet. Zo

7. Voor meer bijzonderheden over TCP/IP: zie paragraaf 1.2.

had de NSF voorwaarden gesteld voor het gebruik van het eigen NSF-deel van Internet. Eén van die voorwaarden was dat het NSF-net niet voor commerciële doeleinden gebruikt mocht worden en omdat het NSF-net als backbone van Internet fungeerde, betekende dit *de facto* een verbod van commerciële activiteiten op Internet. In 1992 echter kwam de NSF met een nieuwe beleidslijn: het verbod op commerciële activiteiten zou voortaan uitsluitend gelden voor de NSF-organisatie zelf en daarmee was dit verbod van de baan voor andere gebruikers van NSF-net – en dus in feite voor Internet als geheel.

Internet breekt door

Deze beslissing is even bepalend geweest voor de ontwikkeling van Internet als het eerdere besluit om het TCP/IP protocol vrij te geven: nu commerciële activiteiten niet meer verboden waren, raakte ook het bedrijfsleven geïnteresseerd in Internet. Gevolg was dat Internet definitief doorbrak buiten de kring van de eerste gebruikers – militaire instanties en (wat later) onderzoek- en onderwijsinstellingen – om zich te ontwikkelen tot wat het vandaag de dag is.

Met het opheffen van het verbod op commerciële activiteiten werd het ook aantrekkelijk om niet-openbare, zakelijke netwerken als CompuServe en America OnLine aan Internet te koppelen. De kracht van Internet was evenwel inmiddels zodanig toegenomen dat deze organisaties en hun gesloten netwerken zich gedwongen zagen zich in snel tempo om te vormen tot aanbieder van Internet-diensten. Met als gevolg dat thans hun oorspronkelijke bestaansgrond (het aanbieden van een eigen netwerk) nog maar een relatief bescheiden rol speelt en zij het moeten hebben van toegevoegde diensten. De kracht van het Internet-concept bleek eveneens toen de firma Microsoft in 1995 dacht het succes van Windows 95 te kunnen gebruiken voor het introduceren van een eigen Microsoft Netwerk als concurrent van Internet. Helaas voor Microsoft bleek het grote publiek niet geïnteresseerd te zijn in dit Microsoft Netwerk zodat 'MSN' thans niet meer is dan de naam waaronder Microsoft opereert op Internet.

Het explosief groeiende gebruik van Internet verklaart eveneens waarom overheden er zich de laatste jaren steeds intensiever mee zijn gaan bemoeien. Dominant daarbij is tot op heden vooral de vrees de boot te zullen missen en niet zozeer vrees over mogelijke negatieve gevolgen van Internet. Historisch gezien zijn vooral de volgende rapporten illustratief voor het streven van overheden om in te spelen op Internet.

- Verenigde Staten: White House, *National Information Infrastructure Agenda for Action*, september 1993 – het document dat de term ‘elektronische snelweg’ introduceerde.
- Europese Unie: High Level Group on the information society, *Europe and the global information society: recommendations to the European Council*, Bangemann rapport, mei 1994.
- Nederland: *Nationaal Actieprogramma elektronische snelwegen: van metafoor naar actie*, december 1994.

De oude werkpaarden van het eerste uur – ARPA-net, CS-net en ook NSF-net – zijn inmiddels vervangen door betere netwerken. Op dit moment bestaat Internet naar schatting uit meer dan tienduizend aan elkaar gekoppelde netwerken, elk op zich weer bestaande uit een (soms groot) aantal afzonderlijke computers. Het aantal gebruikers wereldwijd wordt thans geschat op 50 à 75 miljoen (in ruim 150 landen) en het Internet-verkeer groeit met ongeveer 10 procent per maand. De kracht en de dynamiek van Internet laten zich afleiden niet alleen uit deze getallen, maar vooral ook uit het feit dat ze niet exacter te ramen zijn: Internet is een fenomeen dat verandert terwijl u deze zin leest.

1.2 Techniek

Adressen op Internet

Internet is dus het netwerk van de netwerken. Die omschrijving bepaalt grotendeels wat hierna – zeer globaal – aan de orde komt. Het zal dus niet gaan om de technische aspecten van het local area network (LAN) dat in uw kantoor wordt gebruikt, het gaat ook niet om de koppeling van dat netwerk aan een specifiek ander netwerk (bijvoorbeeld in een ander gebouw of aan een niet-openbaar systeem), maar het gaat om het netwerk dat uw

computer verbindt met alle andere aan Internet gekoppelde computers – waar ter wereld die zich ook bevinden. En waarvan u meestal het bestaan niet eens kent. Een goede eerste vraag is dus hoe uw computer de weg vindt op Internet.

Het antwoord ligt in het al eerder genoemde TCP/IP protocol. TCP 'hakt' alle gegevensverkeer in stukjes ('pakketjes') zodat deze tezamen met andere pakketjes van vele andere gebruikers over Internet verzonden kunnen worden. TCP zorgt er ook voor dat na ontvangst de pakketjes weer samengevoegd kunnen worden tot het oorspronkelijke bericht. IP regelt daarbij de adressering zodat elk pakketje op de goede plaats terecht komt. Dit betekent dat iedere computer die aan Internet is gekoppeld een eigen, uniek IP-adres moet hebben. Dat adres bestaat uit vier groepen van drie cijfers – zeg: 131.211.203.53 – waarbij de eerste twee groepen (131.211.) aan een organisatie worden toegewezen (in dit geval de Universiteit Utrecht (211) in Nederland (131)) en waarbij die organisatie de laatste twee groepen zelf mag gebruiken voor het aanduiden van de computers die het aan Internet wil koppelen (203 = Fakulteit der Rechtsgeleerdheid; 53 = computer A.W. Koers). Omdat er in het verleden royaal werd omgesprongen met het toewijzen van IP-adressen aan organisaties (de eerste twee groepen van drie cijfers) en de meeste organisaties slechts een klein deel van hun eigen ruimte aan adressen (in de laatste twee groepen van drie cijfers) gebruikten, is er nu een wereldwijd tekort aan IP-adressen ontstaan.⁸

IP-adressen zijn lastig te onthouden en daarom wordt er in de praktijk meestal gewerkt met domein-adressering. Daarbij zijn de vier reeksen cijfers vervangen door afkortingen die gemakkelijker te begrijpen zijn. Zo is mijn e-mail adres: a.koers@rgl.ruu.nl en daaruit valt al snel af te leiden (van rechts naar links) dat mijn adres zich bevindt op een computer in Nederland ('nl'), daarin-

8. Er wordt daarom gewerkt aan een nieuwe generatie IP-adresseringen en aan een systeem waarbij IP-adressen niet gebonden zijn aan een vast opgestelde computer (53 staat voor mijn PC in mijn werkkamer), maar waarbij een computer wordt herkend los van de plaats waar die computer fysiek staat opgesteld. Een dergelijk systeem maakt Internet nog weer aantrekkelijker voor niet aan een bepaalde werkplek gebonden 'flexi-werk' of 'flexi-werkers'.

nen op een computer van de (rijks)Universiteit Utrecht ('ruu'), daarbinnen op een computer van de Fakulteit der Rechtsgeleerdheid ('rgl') en dat schrijver dezes daarop bekend staat onder de naam 'a.koers'. Het @-teken (apestaartje) moet gelezen worden als 'op' of (in het jargon) als 'at'. Zo'n domein-adres is dus heel wat gemakkelijker te onthouden dan het IP-equivalent: a.koers@203.211.131. Overigens blijft het (numerieke) IP-adres de officiële naam van elke computer in Internet en dit betekent dat er speciale systemen zijn om het domein-adres dat een gebruiker opgeeft om te zetten in een IP-adressering.⁹

In de kern is het dus eigenlijk heel simpel: TCP/IP hakt de via Internet te verzenden berichten in hapklare brokken en doet ze in een 'enveloppe' met een keurig IP-adres erop – zodat ze bij Internet op de post gedaan kunnen worden. In feite dus niet wezenlijk anders dan hoe het er met een gewone brief aan toe gaat.

Andere Internet-protocollen

TCP/IP zijn weliswaar de meest belangrijke Internet-protocollen, maar ze zijn bepaald niet de enige. Net als TCP/IP zijn ook deze andere protocollen publiek bezit.

- File Transfer Protocol (FTP): afspraken om het mogelijk te maken complete bestanden van de ene computer over te zenden naar een andere computer.
- HyperText Transfer Protocol (HTTP): afspraken om grafisch opgemaakte pagina's te verzenden (en zo de basis van het World Wide Web).
- Internet Relay Chat (IRC): afspraken om Internet-gebruikers interactief met elkaar tekstberichten te laten uitwisselen (e-mail is niet interactief).
- Network News Transfer Protocol (NNTP): afspraken voor het uitwisselen van berichten binnen een bepaalde groep gebruikers (nieuwsgroepen).

9. In de Verenigde Staten worden in domein-adressen ook nog codes gebruikt ter aanduiding van het type organisatie (zoals: com = commercial; edu = education; gov = government; en mil = military).

- Point to Point Protocol (PPP): afspraken om Internet aansluitingen tussen twee computers tot stand te brengen.
- Serial Line Internet Protocol (SLIP): eveneens afspraken om een PC aan te sluiten op Internet via de computer van een provider.
- Simple Mail Transfer Protocol (SMTP): afspraken voor het (niet interactief) uitwisselen van elektronische post (e-mail).
- Telnet: afspraken om een Internet-gebruiker in staat te stellen interactief gebruik te maken van (programma's op) een andere computer.

Van een andere orde dan de zojuist genoemde protocollen is het OSI-model. OSI staat voor 'Open Systems Interconnections' en het model biedt een ordening van de functies die een netwerk moet hebben opdat in dat netwerk de ene gebruiker kan samenwerken met de andere. Het OSI-model bestaat uit zeven lagen, onderaan beginnend met afspraken over de fysieke verbinding tussen twee computers en eindigend met afspraken over de toepassingsprogrammatuur die op de aan elkaar gekoppelde computers wordt gebruikt. Protocollen als zojuist beschreven zijn dus in wezen afspraken met betrekking tot een bepaalde laag van het OSI-model. Dat model is dus niet zelf een protocol, maar een concept om protocollen te ordenen.¹⁰

Werken met en op Internet

Als dit dus de manier is waarop Internet erin slaagt al die miljoenen berichten op de goede plaats af te leveren, wat heeft iemand dan nodig om met Internet te kunnen werken? Er moet onderscheid worden gemaakt tussen twee situaties.

- Internet wordt benaderd vanuit een PC die gekoppeld is aan een LAN (bijvoorbeeld op kantoor) dat gekoppeld is aan Internet.
- Internet wordt benaderd vanuit een PC die niet aan een LAN is gekoppeld – met als meest voorkomende situatie: de PC thuis.

¹⁰. Probleem daarbij is dat het OSI-model in Europa meer aanhang heeft dan in de Verenigde Staten zodat de diverse, sterk door Amerika beïnvloede Internet-protocollen niet goed aansluiten bij het OSI-model.

In het eerste geval is het regelen van de toegang tot Internet niet een zaak van de individuele gebruiker, maar van de systeembeheerder. Daarom gaat het hierna uitsluitend over de tweede situatie, al zijn er aanzienlijke overeenkomsten tussen beide situaties.

Stel dat u vanuit uw PC thuis wilt gaan surfen op Internet, wat is er dan nodig aan techniek?

- Een krachtige PC met goede grafische eigenschappen – maar die is vaak reeds aanwezig.
- Een modem om berichten te kunnen verzenden en ontvangen via het openbare telefoonnet.
- Een browser: een programma dat u in staat stelt op Internet te zoeken en informatie¹¹ op te vragen.
- Toegang (via de telefoon) tot een computer van een Internet provider die u toegang geeft tot Internet.
- Veel geduld – want Internet is vaak uitermate traag, vooral bij het verzenden van beelden.

In het kader van deze paragraaf (over Internet als zodanig) is van bovenstaand lijstje het laatste item het meest interessant omdat veel van de inspanningen op technisch gebied nu juist gericht zijn op het sneller maken van Internet, vooral als het benaderd wordt via een normale telefoonlijn. Probleem is dat het reguliere telefoonsysteem¹² grenzen stelt aan de hoeveelheid gegevens die er per seconde op een betrouwbare manier over verzonden kunnen worden. Om een indicatie te geven: een state-of-the-art modem kan onder optimale condities in één seconde ongeveer een pagina tekst verzenden over een normale (analoge) telefoonlijn, maar vaak zijn de condities niet optimaal en duurt het veel langer. En beelden vragen veel meer opslagcapaciteit dan een pagina tekst – en dus duurt het verzenden van beelden zeer veel langer dan het verzenden van een pagina tekst. Om van bewegende beelden nog maar helemaal niet te spreken.

11. Daarmee vereenvoudig ik Internet wel tot het WWW; zie paragraaf 1.4 voor de verschillen. De op te vragen informatie kan (als eerder opgemerkt) bestaan uit tekst, geluid, stilstaande beelden en/of bewegende beelden, althans indien de browser die u gebruikt dat mogelijk maakt.

12. Ook wel aangeduid als POTS: het 'Plain Old Telephone System'.

Natuurlijk wordt het probleem van de traagheid erger doordat het aantal Internet-gebruikers zo sterk groeit.¹³ Er wordt daarom op allerlei manieren geprobeerd het probleem van de traagheid van Internet aan te pakken.¹⁴

- Ten eerste, overal ter wereld zijn de leveranciers van telefoon- en aanverwante diensten druk bezig het bestaande netwerk van koperdraad te vervangen door veel snellere glasvezel-verbindingen.
- Ten tweede, POTS-aansluitingen worden in toenemende mate vervangen door ISDN-lijnen. ISDN staat voor 'Integrated Services Digital Network'. Technisch gezien betekent ISDN dat het gegevensverkeer tot en met de aansluiting thuis volledig digitaal wordt afgewikkeld.¹⁵ Dit leidt tot een aanzienlijk hogere snelheid.
- Ten derde, in Nederland zijn relatief veel huizen aangesloten op de kabel. Over het kabelnet zijn veel hogere snelheden mogelijk dan over POTS en (zelfs) ISDN en dus experimenteren kabelmaatschappijen met het aanbieden van toegang tot Internet via de kabel.
- Ten vierde, de omvang van de te verzenden berichten kan gereduceerd worden door ze volgens een bepaald protocol te comprimeren voorafgaand aan verzending en ze volgens datzelfde protocol te de-comprimeren na ontvangst.¹⁶
- Ten vijfde, zo langzamerhand beginnen geheel nieuwe technologieën om op een veel snellere manier gegevens over te dragen het laboratorium te verlaten. De vereiste investeringen zijn

13. Hoe krap Internet op dit moment in zijn jasje zit, blijkt uit het feit dat een Europese gebruiker er goed aan doet zijn Internet-zaken in de ochtend af te handelen, dus voordat Amerika aan de arbeid gaat.

14. Let wel: dit probleem doet zich dus vooral voor als er gewerkt wordt vanuit een stand-alone PC en het is in veel mindere mate een probleem als er gewerkt wordt vanuit een PC die is opgenomen in een LAN dat gekoppeld is aan Internet.

15. Bij het POTS is het telefoonsysteem zelf ook volledig digitaal, maar is er nog een analoge verbinding tussen centrale en huisaansluiting; vandaar de noodzaak van een modem.

16. Compressie en de-compressietechnieken worden vooral gebruikt voor het verzenden van beelden omdat deze het meest omvangrijk zijn en zich goed lenen voor compressie. 'JPEG' is een compressietechniek voor stilstaande beelden en 'MPEG' is een soortgelijke techniek voor bewegende beelden.

evenwel zodanig dat grootschalige toepassing nog wel enige tijd op zich zal laten wachten.¹⁷

In de kern laten zich twee lijnen onderscheiden in deze ontwikkelingen: enerzijds wordt de snelheid van Internet opgevoerd door het aanleggen van verbindingen met meer bandbreedte en anderzijds wordt de snelheid vergroot door het inkorten van de gegevensstroom met behulp van steeds betere compressietechnieken.

Beveiliging, hacken en intranetten

Er wordt niet alleen veel geïnvesteerd in het vergroten van de snelheid van Internet, maar dat geldt ook voor het verbeteren van de beveiliging.

Hacking is het inbreken in computers. In de termen van art. 138a van het Wetboek van Strafrecht gaat het om 'computervredbreuk' en dat is strafbaar met een 'gevangenisstraf van ten hoogste zes maanden of een geldboete van de derde categorie'. Hacking wordt bestreden door klassieke middelen als toegangs-codes, terwijl er ook speciale barricades (firewalls) kunnen worden opgeworpen in een aan Internet gekoppelde computer tegen ongeautoriseerde toegang tot die computer. Hoewel er zich zo af en toe spectaculaire computerinbraken voordoen, lijkt hacking tot nu toe in de praktijk een betrekkelijk marginaal verschijnsel te zijn. In veel opzichten is Internet een heel wat veiliger omgeving voor berichtenverkeer dan een modaal kantoor waar alle deuren open staan of het telefoonverkeer via POTS want dat kan zeer gemakkelijk worden afgeluisterd.¹⁸ In veel landen zijn niettemin speciale 'Computer Emergency Response Teams' opgericht die ingeschakeld kunnen worden bij problemen met de beveiliging van computernetwerken. Zo kent Nederland 'CERT-NL' voor het netwerk tussen de verschillende universiteiten.

17. Er is een (internationale) werkgroep die werkt aan de specificaties van Internet 2 dat gebaseerd zal zijn op die nieuwe technieken.

18. Het is daarom eigenlijk merkwaardig dat de beveiliging van Internet zelf veel meer aandacht krijgt dan de beveiliging aan de kant van het zendende en ontvangende kantoor. Angst voor het onbekende?

Eén strategie van organisaties om veiliger te kunnen communiceren dan Internet thans mogelijk lijkt te maken, is het inrichten van een eigen intranet. Dit is een netwerk dat gebaseerd is op dezelfde technologie als Internet, dat zich dus voor een gebruiker gedraagt alsof het Internet is en dat gebruikt kan worden met dezelfde software (browser) als Internet. Er is echter één cruciaal verschil: een intranet is fysiek niet of maar zeer beperkt toegankelijk vanuit Internet; in elk geval zit er een zeer stevige firewall tussen Internet en een intranet. Vooral voor een organisatie met meerdere vestigingsplaatsen is het inrichten van een intranet een interessante optie. Dit geldt ook voor de beoefenaren van een bepaalde professie die zo in eigen kring informatie kunnen uitwisselen over hun vak.

Elektronisch berichtenverkeer kan zonder al te veel moeite door derden worden gelezen; speciale programma's daarvoor kunnen zo van Internet worden gehaald. Is dit voor particulieren misschien niet al te bezwaarlijk,¹⁹ de zakelijke gebruiker wil zekerheid over de vertrouwelijkheid van zijn elektronische berichtenverkeer, vooral als het gaat om financiële transacties. Vandaar de opkomst van encryptie: het versleutelen van elektronische berichten zodat alleen de ontvanger die ook de sleutel heeft het bericht kan lezen. Inmiddels zijn er zeer krachtige encryptieprogramma's beschikbaar – soms gratis af te halen op Internet.²⁰ Hoewel in theorie elk gecodeerd bericht te kraken is, is zelfs bij algemeen verkrijgbare encryptieprogramma's de inspanning zo groot dat het kraken in de praktijk al gauw een onrealistische optie wordt. De overheid maakt zich dan ook terecht zorgen over de onmogelijkheid dit soort berichtenverkeer nog 'af te luisteren' als dat nodig is, bijvoorbeeld voor de opsporing van strafbare feiten. Feit is echter dat alle pogingen van overheden om encryptie te verbieden stuk zijn gelopen, enerzijds op de terechtwens van (zakelijke) Internet-gebruikers tot vertrouwelijkheid

19. Mijn e-mail berichten zijn volgens mij hoogst oninteressant voor anderen.

20. Zoals PGP: Pretty Good Privacy. Het idee achter PGP is als volgt. Als A een vertrouwelijk bericht aan B wil sturen, gebruikt A de (algemeen beschikbare) publieke sleutel van B om het bericht te versleutelen. Naast de publieke sleutel heeft B ook nog een eigen (geheime) private sleutel en alleen daarmee kan het bericht van A na ontvangst worden ontsleuteld. Publieke en private sleutel vormen dus één geheel.

van berichtenverkeer en anderzijds op de algemene beschikbaarheid van zeer krachtige en in de praktijk niet te kraken encryptie-programma's.

Een blik naar de toekomst

Ter afronding van deze paragraaf een kleine blik richting toekomst. Het beeld dat tot nu toe van Internet werd geschetst en dat ook het beeld zal zijn van de meeste gebruikers houdt in dat Internet een groot reservoir is waar een schat aan informatie is te vinden – als je de weg weet en enig geduld hebt. Er is echter een ontwikkeling gaande die – mogelijkserwijs – dit beeld radicaal kan veranderen: Java en aanverwante producten. Java is een computertaal waarmee programma's kunnen worden ontwikkeld en op Internet aangeboden die direct gebruikt kunnen worden door een daarvoor geschikte browser. Dit betekent dat niet alleen de gegevens van Internet kunnen worden gehaald, maar ook de programma's (of programma-onderdelen, applets genaamd) om die gegevens te bewerken.

- Niet alleen het document komt van Internet, maar ook de tekstverwerker om er mee aan de slag te gaan.
- Niet alleen het plaatje komt van Internet, maar ook het programma om het te bekijken of te bewerken.

Als deze ontwikkeling zich zou doorzetten, dan zal dit leiden tot een wezenlijk ander gebruik van computers omdat dan een Internet browser het enige programma zal zijn dat iemand nog nodig zal hebben op de eigen PC. De rest – gegevens en programma's – komen immers van Internet telkens als daaraan behoefte is. Als deze ontwikkeling zich doorzet, heeft dat niet alleen ingrijpende gevolgen voor gebruikers, maar ook voor de gehele computerindustrie. Zo zullen producten als Windows 95 overbodig worden.²¹

21. Vandaar dat de firma Microsoft zich zorgen maakt om deze ontwikkeling en het gebruik van Java en applets zoveel mogelijk probeert te ontmoedigen, dan wel poogt beide producten te vervangen door eigen Microsoft producten.

1.3 Organisatie

Weinig formele structuren

Wie denkt dat achter Internet een gigantische wereldwijde organisatie zit, komt bedrogen uit. Eén van de verrassende aspecten van Internet is juist het grotendeels ontbreken van een leidende of verantwoordelijke organisatie of instantie. In feite zit de ordening van Internet in de hierboven besproken technische protocollen en iedereen die zich daaraan wil en kan conformeren, mag meedoen. In die zin is Internet dus eerder een organisme dat zich geleidelijk (maar soms onvoorspelbaar) ontwikkelt dan een organisatie in de klassieke betekenis van de term. Of is Internet nu juist de voorbode van de organisatie van de toekomst: open, flexibel en met een minimum aan formele structuren en regels?

Toch moet er natuurlijk wel wat worden geregeld en dat gebeurt de tot voor kort vooral onder de vlag van de Amerikaanse National Science Foundation (NSF; zie paragraaf 1.1). Hoewel de NSF zich uit die rol heeft teruggetrokken, zijn veel van de door de NSF ontwikkelde procedures blijven bestaan. Als het om Internet als zodanig gaat, richten de organisatorische arrangementen (voor zover ze er zijn) zich vooral op het genereren en onderhouden van de technische protocollen, immers het hart van Internet.

- In 1992 werd de Internet Society (ISOC) opgericht als forum voor overheden, bedrijfsleven en individuen om te discussiëren over (de toekomst van) Internet. ISOC organiseert daartoe periodiek een internationale bijeenkomst.
- Niet alleen de ISOC houdt zich bezig met (technische) standaardisatie, maar dat doen ook de Internet Architecture Board (IAB) en (vooral) de Internet Engineering Task Force (IETF).

Het proces om te komen tot nieuwe technische normen en protocollen is in hoge mate informeel. Iedereen kan een voorstel voor nieuwe of andere standaarden indienen bij de IAB. Na een interne ronde kan zo'n voorstel door de IAB worden verheven tot een 'request for comments' (RFC) zodat iedereen er com-

mentaar op kan geven (uiteraard via Internet). In de praktijk worden de meeste RFC's ontwikkeld via werkgroepen van de IETF.

Het is opmerkelijk dat deze informele en zeer flexibele manier van werken is blijven bestaan, ook nadat Internet buiten de min of meer gesloten wereld van onderwijs en onderzoek trad. Feit is immers dat standaarden en protocollen niet alleen technisch gezien interessant zijn, maar dat zij bepaalde producten en bedrijven kunnen maken en breken. Een bedrijf dat er in slaagt een eigen technologie tot Internet standaard te verheffen (formeel of informeel), heeft daarmee een niet te onderschatten economisch voordeel.²² Wellicht heeft de manier waarop de standaarden voor Internet nog steeds tot stand komen veel van doen met het feit dat Internet in Amerika ontstond.

Informele gedragsregels: netiquette

Naast enkele simpele structuren en procedures om tot standaarden te komen, is er dus op Internet-niveau eigenlijk geen formele organisatie. Wèl is er netwerk-etiquette oftewel netiquette. Zoals het woord al aangeeft gaat het hierbij niet om formele regels waaraan Internet-gebruikers zich moeten houden, maar om informele gedragsregels die, net als fabels en legenden, door informele overlevering worden overgedragen. Netiquette is daarom meer dan een set gedragsregels: het is in feite een expressie van een eigen Internet-cultuur. Een paar voorbeelden ter verduidelijking.

- Tegen de regels is het verzenden van een spam: een bericht dat naar een groot aantal gebruikers wordt gezonden, terwijl duidelijk is dat het die gebruikers niet zal interesseren.
- Niet tegen de regels is een flame: een bericht waarin op fellic, onvriendelijke toon wordt gereageerd op gebruikers die zich niet aan de netiquette houden.
- Als een boodschap misschien verkeerd kan overkomen, kan er een smiley aan worden toegevoegd: een teken dat aangeeft

22. Zo ontwikkelde Netscape, het bedrijf dat met de eerste echt populaire browser op de markt kwam, zich in enkele jaren tot een miljardenonderneming.

wat de emotionele lading van een woord of zin. Is %-(een goede aanduiding van uw stemming op dit moment?

– Regel is ook om soepel om te gaan met de fouten van een newbie: een beginnende gebruiker van Internet die zich (nog) niet houdt aan netiquette omdat hij niet weet wat de regels zijn.

Lange tijd waren commerciële boodschappen strikt tegen de regels van netiquette. Een overtreder van dit verbod kon rekenen op een ware stortvloed aan flames (waaraan vaak de volledige tekst van de bijbel was toegevoegd om het berichtenverkeer van en naar de 'zondaar' grondig te ontregelen). Het verbod op commerciële boodschappen geldt niet langer voor Internet als geheel, integendeel Internet wemelt thans van de reclame. Toch zijn er nog steeds groepen binnen Internet die in hun onderlinge communicatie vasthouden aan de oude norm en die geen commerciële boodschappen dulden.

De diverse providers

Internet heeft dus een zeer kleine (en zwakke) formele organisatie om te komen tot technische standaardisatie en het heeft een informele organisatie in de vorm van netiquette. Dit volstaat voor Internet als zodanig, maar er moet natuurlijk meer gebeuren om daadwerkelijk informatie aan te bieden via Internet en om gebruikers daadwerkelijk toegang te geven tot Internet. Kortom, er zijn providers nodig: personen of organisaties die informatie aanbieden via Internet en/of die aan particulieren of organisaties toegang geven tot Internet. Uit deze formulering valt af te leiden dat er verschillende soorten providers zijn.

– De network-provider houdt zich bezig met het aanleggen, beheren en aanbieden van het fysieke netwerk waarover het gegevensverkeer wordt afgewikkeld. Dit netwerk omvat naast kabels en radio- en satellietverbindingen ook de computers die nodig zijn om het Internet-verkeer te besturen.

– De specifieke functie van een access-provider is het verzorgen van de toegang tot Internet, hetzij aan individuele gebruikers (meestal via POTS of ISDN), hetzij aan organisaties (meestal via directe koppeling van computers).

– Een service-provider biedt algemene Internet-diensten aan,

bijvoorbeeld bij het ontwikkelen van een site op Internet, dat wil zeggen: een adres waarop een individu of organisatie informatie of diensten aanbiedt.²³

– De information-provider is een variatie van de service-provider: zoals het woord al zegt, gaat het hier om het verzamelen en via Internet aanbieden van informatie voor een bepaalde doelgroep of over een bepaald onderwerp.

Deze indeling kent geen harde grenzen: er is heel wat overlap, terwijl veel organisaties meerdere rollen vervullen. Vooral de combinatie access-provider en information-provider komt vaker wel voor dan niet. Mede door de snelle ontwikkeling van Internet is er bovendien sprake van een continu proces van herschikking van posities en rollen. Ook het overheidsbeleid inzake de privatisering van de telecommunicatiesector is daarbij van invloed.

Bij wijze van afsluiting van deze paragraaf nog één praktische kwestie: het toekennen van een domein-naam. Uit paragraaf 1.2 valt af te leiden dat elke aan Internet gekoppelde computer een eigen IP-adres/domein-naam moet hebben. Vooral voor bedrijven is het aantrekkelijk dat die domein-naam zoveel mogelijk overeenstemt met de bedrijfsnaam: dat maakt de zoektocht naar dat bedrijf op Internet heel wat gemakkelijker. Probleem is natuurlijk dat een domein-naam maar één keer kan worden uitgegeven zodat de firma DAF de domein-naam 'daf.nl' kan vergeten als (bijvoorbeeld) de vereniging 'De Antieke Fiets' reeds die domein-naam toegewezen heeft gekregen. Vandaar dat er in Nederland een Stichting Internet Domeinregistratie in het leven is geroepen die domein-namen goedkeurt en registreert.²⁴

Er zijn natuurlijk tal van andere organisaties die zich bezig hou-

23. Zo kan een service-provider bijvoorbeeld helpen bij het aanmaken van een homepage, dat wil zeggen: een grafisch opgemaakt beeldscherm dat een bezoeker van de site informeert over de mogelijkheden op die site. Kennis van de HyperText Markup Language (HTML) is daarvoor essentieel en niet iedereen wil zich daarin verdiepen. De laatste versies van Wordperfect en Word bieden evenwel al een optie om teksten te converteren naar HTML. Het maken van een homepage wordt dus steeds gemakkelijker.

24. Internet zou Internet niet zijn als er voor de slimmeriken niet een weg zou zijn om deze procedure te omzeilen.

den met (de toekomst) van Internet, variërend van de Vereniging van Internet Providers tot de Digitale Burgerbeweging Nederland. Daarop nader ingaan, zou hier evenwel te ver voeren.

1.4 Functies

Het andere Internet

Afgezien van de basisprotocollen van Internet (TCP/IP) zijn de in paragraaf 1.2 besproken protocollen (FTP, IITTP, IRC, NNTP, PPP, SLIP, SMTP en Telnet) meestal direct gerelateerd aan de functies²⁵ die Internet een gebruiker kan bieden.

E-mail, het versturen van elektronische post op basis van het SMTP protocol, is zo langzamerhand in veel organisaties volledig ingeburgerd geraakt. Het leeghalen van de elektronische brievenbus is voor velen net zo belangrijk geworden als het leeghalen van het postvakje bij het secretariaat. De snelle groei van e-mail hangt ongetwijfeld samen met de snelheid waarmee berichten de geadresseerde bereiken (meestal een paar seconden, zelfs tussen continenten²⁶), met de zeer lage kosten (verwaarloosbaar) en met het gemak waarmee het kan worden gebruikt. Handig is ook dat hele bestanden met rapporten, etc. aan een e-mail bericht gekoppeld kunnen worden. Nadeel van e-mail is dat de berichten gemakkelijk kunnen worden onderschept en gelezen kunnen worden. Het gericht zoeken naar een bepaald e-mail bericht in al het Internet-verkeer is echter een lastige opgave en bovendien kan een e-mail bericht gemakkelijk onleesbaar worden gemaakt voor derden met behulp van een encryptie-programma. Dit levert een vrijwel waterdichte beveiliging op tegen ongewenste mee-lezers. Voor e-mail is een afzonderlijk programma nodig, al dan niet als onderdeel van een browser. De betere e-mail programma's kunnen aan de hand van de afzender of de inhoud van een bericht een wijze van afhandeling bepalen.

25. Soms wordt hiervoor ook wel de term 'dienst' gebruikt. De term 'functies' geeft evenwel beter aan dat het hier gaat om een technische voorziening die, al dan niet tezamen met andere functies, door een provider kan worden gebruikt voor het aanbieden van een 'dienst'.

26. Behalve Afrika waar de fysieke infrastructuur vaak ontoereikend is.

FTP is het protocol dat een gebruiker in staat stelt bestanden van een andere computer – waar ook ter wereld – over te halen naar de eigen computer; vandaar de aanduiding File Transfer Protocol. Die bestanden kunnen tekst bevatten, maar ook beelden, geluid en programma's. Vooral deze laatste mogelijkheid heeft *FTP* zeer populair gemaakt,²⁷ in het bijzonder na de introductie van het zogenaamde anonymous *FTP*. Anonymous *FTP* betekent dat een gebruiker via Internet toegang heeft tot een andere computer zonder daarvoor een toegangscode nodig te hebben. Het intikken van 'anonymous' is voldoende om toegelaten te worden en om bestanden te mogen downloaden, dat wil zeggen: kopiëren naar de eigen computer. Daarbij wordt vaak gebruik gemaakt van compressie-technologieën om het bestand kleiner te maken zodat het verzenden minder tijd vergt. Na ontvangst volgt decompressie met een speciaal (maar overal verkrijgbaar) programma.²⁸

In zekere zin is het concept van *Telnet* ouder dan Internet zelf. In de tijd dat grote mainframe computers nog het rijk alleen hadden, zaten gebruikers achter een terminal (alleen een beeldscherm met toetsenbord) en gebruikten ze gezamenlijk de rekenkracht van één centrale computer. *Telnet* doet in wezen hetzelfde. Met behulp van *Telnet* logt iemand via Internet in op een andere computer, tikt de goede toegangscode in en kan dan op die andere computer werken alsof hij achter een terminal zit. Dit betekent dat er programma's gestart kunnen worden en dat er op die andere computer gewerkt kan worden alsof je er naast zit. Het zal duidelijk zijn dat het aanbieden van *Telnet*-faciliteiten aan derden wel de nodige eisen stelt aan de beveiliging van het computersysteem dat ter beschikking wordt gesteld. *Telnet* is een functie die bijvoorbeeld kan worden gebruikt voor het

27. Waarbij er geen sprake hoeft te zijn van illegaal kopiëren. Op Internet is heel veel shareware programmatuur te vinden, soms geheel gratis, soms als eerste kennismaking (met betaling als het programma bevalt en behouden wordt). Veel grote software-leveranciers gebruiken Internet voor het distribueren van updates van hun programmatuur.

28. Bij het zoeken naar een bepaald programma in de grote en onoverzichtelijke anonymous-*FTP*-wereld kan een beroep worden gedaan op Archie: een programma dat aan de hand van zoekwoorden van de gebruiker op zoek gaat naar bijpassende programma's op *FTP*-sites.

doorzoeken van een catalogus van een bibliotheek met behulp van de eigen programmatuur van die bibliotheek.

NNTP is de basis voor *News* – ook wel aangeduid als *Usenet*. *News* bestaat uit een groot aantal nieuwsgroepen, dat wil zeggen: een groep personen die geïnteresseerd is in een zeker onderwerp en die daarover met elkaar communiceert via een berichtensysteem op een bepaalde computer. Alle berichten worden naar dat systeem verzonden en daar moeten ze worden gelezen (om eventueel gedownload te worden). In oorsprong waren nieuwsgroepen vooral gericht op wetenschappelijke onderwerpen, maar vandaag zijn er nieuwsgroepen voor alle onderwerpen onder de zon – inclusief minder smakelijke of zelfs illegale. Nieuwsgroepen zijn in principe openbaar en na aanmelding kan iedereen deelnemen aan de uitwisseling van berichten door het leggen van een verbinding met de centrale computer van de groep. Sommige nieuwsgroepen hebben een moderator die de discussie stuurt en de kwaliteit bewaakt – andere groepen zijn volstrekt ongestructureerd. Juist door hun (zeer) grote aantal en de daaruit voortvloeiende onoverzichtelijkheid bieden nieuwsgroepen een goede vrijplaats voor het aanbieden van pornografisch of racistisch materiaal. Dit des te meer als ze zich afficheren met een onschuldige klinkende naam en als er geen enkele check is op de identiteit van de deelnemers en wat ze op de computer van de groep plaatsen of er vanaf halen.

Mailing lists zijn vergelijkbaar met *News*. Ook hier gaat het om een groep personen die is geïnteresseerd in een bepaald onderwerp, maar de techniek van het uitwisselen van berichten is anders. Binnenkomende berichten worden namelijk niet op een centrale computer gezet om daar bekeken te worden (zoals bij *News*), maar direct door de computer waarop de lijst is geïnstalleerd, doorgezonden naar alle deelnemers aan de lijst. Een bericht aan de mailing-list-computer volstaat dus om alle leden van de groep te bereiken. Deelname aan een paar mailing lists garandeert daarom een welgevulde elektronische brievenbus – met vaak een schat aan informatie als u belangstelling heeft voor het onderwerp.

Chatten (op basis van IRC) is het Internet equivalent van een

bezoek aan het café: een mogelijkheid om via het uitwisselen van teksberichten met andere Internet-gebruikers te communiceren. Het verschil met e-mail is dat chatten interactief is en in real time plaats vindt. De beperking van chatten is dat de deelnemers elkaar niet kunnen zien.²⁹ Dat ligt anders bij *video-conferencing* waarbij de deelnemers niet alleen berichten kunnen intikken, maar elkaar ook kunnen zien en met elkaar kunnen praten. Video-conferencing stelt hoge eisen aan de snelheid van de Internet-verbinding en aan de gebruikte computers. Om deze reden is het tot dusverre vooral een zakelijke toepassing, maar het ligt in de lijn der verwachting dat video-conferencing over enkele jaren niets bijzonders meer zal zijn. Internet kan eveneens worden gebruikt om te *telefoneren*. Ook geluid laat zich omzetten in bytes en die kunnen vervolgens via Internet worden verzonden – om aan de andere kant weer samengevoegd te worden tot geluid. Internet telefonie is tot dusverre niet echt populair geworden (ondanks de lage kosten, ook voor internationale gesprekken) omdat het alleen werkt als beide partijen gelijktijdig achter de computer zitten. Er wordt echter gewerkt aan de integratie van (internationale) Internet telefonie en (lokale) gewone telefonie.

World Wide Web

En dan is er natuurlijk het *World Wide Web* (WWW). Het WWW ontstond in 1990 aan het CERN in Genève. Oorspronkelijk doel van CERN was een nieuwe manier van werken met tekstberichten binnen de eigen organisatie. In die berichten werden zogenaamde hyperlinks opgenomen, dat wil zeggen: woorden op het beeldscherm die aangeklikt kunnen worden met de cursor en die dan andere documenten met nadere informatie over het woord in kwestie activeren en op het scherm zetten.³⁰ Gebruikers van Windows kennen het systeem van de schermen met

29. Hetgeen aanleiding is tot allerlei verhalen over wat er gebeurde toen twee chatters besloten elkaar te ontmoeten.

30. Aanklikken van het woord 'Vereniging' in de zin 'De jaarvergadering van de Nederlandse Juristen Vereniging komt in vrolijkheid bijeen' leidt de gebruiker zo naar een document met nadere informatie over de NJV – en op de pagina's van dat document staan weer nieuwe hyperlinks naar andere documenten, etc.

help-informatie. Het idee om informatie aan te bieden via door hyperlinks verbonden documenten sloeg zodanig aan dat het binnen de kortste keren ook buiten CERN werd gebruikt.³¹

In 1994 brak het WWW wereldwijd door omdat het toen mogelijk werd op een WWW-pagina niet alleen tekst (met hyperlinks) op te nemen maar ook afbeeldingen, geluid en (wat later) bewegende beelden – die dan ook weer met hyperlinks gekoppeld konden worden aan alle andere vormen van informatie. Essentieel daarbij was – en is nog steeds – dat zo'n hyperlink kan verwijzen niet alleen naar een andere WWW-pagina of -document op dezelfde computer, maar ook naar een WWW-pagina of -document op een totaal andere computer. Het is juist die eigenschap die Internet-gebruikers in staat stelt over de wereld de surfen: van de ene computer naar de andere en zonder te weten waar die computers fysiek zijn opgesteld. Daarmee was dus in feite het Internet ontstaan zoals wij dat vandaag kennen. Voor velen is het WWW dan ook synoniem met Internet, hoewel het (zie boven) eigenlijk 'maar' één van de functies is van Internet.

Om van het WWW gebruik te kunnen maken is niet alleen toegang tot Internet nodig (via een access-provider) maar ook een speciaal programma (de browser). De browser haalt de met behulp van HTML³² opgemaakte WWW-pagina's of -documenten van Internet, decodeert ze en zet ze op het scherm van de gebruiker (waarop ze, indien gewenst, als bestand kunnen worden opgeslagen of direct kunnen worden geprint). Als er vervolgens op zo'n pagina een hyperlink wordt aangeklikt, haalt de browser de bij die link behorende pagina's of documenten op – als gezegd: ongeacht op welke computer waar ter wereld die pagina's of documenten zich bevinden.

Het moge duidelijk zijn dat dit een speciaal systeem van adresering vergt om de links met elkaar te verbinden. Vandaar dat de term 'Universal Resource Locator' (URL) een kernbegrip is in de wereld van het WWW. Een URL kan opgevat worden als de

31. Hetgeen CERN voor de nodige problemen plaatste. Ik herinner mij nog de mededeling dat maximaal 40 externen op het CERN-systeem welkom waren.

32. HyperText Markup Language; zie paragraaf 1.2.

unieke aanduiding van een specifieke informatiebron. Soms is dat de homepage van een site, maar een URL kan ook verwijzen naar een specifieke pagina van een specifiek document op die site. Binnen een URL bestaat daarom een onderlinge hiërarchie.

- <http://www.ruu.nl> is de URL die leidt naar de homepage van de site van de Universiteit Utrecht.³³
- <http://www.rgl.ruu.nl> leidt binnen de site van de Universiteit Utrecht naar de homepage van de Faculteit der Rechtsgeleerdheid.
- <http://www.jb.rgl.ruu.nl> leidt naar de homepage van de juridische bibliotheek van de Faculteit der Rechtsgeleerdheid van de site van de Universiteit Utrecht.
- Etc – desnoods tot het niveau van een individuele pagina van een boek in de bibliotheek van de Faculteit der Rechtsgeleerdheid te Utrecht.

Kern van het WWW is (nogmaals) dat het aanklikken van een hyperlink op een WWW-pagina die naar één van deze URLs verwijst de bijbehorende pagina op uw scherm doet arriveren.³⁴

Het kan natuurlijk heel boeiend zijn om van de ene WWW-pagina naar de andere te surfen, maar het kan ook uitermate frustrerend zijn om maar eindeloos te zoeken naar specifieke informatie omdat de URL van die informatie(bron) niet bekend is. Een veel gebruikte uitweg uit zo'n situatie is op bezoek te gaan bij een search engine, dat wil zeggen: een programma dat aan de hand van opgegeven zoekwoorden op zoek gaat naar URLs met informatie over die zoekwoorden. Bekende voorbeelden van zoeksystemen zijn:

- <http://www.altavista.digital.com>
- <http://www.infoseek.com>
- <http://www.lycos.com>
- <http://www.yahoo.com>

Deze zoeksystemen scannen elk op hun eigen manier Internet

33. Inmiddels kunnen ook veel andere Internet-functies worden benaderd via het WWW. Als het daarbij om een FTP-site gaat, begint de URL niet met 'http', maar met 'ftp'.

34. Zij het vaak met enige vertraging als Internet zwaar is belast.

en bouwen zo databases op met informatie over URLs. Als een gebruiker een zoekwoord intikt, worden de zo opgebouwde databases doorzocht (en dus niet Internet zelf). Dit betekent dat elk zoekstelsel eigen sterke en zwakke kanten heeft. Algemeen is het probleem dat het aantal hits vaak veel te groot is – zodat het nog zoeken blijft.

En – ter afsluiting van dit deel – dan zijn er nog de cookies. Nee, geen koekje van eigen deeg, maar een klein bestandje dat sommige Internet-sites zomaar, zonder dat u het weet, op de harde schijf van uw computer zetten. Doel daarvan zou zijn u meer gericht van dienst te kunnen zijn bij een volgend bezoek aan de site in kwestie want het cookie verschaft de site dan informatie over wat u eerder deed. Misschien een honorabele bedoeling, maar wel illustratief voor een fundamenteel dilemma: als u op zoek gaat naar informatie op Internet-sites, dan verschaft u die sites onvermijdelijk heel wat informatie over uzelf.³⁵ Dus toch een koekje van eigen deeg?

2 INTERNET ALS SOCIAAL SYSTEEM

2.1 Perspectief

Technologie als sociaal systeem

In de Inleiding heb ik³⁶ mij verzet tegen technologisch determinisme: het idee dat technologie bepalend is voor veranderingen in de samenleving. De maatschappelijke implicaties van een technologie worden immers niet bepaald door de technologie als zodanig, maar door het gebruik dat mensen en organisaties besluiten te maken van die technologie – dus door de keuzen van mensen en niet door inherente eigenschappen van de technologie. Bovendien zijn (mogelijke) maatschappelijke implicaties niet alleen factoren die beïnvloed worden door het gebruik

35. Dit wordt wel aangeduid als het achterlaten van digitale sporen. Slimme cybercops (of criminele organisaties) weten die sporen net zo goed te lezen als hun counterparts in de fysieke wereld.

36. In deel 1 was de ik-vorm niet nodig, maar deel 2 is zo persoonsgebonden dat helder moet zijn wie aan het woord is.

van een technologie, maar die factoren beïnvloeden ook zelf het verloop en de uitkomst van technologische ontwikkelingen.³⁷ Het afwijzen van technologisch determinisme zegt evenwel meer over hoe er – wat mij betreft – *niet* naar technologie gekeken moet worden dan over de vraag hoe er *wel* naar technologie gekeken kan worden. Omdat die laatste vraag van wezenlijk belang is voor elke discussie over de betekenis van Internet (in deze verhandeling, maar ook in de preadviezen van mijn collegae) eerst enkele opmerkingen over hoe er in het algemeen over technologie gedacht kan worden.

Uitspraken als 'Biotechnologie vormt een bedreiging voor de kwaliteit van ons voedsel', 'Duurzame technologie is goed voor de werkgelegenheid' of 'Informatietechnologie leidt tot verarming van menselijke relaties' zijn – in elk geval qua formulering – niet alleen een uiting van technologisch determinisme, maar ze zetten ook in andere opzichten de discussie al direct op het verkeerde been. Daarbij doel ik niet primair op het feit dat er inhoudelijk heel wat op de genoemde uitspraken valt af te dingen: mijn probleem is van een andere orde. Al dit soort uitspraken trekt namelijk impliciet een grens tussen het domein van de technologie en het domein waarin menselijke activiteiten en relaties zich afspelen. Alsof technologie dus niet tot dat laatste domein behoort, maar afkomstig is van een andere wereld die buiten de mens staat. Anders gezegd: mijn probleem met technologisch determinisme is dus niet alleen de simplistische oorzaak-gevolg relatie, maar ook dat het schotten veronderstelt tussen techniek en maatschappij die er helemaal niet zijn.

Juister en productiever is de opvatting is dat technologie niet te scheiden is van sociale systemen.³⁸ Sterker nog: dat technologie zelf een sociaal systeem is. Elke (door de mens gebruikte) machine is gebaseerd op een veelheid aan opvattingen over de toe-

37. Als dat niet het geval zou zijn, zouden de onderhavige preadviezen geen enkele zin hebben.

38. Hier opgevat als een samenhangend geheel van waarden, normen, overtuigingen, praktijken, tradities, rituelen, kennis en taal – waarbij elk mens in een groot aantal sociale systemen functioneert en waarbij sommige systemen slechts kort bestaan en andere zo sterk zijn geïnstitutionaliseerd dat ze het eeuwige leven lijken te hebben.

komstige gebruikers, hun wensen en verlangens, hun normen en waarden, hun vaardigheden, hun sociale relaties, etc. In die zin is een machine een neerslag van een verondersteld (toekomstig) sociaal systeem tussen ontwerpers, producenten en gebruikers: technologie als toegepaste sociale wetenschap. En als een nieuw apparaat het niet maakt op de markt, dan is dat meestal niet omdat de technologie in de klassieke betekenis van het woord niet deugt, maar omdat de technologie als sociaal systeem niet deugt: als blijkt dat de in het apparaat neergelegde opvattingen over mensen, menselijke relaties en menselijke normen niet kloppen.

Implicaties van dit perspectief

Waarom dit betoog? In de kern omdat de zojuist geschetste betekenis van technologie in een aantal opzichten anders is dan het beeld dat veel juristen – impliciet of expliciet – hanteren bij het nadenken over de maatschappelijke betekenis van technologische ontwikkelingen. Ik noem een paar aspecten.

- In het recht wordt technologie veelal opgevat als iets dat buiten de sociale werkelijkheid staat – terwijl in bovenstaande opvatting technologie deel is van de sociale werkelijkheid.
- Voor juristen is technologie iets dat door anderen wordt geproduceerd – terwijl uit bovenstaande opvatting volgt dat ook juristen mede-producent zijn van technologie.
- Voor juristen is technologie een fenomeen dat getoetst moet worden op het moment dat het binnenkomt in de samenleving – terwijl in bovenstaande opvatting de technologie dan al lang binnen is.³⁹

Als technologie opgevat wordt als sociaal systeem, dan ontstaat er dus een wat ander beeld van de relatie tussen recht en technologie. In dat beeld passen dan niet meer uitspraken als hierboven vermeld en van het standaard-formaat "Technologie X leidt tot verschijnsel Y en dat noopt tot het stellen van regel Z".

39. Zodat er nog maar beperkte mogelijkheden zijn om iets te doen aan minder wenselijk geachte aspecten – in elk geval minder dan in de ontwerpfase van de technologie.

Immers, of het nu gaat om biotechnologie, genetische manipulatie of informatietechnologie, in dat andere beeld is duidelijk dat er geen simpele causale verbanden zijn tussen technologie en de betekenis daarvan in en voor de samenleving. Het toch baseren van wet- en regelgeving op dit soort al te simpele verbanden heeft daarom veel overeenkomst met deelname aan een loterij: soms werkt het. Maar meestal niet omdat de uitwerking van die wet- en regelgeving anders is dan gedacht.

Een voorbeeld ter illustratie. Stel dat databestanden niet worden gezien als een technisch systeem, maar als een sociaal systeem, dat wil zeggen: als expressie van relaties tussen mensen en organisaties. De discussie is dan niet meer hoe de relaties tussen het technische⁴⁰ domein en het sociale domein ingericht moeten worden, maar welke regels er (eventueel) gesteld moeten worden met betrekking tot de relaties tussen dit specifieke sociale systeem en andere sociale systemen.

- Zo'n ander perspectief verplaatst de discussie al direct van eisen te stellen aan systeem-interne aspecten (zoals opslag en verwerking), naar systeem-externe eisen aan het gebruik van gegevens in relaties tussen mensen en organisaties.
- Het is ook direct duidelijk dat het sociale systeem 'databestanden' allerlei interacties heeft met andere (deels concurrerende) sociale systemen en dat elke vorm van wet- en regelgeving richting 'databestanden' direct zal doorwerken naar andere sociale systemen.
- Tenslotte: zoals alle sociale systemen ontleent ook elk sociaal systeem 'databestand' zijn identiteit in belangrijke mate aan de context. Dit maakt direct helder waarom het zo lastig is universeel bruikbare juridische definities te ontwikkelen voor technische termen als 'opslag' en 'verwerking': die termen krijgen pas betekenis in hun eigen, specifieke context en die context varieert per sociaal systeem 'databestand'.⁴¹

40. 'Technisch' in de klassieke betekenis van bouwen en moeren.

41. Naar mijn opvatting ligt hier een belangrijke verklaring voor het feit dat het na alle jaren nog steeds niet is gelukt om tot eenduidige definities te komen in de discussie over privacy-bescherming in relatie tot persoonsgegevens: er wordt een eenheid van context verondersteld die er niet is.

Het bovenstaande laat zich in belangrijke mate samenvatten in de uitspraak dat de betekenis van elke technische ontwikkeling inherent dubbelzinnig⁴² is: het kan zowel goed als slecht zijn, het kan een zegen zijn en een ramp, het is enerzijds een stap vooruit en anderzijds een stap achteruit, het kan leiden tot groei en bloei en het kan leiden tot misère en achteruitgang. Kortom: technische systemen zijn (net) sociale systemen.

Het is vanuit dit perspectief dat ik mij hierna waag aan de vraag naar de mogelijke betekenis van Internet. Verwacht daarom geen stellige uitspraken en krachtige conclusies: net als u ben ook ik zoekende. En vandaar dat ik het hierna liever heb over 'betekenis(sen)' dan over 'de' betekenis.⁴³

2.2 Betekenis(sen)

Een eigen Internet-cultuur

Natuurlijk is er in relatie tot Internet sprake van heel wat hype, overdrijving en opgeklapte lucht. Het is allemaal niet zo fantasistisch als wordt beweerd: surfen op Internet is maar al te vaak zoeken naar een speld in een hooiberg van ongekende afmetingen en dat met de snelheid van een slak. Echter, die constateringen vormen geen enkele reden om nu af te haken en te denken dat welwillende verwaarlozing de beste manier is om met Internet om te gaan. Integendeel, ik behoor tot diegenen die van mening zijn dat Internet nu al een belangrijke kracht is achter werkelijk fundamentele veranderingen en dat we nog maar aan het begin staan. Ik weet alleen niet precies om welke veranderingen het zal gaan en ik vrees bovendien dat de dynamiek zo groot is dat ik dat ook nooit precies zal weten. Toch zijn er, ook nu al, wel een paar lijnen aan te geven die van belang lijken te zijn.

Als direct uitvloeisel van de vorige paragraaf: Internet is veel meer dan een technisch systeem waarvan enige maatschappelijk

42. Met dank aan Paul Frissen, hoogleraar bestuurskunde aan de Katholieke Universiteit Brabant en onder meer auteur van het boek *De virtuele staat*, Academic Service, 1996.

43. Mocht die verkenning naar meer smaken: nog steeds is S. Negroponte, *Being digital*, MIT Press, Cambridge Mass. 1996, een absolute aanrader.

minder plezierige kanten moeten worden weggeslepen met wat aanpassingen in bestaande juridische concepten of wetgeving.⁴⁴ Een dergelijke opvatting is niet alleen een uiting van de benadering waartegen ik in de vorige paragraaf in verzet kwam, maar gaat ook voorbij aan het feit dat Internet een sociaal systeem is met een zeer groot aantal deelnemers en een grote mate van complexiteit. Zoals alle sociale systemen heeft Internet eigen kenmerken en een eigen structuur en cultuur en dat onderkennen is de eerste, essentiële stap in de zoektocht naar maatschappelijke betekenis(sen) van Internet.

- Het is gemakkelijk om termen als ‘cyberspace’, ‘cybernauts’, ‘cybercivilians’ en ‘cybercops’ te ridiculiseren, maar dat neemt niet weg dat voor miljoenen mensen die termen een expressie zijn van gedeelde normen en overtuigingen – dus van een eigen cultuur.
- Hoe sterk die cultuur is, blijkt uit het feit dat elke majeure gebeurtenis ergens op aarde direct leidt tot het spontaan ontstaan van groepen mensen die het laatste nieuws uitwisselen via Internet.
- Het feit dat, ondanks alle verzakelijking, netiquette nog steeds een rol speelt, kan ook worden opgevat als bevestiging van de waarde van de eigen Internet-cultuur, vooral in relatie tot niet-commerciële functies en diensten.

De kracht van de Internet-cultuur blijkt eveneens als een overheid – waar ook ter wereld – iets wil ondernemen dat in strijd is met die cultuur. De Amerikaanse overheid merkte het met wetgeving tegen het aanbieden van pornografie via Internet en de Nederlandse overheid merkte het met de plannen tot het verbieden van encryptie. Beide plannen riepen spontaan massaal verzet op.⁴⁵

44. Naar mijn indruk is dit echter wel de meest gangbare benadering in veel rechtswetenschappelijk onderzoek naar de gevolgen van Internet. Waarbij de term ‘gevolgen’ al een aanzienlijke vereenvoudiging is; zie paragraaf 2.1.

45. In het eerste geval vanwege het belang van vrijheid van meningsuiting op Internet (en dus niet vanwege waardering voor Internet-pornografie). In het tweede geval vanwege het belang van vertrouwelijke communicatie op Internet. Beide plannen zijn inmiddels van de baan: het eerste sneuvelde uiteindelijk in het Supreme Court, het tweede in de realisatie dat een verbod op encryptie niet handhaafbaar zou zijn.

Meest opvallend van Internet als sociaal systeem is vooral de afwezigheid van hiërarchie en formele organisatie; zie ook paragraaf 1.3. Enerzijds maximaliseert dit de vrijheid van degenen die deel uitmaken van de Internet-gemeenschap – anderzijds betekent het dat er geen aanspreekbare en verantwoordelijk te stellen instantie is. De orde(ning) van Internet is gebaseerd op coördinatie via technische protocollen (zie paragraaf 1.2) – en dus niet op hiërarchie en/of een formele allocatie van taken en bevoegdheden. Alleen al hierom verdient Internet het bestudeerd te worden door organisatiekundigen. Dit alles maakt het wel uitermate lastig voor overheden om regels te stellen en af te dwingen anders dan in relatie tot (al die miljoenen onzichtbare en ongrijpbare) *individuele* gebruikers.

Opvallend voor een sociale gemeenschap is verder dat op Internet (zoals het thans functioneert) direct visueel contact niet gangbaar is bij onderlinge communicatie. Het is denkbaar dat dit in de toekomst zo zal blijven, zelfs als de technische beperkingen aan het verzenden van beelden zijn verdwenen want het ontbreken van visueel contact is (voor velen) juist deel van de Internet-cultuur. Een 'Internetter' speelt met smileys om emotie over te brengen; voor velen ligt het plezier van chatten nu juist in het aannemen van een andere identiteit; en het in anonimiteit in cyberspace kunnen surfen is wat velen naar Internet trekt. Veel gebruikers van Internet hebben dus meerdere identiteiten en spelen daarmee in contacten met andere gebruikers. En dan helpt het ontbreken van visueel contact. Dit roept overigens wel de vraag op wat het juridisch betekent als één en dezelfde fysieke persoon onder meerdere identiteiten aan het rechtsverkeer op Internet gaat deelnemen.

De groei van Internet heeft ertoe geleid dat er minder sociale cohesie is voor Internet als geheel. Er beginnen zich binnen Internet meerdere (sub)culturen af te tekenen, elk met eigen kenmerken. Zo wijken de mores van veel nieuwsgroepen en van mailing lists sterk af van de mores op het WWW en de culturele afstanden lijken groter te worden. Maar dat bevestigt alleen maar dat Internet een sociaal systeem is: de fragmentatie van normen

en waarden die zich in andere sociale systemen heeft voorgedaan, doet zich ook op Internet voor.

Internet opvatten als sociaal systeem betekent dat het een centrale plaats krijgt in de grote maatschappelijke veranderingen van deze tijd. Daarbij is Internet enerzijds een expressie van die veranderingen en anderzijds een drijvende kracht achter de veranderingen. Zo wordt in veel toekomstscenario's uitgegaan van drie grote trends: globalisering, liberalisering en technologisering. Deze trends hebben, zo wordt gesteld, zoveel kracht en dynamiek dat het eigenlijk niet mogelijk is (en in elk geval niet verstandig) er tegen in te gaan. Internet heeft alles van doen met elk van deze trends. Bij globalisering en technologisering ligt dit zo voor de hand dat nadere toelichting overbodig lijkt. Internet *is* globalisering en technologisering: het draagt er aan bij en het wordt er door gestimuleerd. Maar ook liberalisering heeft een directe relatie met Internet juist omdat Internet als sociaal systeem tot dusverre grotendeels ontoegankelijk en ongrijpbaar is gebleken voor overheden en overheidsinterventies. Zelf-regulering en marktwerking zijn typische kenmerken van de Internet-cultuur: zo is Internet ontstaan en zo is het nog steeds georganiseerd. Zie ook paragraaf 1.1 en 1.3.

Als het gaat om de maatschappelijke betekenis(sen) van informatietechnologie in het algemeen, dan vallen al snel termen als 'de-materialisering' en 'virtueel'. Die termen zijn ook bij uitstek relevant in relatie tot Internet. De-materialisering ziet daarbij op het feit dat door informatietechnologie – en dus ook op Internet – fysieke handelingen en fysieke producten vervangen worden door symbolische handelingen en symbolische producten.⁴⁶ Op Internet volstaat een druk op de knop (van de muis) om een opdracht te geven en op Internet gaat het om informatie en kennis en niet om fysieke producten als zodanig. Dat op Internet eenzelfde fysieke persoon meerdere identiteiten kan aannemen is ook een voorbeeld van de-materialisering. Als tegenhanger van de fysieke wereld ontstaat er zo een virtuele wereld met virtuele personen, virtuele producten en virtuele handelingen. En

46. Een voorbeeld van de-materialisering: van goud naar munten naar papiergeld naar bankafschriften naar digitaal geld.

dus onvermijdelijk ook met virtueel rechtsverkeer. Internet is bij uitstek de belichaming van die virtuele wereld.

Internet en de elektronische snelweg

Er is nog één onderwerp waarover ik in deze paragraaf iets wil zeggen: de metafoor van de elektronische snelweg. Elders⁴⁷ heb ik betoogd dat deze metafoor ons zo langzamerhand op het verkeerde been zet. Oorspronkelijk bedoeld om een zo ongrijpbaar fenomeen als Internet te duiden in termen die tot de verbeelding spraken van niet-ingewijden, is de metafoor zo langzamerhand een eigen leven gaan leiden en wordt ons denken over Internet versluierd door beelden en associaties die alles van doen hebben met de metafoor, maar weinig of niets met Internet zelf. Al was het alleen maar omdat de metafoor Internet (weer eens) reduceert tot een technisch systeem, terwijl het (eveneens) een sociaal systeem is.

Als Internet aangeduid wordt als een 'elektronische snelweg' dan roept dit – net als elke metafoor – direct allerlei associaties op, bewust of onbewust.

- We weten dat het doel van een fysieke snelweg is om zo snel mogelijk van A naar B te reizen en dus veronderstellen we al snel dat dit ook het doel is van Internet. Terwijl het er voor de meeste Internet-gebruikers juist om gaat ongericht rond te dolen, dan wel om gericht ergens informatie op te halen.
- We weten dat het aanleggen en onderhouden van snelwegen een taak van de overheid is en dus veronderstellen we al snel dat de overheid deze taak ook zal moeten hebben in relatie tot Internet. Terwijl de rol van de overheid bij de aanleg en het onderhoud van Internet minimaal is geweest en zal blijven.
- We weten dat de overheid allerlei regels moet stellen aan het gebruik van snelwegen om het verkeer in goede banen te leiden en dus veronderstellen we al snel dat de overheid dit ook moet gaan doen voor Internet. Terwijl het gebruik van Internet heel andere risico's heeft dan het gebruik van snelwegen.

47. Automatisering Gids, 3 oktober 1997, p. 15.

Zo zijn er vast en zeker nog wel andere associaties te bedenken, maar het punt is (hoop ik) gemaakt: dat de metafoor van de elektronische snelweg ons denken stuurt en dat er geen enkele garantie is dat die sturing iets van doen heeft met het 'echte' Internet. Want stel nu eens dat Internet niet meer wordt vergeleken met een elektronische snelweg, maar met een elektronische markt: er ontstaan direct wezenlijk andere associaties en veronderstellingen over de aard van Internet.

– We weten allemaal dat er allerlei verschillende markten zijn, variërend van de arbeidsmarkt en de aandelenbeurs tot zwarte markten in veilinghallen en illegale markten in steegjes achteraf. En is dat niet wat Internet eigenlijk ook is: een grote diversiteit aan markten, elk met een eigen karakter?

– We weten allemaal dat de overheid slechts in zeer uitzonderlijke gevallen zelf een markt schept en dat de overheid er naar streeft zoveel mogelijk over te laten aan vrije marktwerking. Is dit nu juist niet een positie die de overheid zou moeten gaan innemen in relatie tot Internet?

– We weten allemaal dat de overheid sommige markten zeer intensief reguleert (de arbeidsmarkt bijvoorbeeld) en dat andere markten nu juist vrijplaatsen zijn (tot op zekere hoogte). Sluit die variatie in de rol van de overheid niet beter aan bij Internet dan de rol die de overheid vervult in relatie tot snelwegen?

Zoals uit deze voorbeelden blijkt hebben de andere associaties van de markt-metafoor implicaties voor de rol van de overheid. De verschillen van denken die zo ontstaan met de metafoor van de elektronische snelweg werken daarom direct door in de opvattingen over de noodzaak van wet- en regelgeving in relatie tot Internet. De betekenis(sen) van Internet afleiden uit een metafoor als de elektronische snelweg bergt dus het gevaar in zich dat het gaat om de metafoor en niet meer om Internet zelf. Datzelfde gevaar is uiteraard ook aanwezig in de metafoor van de elektronische markten. En dus lijkt het verstandig niet in de metafoor gevangen te raken.

2.3 Voor het recht

Rechtsverkeer in een virtuele wereld

Als sociaal systeem heeft Internet voor het recht in principe net zoveel of net zo weinig betekenis als andere sociale systemen. De relevantie(s)⁴⁸ van Internet voor het recht kan/kunnen dus wat mij betreft heel wat fundamenteeler zijn dan de bij veel juristen nog gangbare opvatting dat er met Internet wat problemen zijn die met enige juridische creativiteit opgelost kunnen worden. Die problemen zijn er en die creativiteit is nodig, maar er is meer aan de hand. Kern van dat 'meer' is dat het rechtsverkeer in een gede-materialiseerde en (dus) virtuele wereld als Internet er wezenlijk anders uit zal gaan zien – zeker op termijn.

Het andere karakter van het rechtsverkeer op Internet heeft – ik liep er in de vorige paragraaf al op vooruit – in de eerste plaats betrekking op de partijen die aan het rechtsverkeer zullen gaan deelnemen. Er ontstaan virtuele identiteiten die rechtshandelingen zullen gaan verrichten die niet te onderscheiden zijn van rechtshandelingen door fysieke entiteiten. Zonder bijzondere voorzieningen (technisch en juridisch) zal het daarom op Internet onmogelijk zijn onderscheid te maken tussen virtuele identiteiten en al dan niet daarmee verbonden natuurlijke personen of rechtspersonen. En als al vaststaat dat het om een natuurlijk persoon gaat, kan er vervolgens misschien geen verschil worden gemaakt tussen meer- en minderjarigen – om maar één juridisch significant onderscheid te noemen.

Bij wijze van illustratie: er zijn programma's (agents genaamd) die Internet kunnen afsporen naar informatie en die desgewenst een bestelling kunnen plaatsen. Natuurlijk is de afzender aansprakelijk al er iets fout gaat met zijn agent. Of geldt dat ook voor de maker van het programma? Of voor de leverancier als zijn programmatuur niet deugt? En wat als een agent actief blijft als de eigenaar overleden is? En zaken blijft doen met de agents van anderen? Die ook misschien al zijn overleden. Mag een sys-

48. Net als bij betekenis(sen) geeft de '(s)' aan dat ik niet de pretentie heb om even een antwoord te geven.

teembcheerder een agent om zeep helpen? Absurde vragen? Misschien – misschien niet.

Natuurlijk kunnen de meeste van dit soort specifieke problemen worden opgelost met een gezonde dosis juridische creativiteit, maar ik betwijfel of dit ook geldt voor het totaal van al dit soort ontwikkelingen. Waarschijnlijker lijkt dat Internet het op termijn noodzakelijk zal maken meer fundamenteel na te gaan denken over alles wat samenhangt met het leerstuk van de rechts-subjectiviteit.

Niet alleen de partijen veranderen, maar ook het rechtsverkeer zelf verandert van karakter: het wordt onzichtbaar, virtueel.⁴⁹ Dit kan, zo vermoed ik, op termijn ingrijpende consequenties hebben. Ter onderbouwing wijs ik op het volgende.

- Ten eerste, virtueel/elektronisch rechtsverkeer verloopt zeer veel sneller dan fysiek/papieren rechtsverkeer – dat is zelfs de reden bij uitstek voor de overstap van fysiek naar virtueel.
- Ten tweede, door die grotere snelheid, maar ook door andere eigenschappen⁵⁰ is het bij geschillen achteraf veel lastiger (zo niet onmogelijk) te reconstrueren hoe een bepaalde procedure precies is verlopen.
- Ten derde, doordat reconstructie achteraf lastig/onmogelijk is geworden, is ook het vaststellen van oorzaak-gevolg relaties uitermate lastig/onmogelijk geworden.
- Ten vierde, dit betekent dat alle juridische leerstukken die uitgaan van causaliteit (zoals: schuld, aansprakelijkheid, strafbaarheid) het moeilijk gaan krijgen in de wereld van het virtuele rechtsverkeer op Internet.⁵¹

Virtueel rechtsverkeer heeft dus in een aantal opzichten wezenlijk andere kenmerken dan fysiek rechtsverkeer en dit stelt nieuwe eisen aan het recht. De werkelijke betekenis van virtueel rechtsverkeer moet nog blijken, maar het belang van de zaak lijkt

49. En dit geldt ook voor het onrechtsverkeer, dat wil zeggen: de criminaliteit.

50. Zoals het gemak waarmee encryptie van berichten mogelijk is.

51. Hangt de groei van risico-aansprakelijkheid hiermee samen? Bij risico-aansprakelijkheid behoeft er immers niet meer een oorzaak-gevolg relatie gereconstrueerd te worden.

mij zodanig groot dat ontkenning of welwillende verwaarlozing van de ontwikkelingen een onaantrekkelijk scenario is.⁵²

Implicaties voor overheid en recht

Internet verandert niet alleen de aard van het rechtsverkeer – daarmee een aantal juridische leerstukken ter discussie stellend – maar het roept ook vragen op in relatie tot de rol van het recht en van de overheid in het algemeen. Als steeds meer maatschappelijke activiteiten zich verplaatsen naar Internet, dan rijst de vraag of het recht en de overheid nog wel in staat zijn datgene te doen wat recht en overheid traditioneel plegen te doen: het bevorderen van maatschappelijke orde en rechtvaardigheid.⁵³

Veel van het berichtenverkeer op Internet speelt zich af over de landgrenzen heen, zeker voor een klein land als Nederland. En veel van dit berichtenverkeer is niet te traceren en, als het al te traceren is, dan is het gecodeerd (of kan het gemakkelijk gecodeerd worden). Lang niet al het berichtenverkeer is rechtens relevant, maar een steeds groter deel wordt dat wel, vooral naarmate het zakelijk gebruik van Internet toeneemt. Daarbij gaat het niet alleen om het uitwisselen van informatie over zakelijke transacties, maar ook om het aangaan en afwickelen van zulke transacties.⁵⁴ Internet is niet alleen een medium voor informatie- en kennisoverdracht: het is ook – en steeds meer – een medium voor het aanbieden en afnemen van zakelijke diensten.

Een vraag die dan direct opkomt is hoe het zit met de fiscaliteit van zakelijke transacties op Internet en of zij überhaupt wel zichtbaar zijn voor de belastingheffende overheid, vooral als ook de betalingen virtueel worden afgewikkeld. Het moge duidelijk zijn dat het voor de overgrote meerderheid van burgers en be-

52. Dit geldt, als gezegd, ook voor onrechtsverkeer. Als digicash de anonimiteit van betaler en ontvanger volledig waarborgt – zoals de ontwerpers van het systeem claimen – lijkt digicash een prima betaalsysteem voor afpersers, gijzelnemers en terroristen.

53. Elke redelijke omschrijving is op voorhand akkoord: het gaat hier niet om de rol van overheid en recht als zodanig, maar uitsluitend om het feit dat die rol verandert.

54. Bijvoorbeeld via Electronic Data Interchange (EDI): een set afspraken voor zakelijk berichtenverkeer.

drijven geen verschil uitmaakt als er zaken worden gedaan via Internet: ze houden zich aan de regels, Internet of niet. Maar feit blijft dat Internet het gemakkelijker maakt om belastingen te ontduiken, terwijl het ook methoden om belastingdruk te ontwijken binnen het bereik brengt van een veel grotere groep bedrijven. Konden tot voor kort alleen grote multinationals hun betalingen zodanig over de wereld routen dat de belastingdruk minimaal is, Internet brengt die mogelijkheden binnen het bereik van de kleinste onderneming, ja zelfs van particulieren. Fiscalisten en de Belastingdienst bezinnen zich dan ook reeds op de vraag hoe de overheid haar belastinginkomsten op peil houdt in een wereld van virtuele transacties, zowel zakelijk als particulier.⁵⁵

Meer in het algemeen heeft Internet tot gevolg dat bedrijven (en particulieren) footloose worden, dat wil zeggen: minder gebonden aan een bepaalde fysieke vestigingsplaats. Dit geldt uiteraard in het bijzonder voor bedrijven die de kost verdienen op Internet zelf. Een korte blik op het systeem van IP-adressen en URLs (zie deel 1) maakt duidelijk dat een bedrijf overal ter wereld bereikbaar is mits er een redelijke telecommunicatie infrastructuur aanwezig is. Het is zelfs meestal zo dat een gebruiker van Internet niet weet waar de site van een bepaald bedrijf fysiek is gevestigd: het aanklikken van een icoon is voldoende om te switchen van een site in (bijvoorbeeld) Duitsland naar een site in Zuid Afrika – en dat zonder dat de gebruiker weet waar die sites zich bevinden. Dit betekent dat bedrijven (en particulieren) veel gemakkelijker dan voorheen op zoek kunnen gaan naar een vestigingsplaats die qua belastingregime of qua wetgeving het meest aantrekkelijk is.

- En niets let een bedrijf om activiteit X te localiseren op een site in het ene land en activiteit Y (die daar misschien verboden is) op een site in een ander land.
- Waarbij het verder nog de vraag is of het überhaupt mogelijk

55. Er zijn fiscalisten die het einde voorzien van de Inkomstenbelasting: veel te afhankelijk van informatie die in een virtuele omgeving ontraceerbaar is of dat gemakkelijk gemaakt kan worden. Zij bepleiten derhalve de belastingheffing over te hevelen naar vormen die minder afhankelijk zijn van allerlei informatie over transactie of belastingplichtige.

is te bepalen op welke site (of sites) een bepaalde (rechts)handeling werd verricht.

Het voorafgaande is *mutatis mutandis* ook direct relevant voor het opsporen en vervolgen van strafbare feiten. Want het staat vast dat er op Internet sprake is van strafbare handelingen: het aanbieden van kinderpornografie is daarvan op dit moment het meest bekende voorbeeld. Het juridische principe lijkt eenvoudig genoeg: wat in de gewone/fysieke wereld is verboden, moet uiteraard ook verboden zijn in de virtuele wereld van Internet. Echter, principe of niet, feit blijft dat het met de handhaafbaarheid van regels wezenlijk anders is gesteld in de wereld van Internet dan in de fysieke wereld. Als het gaat om het opsporen van strafbare feiten vormt encryptie inderdaad een zeer wezenlijke beperking en vandaar de (tot dusverre mislukte) pogingen van overheden om encryptie aan banden te leggen.

Toch zou het een misverstand zijn te denken dat Internet immuniteit biedt aan criminelen. Met het groter worden van de ervaring van opsporingsinstanties begint duidelijk te worden dat Internet misschien veel betere mogelijkheden biedt voor het opsporen van strafbare handelingen dan oorspronkelijk gedacht.⁵⁶ Elk gebruik van Internet laat digitale sporen na⁵⁷ en zo langzamerhand leren opsporingsinstanties die sporen te herkennen. Bovendien: als iedereen op Internet vrijelijk een andere identiteit mag aannemen, waarom zouden opsporingsinstanties dat dan ook niet mogen doen om zo wetsovertreders te betrappen?⁵⁸ Wat betreft het vervolgen van strafbare feiten: een steeds terugkerende vraag zal zijn in welk land een bepaalde handeling zich heeft voorgedaan. Als eerder opgemerkt, Internet maakt het lastig om oorzaak-gevolg relaties te reconstrueren want contacten in de virtuele wereld zijn snel en vluchtig en spelen zich af over de gehele aardbol.

56. Het vergroten van de Internet-intelligentie van opsporingsinstanties lijkt daarom een betere strategie ter verbetering van de rechtshandhaving op Internet dan het uitvaardigen van allerlei nieuwe geboden en verboden.

57. Bijvoorbeeld in de registraties van access-providers en van bedrijven die informatie aanbieden op Internet.

58. Wat direct de vraag oproept naar de legitimiteit van Internet opsporingsmethoden. Als inkoopoperaties niet mogen in de fysieke wereld, mogen ze dan wel in de wereld van Internet?

Nieuwe vragen en aandachtspunten

Gevolg van dit alles is dat de ordenende en sturende rol van de overheid en het recht ter discussie komt te staan. Bij elk gebod en verbod in relatie tot activiteiten op Internet zal een overheid zich steeds twee vragen moeten stellen: kan het gebod of verbod worden ontkracht door naar andere landen uit te wijken en is overtreding van een gebod of verbod op te sporen? En een eventuele vraag naar het effect van een voorgenomen maatregel op de werkgelegenheid wordt eveneens heel wat pregnanter nu bedrijven zich veel sneller en gemakkelijker kunnen verplaatsen. Ik vrees (want ik geloof in het maatschappelijk belang van een goed functionerende overheid en rechtsstelsel) dat in veel gevallen het antwoord op dit soort vragen ontvullend zal werken op de sturingspretenties van de overheid en bijgevolg op de effectiviteit van het recht in het algemeen en van wet- en regelgeving in het bijzonder.

Is het bovenstaande nu reden tot grote somberheid? Naar mijn mening is daar tot dusverre weinig reden voor als het gaat om criminaliteitsbestrijding. Een nuchtere blik op de realiteit leert dat het best meevalt met de criminaliteit op Internet. Het aanbieden van kinderpornografie mag niet worden gebagatelliseerd, maar het aanbod was er voor Internet, is er buiten Internet en zal er zijn na Internet. Bovendien beginnen opsporingsinstanties juist hier effectief te worden, onder meer door Internet zelf in te zetten om aanbieders in de val te laten lopen. Wat betreft andere vormen van criminaliteit lijken de incidenten die er zijn geweest⁵⁹ in de publiciteit meer aandacht gekregen te hebben dan ze eigenlijk waard zijn.

Anders ligt het naar mijn oordeel met de gevolgen van Internet voor de overheidsfinanciën en de rol van de overheid en het recht in relatie tot maatschappelijke orde en rechtvaardigheid. Op die beide terreinen zou Internet wel eens tot wezenlijke veranderingen kunnen nopen. Waarbij wat mij betreft op dit moment de belangrijkste vraag is of overheden – nationaal en internationaal – wel in staat zijn tot handelen met voldoende snelheid

59. In het bijzonder het inbreken op andere computers (hacken) via Internet.

en kwaliteit, bijvoorbeeld als het gaat om het ontwikkelen van aangepaste vormen van belastingheffing. Als overheden daarin niet zouden slagen, verzwakt dat hun positie nog verder – zodat ze nog weer minder kans maken het tij te keren.

Deze overwegingen onderstrepen het belang dat de overheid Internet niet langer blijft zien als technisch systeem dat aan banden moet worden gelegd, maar als één van de sociale systemen waarin mensen en organisaties met elkaar verkeren, zowel persoonlijk als zakelijk en zowel binnen de grenzen van de wet als daarbuiten. Ook dit geeft aan dat het productief is af te stappen van de metafoor van de elektronische snelweg en over te stappen op de metafoor van de elektronische markten; als sociaal systeem doen markten het in deze tijd heel wat beter dan snelwegen.

Het bovenstaande overziende is (hopelijk) één ding duidelijk geworden: dat Internet niet alleen belangwekkende juridisch-inhoudelijke vragen oproept, maar dat het ook uitdagingen aan het recht presenteert van meer fundamentele aard, zeker op termijn. Daarbij gaat het vooral om de volgende drie ontwikkelingen.

- De-materialisering: fysieke producten worden vervangen door elektronische.
- De-territorialisering: bedrijven en individuen zijn minder gebonden aan plaats.
- Virtualisering: naast fysieke identiteiten ontstaan er ander-soortige identiteiten.

Daarmee is het beeld niet volledig, maar het zou te ver voeren om hier ook nog in te gaan op zaken als het gevaar van een maatschappelijke tweedeling tussen informatie-rijken en informatie-armen en op de vraag hoe Internet en alles wat daarmee samenhangt een plaats kan krijgen in het onderwijs.

2.4 Voor juristen

Implicaties voor het werk van juristen

Het bovenstaande suggereert dat er werk aan de winkel is voor juristen. Ik redeneer als volgt.

- Informatie- en communicatietechnologie is ongetwijfeld één van de factoren die bijdragen tot, dan wel faciliteiten bieden voor, de zeer snelle groei van het aantal juridisch relevante transacties tussen de deelnemers aan het maatschappelijke rechtsverkeer. Hetzelfde geldt voor de steeds groter complexiteit van die transacties.⁶⁰
- Als we nu, bij wijze van hypothese, aannemen dat het aantal geschillen constant blijft bij gelijke complexiteit van transacties, dan identificeert bovenstaande uitspraak twee factoren met een positief effect op de werkgelegenheid voor juristen: steeds meer transacties en een steeds grotere complexiteit.

Toch is er meer aan de hand en is Internet ook in andere opzichten één van de elementen die een rol spelen bij de veranderingen in het werk van juristen. Ontwikkelingen als globalisering en liberalisering zijn niet alleen van invloed op dat werk via het verschijnsel Internet, maar zijn evenzeer autonome krachten achter allerlei veranderingen, ook in het werk van juristen. Wat is oorzaak en wat is gevolg?

Is er dus meer te zeggen over de relatie(s)⁶¹ tussen Internet en het werk van juristen? Ik benader die vraag vanuit twee perspectieven: het werk van juristen als *proces* (de manier van werken) en dat werk als *product* (de uitkomst van het werk).

60. Men denke bijvoorbeeld aan de variatie in verzekeringsvormen en in spaarregelingen: allemaal alleen maar mogelijk vanwege de grootschalige inzet van computers. Massa-maatwerk is een toepasselijke term voor dit, met informatisering samenhangend verschijnsel.

61. Ook hier weer '(s)' want het blijft speculeren net als in de eerdere paragrafen.

Veranderingen in het werkproces

Informatie- en communicatietechnologie leiden, zo wordt gesteld, tot horizontalisering van werkverhoudingen, dat wil zeggen: er ontstaan tussen mensen en tussen organisaties meer horizontale relaties van (meer) gelijkwaardige partijen. In deel 1 werden van die ontwikkeling reeds enkele voorbeelden gegeven in relatie tot Internet, in het bijzonder bij de Internet-functies News en mailing lists. In beide gevallen gaat het immers om mensen en organisaties die zich spontaan verenigen rondom een bepaald thema en die daarover informatie delen: Internet als horizontaal sociaal systeem tussen gelijkwaardige partijen.

Als juridisch werk wordt opgevat als proces, zal horizontalisering ook voor juristen wel degelijk van belang zijn. Onder meer omdat ook juristen via Internet informatie zullen gaan uitwisselen. En dit zowel ten behoeve van hun professionele ontwikkeling, als ten behoeve van hun dagelijkse werkzaamheden. Op dit moment biedt Internet al heel wat informatie die voor juristen van belang kan zijn,⁶² maar het is zeker niet zo dat een jurist zonder Internet reeds nu professioneel achter raakt of zijn werk niet meer goed kan doen. De vraag is echter hoe lang deze situatie nog zal voortduren. Ik vermoed dat de echte verandering zich zal voltrekken via het ontstaan van juridische intranetten⁶³ (bijvoorbeeld tussen advocatenkantoren of tussen de rechterlijke macht en de advocatuur) en dat het daarna een kleine stap zijn naar het op grotere schaal doorbreken van Internet zelf. Wellicht in eerste instantie voor zakelijk verkeer over de grens want ook juristen ontkomen niet aan de verdere internationalisering van hun werk. Het moment dat een jurist zonder Internet zijn vak niet meer goed kan beoefenen, ligt naar mijn mening niet erg ver meer in de toekomst. Ook niet als het gaat om typisch nationale rechtsgebieden als strafrecht en bestuursrecht.

Dit lezende – en als ze het al willen geloven – zullen veel juristen zich direct afvragen hoe het gesteld is met de vertrouwelijkheid

62. Zie het eerdergenoemde boek van Van der Wees en Renden, noot 1.

63. Zeg maar: besloten versies van het openbare Internet; zie verder deel 1. Er zij al dergelijke intranetten voor accountants en notarissen.

van het (juridische) berichtenverkeer: Internet is immers een openbaar systeem. Zoals eerder werd gezegd,⁶⁴ zijn berichten via Internet relatief gemakkelijk te onderscheppen, maar is het gebruik van encryptie een zeer effectieve waarborg tegen schendingen van de vertrouwelijkheid.⁶⁵ Het is in feite heel wat lastiger de vertrouwelijkheid te garanderen van documenten in papieren vorm dan van documenten in elektronische vorm.

Horizontalisering is niet het enige aspect van Internet dat van belang is voor de manier van werken van juristen. Ook kennis-technologie begint zo langzamerhand door te dringen in het juridische domein. Kennissystemen maken niet alleen juridische informatie toegankelijk voor een gebruiker, maar zij ondersteunen een gebruiker ook met het redeneren met die informatie doordat ze beschikken over kennis van de rechtsregels met betrekking tot een bepaald juridisch onderwerp. Combineer deze ontwikkeling met Internet als medium om juridische kennissystemen overal en altijd toegankelijk te maken voor juristen en de rechtzoekende zelf en er ontstaat een situatie die op allerlei manieren van invloed zal zijn op het werk van juristen.

- Er zijn al advocatenkantoren die bepaalde formulieren en standaard-contracten aanbieden via Internet direct aan de rechtzoekende. Voeg daar redeneermechanismen aan toe die een leek-gebruiker helpen bij het maken van de keuzen of bij het invullen van de formulieren: zie daar, individueel juridisch advies via Internet.⁶⁶
- Natuurlijk zal het daarbij, zeker in het begin, om juridisch zeer simpele kwesties gaan, veelal vragen die een jurist kan beantwoorden zonder enig nadenken. Echter, de aangeduide systemen zullen niet op dat niveau blijven steken, vooral als er con-

64. Paragraaf 1.2.

65. In principe kan een met encryptie versleuteld bericht altijd worden gekraakt, maar als een supercomputer daarvoor een paar duizend uren moet rekenen, dan is dat voor de meeste berichten afdoende garantie van vertrouwelijkheid.

66. Het notariaat heeft die stap al gezet door het aanbieden van een site waarop gebruikers interactief kunnen uitrekenen wat de financiële gevolgen zijn van het al dan niet hebben van een testament.

currentie gaat ontstaan tussen aanbieders van juridisch advies via Internet, lid van de advocatuur of niet.

– Bovendien wordt het voor het bedrijfsleven zo nog weer gemakkelijker zich voor advies direct te wenden tot de site van een advocatenkantoor in het land waar een rechtsvraag of een geschil zich voordoet.

De combinatie van kennistechnologie en Internet zal op termijn veel routinematig werk weg kunnen halen van het bureau van een jurist. Enerzijds een zegen – anderzijds ook minder omzet, vooral voor jonge, minder ervaren krachten. Daar komt nog bij dat niet alleen juridische dienstverleners kennis via Internet zullen gaan aanbieden, maar dat dit ook gedaan zal worden door actoren die traditioneel heel wat werk genereren voor juristen, in het bijzonder de overheid. Voor mij staat vast dat er een moment zal komen waarop een burger veel van het standaard-rechtsverkeer met de overheid (vergunningen, belastingen, etc.) kan afhandelen via Internet. Als de overheid daarbij kennistechnologie inzet om die burger ook in juridisch opzicht te ondersteunen, dan zal dit van invloed zijn op omvang en aard van werkzaamheden die veel juristen traditioneel tot hun vak- en afzetgebied rekenen.

Een laatste aspect van de relatie tussen Internet en de manier van werken van juristen. Juristen zijn – het is een open deur – informatieverwerkers pur sang. Internet zal de hoeveelheid direct te raadplegen juridische documentatie in snel tempo veel en veel groter maken. Dat wil evenwel niet zeggen dat daarmee de kwaliteit van de juridische informatievoorziening beter is geworden. Integendeel: als juristen niet de weg weten te vinden in die heel veel grotere hoeveelheid documentatie, dan leidt Internet alleen maar tot minder informatie.⁶⁷ En dus tot verlies van kwaliteit. Natuurlijk ligt hier een taak voor de ontwikkelaars van juridische documentatiesystemen en het is dan ook verheugend

67. Vandaar mijn (achterhoede)gevecht tegen het gelijkschakelen van de begrippen 'gegevens' en 'informatie'. Documentatie bevat gegevens en gegevens zijn pas informatie als ze bij de gebruiker een vraag beantwoorden of een onzekerheid verminderen.

dat er echt innovatieve systemen beschikbaar beginnen te komen.

De handschoen ligt evenwel ook in de kring van de juridische beroepsgroep. Evenals reeds het geval is in andere professies zullen juristen (nog) meer vaardigheid moeten gaan ontwikkelen in het met zo gering mogelijke inspanning vinden van de juiste juridische informatie in die nog steeds sneller groeiende hooiberg van Internet. Het moge duidelijk zijn dat deze uitspraak eveneens implicaties heeft voor het rechtswetenschappelijke onderwijs: ook daar zal veel meer gedaan moeten worden aan het trainen van studenten in het zoeken naar informatie op Internet.

Veranderingen in relatie tot het product

Kom ik – als tweede perspectief – bij het product van al dat juridische werk. Er zijn natuurlijk andere uitkomsten van het werk van een jurist – bijvoorbeeld een tevreden cliënt of rechtzoekende – maar voor hetgeen ik hierna aan de orde wil stellen, volstaat het de discussie te beperken tot één soort product: de ‘juridische beslissing’.

In het voorafgaande gaf ik reeds aan te verwachten dat in de toekomst steeds meer (routinematige) juridische beslissingen gegenereerd zullen worden door een directe interactie via Internet tussen de persoon die een beslissing vraagt en de instantie die de beslissing moet nemen, vaak een overheidsdienst. Dit kan betekenen dat juristen op meer afstand komen te staan van het product ‘juridische beslissing’. In het geschetste scenario is hun rol niet meer het zelf nemen van beslissingen of het geven van leiding aan medewerkers die daarmee zijn belast, maar is het hun taak er voor in te staan dat het systeem dat de burger gebruikt, juridisch correcte beslissingen neemt (inclusief passende motivering). Dus: het systeem neemt de concrete juridische beslissing in het individuele geval en juristen moeten er voor zorgen dat het systeem juridisch correct functioneert.⁶⁸ Bij

68. Een ontwikkeling die zich ook in andere professionele beroepsgroepen voordoet, van piloten tot medici. Een piloot van een modern vliegtuig vliegt – als alles goed gaat – dat toestel niet meer zelf, maar bewaakt het goed functioneren van alle automatische systemen aan boord.

wijze van illustratie: stel dat een burger via Internet een uitkering kan aanvragen en dat het systeem zelf beslist over het al dan niet verlenen van die uitkering (misschien zelfs de overboeking automatisch in orde maakt), dan zullen terzake kundige juristen niet alleen het systeem moeten helpen inrichten, maar zullen zij eveneens de juridische kwaliteit van dat systeem moeten kunnen garanderen.

Als Internet op deze manier wordt ingezet – en dat is in mijn optiek alleen maar een kwestie van tijd – dan produceren juristen niet meer zelf individuele juridische beslissingen, maar produceren zij dus uitsluitend de juridische kwaliteit van dergelijke systemen. Waarbij het, zeker in het begin, zal gaan om juridisch eenvoudige beslissingen, maar dat is wel de categorie met het grootste volume.⁶⁹

Een tweede overweging vanuit een product-perspectief. Informatie- en communicatietechnologie (en dus ook Internet) maken de wereld in bepaalde opzichten meer transparant: er worden steeds meer gegevens over mensen en organisaties opgeslagen en de mogelijkheden al die gegevens onderling te koppelen worden voortdurend groter. Die grotere transparantie heeft ook betekenis voor juridische beslissingen. Zo is de rechterlijke macht terecht meer beducht dan vroeger voor slecht verklaarbare inconsistenties tussen uitspraken. Tot voor kort waren onderling tegenstrijdige uitspraken (vooral in eerste aanleg) slecht waarneembaar zowel voor de buitenwereld, als voor de rechterlijke macht zelf, maar dat ligt op dit moment al anders. Terwijl het helemaal anders komt te liggen als rechterlijke uitspraken via Internet raadpleegbaar zouden zijn.

Hetzelfde geldt *mutatis mutandis* voor allerlei andere juridische beslissingen, bijvoorbeeld in de sfeer van de sociale zekerheid. En als er eenmaal (ogenschijnlijk) onverklaarbare verschillen tussen juridische beslissingen zijn geïdentificeerd, dan is het zeer eenvoudig, zelfs voor een individueel persoon, om daar via Internet de nodige publiciteit aan te geven (bijvoorbeeld via een mailing list). Die toegenomen transparantie van de juridische

69. Waardoor de noodzakelijk investeringen al snel rendabel zullen zijn.

wereld als gevolg van Internet zal dus extra eisen stellen aan de kwaliteit van juridische beslissingen en hun motivering.

De vraag rijst welke invloed dit soort ontwikkelingen zullen hebben op de onderlinge verhoudingen binnen de beroepsgroep van de juridische dienstverleners. Enerzijds lijkt het er op dat Internet de huidige trend tot schaalvergroting en netwerkvorming weer wat kan afzwakken omdat, via horizontale werkverbanden, de zelfstandige jurist of het kleine kantoor gemakkelijker aan de noodzakelijke informatie kan komen en gemakkelijker met de omgeving kan communiceren dan voorheen.⁷⁰ Anderzijds lijkt Internet voordelen te bieden aan grotere organisaties, vooral als er meer concurrentie komt doordat het volume aan routinezaken afneemt en doordat een rechtzoekende net zo gemakkelijk (bijvoorbeeld) een Amerikaans kantoor kan raadplegen als een kantoor in Nederland.

De toekomst zal uitwijzen wat het netto-effect van deze, deels tegengestelde krachten zal zijn, maar één ding lijkt redelijk zeker: juist binnen een traditioneel sterk gesloten beroepsgroep als die van de juridische dienstverleners zou Internet wel eens een fenomeen kunnen zijn dat de verhoudingen grondig ter discussie stelt. Met als meest waarschijnlijke uitkomst dat de onderlinge concurrentie binnen de beroepsgroep en de concurrentie met andere, aangrenzende beroepsgroepen heel wat groter zal worden – waarbij de mate van waarschijnlijkheid van deze uitkomst recht evenredig is met de openheid van de markt waarin wordt geopereerd.⁷¹

Experimenteren is investeren

Het is een soort ervaringsregel dat elke nieuwe technologie drie fasen doorloopt bij het (al dan niet) verwerven van maatschappelijke acceptatie.

- Eerst wordt een nieuwe technologie eigenlijk alleen maar op

70. Mits er over de noodzakelijke vaardigheden wordt beschikt en dat is juist in kleine kantoren vaak lastig te realiseren.

71. Hetgeen suggereert dat, net als in andere branches, kleine spelers er goed aan doen zich meer dan voorheen op niche-markten te gaan richten.

dezelfde manier en voor dezelfde doeleinden gebruikt als de oude technologie.⁷²

– In een tweede fase is het motto ‘meer van hetzelfde’: in de kern wordt de nieuwe technologie nog voor de oude functies en doelen ingezet, maar er wordt wel meer mee gedaan en/of geproduceerd.⁷³

– Pas in de derde fase leidt de nieuwe technologie tot andere manieren van werken en nieuwe producten en pas dan wordt ook echt duidelijk(er) wat de maatschappelijke betekenis(sen) zijn.⁷⁴

Informatie- en communicatietechnologie beginnen zo langzamerhand de derde fase te bereiken en Internet past in die lijn omdat het leidt tot andere manieren van werken en nieuwe producten. Dit impliceert wel dat op dit moment Internet eerder een proeftuin is dan een bewezen systeem en dat pas na heel wat experimenteren zal blijken wat uiteindelijk de betekenis van Internet is voor het werk (proces en product) van juristen. In andere landen – uiteraard de Verenigde Staten voorop – wordt er daarom ook door juristen volop geëxperimenteerd met de mogelijkheden van Internet. Veel van wat Internet op dit moment juristen te bieden heeft is daarom te vinden op Amerikaanse sites. Daarmee vergeleken is de Nederlandse juridische wereld nog weinig actief. Naar de redenen hiervan kan alleen maar worden gegist: gebrek aan interesse, gebrek aan kennis, te weinig toekomstgerichtheid, te kleinschalig, te druk met andere zaken? Feit is natuurlijk ook dat experimenteren met Internet niet direct nieuwe omzet oplevert.

Wat echter de redenen zijn, nu investeren in experimenten met het gebruik van Internet is naar mijn mening voorwaarde om die kennis en ervaring op te doen die nodig zijn om op termijn volwaardig gebruik te kunnen maken van de potenties van Internet in relatie tot het werk van juristen. Daarbij gaat het om meer dan werkgelegenheid, omzet en concurrentie met andere be-

72. Auto als koets en computer als tikmachine.

73. Met auto's meer kilometers dan met de koets en met de computer meer pagina's dan met de tikmachine.

74. In het geval van auto's: het ontstaan van slaapsteden, woon-werkverkeer, recreatieve mobiliteit, milieuproblemen, etc.

roepsgroepen: ook de maatschappelijke acceptatie en kwaliteit van het recht en de rechtspleging zijn in het geding. Daarom is er alle reden de vraag te stellen hoe kan worden bereikt dat Nederlandse juristen meer actief op zoek gaan naar de kansen die Internet ook aan hen biedt tot verbetering en vernieuwing van hun werk. En de rechtsstaat.

UITLEIDING

Deel 1 van dit preadvies is verre van compleet en deel 2 is verre van consistent. Voor een deel zullen die feilen mij aan te rekenen zijn, maar ik meen dat het redelijk is de tekortkomingen van dit verhaal voor een deel ook toe te rekenen aan het onderwerp zelf. Internet is zo veelomvattend en tegelijkertijd nog zo volop in beweging dat elke poging tot beschrijving en karakterisering aangemerkt moet worden als *mission impossible* – het equivalent van een poging tot biljarten op een schip in de storm.

Daarom hier al helemaal geen poging tot het trekken van eindconclusies uit hetgeen zojuist werd opgemerkt: dat zou de zaak alleen maar erger maken want het zou suggereren dat er antwoorden zijn waar er alleen maar vragen zijn. In plaats daarvan een korte tour d'horizon van mijn ankers in de zee van verwarring die Internet heet.

- Juist vanwege alle vragen en verwarring vermijdt dit preadvies zoveel mogelijk krachtig klinkende, maar daarom niet minder ongefundeerde uitspraken over de 'effecten van Internet' en wat daarmee 'gedaan moet worden'.⁷⁵
- Cruciaal is de boodschap dat Internet meer is dan een technisch systeem: het is tevens een sociaal systeem en het is dus een misrekening Internet uitsluitend op te vatten en te duiden als een (indrukwekkend) stuk techniek.
- Als Internet wordt opgevat als sociaal systeem, dan is direct duidelijk waarom de maatschappelijke betekenis(sen) ervan dubbelzinning is (zijn): het hangt er maar net vanaf welke keu-

75. Dat geldt ook voor deze samenvatting, al zijn de formuleringen daarvan noodzakelijkerwijs zo hier en daar wat kort door de bocht.

zen mensen en organisaties maken in relatie tot het gebruik van Internet.

- Als sociaal systeem heeft Internet een eigen cultuur met een eigen taal en met eigen normen en waarden en die cultuur leeft voor miljoenen mensen net zo sterk als de cultuur van het land waarin zij wonen – voor sommigen zelfs heel wat meer.
- Internet is oorzaak en gevolg van de de-materialisering van maatschappelijke processen en het schept mede daardoor een virtuele wereld waarin fysieke zaken zijn vervangen door hun symbolische representaties.
- Al deze ontwikkelingen tezamen betekenen dat Internet – zeker op termijn – van het recht en van juristen meer zal vragen dan het repareren van wat barstjes in de dogmatiek: het oprekken van oude concepten zal niet blijven voldoen.
- Internet schept virtuele rechtssubjecten en op termijn zullen deze autonoom in en via Internet rechtshandelingen gaan verrichten, mogelijk zelfs tegen de wil van het oorspronkelijke fysieke rechtssubject in.
- Internet zal de drager worden van virtueel rechtsverkeer dat veel sneller zal verlopen dan het fysieke, dat geen grenzen kent en dat – mede hierdoor – zich minder gemakkelijk zal lenen voor reconstructies achteraf van oorzaak-gevolgrelaties.
- Het wegvallen van grenzen en het (eventueel) onzichtbaar worden van oorzaak-gevolgrelaties hebben fundamentele betekenis voor het recht (aansprakelijkheid en opsporing) en de positie van de overheid (regelbereik en fiscaliteit).
- Dit alles betekent dat er werk aan de winkel is voor juristen, maar Internet betekent ook dat dit werk anders zal zijn, zowel qua manier van werken (meer horizontale verbanden), als qua uitkomst (meer transparantie en concurrentie).
- Tegen deze achtergrond valt op dat er – juist vanwege alle vragen en verwarring – zo weinig door Nederlandse juristen wordt geëxperimenteerd met het opbouwen van kennis over en ervaring met Internet.

Als geheel brengen al deze overwegingen mij tot de volgende wens: dat het recht en juristen Internet de ruimte geven om te experimenteren en om in de praktijk te ontdekken waar Internet maatschappelijke meerwaarde heeft en waar het leidt tot maatschappelijke schade. Daarom zou het, wat mij betreft, voor-

Iopig moeten blijven bij het principe dat wat in de gewone wereld verboden is, ook verboden is op Internet. Uitzonderingen op dit principe s.v.p. uitsluitend als de praktijk – en niet allerlei veronderstellingen of opgewonden verhalen – onomstotelijk uitwijst dat er moet worden ingegrepen door de overheid, al dan niet met juridische middelen. Dus wèl de vinger aan de pols, wèl ervaring opdoen en wèl kennis opbouwen, maar qua nieuwe wet- en regelgeving zeer veel terughoudendheid.

Internet is een nieuw sociaal systeem dat in veel opzichten wezenlijk anders zal zijn dan de sociale systemen die wij nu (menen te) kennen. De echte potentie van Internet kan daarom alleen maar worden ontdekt als het voldoende speelruimte krijgt om zich verder te ontwikkelen. En dat is niet het geval als het nieuwe direct aan banden wordt gelegd zodra dat nieuwe lijkt af te wijken van oude concepten, principes of regels. Vandaar mijn pleidooi om niet te streven naar beheersing van alles wat anders is aan Internet, maar te accepteren dat het maatschappelijk productief kan zijn de verwarring of de betekenis(sen) van Internet nog maar even te laten voortbestaan.

Daarom ben ik een tevreden mens als ik bereikt heb dat u – aangekomen bij het einde van deze verhandeling – wat minder in verwarring verkeert over uw verwarring over Internet.

DEEL II

INTERNATIONAAL PRIVAATRECHT: VANGNET VOOR HET INTERNET

preadvies Maurice V. Polak

INHOUD DEEL II

I.	INLEIDING	63
II.	DRIE INTERNET-CASUS	65
III.	DE INVLOED VAN HET PUBLIEKRECHT	67
IV.	JURISDICTIE: VOLKENRECHTELIJKE UITGANGSPUNTEN	69
V.	EENVORMIG PRIVAATRECHT: LEX EN JUDEX INTERNET?	72
VI.	HET IPR ALS NOODZAKELIJK KWAAD?	78
VII.	HET TOEPASSELIJKE RECHT	81
	A. Overeenkomst	81
	B. Onrechtmatige daad	89
	C. Intellectuele en industriële eigendom en ongeoorloofde mededinging	99
VIII.	DE BEVOEGDE RECHTER	105
IX.	DE ERKENNING EN TENUITVOERLEGGING	112
X.	SAMENVATTING EN CONCLUSIE	115

Het manuscript voor dit preadvies is afgesloten op 1 december 1997.

Graag wil ik mijn dank betuigen aan mr. C.G. Kamla Besançon en mr. Myrthe M. Stolp voor hun hulp bij het verzamelen van materiaal ten behoeve van dit preadvies. Het E.M. Meijers Instituut voor Rechtswetenschappelijk Onderzoek van de Rijksuniversiteit Leiden ben ik erkentelijk voor de gastvrijheid die mij in het najaar van 1997 werd geboden.

Ik draag dit preadvies op aan mijn vader, mr. J.M. Polak, preadviseur voor de NJV in 1969 en 1979 en voorzitter van de NJV in 1986-1987, ter gelegenheid van zijn vijfenzeventigste verjaardag op 27 december 1997.

Deel II

*Men moet geen oude schoenen weggooien
voor men nieuwe heeft.*

I. INLEIDING

1. NJV en IPR: geen afkortingen die vaak met elkaar in verband worden gebracht. In de loop van haar 128-jarig bestaan heeft de Nederlandse Juristen-Vereniging slechts driemaal een onderwerp van internationaal privaatrecht centraal gesteld.¹ Bovendien: wat de NJV aan IPR doet, lijkt steeds specialistischer te worden. Mochten I. Kisch en W. Blackstone in 1947 nog preadviseren over de wenselijkheid van codificatie van het IPR,² J.G. Sauveplanne en J.E.J.Th. Deelen moesten zich in 1971 al beperken tot de internationale echtscheiding,³ terwijl het IPR anno 1998 slechts deel uitmaakt van een kwartet preadviezen over – kort gezegd – het Internet.

Is het IPR dan toch eerder mandarijnenwetenschap dan een basisvak?⁴ Of moet de geringe belangstelling van de NJV voor het IPR anderszins worden verklaard? Hoe het zij, de keuze van het bestuur van de NJV om bij de beraadslagingen over de juridische aspecten van het Internet aandacht te besteden aan het IPR, lijkt mij terecht. Immers, zoals ik in het – conform de instructie van het bestuur tot circa 50 bladzijden beperkte – bestek van mijn preadvies hoop aan te tonen, het Internet werpt voor privaatrecht

1. Zie J.H.A. Lokin en G.J.H. Jansen, Tussen droom en daad. De Nederlandse Juristen-Vereniging 1870-1995 (1995) p. 249-268.
2. I. Kisch en W. Blackstone, In hoeverre behoeven de bepalingen onzer Wetgeving rakende het internationaal privaatrecht wijziging of aanvulling?, Hand. NJV 77 (1947) deel 1, p. 3-44 en 45-85.
3. J.G. Sauveplanne en J.E.J.Th. Deelen, Internationaal privaatrechtelijke vraagstukken met betrekking tot de echtscheiding; Internationale echtscheiding, Hand. NJV 101 (1971) deel 1, eerste stuk, p. 3-51 en 53-115.
4. Zie, over deze vraagstelling, L.F.A. Steffens, IPR een basisvak of mandarijnenwetenschap? Verslag van Symposium 11 oktober 1994 te Den Haag, NJB 69 (1994) p. 1531-1532.

rechtelijk georiënteerde juristen eerst en vooral vragen van IPR op.

2. Welke vragen van IPR werpt het Internet op? Eigenlijk alle, dat wil zeggen de drie klassieke vragen van IPR:

(i) Welk recht – supranationaal eenvormig privaatrecht dan wel een of meer nationale stelsels van privaatrecht – beheerst een privaatrechtelijke Internet-verhouding: de kwestie van *het toepasselijke recht*.

(ii) Welke rechter is bevoegd – heeft internationale rechtsmacht – om van een privaatrechtelijk Internet-geschil kennis te nemen: de materie van *de bevoegde rechter*.

(iii) Welke betekenis heeft een rechterlijke uitspraak in een Internet-geschil in een andere rechtsorde: het onderwerp van *de erkenning en tenuitvoerlegging*.

3. Deze drie vragen komen hierna aan bod (in de hoofdstukken VII, VIII en IX), maar voordat ik daaraan toekom, wil ik enkele andere kwesties aansnijden en afdoen.

Om de gedachten te bepalen schets ik eerst (in hoofdstuk II) drie levensechte privaatrechtelijke Internet-casus, die ik in het vervolg van mijn betoog geregeld laat terugkeren.

Vervolgens besteed ik in een intermezzo (in hoofdstuk III) aandacht aan de invloed van het publiekrecht op de hier centraal staande privaatrechtelijke materie.

Daarna probeer ik de eerder geschetste casus op te lossen, hetgeen mij ertoe dwingt de betekenis van diverse niveaus bestaande of nog te vervaardigen regelgeving te onderzoeken: van het volkenrecht (hoofdstuk IV), via het eenvormig privaatrecht (hoofdstuk V) naar het IPR (hoofdstuk VI).

Aangezien ik tot de conclusie kom dat alleen het IPR thans voldoende houvast biedt om de Internet-casus op te lossen, keer ik terug naar het onderscheid tussen de drie reeds genoemde onderwerpen, te weten het toepasselijke recht (hoofdstuk VII), de bevoegde rechter (hoofdstuk VIII) en de erkenning en tenuitvoerlegging (hoofdstuk IX).

Ik rond mijn betoog af met een samenvatting en een conclusie (hoofdstuk X).

4. De centrale vraagstelling in mijn preadvies luidt: is het bestaande IPR in staat om privaatrechtelijke Internet-problemen op te vangen of zijn er geschiktere alternatieven voorhanden? Mijn betoog mondt uit in de conclusie dat zich geen bruikbare alternatieven aandienen, maar dat Internet-problemen met behulp van het bestaande IPR, dat hier en daar wel wijziging of aanvulling behoeft, kunnen worden opgevangen. Vandaar de titel van mijn preadvies: 'Internationaal privaatrecht: vangnet voor het Internet'.

II. DRIE INTERNET-CASUS

5. Fanatieke adepten van het Internet willen nog wel eens beweren dat Cyberspace een wereld op zichzelf is, waarbinnen geen behoefte bestaat aan rechtsregels: het Internet als digitaal Utopia zonder regelneven.⁵ De weerlegging van deze opvatting – alsmede van andere even onhoudbare standpunten die in het verleden zijn gehuldigd ten aanzien van andere vermeende 'rechtsvacua', zoals de volle zee, het luchtruim, de maan en (weer iets dichterbij huis) de leefomgeving van godsdienstige sekten – moet natuurlijk luiden dat het recht en zijn beoefenaars zich niet ongevraagd opdringen zolang er geen rechtens relevante belangen knel raken, maar dat burgers, ondernemingen en overheden 'rechtsbescherming' behoeven zodra hun te respecteren belangen op het spel staan. Anders gezegd: wie zich binnen een door hemzelf gecreëerde wereld behoorlijk gedraagt, gaat rechtens vrijuit; maar wie zich in zijn virtuele wereld misdraagt en daardoor in de reële wereld schade berokkent aan (andere) rechtssubjecten, zal zich in die reële wereld moeten verantwoorden voor het recht en de rechter.

6. Het gaat ons – juristen – dus om Internet-gedragingen die tot rechtens relevante gevolgen in de reële wereld (kunnen) leiden. Lezers van dit preadvies – privatisten – gaat het uiteraard in het bijzonder om privaatrechtelijk gekleurde gevolgen. Bij de

5. A.F.M. Brenninkmeijer, Recht op de elektronische snelweg. Ten geleide bij Speciaal nummer gewijd aan Recht op de elektronische snelweg, NJB 71 (1996) p. 1697: 'Voor sommige wetenschappen heeft de anarchie van Internet veel aantrekkingskracht op auteurs'.

bepaling van onze gedachten over dergelijke gedragingen en gevolgen kunnen de volgende drie, niet willekeurig gekozen Internet-casus wellicht behulpzaam zijn.

Casus A

Burger B, woonachtig in Rotterdam, raadpleegt via het Internet een catalogus van Onderneming O, gevestigd in het land Occidentie, en bestelt – eveneens via het Internet – een partij boeken. In de via het Internet gesloten overeenkomst is bepaald dat de boeken per post van Occidentie naar Rotterdam zullen worden verstuurd, zodra Burger B met behulp van zijn creditcard heeft betaald. Na enige tijd constateert Burger B dat zijn creditcard is gedebiteerd voor het overeengekomen bedrag, maar dat hij de bestelde boeken niet heeft ontvangen. Onderneming O houdt bij hoog en bij laag vol de boeken te hebben verzonden en weigert aansprakelijkheid voor het verlies daarvan te aanvaarden. Nadere bestudering van de overeenkomst leert Burger B dat onderneming O zich vergaand heeft vrijgetkend voor dergelijke aansprakelijkheid en dat geschillen hieromtrent naar Occidentisch recht en ten overstaan van de Occidentische rechter dienen te worden beslecht. Burger B vraagt zich af hoe en waar hij zijn recht moet halen.

Casus B

Stichting S, gevestigd in Amsterdam, is actief op het terrein van de mensenrechten. Op haar via het Internet toegankelijke homepage publiceert Stichting S regelmatig geactualiseerde rapportages van schendingen van mensenrechten. Zo wordt ook de situatie in het land Satania uitvoerig belicht. Stichting S beticht de autoriteiten in Satania onder meer van ‘martelingen, corruptie, racisme en fascistisch gedrag’. De overheid van Satania, die meent dat de beschuldigingen kant noch wal raken, wil van deze smet op haar blazoën af en onderzoekt hoe zij Stichting S kan doen gelasten de homepage te rectificeren.

Casus C

Maatschappij M, gevestigd in het land Barbarije, biedt via het Internet beroemde speelfilms aan. In alle landen van de wereld kunnen Internet-gebruikers deze speelfilms tegen betaling via het Internet downloaden in hun eigen computers en daarna op ieder gewenst moment afspelen. Een van de speelfilms is geproduceerd door Filmbedrijf F, gevestigd in het land Fantasia. Filmbedrijf F wordt in een groot aantal landen, waaronder Nederland, nog steeds als auteursrechthebbende ten aanzien van de betrokken speelfilm beschouwd, maar in Barbarije is de beschermingstermijn verstreken. Filmbedrijf F heeft nimmer toestemming gegeven voor de exploitatie van de speelfilm door Maatschappij M en zou daaraan een einde willen maken in alle landen waar het nog als rechthebbende wordt beschouwd.

7. Zoals gezegd, betreft het hier drie niet willekeurig gekozen voorbeelden van Internet-gedragingen die tot rechtens relevante en privaatrechtelijk gekleurde gevolgen in de reële wereld (kunnen) leiden.

De gemeenschappelijke elementen in de drie casus zijn: (i) het Internet is het instrument waarmee de gedragingen worden verricht, (ii) de gedragingen (kunnen) leiden tot privaatrechtelijk relevante gevolgen en (iii) de gedragingen kennen een grensoverschrijdend karakter, waardoor de in hoofdstuk I opgesomde vragen van IPR (kunnen) rijzen.

Het onderscheidende element betreft het terrein binnen het privaatrecht waarop elke casus ziet. Casus A betreft de overeenkomst, casus B de onrechtmatige daad en casus C de intellectuele en industriële eigendom en de ongeoorloofde mededinging.

De drie casus keren hierna nog regelmatig terug, maar eerst las ik een intermezzo in over de invloed van het publiekrecht op de hier aangesneden materie van privaatrecht.

III. DE INVLOED VAN HET PUBLIEKRECHT

8. Gegeven de beperkte omvang van mijn preadvies voel ik mij vrij om het belang van het publiekrecht voor het hier te bespreken onderwerp van privaatrecht in dit hoofdstuk hooguit

aan te stippen en er in het vervolg van mijn betoog grotendeels aan voorbij te gaan.

9. Het Internet is een communicatiemiddel en draagt derhalve bij aan de fundamentele vrijheid die art. 19 van de Universele Verklaring van de Rechten van de Mens⁶ – in Internet-terminen *avant la lettre!* – omschrijft als ‘de vrijheid om zonder inmenging een mening te koesteren en om door alle middelen en ongeacht grenzen inlichtingen en denkbeelden op te sporen, te ontvangen en door te geven’. Kan de vrijheid van meningsvorming wellicht nog gedijen in een Internet-loze wereld, het opsporen, ontvangen en doorgeven van inlichtingen en denkbeelden – korter gezegd: meningsuiting en informatievergaring – zijn rechtstreeks gebaat bij een zo vrij mogelijk Internet-verkeer.

De in vele verdragen, grondwetten en andere juridisch relevante instrumenten verankerde vrijheid van meningsuiting en vrijheid van informatievergaring zijn in de eerste plaats van belang voor de rol van de overheid – op nationaal niveau en in internationaal dan wel supranationaal verband – ten aanzien van het gebruik van het Internet door burgers en ondernemingen. De potentieel mensenrechtelijke dimensie van Internet-communicatie indiceert terughoudendheid bij overheidsinterventie. Medepreadviseur Buruma schrijft er uitgebreider over.

De zo-even genoemde mensenrechtelijke dimensie van Internet-gebruik kleurt daarnaast de privaatrechtelijke Internet-verhoudingen tussen burgers en ondernemingen onderling. Te denken valt aan de grenzen die de vrijheid van meningsuiting en de vrijheid van informatievergaring stellen aan contractuele beperkingen van Internet-gebruik, aan delictuele aansprakelijkheid voor Internet-uitingen en aan auteursrechtelijke bescherming van werken die via het Internet worden verspreid. Laatstgenoemd onderwerp komt bij medepreadviseur Hugenholtz nader aan bod.

6. Universele Verklaring van de Rechten van de Mens, Resolutie 217 A (III) van de Algemene Vergadering der Verenigde Naties, New York, 10 december 1948, Trb. 1969, 99.

10. Zonder iets te willen afdingen op het belang van de hiervoor genoemde vrijheid van meningsuiting en vrijheid van informatievergaring – in het algemeen dan wel voor het privaatrecht in het bijzonder – kan ik, gegeven de opdracht van het NJV-bestuur om mij tot het IPR te beperken, deze vrijheden in mijn verdere betoog als ‘vaste gegevens’ buiten haakjes plaatsen. Immers, het IPR tracht – onder meer – te bepalen welk privaatrechtelijk stelsel wordt geroepen een Internet-verhouding te reguleren en aanvaardt daarbij tot op zekere hoogte dat de verschillende in aanmerking komende stelsels een uiteenlopend mensenrechtelijk beschermingsniveau kennen. Ik geef onmiddellijk toe dat het hedendaagse IPR erkent dat bij de keuze, in casus B, tussen het onrechtmatigedaadsrecht van Nederland en dat van Satania mede betekenis toekomt aan hun respectieve mensenrechtelijke gehalte – iets wat in onderdeel B van hoofdstuk VII aan de orde komt. Dit neemt niet weg dat het IPR zich, *ook in dit voorbeeld*, uitsluitend ten doel stelt een keuze te maken tussen het recht van Nederland en dat van Satania en niet erop uit is de mensenrechtelijke situatie in beide landen te beïnvloeden. Anders gezegd: het is niet de *methode* van het IPR – de inmiddels wel definitief afgelegde ‘blinddoek van von Savigny’⁷ – waardoor de vrijheid van meningsuiting en de vrijheid van informatievergaring grotendeels buiten mijn gezichtsveld vallen, maar de *functie* van het IPR – kortom de wijsheid: ‘Schoenmaker, blijf bij je leest!’.

IV. JURISDICTIE: VOLKENRECHTELIJKE UITGANGSPUNTEN

11. Het Internet is geen digitaal Utopia dat zich kan onttrekken aan de regelneven van de reële wereld, althans indien en voor zover rechtens relevante gevolgen in het geding zijn – aldus luidde mijn weinig gewaagde stelling in § 5. Interessanter en relevanter is de vervolgvraag: welke rechtsorde in de reële wereld is dan gerechtigd om het Internet (privaatrechtelijk) te re-

7. Zie, voor deze beeldspraak, J.E.J.Th. Deelen, *De blinddoek van von Savigny* (inaugurele rede KHT 1986) (= J.H.M. van Erp c.a. red., *Audienda Verba*. Een selectie uit het werk van Prof. mr. J.E.J.Th. Deelen aangeboden door diens oud-leerlingen, collega's en vrienden ter gelegenheid van zijn afscheid als hoogleraar aan de Katholieke Universiteit Brabant (1989) p. 64-82).

guleren? Gegeven het bestaan van circa 200 soevereine Staten, elk voorzien van een stelsel van privaatrecht en een systeem van privaatrechtelijke rechtspleging, enerzijds en het grensoverschrijdende karakter van het medium Internet anderzijds, rijst hier primair een vraag van rechtsmacht ofwel jurisdictie. Deze vraag luidt: hoe ver reikt de jurisdictie van een Staat ten aanzien van gedragingen die met behulp van het Internet plaatsvinden en – dus – geheel of gedeeltelijk buiten het grondgebied van de betrokken Staat zijn gelokaliseerd?

12. De jurisdictie van soevereine Staten wordt bepaald door het internationaal publiekrecht ofwel volkenrecht. Het is aan het volkenrecht om aan te geven hoever de macht van iedere Staat reikt.

Bestudering van het volkenrecht werpt helaas weinig licht op de zaak. Het volkenrecht blijkt tot op heden niet in staat om de grenzen van de jurisdictie van soevereine Staten duidelijk te definiëren. Reeds in 1927 vond het Permanente Hof van Internationale Justitie weinig houvast:

'Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable.'⁸

Het moderne volkenrecht komt helaas niet veel verder en slaagt er hooguit in om enige terminologische en dogmatische spraakverwarring uit de weg te ruimen. Zo onderscheidt het volkenrecht wetgevende ('legislative' of 'prescriptive'), rechtsprekende ('judicial' of 'adjudicatory') en uitvoerende ('executive' of 'enforcement') jurisdictie, zulks in navolging van en voortbouwende op de bekende driedeling van de staatsmacht. Vervolgens wordt onderscheid gemaakt tussen deze drie vormen van jurisdictie naar gelang het strafrechtelijke, bestuursrechtelijke of privaatrechtelijke materie betreft. Aldus ontstaat een gedifferenti-

8. Permanente Hof van Internationale Justitie 7 september 1927 (The case of the S.S. 'Lotus'), PCIJ Series A, nr. 10.

eerd stelsel, waarbij de jurisdictie van een Staat varieert, zowel naar staatsmacht als naar rechtsgebied.⁹

13. In privaatrechtelijke aangelegenheden, die hier centraal staan, laat het volkenrecht de Staten een grote mate van vrijheid om naar eigen goeddunken meer of minder jurisdictie uit te oefenen. De wetgevende, rechtsprekende en uitvoerende jurisdictie van een Staat is in beginsel zelfs onbeperkt. Dat wil zeggen: het volkenrecht bevat geen algemeen aanvaarde rechtsregel die een Staat verbiedt zijn privaatrecht een wereldwijde reikwijdte toe te kennen, zijn rechterlijke macht open te stellen voor ieder privaatrechtelijk geschil, waar ook ter wereld gelokaliseerd, dan wel voor zijn rechterlijke uitspraken universele gelding te claimen. Slechts ten aanzien van de uitvoerende jurisdictie erkent het volkenrecht een duidelijke beperking. Een Staat is niet bij machte om in privaatrechtelijke zaken executiemaatregelen op het grondgebied van een andere Staat te treffen. De uitvoerende jurisdictie van een Staat – hier te begrijpen als de inschakeling van het statelijk geweldsmonopolie – is derhalve beperkt tot het grondgebied van de betrokken Staat.¹⁰

14. Toegepast op de in hoofdstuk II geschetste Internet-casus brengt het vorenstaande mee dat Nederland alsmede de fictieve Staten Occidentiië, Satania, Barbarije en Fantasia niet in strijd met het volkenrecht zouden handelen als zij elk zouden bepalen dat hun privaatrecht alle geschetste grensoverschrijdende Internet-gedragingen bestrijkt, dat hun rechterlijke instanties bevoegd zijn zich over alle daaruit voortvloeiende geschillen te buigen en dat de uitspraken van deze instanties wereldwijd effect

9. Zie, in het algemeen, F.A. Mann, *The Doctrine of Jurisdiction in International Law*, Rec. des Cours 111 (1964-I) p. 9-162; I. Brownlie, *Principles of Public International Law* (4e druk 1990) p. 298-311; O. Schachter, *International Law in Theory and Practice*, Series Developments in International Law, volume 13 (1991) p. 253-257; P.H. Kooijmans, *Internationaal publiekrecht in vogelvlucht* (6e druk 1996) p. 45-46 en 62-66; P. Malanczuk, *Akehurst's Modern Introduction to International Law* (7e druk 1997) p. 109-117; I. Seidl-Hohenveldern, *Völkerrecht* (9e druk 1997) Rz. 1359-1377. Zie tevens P. Peters, *Volkenrechtelijke aspecten van extraterritoriale wetgeving* (preadvies), Med. Ned. Ver. Int'l Recht, nr. 89 (1984) p. 5-6.

10. Zie Mann, *supra* noot 9, p. 73-81; Schachter, *supra* noot 9, p. 253-257; Kooijmans, *supra* noot 9, p. 62; Malanczuk, *supra* noot 9, p. 110; Seidl-Hohenveldern, *supra* noot 9, Rz. 49, 1359-1373 en 1504-1518.

sorteren. Anderzijds is ieder van de genoemde Staten bij uitsluiting bevoegd om te bepalen in hoeverre een buitenlandse rechterlijke uitspraak voor erkenning en tenuitvoerlegging in de betrokken Staat in aanmerking komt.

15. Deze grove schets van de huidige stand van zaken in het volkenrecht moge volstaan om te concluderen dat van het volkenrecht geen concrete oplossingen voor de in hoofdstuk II geschetste Internet-casus mogen worden verwacht. Het volkenrecht vervult hier slechts een bescheiden rol, gelegen in de toedeling – helaas in weinig concrete termen – van jurisdictie in privaatrechtelijke aangelegenheden aan de Staten. Hieruit volgt dat de oplossingen voor de drie casus moeten worden gezocht in het privaatrecht dat de Staten – met inachtneming van deze ruime jurisdictie – hebben ontwikkeld. Dit privaatrecht is niet noodzakelijkerwijs het nationaal privaatrecht, aangewezen door het IPR – daarover meer in de hoofdstukken VI-IX – maar zou ook supranationaal eenvormig privaatrecht kunnen betreffen. Over dit laatste handelt hoofdstuk V.

V. EENVORMIG PRIVAATRECHT: LEX EN JUDEX INTERNET?

16. Naast de in § 5 ten tonele gevoerde groep fanaticke Internet-adepten die wil beweren dat Cyberspace een rechtsvacuüm is en moet blijven, bestaat er een groep 'realo's' die bereid is de 'juridisering' van het Internet als een onvermijdelijke ontwikkeling te aanvaarden, mits deze ontwikkeling uitmondt in een speciaal voor het Internet geschreven rechtstelsel: lex Internet. Deze lex Internet zou – zo luidt de redenering – alle personen, ondernemingen en overheden moeten binden, indien en voor zover zij zich van het Internet bedienen en aldus wereldwijde toepassing genieten.¹¹ Soms wordt in één adem gepleit voor de oprichting van speciale rechterlijke of quasi-rechterlijke instanties – bij voorkeur toegankelijk en rechtsprekend via het Internet –

11. Zie bijv. C.E. Drion en J.J. Linnemann, Aansprakelijkheidskwesties en andere uitdagingen van het Internet aan de nationale rechtsorde, NJB 71 (1996) p. 1740 (Speciaal nummer gewijd aan Recht op de elektronische snelweg); M.R. Burnstein, Conflicts on the Net: Choice of Law in Transnational Cyberspace, Vanderbilt J. Transnational L. 29 (1996) p. 108-110.

die bij uitsluiting bevoegd zouden moeten zijn om Internet-geschillen te beslechten, zulks aan de hand van de *lex Internet*.¹² De lege *Internet curat judex Internet*.

Wat te denken van dergelijke pleidooien voor een specifiek en eenvormig rechtsregime en een gespecialiseerd geschillenbeslechtsingsmechanisme? Zijn het hersenschimmen of betreft het reële voorstellen? Ik kom in het midden uit.

17. Ik begin bij de premisse die aan ieder voorstel voor een *lex* en een *judex Internet* ten grondslag ligt. Deze vaak onuitgesproken premisse luidt – zo neem ik aan – dat het bestaande privaatrecht en de gangbare privaatrechtelijke rechtspleging wezenlijk tekort schieten zodra zich een Internet-probleem voordoet. Anders gezegd: met het juridisch instrumentarium dat thans voorhanden is, kan de jurist in Cyberspace onvoldoende uit de voeten. Van wijziging of aanvulling van het bestaande instrumentarium valt blijkbaar onvoldoende heil te verwachten, slechts de totstandkoming van een *lex* en een *judex Internet* biedt soelaas.

Is zoveel somberheid over het huidige privaatrecht en de bestaande privaatrechtspleging terecht? Ik waag dat te betwijfelen. Ongetwijfeld roept het Internet problemen op waarvoor ons vermogensrecht en onze rechterlijke instanties niet rechtstreeks en meteen adequate voorzieningen kennen. Ik denk dan met name aan het terrein van het auteursrecht, waarover medepreadviseur Hugenholtz schrijft. Het Internet – als exponent van de digitalisering van informatie – lijkt grote delen van het traditionele auteursrecht in de kern aan te tasten.¹³ Op andere terreinen van het privaatrecht ligt de situatie mijns inziens anders. Contractuele relaties en delictuele verhoudingen die via het Internet tot stand komen, vragen niet om een radicaal ander verbintenissenrecht dan thans in Boek 6 van het Burgerlijk Wetboek is te vinden. En evenmin zie ik in waarom de Nederlandse overheids-

12. Zie bijv. Drion en Linnemann, *supra* noot 11, p. 1740. K. Benyekhlef, *Dematerialized Transactions on Electronic Pathways: A Panorama of Legal Issues*, in F. Mackaay e.a. eds., *The Electronic Superhighway. The Shape of Technology and Law to Come* (1995) p. 115, pleit zelfs voor 'a sort of network ombudsman ... to decide electronic conflicts'.

13. Zie, in het algemeen, E.J. Dommering, *Het auteursrecht spoelt weg door het elektronisch vergiet. Enige gedachten over de naderende crisis van het auteursrecht*, *Computerrecht* 10 (1994) p. 109-113.

rechter niet in staat zou zijn dit verbintenissenrecht op Internet-geschillen toe te passen. De roep om een lex en een judex Internet ter vervanging van het huidige privaatrecht en de bestaande privaatrechtspleging lijkt mij dan ook te zwaar aangezet. En in ieder geval rust de bewijslast voor het tekortschieten van ons privaatrecht en onze privaatrechtelijke rechtspleging op de voorstanders van een lex en een judex Internet. Reeds daarom – en vanwege de omvang die dit preadvies mag hebben – ligt het niet op mijn weg om de Internet-compatibiliteiten en incompatibiliteiten van ons burgerlijk recht en burgerlijk procesrecht hier uit te meten.

Terug naar de premisse. Moeten de voorstellen voor een lex en een judex Internet misschien anders worden geduid? Luidt de premisse soms dat het vrij verkeer op het Internet niet kan gedijen in een wereld van rechtsverscheidenheid en versnippering van rechtsbedeling? Het is dan niet zozeer de (on)geschiktheid van het Nederlandse privaatrecht of de Nederlandse rechtspleging die tot verandering noopt, maar veeleer de rechtsonzekerheid en inefficiëntie waartoe het naast elkaar bestaan van circa 200 stelsels van privaatrecht en privaatrechtelijke rechtspleging in onze huidige wereld leidt. Lex en judex Internet, niet omwille van de modificatie, maar omwille van de unificatie.

Aldus begrepen lijkt de idee van een lex en een judex Internet iets beter te verdedigen. Unificatie van privaatrecht en van privaatrechtelijke rechtspleging ten behoeve van een vrij Internet-verkeer is immers een loffelijk streven? Niettemin rijst voor mij de vraag waarom de unificatie dan tot het Internet beperkt zou blijven. Geldt voor het Internet iets anders dan voor de traditionelere instrumenten van het grensoverschrijdende verkeer: auto, schip, vliegtuig, telefoon, radio en televisie? Zouden wij nu opeens ten behoeve van het Internet-verkeer het privaatrecht moeten unificeren, terwijl de oudere communicatiemiddelen tot op heden in een wereld van rechtsverscheidenheid hebben gedijd? Internet-deskundigen zullen wellicht riposteren dat de grensoverschrijdende communicatie met behulp van het Internet oneindig veel omvangrijker is dan dergelijke communicatie met behulp van de pre-Internet media. Daarop zou ik slechts willen reageren met de vraag of deze reusachtige schaalvergroting zich ook uit – naar het zich nu laat aanzien – in een forse groei van het aantal grensoverschrijdende geschillen. Anders ge-

zegd: ondervindt het Internet, meer dan de traditionele communicatiemiddelen, nadeel van de rechtsverscheidenheid die het gevolg is van het ontbreken van eenvormig privaatrecht? Ook hier rust de bewijslast op de voorstanders van een lex en een judex Internet.

18. Aangenomen dat de roep om een lex en een judex Internet op een deugdelijke premisse berust, doemt het probleem van de haalbaarheid op. Is het reëel te streven naar eenmaking van privaatrecht ten behoeve van het Internet en naar de oprichting van een forum voor Internet-geschillen?

Voorstanders van unificatie van privaatrecht moeten opboksen tegen sceptici die met legio voorbeelden van faliekante mislukkingen het utopisch karakter van het eenvormig privaatrecht willen aantonen. Anderzijds kunnen de voorstanders op diverse terreinen van het privaatrecht succes claimen. Ik wil niet proberen hier de balans en de winst- en verliesrekening op te maken. Evenmin waag ik mij aan een – te snel verouderend – overzicht van de eerste resultaten die op het terrein van lex en judex Internet zijn bereikt.¹⁴ I liever beperk ik mij tot drie wenken voor de uitvoerders van de (verdere) unificatie op dit terrein.

De geschiedenis van de rechtsunificatie leert dat het verstandig is om te beginnen met de eenmaking van terreinen die in rechtspolitieke zin als 'neutraal' zijn aan te merken. Als vuistregel geldt: hoe geringer de invloed van levensbeschouwelijke, religieuze, culturele en sociaal-economische overwegingen, des te beter zijn de vooruitzichten op unificatie. Regels van privaatrecht lenen zich dan ook eerder voor unificatie dan regels van publiekrecht; binnen het privaatrecht laat het verbintenissenrecht zich gemakkelijker unificeren dan het personen- en familierecht. In termen van het Internet betekent dit dat het werk aan een lex Internet bij voorkeur dient te beginnen bij het verbintenissenrecht, in het bijzonder bij de regels over de totstandkoming van overeenkomsten die via het Internet worden gesloten. Regels over de wijze van totstandkoming van contractuele relaties zijn immers tot op grote hoogte rechtspolitiek 'neu-

14. Een belangrijke modelregeling lijkt te zijn de UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 (uitgave van de United Nations, New York, 1997).

traal'. Vervolgens zou kunnen worden gewerkt aan speciale regels ter bescherming van consumenten die met behulp van het Internet contractuele relaties aangaan. Hier is al iets meer sprake van rechtspolitieke gevoeligheid. Nog een graad gevoeliger ligt het terrein van de delictuele aansprakelijkheid voor uitingen via het Internet, gegeven de in hoofdstuk III genoemde invloed van de vrijheid van meningsuiting. Minstens even moeilijk lijkt de eenmaking van het auteursrecht, niet alleen vanwege de zo-even genoemde publiekrechtelijke dimensie, maar ook door de grote invloed van belangenorganisaties. De recente, voor een belangrijk deel mislukte poging van de WIPO om het auteursrecht aan te passen aan de eisen van het digitale tijdperk, toont dit aan.¹⁵

De tweede wenk behelst het advies om niet aanstonds volledig nieuwe regels te ontwerpen, maar eerst te bezien of uitbreiding van bestaand eenvormig privaatrecht tot het Internet soelaas biedt. Zo laat zich denken dat voor de wijze van totstandkoming van overeenkomsten met behulp van het Internet een bestaand supranationaal rechtsregime van toepassing wordt verklaard. Anderzijds lijkt het weinig zinvol om te volstaan met een ogenschijnlijk eenvoudig declaratoir als de Agreed Statement behorende bij art. 1 lid 4 van het recente WIPO-Auteursrechtverdrag, luidende:

'The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. [...]'¹⁶

15. Zie E.J. Arkenbout, Nieuwe verdragen over auteursrecht en naburige rechten, *Informatierecht/AMI* 21 (1997) p. 67-73; F.W. Grosheide, Enkele kanttekeningen bij het WIPO Copyright Treaty 1996, *Informatierecht/AMI* 21 (1997) p. 74-78; P.B. Hugenholtz, De WIPO-verdragen: Ongeregeld goed, *Informatierecht/AMI* 21 (1997) p. 79-83. Ook in de Brief inzake 'Nieuw verdrag auteursrecht', d.d. 21 januari 1997, Kamerstukken II, 1996-1997, 25 154, nr. 3, p. 4, geeft de Minister van Justitie toe dat de conclusie 'dat de [WIPO]-conferentie een evenwichtig resultaat heeft bereikt', tot de gevolgtrekking leidt: 'Voor Nederland zullen wijzigingen die voortvloeien uit de verdragen beperkt blijven'.

16. Agreed Statements concerning the WIPO Copyright Treaty, adopted by the Diplomatic Conference, Genève, 20 december 1996, WIPO-document CRNR/DC/96, 23 december 1996, *Informatierecht/AMI* 21 (1997) bijlage bij nr. 4, p. 7 (Agreed Statements niet opgenomen in Trb. 1997, 318).

Een dergelijk declaratoir roept meer vragen op dan het beantwoordt.

Ten slotte lijkt het aanbevelenswaardig om voorlopig niet te streven naar een *lex Internet* en/of een *judex Internet* met exclusieve werking ten opzichte van het bestaande nationaal privaatrecht en de gangbare nationale geschillenbeslechtsmechanismen. Meer heil valt te verwachten van een model-*lex Internet*, waaraan partijen zich vrijwillig kunnen onderwerpen, en van een optioneel *Internet-forum*. *Lex* en *judex Internet* zouden dan naast en niet in de plaats van het nationaal privaatrecht en de nationale rechtspleging treden. Zolang het ons – juristen – aan voldoende inzicht in alle juridische aspecten van het *Internet* ontbreekt, is een bescheiden geldingspretentie van een nieuwe *lex* en *judex Internet* raadzaam. Bovendien leert de ervaring opgedaan met het bestaande supranationaal eenvormig privaatrecht en met de bestaande alternatieve geschillenbeslechtsmechanismen dat veel justitiabelen, inclusief ondernemingen, de voorkeur geven aan nationaal privaatrecht boven supranationaal eenvormig privaatrecht en aan nationale overheidsrechtspraak boven a-nationale, particuliere rechtspraak.

19. *Lex* en *judex Internet*: hersenschimmen of reële voorstellen? Zoals aangekondigd, kom ik in het midden uit. Als het bestaande recht en de bestaande rechtspleging ernstige *Internet-incompatibiliteiten* zouden vertonen dan wel het vrije *Internet-verkeer* serieuze hinder zou ondervinden van de huidige rechtsverscheidenheid, dan zou een voorzichtige en bescheiden poging kunnen worden ondernomen om tot een alternatieve, supranationale *lex Internet* en een additioneel, a-nationaal *Internet-forum* te komen.

Het vorenstaande impliceert dat het nationaal privaatrecht en de nationale overheidsrechtspraak noodgedwongen hun betekenis voor de regulering van *Internet-verhoudingen* en geschillen behouden, en wel zolang én voor zover zich geen algemeen aanvaarde *lex* en *judex Internet* aandienen. Deze constatering brengt mij terug bij de reeds in hoofdstuk I gestelde vragen van IPR: om welk nationaal privaatrecht en om welk nationaal stelsel

van privaatrechtspleging gaat het dan? Over deze vragen handelen de hoofdstukken VI tot en met IX.

VI. HET IPR ALS NOODZAKELIJK KWAAD?

20. Aan het adres van beoefenaars van het IPR worden regelmatig twee verwijten gericht. Het eerste verwijt luidt dat deze discipline een even kunstzinnige als kunstmatige oplossing van reële casus oplevert. Immers, het IPR reikt geen inhoudelijke beslissing van het grensoverschrijdende geval aan, maar bewerkstelligt slechts een toedeling van dit geval aan een nationaal stelsel van privaatrecht en privaatrechtspleging. En – aldus het tweede, nog ernstigere verwijt – deze toedeling geschiedt ook nog eens met behulp van IPR-regels die in beginsel in iedere Staat anders in elkaar steken. ‘Is dat alles wat het IPR te bieden heeft?’, zo klinkt het smalend.

Mijn reactie op het eerste verwijt luidt dat van het IPR – ingeklemd als het zit tussen het volkenrecht enerzijds en het nationaal privaatrecht anderzijds – helaas niet meer kan worden verwacht dan enige ‘coördinatie van chaos’ in het grensoverschrijdende verkeer. Waar het volkenrecht de Staten een grote mate van vrijheid gunt om hun privaatrecht en privaatrechtspleging naar goeddunken in te richten en de Staten slechts in bescheiden mate tot eenmaking van privaatrecht en rechtsbedeling zijn overgegaan, is het IPR een noodzakelijk kwaad om enige orde te scheppen in de rechtsverscheidenheid die beide andere rechtsgebieden in het leven roepen. Het IPR kan de huidige rechtsverscheidenheid niet worden verweten; integendeel, het IPR probeert er het beste van te maken.

Het tweede verwijt tracht ik te ontzenuwen door uit te leggen dat mét de (in hoofdstuk IV besproken) wijde marges die het volkenrecht de Staten laat om hun privaatrecht en privaatrechtspleging striktere of ruimere grensoverschrijdende reikwijdte toe te kennen, onontkoombaar is dat het IPR zelf ook binnen de jurisdictie van de Staten valt en onderdeel is (niet van het per definitie eenvormige volkenrecht, maar) van het nationaal (privaat)recht, met als gevolg dat het (evenals het nationaal privaatrecht) door en voor iedere Staat naar eigen smaak wordt, althans kan worden ingericht. Kernachtiger dan S. van Brakel kan ik het niet onder woor-

den brengen: 'Internationaal privaatrecht is nationaal recht, voor internationale rechtsverhoudingen geschreven'.¹⁷

Tussenconclusie: het IPR is een noodzakelijk nationaal kwaad, dat iedere Staat nodig heeft om zijn justitiabelen houvast te bieden in een wereld van rechtsverscheidenheid. Deze tussenconclusie doet zeker opgeld op het terrein van Internet-verhoudingen en geschillen, waar supranationale eenvormige regels en rechtsbedeling ontbreken. Burger B van casus A, de overheid van Satania in casus B en Filmbedrijf F van casus C hebben – zowel in Nederland als in iedere andere Staat – het IPR nodig om te weten welk nationaal privaatrechtsstelsel bepaalt welke rechten en verplichtingen zij genieten en welke nationale stelsels van privaatrechtspleging zij kunnen en moeten inschakelen om hun recht te krijgen en te halen.

21. Deze tussenconclusie moet ik nog in één opzicht nuanceren. Al is het IPR een noodzakelijk kwaad, dat in beginsel op nationaal niveau wordt vormgegeven, er is alle reden om bij de vormgeving het doel – coördinatie van chaos in het grensoverschrijdende verkeer – voor ogen te houden. Dit doel vraagt om coördinatie van vormgeving, teneinde een zo groot mogelijke mate van internationale uniformiteit bij de totstandkoming en de toepassing van regels van IPR te garanderen. Dit keer citeer ik niet Van Brakel, maar E.M. Meijers: 'Stel Uw regels van internationaal privaatrecht zo op, dat zij ook in een wereldrecht niet misplaatst zouden zijn'.¹⁸ Meijers dacht daarbij vooral aan de nationale (Nederlandse) dan wel regionale (Benelux) wetgever die bij zijn codificerende werk rekening dient te houden met de belangen van het internationale rechtsverkeer. Inmiddels is een aanzienlijk deel van het IPR-regelgevende werk overgenomen door een handvol internationale verdragswetgevers. Deze ontwikkeling valt toe te juichen: vormgeving van IPR-regels door

17. S. van Brakel, *Grondslagen en Beginselen van Nederlands Internationaal Privaatrecht* (3e druk 1953, bewerkt door I. Kisch) p. 13 (voetmoot wegge-
laten; MVP).

18. Zie de (door E.M. Meijers voorbereide) MvT op de goedkeuringswet van het oorspronkelijke Benelux-Verdrag tot het invoeren van een eenvormige wet betreffende het internationaal privaatrecht, *Bijl. Hand. II*, 1951-1952, 2329, nr. 3, p. 5.

internationale gremia komt a priori de internationale uniformiteit ten goede.

De eerstkomende jaren zal de vormgeving van IPR-regels ten behoeve van Internet-casus voornamelijk daar geschieden waar concrete IPR-problemen moeten worden opgelost: in de rechtspraak. Daarbij zal de doctrine enige steun kunnen verlenen. Geleidelijk zal duidelijk worden of het Internet stelselmatig zulke serieuze IPR-casus opwerpt dat speciale geschreven regels van IPR nodig zijn. Eerst dan breekt de tijd aan om op supranationaal niveau – en wellicht daarop vooruitlopend én voortbouwend, in nationaal verband – tot codificatie over te gaan.¹⁹ In elk stadium zal de alsdan tot actie geroepen vormgever van het IPR – rechter, rechtsgeleerde, verdragsinstantie en nationale wetgever – zich het zo-even aangehaalde gebod van Meijers voor ogen moeten houden. IPR-regels ten behoeve van het Internet dienen in de sleutel van de internationale uniformiteit en de wereldwijde aanvaardbaarheid te zijn gezet.

22. Eindconclusie: het IPR is een noodzakelijk nationaal kwaad, ook voor de in hoofdstuk II geschetste Internet-casus, maar dit IPR dient wel een internationalistisch karakter te bezitten. Deze eindconclusie verklaart waarom ik in de volgende drie hoofdstukken onderzoek hoe het nationaal-Nederlands geaarde, maar tevens internationalistisch getinte IPR ten behoeve van Internet-casus dient te luiden. Zoals aangekondigd in § 4 toets ik daarbij het bestaande IPR op zijn bruikbaarheid voor het Internet.²⁰

19. De Haagse Conferentie voor Internationaal Privaatrecht heeft het onderwerp van 'the problems of private international law raised by electronic data interchange, and protection of privacy in connection with transfrontier data flows' op de Agenda van de Conferentie geplaatst, 'but without priority'. Zie Conférence de La Haye de droit international privé/Hague Conference on private international law, Acte final de la Dix-huitième session/Final Act of the Eighteenth Session, 's-Gravenhage, 19 oktober 1996, onderdeel B, nr. 4 aanhef en onder b. Zie tevens Note on problems which, in the area of commercial law, arise from the utilization of electronic processes, drawn up by M. Pelichet, Preliminary Document nr. 3 of April 1992, Conférence de La Haye de droit international privé/Hague Conference on private international law, Actes et documents de la Dix-septième session/Proceedings of the Seventeenth Session (1993), Tome I - Première partie/First Part, Matières diverses/Miscellaneous matters, p. 89-95.

20. Zie, voor een overzicht van het bestaande Nederlandse IPR, L. Strikwerda, Inleiding tot het Nederlandse internationaal privaatrecht (5e druk 1997); R. van Rooij & M.V. Polak, Private International Law in the →

VII. HET TOEPASSELIJKE RECHT

23. In dit hoofdstuk zoek ik het antwoord op de eerste van de in hoofdstuk I gestelde vragen van IPR, te weten: welk recht beheerst een privaatrechtelijke Internet-verhouding? In hoofdstuk V gaf ik aan dat en waarom het toepasselijke recht meestal geen supranationaal eenvormig recht, maar nationaal privaatrecht zal zijn. Gegeven de verschillen tussen de nationale privaatrechtsstelsels rijst dan onmiddellijk de vraag: welk nationaal privaatrecht? Om deze vraag te beantwoorden, moet het conflictenrecht – het geheel van zogenaamde verwijzingsregels – te hulp schieten, teneinde de voorliggende Internet-casus te verwijzen naar het meest in aanmerking komende nationaal privaatrecht. Zoals het Nederlandse materieel privaatrecht op het Internet toegesneden regels ontbeert, zo ontbreken in het Nederlandse IPR speciale Internet-verwijzingsregels. Bij mijn weten is de situatie in andere Staten op dit moment niet anders. Dat doet de (in hoofdstuk VI reeds in algemene termen opgeworpen) vraag rijzen of hier sprake is van een serieuze lacune in het IPR dan wel dat het thans bestaande conflictenrecht, met hier en daar een wijziging of aanvulling, ook Internet-verhoudingen naar het meest in aanmerking komende nationaal privaatrecht kan verwijzen. Beantwoording van deze vraag noopt uiteraard tot onderzoek van het bestaande conflictenrecht op zijn Internet-bestendig karakter. Ik verricht dat onderzoek aan de hand van de drie in hoofdstuk II geschetste casus. Zoals daar al opgemerkt, betreft het geen willekeurig gekozen casus; integendeel, zij stellen mij in staat de voor het Internet interessantste deelgebieden van het IPR te betreden en ontslaan mij van de verplichting om volledigheid na te streven.

A. Overeenkomst

24. In dit onderdeel staat casus A van hoofdstuk II centraal. Welk recht beheerst de overeenkomst die de Nederlandse Burger B via het Internet met de in Occidentieë gevestigde onderne-

→ Netherlands (1987), en Supplement (1995). Korthedshalve zie ik in de volgende hoofdstukken van verdere verwijzingen naar deze overzichtswerken af.

ming O heeft gesloten? Komt daarbij enige betekenis toe aan het contractisbeding dat het Occidentische recht van toepassing verklaart?

25. Kenners van het IPR zullen onmiddellijk naar het zogenaamde EVO – het Europees Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst van 1980²¹ – grijpen. Hier biedt zich immers een modern verdragsrechtelijk systeem van verwijzingsregels aan dat in drie opzichten ruime kaders kent:

(i) Zo bestrijkt het EVO – in materiële zin – ‘verbintenissen uit overeenkomst’ (art. 1 lid 1) en is het dus niet beperkt tot bepaalde typen overeenkomsten. De benaming – koop, huur, huurkoop, lease, licentie – is daarbij niet van belang, relevant is slechts of er sprake is van contractuele verbintenissen.

(ii) Het EVO kent – in formele zin – een zogenaamde universele reikwijdte (art. 2), hetgeen betekent dat het in de verdragsluitende Staten, waaronder Nederland, moet worden toegepast, ongeacht met welke aangesloten of niet-aangesloten Staten de voorliggende casus is verbonden. Iedere grensoverschrijdende overeenkomst die aan de Nederlandse rechter of aan een van zijn Europese collega’s wordt voorgelegd, dient via het EVO aan een toepasselijk rechtsstelsel van een aangesloten dan wel een niet-aangesloten Staat te worden gekoppeld.

(iii) Het EVO is ‘mediumneutraal’ en ‘techniekonafhankelijk’: de wijze waarop een grensoverschrijdende overeenkomst tot stand komt – mondeling of schriftelijk, ‘live’ of door de telefoon, per brief of via het Internet – is irrelevant.

Contractuele Internet-relaties laten zich aldus zonder grote moeite in het toepassingsgebied van het EVO persen. Is het gevolg – de toepassing van de EVO-verwijzingsregels op contractuele Internet-relaties – even eenvoudig? Hier doemen enige complicaties op.

21. Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst, Rome, 19 juni 1980, PB EG 23 (1980) nr. L 266, p. 1, Trb. 1980, 156.

26. Toepassing van de in art. 3 EVO verankerde rechtskeuzevrijheid op via het Internet gesloten overeenkomsten lijkt mij in beginsel weinig problematisch. De mogelijkheid dat contractspartijen zelf het op hun overeenkomst toepasselijke nationaal privaatrecht kiezen, is thans algemeen aanvaard, niet alleen in de bij het EVO aangesloten Staten, maar ook daarbuiten. Ik ga hier voorbij aan de dogmatische rechtvaardiging die voor deze IPR-partijautonomie is gevonden en volsta met de constatering dat rechtskeuze in grensoverschrijdende overeenkomsten de rechtszekerheid ten goede komt: partijen weten op voorhand welk nationaal privaatrecht hun rechten en verplichtingen beheerst. Ook voor overeenkomsten die met behulp van het Internet worden gesloten, vormt de rechtskeuzevrijheid van art. 3 een bruikbaar instrument.

27. Niettemin ontwaar ik twee problemen rond de rechtskeuzevrijheid als verwoord in art. 3 EVO. Het eerste probleem betreft het voorwerp van de rechtskeuze: het te kiezen recht (zie § 28); het tweede de subjecten die van de rechtskeuzevrijheid gebruik mogen maken: de partijen (zie § 29).

28. Het EVO is opgezet als een traditioneel conflictenrechtelijk systeem, waarbij de verdragsopstellers hebben gedacht aan de situatie dat een keuze moet worden gemaakt – in het kader van art. 3 door de contractspartijen zelf – tussen diverse nationale privaatrechtssystemen. Anders gezegd: een keuze tussen het Nederlandse BW, de Franse Cc of het Duitse BGB. De tekst spreekt immers herhaaldelijk van ‘het recht van het land waar ...’. Daarmee lijkt het EVO de contractspartijen geen ruimte te bieden om hun overeenkomst te onderwerpen aan niet-statelijk recht, zoals het supranationaal eenvormig privaatrecht.²² Deze kwestie is, althans kan te zijner tijd van belang worden voor de in hoofdstuk V besproken lex Internet. Valt de lex Internet inderdaad buiten de partijautonomie van het EVO?

Als de lex Internet is of wordt gegoten in de vorm van een verdrag of een ander juridisch instrument dat voor een Staat in

22. Zie, in het algemeen, L. Strikwerda, De overeenkomst in het IPR, *Praktijkreeks IPR*, deel 11 (1995) nr. 201-203; *losbladige Verbindingenrecht* III.1 (Vonken) art. 3 EVO, aant. 9.

werking is getreden, en derhalve deel uitmaakt van een nationale rechtsorde, dan dient zich in essentie 'recht' aan dat 'van overheidswege' is gegeven. Hier ligt de parallel met het door het EVO bestreken 'zuivere' nationaal privaatrecht voor de hand. Ik zou dan ook willen bepleiten dat contractspartijen ten aanzien van een dergelijke lex Internet een zogenaamde conflictenrechtelijke rechtskeuzevrijheid toekomt: de keuze van deze lex Internet behoeft niet verenigbaar te zijn met de dwingendrechtelijke bepalingen van een objectief toepasselijk nationaal rechtstelsel (waarover meer in § 31), maar zet dit (andersluidende) nationaal privaatrecht juist opzij. Wel zullen partijen – en de rechter die de toelaatbaarheid van een dergelijke rechtskeuze toetst – zich moeten houden aan de voorschriften over de toelaatbaarheid en het effect van een rechtskeuze die de lex Internet zelf bevat.

Als de lex Internet de vorm aanneemt van een (ontwerp)verdrag, een modelregeling of een aanbeveling en zo'n regime (nog) geen deel uitmaakt van het positieve recht van enige Staat, is er geen sprake van 'recht' dat 'van overheidswege' is gegeven. De vraag rijst of de rechtskeuzevrijheid van art. 3 EVO ook in volle omvang op zulk 'quasi-recht' ziet. Op dit punt kies ik voor terughoudendheid. Een lex Internet waaraan geen enkele Staat zich heeft gecommitteerd en die wellicht buiten iedere democratische besluitvorming om tot stand is gekomen, zou ik niet op één lijn willen stellen met nationaal privaatrecht. In het kader van art. 3 zou dit betekenen dat de contractspartijen slechts over een materieelrechtelijke rechtskeuzevrijheid beschikken: de keuze van zo'n lex Internet sorteert uitsluitend effect indien en voor zover deze verenigbaar is met de dwingendrechtelijke bepalingen van het objectief toepasselijke nationaal privaatrecht. Wie deze lex Internet wil kiezen, zit vast aan het kader van het Nederlandse BW, de Franse Cc of het Duitse BGB.

29. Een belangrijke uitzondering op de algemeen geformuleerde rechtskeuzevrijheid van art. 3 EVO is de beperking die art. 5 lid 2 EVO daarop aanbrengt in de relatie consument-professionele wederpartij. Als de consumentenovereenkomst voldoet aan enige materiële criteria (art. 5 leden 1, 4 en 5) en onder bepaalde omstandigheden tot stand is gekomen – kort gezegd: als de 'passieve' consument 'thuis' wordt benaderd door de

'agressieve' professionele wederpartij – (art. 5 lid 2), kan een rechtskeuze de consument niet de bescherming ontnemen die hem wordt geboden door de dwingendrechtelijke bepalingen van het recht van zijn gewone verblijfplaats. De ratio van deze beperking is gelegen in de beschermingsgedachte: de consument – de in sociaal-economisch opzicht zwakkere partij – wordt beschermd tegen een rechtskeuze die hem wellicht door de professionele wederpartij wordt opgedrongen, indien en voor zover de rechtskeuze tot gevolg heeft dat het beschermingsniveau van de 'leefomgeving' van de consument wordt aangetast.

Naast de nog niet beantwoorde vraag hoe art. 5 precies moet worden uitgelegd, doemt in de Internet-context de vraag op in hoeverre deze bepaling doorwerking heeft dan wel verdient in consumentenovereenkomsten die via het Internet worden gesloten. Zoals vaker in het recht kan men hier twee kanten op. Enerzijds valt te verdedigen dat de consument die gebruik weet te maken van het Internet, geen 'passieve' partij is, maar juist blijkt geeft van een grote mate van deskundigheid en zelfstandigheid, hetgeen rechtvaardigt dat hij niet in sterkere mate wordt beschermd dan een professionele partij die het Internet benut. Anderzijds is verdedigbaar dat de bescherming van art. 5 rechtstreeks of naar analogie toekomt aan de consument die via het Internet zaken doet met een professionele wederpartij. In laatstgenoemde benadering rijst de vervolgvraag in welke gevallen de consument de bescherming van art. 5 verdient: in alle gevallen en ongcacht hoe de overeenkomst precies tot stand is gekomen, uitsluitend in gevallen waarbij deze totstandkoming een van de situaties van art. 5 lid 2 evenaart of in minder gevallen?²³

Van deze alternatieven kies ik voor toepassing van art. 5 lid 2 op alle via het Internet gesloten consumentenovereenkomsten. In de eerste plaats vind ik de aan art. 5 ten grondslag liggende beschermingsgedachte te belangrijk om het Internet van het IPR-consumentenrecht te 'ontheffen'. Vervolgens is het vanuit een oogpunt van hanteerbaarheid gewenst om de toepassing van art. 5 niet afhankelijk te stellen van de huidige (= pre-Internet) of

23. Zie K.R.S.D. Boele-Woelki, Internet, consument en ipr: een verkenning, in J.M. van Buren-Dee e.a. red., Consument zonder grenzen. Opstellen aangeboden aan mr. M. van Delft-Baas ter gelegenheid van haar afscheid van het Molengraaff Instituut voor Privaatrecht, Serie Consument en recht (1996) p. 309-311.

van daarmee vergelijkbare voorwaarden rond de totstandkoming van de overeenkomst. Als uitgangspunt kan dienen dat van iedere professionele partij die haar producten, diensten of de financiering daarvan (zie art. 5 lid 1) op het Internet aanbiedt, mag worden verwacht dat zij zich op de hoogte stelt van de hoedanigheid van haar 'cliënt' en, als het een consument betreft, rekening houdt met de dwingendrechtelijke bepalingen van diens woonplaatsrecht. Dit uitgangspunt maakt het mogelijk de nodeloos complexe casuïstiek van art. 5 lid 2²⁴ te vervangen door een algemeen geformuleerd toepassingsgebied, waarbij 'iedere via het Internet gesloten overeenkomst tussen een consument en een professionele wederpartij' binnen het bereik van art. 5 lid 2 valt.

De door mij voorgestane interpretatie van art. 5 lid 2 staat op gespannen voet met de tekst van de bepaling – en dan druk ik mij voorzichtig uit. Mocht de rechtspraak zich niet vrij voelen om deze interpretatie te volgen, dan zou wijziging van art. 5 aanbeveling verdienen.

Zou men besluiten om tot wijziging van art. 5 over te gaan, dan biedt dat een mooie gelegenheid om tevens tot een betere afstemming te komen tussen deze bepaling enerzijds en de scope rules van de diverse Europese richtlijnen die beogen het materiële consumentenrecht te harmoniseren, anderzijds. Voor de Internet-consumentenovereenkomst gaat het dan met name om de afstemming tussen enerzijds art. 5 EVO en anderzijds art. 12 lid 2 van de Richtlijn verkoop op afstand, dat bepaalt:

'De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de consument de door deze richtlijn geboden bescherming niet wordt ontzegd door de keuze van het recht van een derde land als recht dat op de overeenkomst van toepassing is, wanneer er een nauwe band bestaat tussen de overeenkomst en het grondgebied van een of meer lidstaten.'²⁵

Hoe deze bepaling en de scope rules van de andere richtlijnen

24. Zie, in deze zin, C.A. Joustra, *De internationale consumentenovereenkomst* (diss. UU 1997) p. 89.

25. Richtlijn 95/7/EG van het Europees Parlement en de Raad van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten, PB EG 40 (1997) nr. L 144, p. 19.

zich tot art. 5 EVO verhouden, is niet geheel duidelijk – en dan druk ik mij opnieuw voorzichtig uit.²⁶ Om aan deze onduidelijkheid een einde te maken zou ik ervoor willen pleiten om de scope rules van de richtlijnen te schrappen en de (niet-)toepasselijkheid van het (al dan niet geharmoniseerde) consumentenrecht uitsluitend door het gewijzigde art. 5 EVO te laten bepalen.

30. Tot zover de rechtskeuzevrijheid die bij contractuele Internet-relaties een belangrijke rol speelt. Welk recht is nu van toepassing als partijen geen rechtskeuze hebben uitgebracht? Hoe moet de rechter dan tot aanknoping van de contractuele Internet-verhouding aan een nationaal privaatrechtsstelsel komen?

Opnieuw dient zich het EVO aan, op grond van de hiervoor in § 25 geschetste ruime toepassingskaders. Zijn de daarin vervatte objectieve verwijzingsregels voor overeenkomsten in het algemeen (art. 4) en voor consumentenovereenkomsten in het bijzonder (art. 5 lid 3) geschikt voor toepassing op overeenkomsten die via het Internet worden gesloten?

31. Voor 'gewone' overeenkomsten kent art. 4 EVO een driedelige verwijzingsregel. Aanknoping aan het nauwst verbonden recht staat voorop (lid 1). Deze wordt eerst geconcretiseerd met behulp van het vermoeden dat een overeenkomst het nauwst is verbonden met het land van de woon- of vestigingsplaats van de partij die de kenmerkende prestatie dient te verrichten (lid 2). Ten slotte wordt dit vermoeden weer gecorrigeerd aan de hand van 'het geheel der omstandigheden' (lid 3).

Bij overeenkomsten die via het Internet tot stand komen, zal het vermoeden van de kenmerkende prestatie alleen functioneren als tussen partijen voldoende duidelijk is (i) wie de kenmerkende prestatie verricht en (ii) waar deze partij is gevestigd. Het eerste punt zal bij veel bijzondere contractstypen – koop, huur, huurkoop, lease, licentie – weinig problemen opleveren.²⁷ Een complicatie kan zich voordoen bij overeenkomsten tussen drie of meer partijen, waarvan twee of meer elk een kenmerkende

²⁶ Zie Joustra, *supra* noot 24, p. 320-347.

²⁷ Zie, in het algemeen, losbladige Verbintenissenrecht III.1 (Vonken) art. 4 EVO, aant. 4.4.

deelprestatie verrichten. Hier zal de correctie aan de hand van het geheel der omstandigheden uitkomst moeten bieden.²⁸ De vaststelling van de vestigingsplaats van de partij die de kenmerkende prestatie verricht, zal doorgaans evenmin grote problemen opwerpen. Men mag toch aannemen dat partijen zich ook bij een via het Internet gesloten overeenkomst vergewissen van de identiteit en de vestigingsplaats van hun wederpartij(en).

32. Bij de objectieve aanknoping van de Internet-consumentenovereenkomst rijst wederom de in § 29 behandelde vraag of en, zo ja, hoe de speciale verwijzingsregel voor consumentenovereenkomsten – hier: art. 5 lid 3 EVO – moet worden toegepast. Dient een consumentenovereenkomst die via het Internet wordt gesloten, op de voet van art. 5 lid 3 steeds te worden aangeknoopt aan het recht van de gewone verblijfplaats van de consument en welke rol spelen de speciale voorwaarden met betrekking tot de totstandkoming van art. 5 lid 2 hierbij? Ik kies hier voor de benadering die ik ook in § 29 verdedigde, dat wil zeggen voor toepassing van art. 5 lid 3 op alle consumentenovereenkomsten die via het Internet worden gesloten, ongeacht of hun totstandkoming voldoet aan de voorwaarden van art. 5 lid 2.

33. Het vorenstaande leidt tot de volgende getrapte verwijzingsregel voor overeenkomsten die via het Internet tot stand komen:

- (i) De overeenkomst die via het Internet wordt gesloten, wordt beheerst door het recht dat partijen met inachtneming van art. 3 EVO hebben gekozen.
- (ii) Bij gebreke van een rechtskeuze wordt deze overeenkomst beheerst door het recht dat overeenkomstig art. 4 EVO van toepassing is.
- (iii) Bij de consumentenovereenkomst in de zin van art. 5 leden 1, 4 en 5 EVO, die via het Internet wordt gesloten, kan een rechtskeuze er niet toe leiden dat de consument de bescherming verliest die hij geniet op grond van de dwingende bepalingen van het recht van het land waar hij zijn gewone verblijfplaats

²⁸ Zie, in het algemeen, M.V. Polak, Vermogensrechtelijke meerpartijenverhoudingen, *Praktijkrechts IPR*, deel 15 (1993) nr. 88-94.

heeft, ongeacht of de overeenkomst tot stand is gekomen overeenkomstig de voorwaarden genoemd in art. 5 lid 2 EVO.

(iv) Bij gebreke van een rechtskeuze wordt deze consumentenovereenkomst beheerst door het recht van het land waar de consument zijn gewone verblijfplaats heeft, ongeacht of de overeenkomst tot stand is gekomen overeenkomstig de voorwaarden genoemd in art. 5 lid 2 EVO.

34. Ten slotte wijs ik nog op de voorschriften vervat in de art. 7 en 16 EVO. Eerstgenoemd voorschrift vormt de legitimatie voor de toepassing van zogenaamde 'voorrangsregels', laatstgenoemde bepaling biedt ruimte voor inschakeling van de 'openbare orde'. Beide verdragsvoorschriften behouden ten volle hun betekenis in de Internet-context. Helaas ontbreekt mij de ruimte om de consequenties van deze algemene stelling nader te onderzoeken.

35. Ter afsluiting van dit onderdeel keer ik terug naar de vraag waarmee Burger B van casus A worstelt: welk recht is van toepassing op zijn overeenkomst met onderneming O en welke betekenis komt daarbij toe aan het contractsbeding waarin naar het Occidentische recht wordt verwezen? In het voorafgaande heb ik bepleit dat deze overeenkomst bij gebreke van een rechtskeuze is onderworpen aan het recht van het land waar Burger B zijn gewone verblijfplaats heeft – hier het Nederlandse recht – en dat Burger B een rechtskeuze voor het Occidentische recht kan negeren als dit recht hem minder bescherming biedt dan het dwingendrechtelijke Nederlandse (consumenten)recht. Daarbij zou ik willen abstraheren van de precieze totstandkomingsgeschiedenis van de transactie: het enkele feit dat via het Internet een consumentenovereenkomst tot stand is gekomen, vind ik voldoende om Burger B onder het bereik van art. 5 EVO te brengen. Dit laatste vergt wellicht wijziging van art. 5 lid 2.

B. Onrechtmatige daad

36. Welk recht beheerst een onrechtmatige daad, bestaande uit het aanbieden van onjuiste en beledigende informatie op het Internet? Deze vraag van IPR rijst in casus B van hoofdstuk II: de overheid van het land Satania voelt zich onheus bejegend door

de tekst op de homepage van de in Nederland gevestigde Stichting S en wenst rectificatie. Welk delictsstatuut is van toepassing?

37. Ik begin met de constatering dat het huidige Nederlandse IPR geen speciale geschreven of ongeschreven verwijzingsregel voor de aan het Internet gerelateerde onrechtmatige daad kent en dat een dergelijke specifieke regel evenmin is voorzien in het voorstel van de Staatscommissie voor het Internationaal Privaatrecht voor een Wet conflictenrecht onrechtmatige daad.²⁹ Dit betekent dat ik moet en mag uitgaan van het 'gewone' (pre-Internet) IPR, waarvoor de Hoge Raad de hoofdregel heeft geformuleerd dat 'een vordering uit onrechtmatige daad ... in beginsel [wordt] beheerst door het recht van het land waar de onrechtmatige daad heeft plaatsgevonden'.³⁰ Is deze verwijzingsregel ook geschikt voor het Internet?

38. Wie zich bezint op een verwijzingsregel ten behoeve van de aansprakelijkheid uit onrechtmatige daad voor Internet-uitingen, stuit op twee wezenskenmerken van het Internet.

In de eerste plaats is er het wereldwijde bereik van alle informatie die op het Internet beschikbaar wordt gesteld. Bij de huidige stand van de techniek, waarover medepreadviscur Koers uitvoeriger schrijft, is het niet mogelijk om dit wereldwijde bereik in te perken, noch voor de persoon die de informatie op het Internet aanbiedt, noch voor hem die het Internet raadpleegt, noch voor de verschillende technische tussenschakels – de diverse typen providers en de telecommunicatie-exploitanten – noch voor de nationale overheden. Het is alles of niets: wie het Internet betreedt, treedt toe tot een mondiaal netwerk. Afscheiding of compartimentering is nog toekomstmuziek. De zaak ligt anders bij een besloten Intranet, maar dit andersoortige fenomeen blijft hier buiten beschouwing.

Vanuit het IPR bezien is het van belang dat de gebruikers van het Internet weet hebben, althans redelijkerwijs weet kunnen

29. Advies van de Staatscommissie voor het Internationaal Privaatrecht aan de Minister van Justitie d.d. 23 december 1996 (met Voorstel van de Staatscommissie tot regeling van het conflictenrecht met betrekking tot verbintenissen uit onrechtmatige daad) nr. 5 (nog niet openbaar gemaakt).

30. HR 19 november 1993 (COVA/BGL c.s), NJ 1994, 622 (JCS en PvS), AA 1994, p. 165 (ThMdB).

hebben van dit wezenskenmerk van het Internet. Met name voor de aanbieder van informatie kan en mag de wereldwijde inwerking van zijn informatie geen verrassing vormen. Het aan het Internet inherent grensoverschrijdende karakter is voor hem redelijkerwijs te voorzien. Deze voorzienbaarheid legitimeert het IPR om de kwestie van de delictuele aansprakelijkheid voor een Internet-uiting zo nodig aan te knopen aan een ander rechtstelsel dan dat van de woon- of vestigingsplaats van de aanbieder. Immers, hij die willens en wetens via een wereldwijd communicatiesysteem informatie aanbiedt, kan redelijkerwijs voorzien dat andere dan zijn lokale fatsoensnormen beslissend zijn bij de beantwoording van de vraag of hij jegens een ander onrechtmatig heeft gehandeld.

Het tweede wezenskenmerk van het Internet is dat de transmissie van Internet-informatie – in jargon: de ‘routing’ – van de aanbieder naar een of meer ontvangers niet langs één weg verloopt, maar juist via verschillende wegen. Het medium is al even mondiaal als zijn gebruikers. Een pakket informatie reist via talloze alternatieve wegen van de zender naar de ontvanger(s). Voor het IPR brengt dit wezenskenmerk mee dat de transmissie zelf geen relevant geografisch aanknopingspunt oplevert. De reis van de informatie verloopt immers langs diverse volstrekt willekeurige wegen.

Met een soortgelijke redenering verwerp ik het ‘vastpinnen’ van Internet-uitingen op de vestigingsplaatsen van de diverse technische tussenschakels, zoals de verschillende typen providers en de telecomunicatie-exploitanten. Hun rol bij de transmissie van informatie is in beginsel even willekeurig als de rol van de traditionele communicatieorganisaties, zoals de postdiensten, bij de totstandkoming van (grensoverschrijdende) rechtsverhoudingen in het pre-Internet tijdperk. En waar het pre-Internet IPR bij de lokalisatie van grensoverschrijdende rechtsverhoudingen dergelijke tussenschakels buiten beschouwing liet, dient het IPR in het Internet-tijdperk eveneens ‘mediumneutraal’ te zijn.³¹ De zaak ligt uiteraard anders indien een technische tussenschakel zelf als laedens of gelaedeerde ter zake van een Internet-uiting optreedt. In het laatste geval kan diens vestigingsplaats wel een relevant

31. Anders Burnstein, *supra* noot 11, p. 102-108, die in bepaalde situaties aanknopings aan het recht van de vestigingsplaats van de access provider bepleit.

aanknopingspunt vormen, maar dan dient zich ook een rolwisseling aan: de technische tussenschakel wordt zelf rechtens relevante partij bij een Internet-casus.

Alle irrelevante geografische gegevens wegstrepend, houd ik slechts twee bruikbare aanknopingspunten over. Enerzijds is er de plaats waar de Internet-informatie haar oorsprong vindt, hetgeen doorgaans de woon- of vestigingsplaats van de aanbieder van de Internet-informatie is. Anderzijds is c.q. zijn er de plaats of plaatsen waar de Internet-informatie haar schadelijke inwerking heeft, dat wil zeggen de plaats of plaatsen waar de gelaedeerde stelt de schadelijke gevolgen van de Internet-uiting te ondervinden.

Samengevat leveren de geschetste wezenskenmerken van het Internet twee belangrijke gezichtspunten op:

(i) De grensoverschrijdende inwerking van een Internet-uiting is voor de aanbieder voorzienbaar, hetgeen het IPR legitimeert om de aanbieder aan vreemd recht te onderwerpen.

(ii) Voor de lokalisatie van een Internet-uiting kunnen noch de 'routing' van de informatie noch de vestigingsplaatsen van de technische tussenschakels, maar slechts de plaats van oorsprong en de plaats(en) van de schadelijke inwerking van de Internet-uiting worden benut.

39. De in § 38 gevonden gezichtspunten transplanterend naar het bestaande IPR, ontwaar ik twee verwijzingsregels: toepassing van het onrechtmatigedaadsrecht van de plaats waar de relevante informatie haar oorsprong vindt – het alternatief van de 'lex originis' – versus toepassing van het onrechtmatigedaadsrecht van de plaats of plaatsen waar de informatie haar schadelijke inwerking heeft en de gelaedeerde in zijn belang wordt getroffen – het alternatief van de 'lex protectionis'. Ik werk beide alternatieven nader uit.

40. Het alternatief van de lex originis past in het bestaande IPR. De plaats waar de informatie haar oorsprong vindt, kan worden beschouwd als 'de plaats waar de onrechtmatige daad heeft plaatsgevonden', de locus delicti. Dit argument lijkt op het eerste gezicht zwak, omdat ook de plaats waar de informatie haar inwerking heeft, aanspraak kan maken op het predikaat locus

delicti. Het IPR is echter gewend aan zo'n uiteenvallen van 'Handlungsort' – zeg: de plaats waar de informatie haar oorsprong vindt – en 'Erfolgsort' – zeg: de plaats waar de informatie haar inwerking heeft – en maakt dan een keuze tussen beide (in beginsel evenwaardige) aanknopingspunten. Aanknoping aan het Handlungsort is dus een alternatief dat strookt met het bestaande IPR.

Het alternatief van de *lex originis* biedt voorts het voordeel dat het niet berust op de aanvaardbaarheid van het eerste in § 38 gevonden gezichtspunt – de voorzienbaarheid van de wereldwijde inwerking van een Internet-uiting – en iedere discussie over de gerechtvaardigdheid van de toepassing van een ander recht dan dat van de woon- of vestigingsplaats van de aanbieder vermijdt.

Ten slotte strookt dit alternatief met het tweede in § 38 gevonden gezichtspunt inzake de bruikbare aanknopingspunten, aangezien het aanknoopt aan de plaats van oorsprong van de relevante informatie. Desgewenst zou de verwijzingsregel nog kunnen worden gepreciseerd met behulp van een weerlegbaar vermoeden, in die zin dat informatie wordt geacht op het Internet te zijn geplaatst in de woon- of vestigingsplaats van de aanbieder, tenzij deze aannemelijk maakt dat zulks op een andere plaats is gebeurd.

Conclusie: de *lex-originisaanknoping* past in het bestaande IPR en is niet strijdig met de eerder gevonden gezichtspunten. Zijn er nog andere argumenten pro en contra deze aanknoping aan te voeren?

Vóór het alternatief van de *lex originis* pleiten de hanteerbaarheid en voorspelbaarheid waartoe deze aanknoping leidt. De *lex-originisaanknoping* is *hanteerbaar*, omdat de delictuele aansprakelijkheid van de aanbieder enkel en alleen wordt beoordeeld naar de maatstaven van het recht van diens woon- of vestigingsplaats – uitgaande van het eerder bepleite vermoeden dat de informatie daar haar oorsprong vindt – en abstraheert van de plaats of plaatsen waar de informatie haar inwerking heeft. De hierna te bespreken *lex-protectionisaanknoping*, daarentegen, kan tot toepassing van een cascade van rechtsstelsels nopen. De *lex-originisaanknoping* komt voorts de *voorspelbaarheid* ten goede, omdat de aanbieder van informatie kan volstaan met inachtneming van zijn eigen, lokale normen en zich niet behoeft in te

laten met de vraag of en in hoeverre de informatie onrechtmatig zal zijn volgens het recht van de plaats of plaatsen waar zij haar inwerking heeft.

Tegen het alternatief van de *lex originis* pleit zijn weinig realistische karakter. Ik kan mij niet goed voorstellen dat dit alternatief binnen afzienbare tijd op wereldwijde steun kan rekenen. Het terrein van de onrechtmatige daad, in het bijzonder het deelgebied van de beledigende publicaties, is sterk rechtspolietiek gekleurd, vooral door de rechtstreekse band met de in hoofdstuk III aangestipte vrijheid van meningsuiting. Fatsoensnormen ten aanzien van publicaties zijn cultureel bepaald en verschillen daarmee van land tot land. Zolang het materiële recht op dit terrein zo sterk varieert, is aanvaarding van de *lex originis*aanknopning en de daaruit voortvloeiende toepassing van buitenlands onrechtmatigedaadsrecht op een Internet-uiting die lokaal haar inwerking heeft, een onhaalbaar en wellicht ook onwenselijk alternatief. Misschien kan de *lex originis*aanknopning gedijen op Europees niveau, ervan uitgaande dat het materiële recht inzake de onrechtmatige daad binnen Europa in sterke mate zal worden geharmoniseerd. Wereldwijde hanterring van dit alternatief lijkt mij vooralsnog echter te hoog gegrepen, hetgeen betekent dat dit alternatief niet in overeenstemming is met het in § 21 aangehaalde gebod van Meijers.

41. Ook het alternatief van de *lex protectionis* strookt met het bestaande IPR. Aanknopning aan de *lex protectionis* kan als Internet-verbijzondering van aanknopning aan het Erfolgsort worden beschouwd. De onrechtmatige daad wordt hier aangeknoopt aan het recht van het land of de landen waar de Internet-uiting haar inwerking heeft en schade berokkent aan de geïlaedeerde.

Vervolgens is van belang dat de aanknopning aan het recht van het land waar de informatie haar inwerking heeft, jegens de aanbieder van de informatie kan worden gerechtvaardigd met een beroep op de in § 38 geschetste voorzienbaarheid dat de Internet-uiting wereldwijd effect sorteert.

Ten slotte is dit alternatief gebaseerd op een in beginsel bruikbaar aanknopingspunt, te weten de plaats(en) waar de informatie haar schadelijke inwerking heeft.

Conclusie: ook het alternatief van de *lex protectionis* verdraagt

zich met het bestaande IPR en met beide gezichtspunten. Welke plussen en minnen kunnen hier verder worden genoteerd?

Een voordeel van de *lex-protectionis*aanknopning is de verdiscontering van het feit dat het recht inzake de onrechtmatige daad sterk rechtspolitiek is gekleurd en van land tot land verschilt. Binnen iedere rechtsorde waar een Internet-uiting haar inwerking heeft, zal toepassing van het lokale recht niet alleen eenvoudiger zijn, maar ook beter aansluiten bij de idee dat lokale (en niet buitenlandse) normen inzake de vrijheid van meningsuiting en inzake de bescherming van de goede naam en de privacy van de gelaedeerde de doorslag behoren te geven. De *lex-protectionis*aanknopning kan zo gemakkelijker op wereldwijde steun rekenen dan de *lex-originis*aanknopning; zij strookt aldus met het gebod van Meijers dat in § 21 ter sprake kwam.

Hierop voortbordurend is verdedigbaar dat de *lex-protectionis*aanknopning goed aansluit bij de in het moderne IPR gehuldigde beschermingsgedachte. In § 29 en 32 passeerde deze gedachte al de revue in het kader van de Internet-consumentenovereenkomst; daar leidde zij tot een pleidooi voor – kort gezegd – aanknopning aan het recht van de woonplaats van de consument. Langs dezelfde lijn is verdedigbaar dat het slachtoffer van een Internet-uiting, als de in beginsel te beschermen persoon, aanspraak moet kunnen maken op bescherming volgens het recht van de plaats waar de schade zich voordoet.

Een groot nadeel van het *lex-protectionis*alternatief is de vaagheid die aan het begrip 'plaats van schadelijke inwerking' kleeft. Waar heeft een Internet-uiting precies haar inwerking? De technicus zal antwoorden dat een Internet-uiting in alle landen van de wereld een potentiële inwerking heeft, omdat de informatie voor iedere Internet-raadpleger waar ook ter wereld beschikbaar is. De jurist zal een zekere reductie mogelijk achten, naar gelang van de aard van de informatie en de bekendheid van de gelaedeerde. Apert onjuiste informatie over een wereldwijd bekende persoon of onderneming heeft in vele landen haar schadelijke inwerking. Openbaarmaking van weinig vertrouwelijke gegevens over een lokale 'beroemdheid' sorteert uitsluitend effect in de woonplaats van de persoon en nergens anders. Tussen deze twee uitersten bevindt zich echter een scala van mogelijkheden, hetgeen een navenant grote mate van rechtsonzekerheid creëert. Wellicht kan deze voor een belangrijk deel worden weg-

genomen door de lex-protectionisaanknopning zo in te kleden dat het aan de gelaedeerde als eisende partij is om aannemelijk te maken dat en in hoeverre de informatie ook buiten haar woon- of vestigingsplaats schade heeft veroorzaakt. Slaagt de eisende partij niet in deze 'aannemelijkmakingsverplichting', dan kan de rechter zich beperken tot de schadelijke inwerking in c.q. het onrechtmatigedaadsrecht van de woon- of vestigingsplaats van de gelaedeerde.

Een tweede nadeel van deze aanknopning ligt in het verlengde van het vorenstaande. Consequente hantering van de lex-protectionisregel kan nopen tot toepassing van verschillende rechtsstelsels, ieder voor de schadelijke inwerking van de uiting in een bepaald land. Als de eisende partij ervoor kiest haar vordering bij één rechter te concentreren, zal deze genoodzaakt zijn de inhoud van deze vreemde rechtsstelsels te achterhalen en toe te passen, hetgeen praktisch onmogelijk kan zijn. Ik zie twee uitwegen die beide het uitgangspunt van de lex-protectionisaanknopning ongemoeid laten. De eerste is de hiervoor geschetste 'aannemelijkmakingsverplichting'. In de minder gewichtige gevallen zal de eisende partij deze verplichting willen ontlopen en haar vordering beperken tot herstel van de lokale schade naar het lokale recht. De tweede uitweg is die welke op het terrein van de intellectuele en industriële eigendom – met name in kort geding – wel wordt ingeslagen. Geconfronteerd met de toepasselijkheid van buitenlands recht hanteert de Nederlandse rechter het 'gelijkheidsvermoeden': het buitenlandse recht wordt geacht niet wezenlijk af te wijken van het Nederlandse, tenzij de belanghebbende partij aannemelijk maakt dat en in hoeverre het buitenlandse recht anders luidt.³² Beide uitwegen kunnen in de praktijk tot een praktische en efficiënte besparing op het rechterlijk werk leiden.

42. Ik kies voor de lex-protectionisaanknopning en neem de mogelijke problemen rond de toepassing daarvan voor lief, in

32. Zie, in het algemeen, S.K. Martens, *Overzicht der Nederlandse Rechtspraak. Internationaal Privaatrecht. Industriële en intellectuele eigendom – ongeoorloofde mededinging* (1979-1984), WPNR 117 (1986) 5771, p. 105-106; J.J. Brinkhof, *Overzicht der Nederlandse Rechtspraak. Internationaal privaatrecht 1990-1993/1994. Intellectuele eigendom (II, slot)*, WPNR 126 (1995) 6180, p. 309-310.

ruil voor de realistische en slachtofferbeschermende aanknop-
ping aan het recht van het land waar de informatie haar schade-
lijke inwerking heeft. De charme van de hanteerbaarheid en de
voorspelbaarheid die eigen is aan de *lex originis*-aanknop-
ping, weegt voor mij niet op tegen haar veronachtzaming van de juri-
disch-culturele verscheidenheid die het terrein van de onrecht-
matige daad kenmerkt.

43. De zo-even bepleite verwijzingsregel wijst het objectief
toepasselijke recht aan. Dit recht dient echter te wijken voor een
door beide partijen – laedens en gelaedeerde – gezamenlijk aan-
gewezen recht, zulks in aansluiting op de rechtskeuzevrijheid die
de Hoge Raad op het terrein van de onrechtmatige daad heeft
aanvaard.³³ Een bijkomend voordeel van een rechtskeuze door
partijen is dat daarmee het in § 41 geschetste probleem van de
toepassing van verschillende rechtssystemen verdwijnt. En waar
deze rechtskeuze doorgaans pas na het intreden van de schade
zal worden overeengekomen, behoeft geen vrees te bestaan voor
een (zoals in § 29 besproken) sociaal-economische ongelijkheid
tussen de partijen.

44. De eerder aangebrachte nuances van de ‘aannemelijkma-
kingsverplichting’ en het ‘gelijkheidsvermoeden’ weglatend,
kom ik tot de volgende verwijzingsregel voor de onrechtmatige
daad, bestaande uit het aanbieden van schadebrengende infor-
matie op het Internet:

(i) De verbintenis uit onrechtmatige daad wegens het aanbieden
van informatie op het Internet wordt beheerst door het recht
dat partijen hebben gekozen.

(ii) Bij gebreke van een rechtskeuze wordt deze verbintenis be-
heerst door het recht van het land waar de informatie haar scha-
delijke inwerking heeft.

45. Pro memorie vestig ik nogmaals de aandacht op de rol van
de in § 34 aangestipte openbare orde. De invloed van culturele
waarden en publiekrechtelijke normen, met name de vrijheid

33. HR 19 november 1993 (COVA/BGL c.s.), NJ 1994, 622 (JCS en PvS), AA
1994, p. 165 (ThMdB).

van meningsuiting, op het terrein van de aansprakelijkheid voor onrechtmatige publicaties is groot. Deze waarden en normen zullen via het leerstuk van de openbare orde een corrigerende invloed op de uitkomst van de zo-even geschetste verwijzingsregel uitoefenen. Kort gezegd: de Nederlandse rechter is slechts bereid om buitenlands onrechtmatigedaadsrecht toe te passen indien en voor zover de bepalingen van dit recht verenigbaar zijn met de Nederlandse openbare orde.

46. Toegepast op casus B van hoofdstuk II leidt de door mij bepleite verwijzingsregel ertoe dat de aansprakelijkheid van Stichting S jegens Satania, bij gebreke van een rechtskeuze, wordt beheerst door het recht van het land waar de informatie haar schadelijke inwerking heeft. Gezien de aard van de informatie en de wereldwijde bekendheid van de Staat Satania vindt deze inwerking in alle landen ter wereld plaats. De op Satania rustende 'aannemelijkmakingsverplichting' ten aanzien van deze wereldwijde inwerking vormt geen grote hindernis. Niettemin ligt het voor de hand dat de door Satania geadicteerde Nederlandse rechter grote betekenis zal toekennen aan de in Nederland geldende normen inzake de vrijheid van meningsuiting en inzake de bescherming van de goede naam tegen onjuiste en beledigende publicaties. In de eerste plaats mag de rechter, op basis van het door mij verdedigde 'gelijkheidsvermoeden', uitgaan van de premisse dat het buitenlandse recht niet wezenlijk afwijkt van het Nederlandse, tenzij de belanghebbende partij – hier: Satania – aannemelijk maakt dat het buitenlandse recht anders – hier: minder liberaal – luidt. In tweede plaats moet de Nederlandse rechter nagaan of de toepassing van dergelijk minder liberaal buitenlands recht verenigbaar is met de Nederlandse openbare orde. Apert minder liberale buitenlandse regels zullen niet door de heugel kunnen en buiten toepassing moeten blijven.

Een buitenlandse rechter aan wie de zaak wordt voorgelegd, zou dezelfde lex-protectionisregel moeten toepassen en, via bovenstaande redenering, eveneens tot toepassing van *zijn* lokale, door *zijn* openbare orde geïnspireerde, recht komen. Dat onderstreept nog eens het belang van de kwestie welke rechter of rechters bevoegd is c.q. zijn én welke rechter door de eisende

partij wordt geadieerd. Deze kwestie laat ik rusten tot hoofdstuk VIII.

C. Intellectuele en industriële eigendom en ongeoorloofde mededinging

47. In dit onderdeel onderzoek ik de vraag naar het toepasselijke recht voor kwesties met betrekking tot inbreuk op rechten van intellectuele en industriële eigendom alsmede ongeoorloofde mededinging. Dit onderwerp komt aan de orde in casus C van hoofdstuk II: Filmbedrijf F uit Fantasia is in een groot aantal landen auteursrechthebbende ten aanzien van een speelfilm en wenst een einde te maken aan de Internet-exploitatie daarvan door Maatschappij M uit Barbarije.

48. Het rechtsgebied van de intellectuele en industriële eigendom en de ongeoorloofde mededinging bestrijkt een groot aantal deelterreinen. Een gebruikelijke tweedeling is die tussen de absolute rechten, zoals het auteurs-, octrooi-, merken-, modellen- en handelsnaamrecht, enerzijds en de aansprakelijkheid ter zake van ongeoorloofde mededinging anderzijds. Deze tweedeling hanteer ik hierna eveneens, hoewel er zich op het niveau van het IPR-conflictenrecht geen grote verschillen tussen beide categorieën voordoen. Ik begin met de absolute rechten (§ 49-50) en kom daarna toe aan de ongeoorloofde mededinging (§ 51-52).

49. Het bestaande IPR scheert de verschillende typen absolute rechten van intellectuele en industriële eigendom in belangrijke mate over één kam. De rechtvaardiging hiervoor wordt gevonden in hun gemeenschappelijke wezenskenmerk: de territoriaal beperkte werking. In beginsel bepaalt iedere Staat voor zijn eigen grondgebied aan wie een recht van intellectuele of industriële eigendom toekomt, op welke wijze het recht ontstaat en tenietgaat, welke rechtsbescherming de rechthebbende geniet en op welke wijze het recht kan worden overgedragen. Voor de absolute rechten die uitsluitend door registratie kunnen ontstaan, ligt dit voor de hand: iedere Staat kent zijn eigen (vorm van) registratie en door inschrijving ontstaat een absoluut recht binnen de betrokken Staat. Maar zelfs het auteursrecht, dat voor

zijn ontstaan niet van registratie afhankelijk is, heeft een territoriaal begrensde karakter. Iedere Staat is in beginsel bij machte zelf de regels voor het ontstaan en het tenietgaan, de beschermingsomvang en de overdracht van het auteursrecht vast te stellen en deze regels gelden uitsluitend voor het door de betrokken Staat toegekende auteursrecht.

De territoriale aard van de rechten van intellectuele en industriële eigendom verandert niet wezenlijk door de verschillende pogingen die op internationaal en supranationaal niveau zijn of worden ondernomen om tot minimumbescherming, non-discriminatie, harmonisatie of eenmaking te komen. Zo leiden het Verdrag van Parijs inzake de industriële eigendom,³⁴ de Berner Conventie inzake het auteursrecht,³⁵ de Universele Auteursrechtconventie³⁶ en het TRIPS-verdrag³⁷ 'slechts' tot een *minimumbescherming* en tot *non-discriminatie* tussen binnen- en buitenlandse rechthebbenden, maar laten zij de territoriale geaardheid van de absolute rechten ongemoeid. Hetzelfde geldt voor de *harmonisatie* van sommige onderwerpen door de Europese Unie, omdat zij de lidstaten slechts op enkele punten een zekere mate van eenvormigheid van hun (nog steeds) nationale rechtstelsels voorschrijft. En zelfs de *eenmaking* binnen de Benelux en de Europese Unie van bepaalde rechten van intellectuele en industriële eigendom is welbeschouwd niet meer dan een vergroting van het grondgebied waarbinnen de betrokken eenvormige rechten functioneren. Geen van deze initiatieven leidt ertoe dat de rechten van intellectuele en industriële eigendom een extra-territoriale werking krijgen.

De territoriale geaardheid van de absolute rechten brengt volgens het bestaande IPR mee dat voor ieder betrokken grondgebied – dus meestal voor iedere Staat afzonderlijk, maar soms voor de Benelux als geheel – naar het aldaar geldende auteurs-, octrooi-, merken-, modellen- en handelsnaamrecht moet worden

34. Herzien Internationaal Verdrag van Parijs van 20 maart 1883 tot bescherming van de industriële eigendom, Stockholm, 14 juli 1967, Trb. 1970, 187.

35. Herziene Berner Conventie van 9 september 1886 voor de bescherming van werken van letterkunde en kunst, Parijs, 24 juli 1971, Trb. 1972, 157.

36. Universele Auteursrechtconventie, herzien te Parijs op 24 juli 1971, Parijs, 24 juli 1971, Trb. 1976, 37.

37. Overeenkomst inzake de handelsaspecten van de intellectuele eigendom, Marrakesh, 15 april 1994, PB EG 37 (1994) nr. L 336, p. 1, Trb. 1995, 130.

beoordeeld (i) welke gedragingen als een inbreuk op dit recht kunnen worden aangemerkt, (ii) welke bescherming de recht-hebbende tegen een inbreuk op zijn recht toekomt en (iii) met welke sancties – schadevergoeding, verbod of gebod – de recht-hebbende een inbreuk kan doen keren. Zowel art. 2 lid 1 Verdrag van Parijs als art. 5 lid 2 Berner Conventie verdisconteert de verschillen die op deze punten tussen de nationale rechtsstelsels bestaan en verwijst voor de rechtsbescherming van de recht-hebbende naar het recht van het land waar deze de bescherming inroept. Het IPR hanteert hier derhalve dezelfde *lex-protectionisaanknoping* die ik hiervoor in onderdeel B bepleitte voor de aansprakelijkheid uit onrechtmatige daad voor Internet-uitingen. Zowel hier als daar voert het recht van de plaats of de plaatsen van de schadelijke inwerking de boventoon.

50. De hiervoor geschetste *lex-protectionisaanknoping* is mijns inziens ook geschikt voor toepassing op inbreuken op rechten van intellectuele en industriële eigendom door middel van Internet-gedragingen.³⁸ Hier gelden grotendeels de pro- en contra-argumenten die ik hiervoor in onderdeel B reeds heb gewogen. Om niet in herhaling te vervallen, volsta ik hier met drie aanvullende opmerkingen.

Aanknoping aan de *lex protectionis* op het onderhavige terrein strookt met het in § 38 besproken gezichtspunt dat gedragingen op het Internet een voorzienbaar wereldwijde inwerking hebben. Een persoon of onderneming die informatie op het Inter-

38. Zie, in deze zin, P.E. Geller, *Conflicts of Law in Cyberspace: International Copyright in a Digitally Networked World*, in P.B. Hugenholtz ed., *The Future of Copyright in a Digital Environment. Proceedings of the Royal Academy Colloquium organized by the Royal Netherlands Academy of Sciences (KNAW) and the Institute for Information Law* (Amsterdam, 6-7 July 1995), *Information Law Series* (1996) p. 27-48; A. Ottow en I. Grootenhuis, *Aansprakelijkheid en Handhaving*, in S.J.H. Gijrath e.a. red., *Intellectueel eigendom in digitaal perspectief. Vormt intellectueel eigendomsrecht een voorwaarde of belemmering voor de digitale maatschappij?* Forumbundel voor het Forum Intellectueel eigendom: voorwaarde of belemmering voor de digitale maatschappij?, georganiseerd door Stichting SURF en de Ned. Ver. Informatietechnologie en Recht (1996) p. 98-101; J.M.B. Seignette, *The Netherlands*, in M. Dellebeke ed., *Copyright in cyberspace. Copyright and the Global Information Infrastructure/Le droit d'auteur en cyberspace. Le droit d'auteur et l'infrastructure mondiale de l'information. Proceedings of the 63rd Congress of the Association Littéraire et Artistique Internationale* (1997) p. 309-317.

net ter beschikking stelt en vervolgens wordt geconfronteerd met de stelling van de rechthebbende dat deze gedraging inbreuk maakt op het auteursrecht dat laatstgenoemde volgens het recht van een of meer Staten toekomt, kan zich niet erop beroepen dat niet voorzienbaar was dat de informatie in deze Staten ter beschikking van derden zou komen. De voorzienbaarheid van de wereldwijde inwerking van Internet-informatie verzet zich tegen de aanvaarding van een dergelijk verweer.

Daarnaast vind ik van belang dat de lex-protectionisaanknopning voor Internet-inbreuken op rechten van intellectuele en industriële eigendom aansluit bij de bestaande IPR-regel voor inbreuken op dergelijke rechten en daarmee een goede kans op wereldwijde aanvaarding maakt. De lex-protectionisaanknopning is acceptabel voor iedere Staat, aangezien zij ertoe leidt dat iedere Staat een rechthebbende volgens de lokale normen beschermt (of niet beschermt) tegen inbreuken door personen of ondernemingen die opereren vanuit andere landen, waar een lager (of een hoger) beschermingsniveau geldt. In een wereld van territoriaal begrensde absolute rechten is de lex-protectionisaanknopning de voor de hand liggende verwijzingsregel. Aldus strookt deze aanknoping met het in § 21 aangehaalde gebod van Meijers.

Ten slotte wijs ik erop dat ook de Europese Commissie na bestudering van de materie tot de conclusie lijkt te zijn gekomen dat de lex-protectionisaanknopning op dit moment de enig haalbare oplossing is. Aanvankelijk was de Commissie sterk gepor-teerd voor aanknoping aan de lex originis: het recht van de lidstaat van waaruit de informatie door middel van digitale transmissie wordt aangeboden, zou kwesties van intellectuele eigendom (auteursrecht en naburige rechten) dienen te beheersen.³⁹ Inspiratie voor deze aanknoping werd gevonden in de Richtlijn satellietomroep en kabeldoorgifte, die weliswaar geen verwijzingsregel voor kwesties van auteursrecht en naburige rechten bij grensoverschrijdende uitzendingen bevat, maar (in art. 1 lid 2 onder (b)) wel een eenduidig aanknopingspunt introduceert:

39. Europese Commissie, Groenboek inzake het auteursrecht en de naburige rechten in de informatiemaatschappij, document COM (95) 382 def., 19 juli 1995, p. 41-42.

'De mededeling aan het publiek per satelliet, vindt slechts plaats in de Lid-Staat waar de programmadragende signalen onder controle en verantwoordelijkheid van de omroeporganisatie worden ingevoerd in een ononderbroken mededelingenketen die naar de satelliet en terug naar de aarde loopt.'⁴⁰

Overigens realiseerde de Commissie zich terdege dat hantering van de *lex-originis*aanknopning voor het Internet-verkeer binnen de Europese Unie een vergenvorderde harmonisatie van het materiële recht van de lidstaten veronderstelt, terwijl toepassing van deze aanknopning op het verkeer met derde Staten nog problematischer zou zijn. Na raadpleging van 'belanghebbende kringen' lijkt de Commissie de bezwaren tegen de *lex-originis*-aanknopning – genoemd worden: de moeilijkheid om de plaats van oorsprong van de transmissie vast te stellen, de thans onvolledige harmonisatie van het materiële recht binnen de Europese Unie en de problemen in het Internet-verkeer met derde Staten – nog zwaarder aan te slaan. De *lex-originis*benadering wordt (nog) niet met zoveel woorden prijsgegeven, maar het voorstel van 'de belanghebbenden' om de bestaande *lex-protectionis*-aanknopning te handhaven en te verduidelijken, is door de Commissie overgenomen.⁴¹

51. Ten aanzien van de ongeoorloofde mededinging is in het IPR een verwijzingsregel ontwikkeld die aanknopning aan het recht van de 'markt' voorschrijft. Als de ene onderneming de andere onderneming beconcurrert, wordt de toelaatbaarheid van de mededingingsgedragingen bepaald door het recht (niet van hun respectieve vestigingsplaatsen maar) van de plaats waar

40. Richtlijn 93/83/EEG van de Raad van 27 september 1993 tot coördinatie van bepaalde voorschriften betreffende het auteursrecht en naburige rechten op het gebied van de satellietomroep en de doorgifte via de kabel, PB EG 36 (1993) nr. L 248, p. 15. Zie, over de mogelijkheid van analogische toepassing van deze Richtlijn op een digitale context, T. Dreier, *The Cable and Satellite Analogy*, in P.B. Hugenholtz ed., *The Future of Copyright in a Digital Environment. Proceedings of the Royal Academy Colloquium organized by the Royal Netherlands Academy of Sciences (KNAW) and the Institute for Information Law* (Amsterdam, 6-7 July 1995), *Information Law Series* (1996) p. 57-65.

41. Europese Commissie, *Vervolg op het Groenboek inzake het auteursrecht en de naburige rechten in de informatiemaatschappij*, document COM (96) 568 def., 20 november 1996, p. 23-24.

de economische strijd plaatsvindt, dat wil zeggen door het recht van de markt die de één ten koste van de ander wenst te veroveren. Ook deze aanknopng is in wezen een variant van de *lex-protectionisaanknopng*. De oneerlijk beconcurrerde onderneming beroept zich immers op de bescherming door het recht van het land waar zij de schadelijke inwerking van de gedragingen van haar concurrente voelt, hetgeen het recht van hun economisch strijdtoneel van toepassing doet zijn.

52. De hiervoor geschetste verwijzingsregel leent zich mijns inziens voor toepassing op ongeoorloofde mededinging die via het Internet wordt begaan. Waar deze verwijzingsregel een variant van de *lex-protectionisaanknopng* is, gelden hier de argumenten die ik hiervoor in onderdeel B en in § 50 reeds heb genoemd. Daarom volsta ik met de stelling dat ongeoorloofde mededinging via het Internet een species is van het genus onrechtmatige daad via het Internet en dat voor beide rechtsgebieden de *lex-protectionisaanknopng* een geschikte verwijzingsregel vormt.

53. Voor kwesties met betrekking tot inbreuk op rechten van intellectuele en industriële eigendom alsmede ongeoorloofde mededinging kan ik nu de volgende verwijzingsregel opstellen:

- (i) De vraag of een gedraging op het Internet als een inbreuk op een recht van intellectuele en industriële eigendom valt aan te merken en welke bescherming de rechthebbende tegen een inbreuk toekomt, wordt beheerst door het recht van het land waar de gedraging haar schadelijke inwerking heeft.
- (ii) De verbintenis uit ongeoorloofde mededinging wegens een gedraging op het Internet wordt beheerst door het recht van het land waar de gedraging haar schadelijke inwerking op de marktpositie van de gelaedede heeft.

54. Voor casus C van hoofdstuk II brengt onderdeel (i) van de zo-even geformuleerde verwijzingsregel mee dat Filmbedrijf F zich kan beroepen op de auteursrechtelijke rechtsbescherming van ieder land, inclusief Nederland, waar de Internet-gedraging van Maatschappij M inbreuk maakt op het hem toekomende auteursrecht. Voor zover deze gedraging zich in andere landen,

waaronder Barbarije, manifesteert, geldt dat Filmbedrijf F geen auteursrechtelijke rechtsbescherming kan inroepen. Uiteraard rijst direct de vraag hoe de Nederlandse rechter te werk moet gaan als Filmbedrijf F een rechterlijk bevel tot beëindiging van 'de' Internet-gedraging van Maatschappij M vordert. De actie moet slagen voor zover zij is gebaseerd op het recht van een van de landen waar Filmbedrijf F rechtsbescherming toekomt, maar dient te stranden voor zover zij op het recht van Barbarije of een soortgelijk land steunt. Deze kwestie komt in hoofdstuk IX aan de orde.

VIII. DE BEVOEGDE RECHTER

55. Dit hoofdstuk is gewijd aan de tweede vraag van IPR die ik in hoofdstuk I aansneed: welke rechter is bevoegd om van een privaatrechtelijk Internet-geschil kennis te nemen? In hoofdstuk V schetste ik het beeld dat de bevoegde rechter een speciaal in het leven geroepen, gespecialiseerde en a-nationale instantie is – *judex Internet* –, maar constateerde tevens dat de nationale overheidsrechter voorlopig onmisbaar blijft. Kortheidshalve concentreer ik mij hier op de internationale bevoegdheid van de nationale overheidsrechter en ga ik voorbij aan alle vormen van particuliere geschillenbeslechting, zoals arbitrage en bindend advies door meer of minder gespecialiseerde instanties en personen.

De internationale bevoegdheid van de nationale overheidsrechter inzake Internet-geschillen zal, evenals de vraag naar het toepasselijke recht, aan de hand van de bestaande, niet speciaal voor het Internet geschreven, regels van IPR moeten worden bepaald. Zoals bekend, bepaalt de Nederlandse rechter zijn internationale bevoegdheid in de eerste plaats aan de hand van verdragen, met name het EEG-Bevoegdheids- en Executieverdrag ('EEX')⁴² en het EEG-EVA-Bevoegdheids- en Executiever-

42. Verdrag betreffende de rechterlijke bevoegdheid en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, Brussel, 27 september 1968, PB EG 15 (1972) nr. L 299, p. 32, Trb. 1969, 101, zoals gewijzigd door het eerste Toetredingsverdrag, Luxemburg, 9 oktober 1978, PB EG 21 (1978) nr. L 304, p. 1, Trb. 1978, 175, het tweede Toetredingsverdrag, Luxemburg, 25 oktober 1982, PB EG 25 (1982) nr. L 388, p. 1, →

drag ('EVEX'),⁴³ en bij gebreke van een toepasselijk verdrag aan de hand van het nationaal procesrecht, te vinden in het Wetboek van Burgerlijke Rechtsvordering.

Zowel de verdragsregels als de nationale regels zijn voor een belangrijk deel zo opgesteld dat zij zich laten toepassen op Internet-geschillen. Zo zal de bevoegdheid van de rechter van de woonplaats van de verwerende partij – het forum aangewezen door art. 2 EEX en EVEX – ook functioneren in de context van het Internet. In casus B zal de overheid van Satania zich voor haar gerechtelijke stappen zonder meer kunnen wenden tot de rechter te Amsterdam, aangezien de verweerder, Stichting S, aldaar is gevestigd. Dergelijke regels laat ik hier terzijde. Ik concentreer mij op twee regels waarbij ik 'Internet-gevoeligheden' ontwaar: in de eerste plaats het contractueel aangewezen forum (§ 56-57); in de tweede plaats het forum bij aansprakelijkheid uit onrechtmatige daad en bij inbreuk op rechten van intellectuele en industriële eigendom (§ 58-59).

56. In onderdeel A van hoofdstuk VII kwam de kwestie van de rechtskeuze bij Internet-overeenkomsten aan de orde. In § 29 pleitte ik voor een beperking van de rechtskeuzevrijheid bij overeenkomsten die via het Internet tussen een consument en een professionele wederpartij worden gesloten, ongeacht de precieze totstandkomingsgeschiedenis van de overeenkomst. Dezelfde aanpak wil ik bepleiten voor de procesrechtelijke tegenhanger van de rechtskeuzevrijheid: de vrijheid van forumkeuze. Daarvoor zijn ook aanknopingspunten te vinden in de bestaande regimes. Zowel het stelsel van het EEX en het EVEX als het nationaal procesrecht stellen grenzen aan de mogelijkheid van forumkeuze bij consumentengeschillen, zulks in afwijking van de vrijheid van forumkeuze die in vermogensrechtelijke zaken voorop staat. Wederom is de ratio van de beperking gelegen in de beschermingsgedachte: de in sociaal-economisch opzicht

→ Trb. 1983, 24, het derde Toetredingsverdrag, Donostia-San Sebastian, 26 mei 1989, PB EG 32 (1989) nr. L 285, p. 1, Trb. 1989, 142, en het (nog niet in werking getreden) vierde Toetredingsverdrag, Brussel, 29 november 1996, PB EG 40 (1997) nr. C 15, p. 1, Trb. 1997, 69.

43. Verdrag betreffende de rechterlijke bevoegdheid en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, Lugano, 16 september 1988, PB EG 31 (1988) nr. L 319, p. 9, Trb. 1989, 58.

zwakkere partij dient te worden beschermd tegen een forumkeuze die hem wellicht door de professionele wederpartij wordt opgedrongen. Weliswaar variëren de modaliteiten waaronder een forumkeuzeclausule in een consumentenovereenkomst is toegestaan van regime tot regime – men vergelijk de art. 15 juncto 13-14 EEX en EVEX, art. 100 juncto 98 lid 3 (huidige) Rv. en art. 1.1.7 leden 3 en 4 juncto art. 1.1.5 aanhef en onder c ontwerp-Rv.⁴⁴ – maar het gaat mij hier om de telkens daaraan ten grondslag liggende beschermingsgedachte.

Voor de Internet-context zou ik deze beschermingsgedachte handen en voeten willen geven door middel van een gemakkelijk(er) te hanteren bevoegdheidsregel die aansluit bij de in § 29 bepleite regel inzake rechtskeuze. Ik kom dan uit bij een regel die een forumkeuzeclausule in een via het Internet gesloten consumentenovereenkomst – ongeacht de wijze waarop de overeenkomst tussen de consument en de professionele wederpartij precies tot stand is gekomen – slechts rechtsgevolg toekent als zij geen afbreuk doet aan de processuele rechtsbescherming van de consument. Een forumkeuzeclausule ontmoet slechts dan geen bezwaar indien zij (i) tot stand komt nadat tussen partijen een geschil is ontstaan dan wel (ii) ertoe leidt dat de consument (maar niet de professionele wederpartij) de toegang tot een additioneel forum wordt geboden.

57. Voor casus A leidt de hiervoor bepleite regel tot een voor Burger B gunstig resultaat. De overeengekomen forumkeuze snijdt hem niet de weg naar de Nederlandse rechter af. Immers, de forumkeuzeclausule was reeds vóór het ontstaan van het geschil overeengekomen en heeft dan slechts het effect dat zij voor Burger B een extra forum – hier de rechter te Occidentie – creëert.

58. Rond het forum voor geschillen inzake aansprakelijkheid uit onrechtmatige daad en bij inbreuk op rechten van intellectuele en industriële eigendom doemen grotere problemen op,

44. Voorstel van wet tot wijziging van de Wet op de rechterlijke organisatie, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafvordering en andere wetten in verband met de integratie van kantongerechten en de arrondissementsrechtbanken (tweede fase herziening rechterlijke organisatie). Kamerstukken II, 1995-1996, 24 651, nr. A en 1-4.

zoals de kwestie van het toepasselijke recht in de onderdelen B en C van hoofdstuk VII ook meer hoofdbrekens opleverde dan in onderdeel A.

Uitgangspunt is art. 5 aanhef en onder 3 EEX en EVEX en het (in het huidige Rv. ontbrekende, maar) daarop geënte art. 1.1.5 aanhef en onder d ontwerp-Rv., waarbij in zaken betreffende verbintenissen uit onrechtmatige daad bevoegdheid wordt toegekend – bij wijze van alternatief voor de hoofdregel die bevoegdheid creëert voor de rechter van de woonplaats van de verweerder – aan de rechter van de plaats waar het schadeveroorzakende feit zich heeft voorgedaan. Reeds in het pre-Internet tijdperk heeft het Hof van Justitie van de Europese Gemeenschappen zich in een reeks zaken moeten buigen over de vraag hoe het begrip ‘de plaats waar het schadebrengende feit zich heeft voorgedaan’ in art. 5 aanhef en onder 3 EEX moet worden begrepen. Drie elementen uit deze jurisprudentie zijn hier van belang:

(i) Als bij de lokalisatie van het schadebrengende feit de plaats van de veroorzakende gebeurtenis die aan de schade ten grondslag ligt – het ‘Handlungsort’ – niet samenvalt met de plaats waar de schade is ingetreden – het ‘Erfolgsort’ –, mag de eisende partij haar actie naar keuze voor de rechter van het Handlungsort dan wel het Erfolgsort instellen.⁴⁵

(ii) Het Erfolgsort is niet de plaats waar de gelaedeerde stelt vermogensschade te hebben geleden als gevolg van een door hem geleden, in een andere verdragsluitende Staat (daadwerkelijk) ingetreden aanvankelijke schade.⁴⁶

(iii) Bij aansprakelijkheid voor een beledigende perspublicatie geldt de verbijzondering dat de rechter van de plaats van vestiging van de uitgever, voor zover dit de plaats is waar de publicatie haar oorsprong vindt en vanwaar de belediging is geuit en in omloop is gebracht, bevoegd is zich over alle schadelijke gevolgen, waar ook ter wereld gelokaliseerd, te buigen; terwijl de rechter van de plaats waar de publicatie is verspreid en waar de gelaedeerde stelt in zijn goede naam te zijn aangetast, slechts ken-

45. HvJ EG 30 november 1976 (21/76, Handelskwekerij G.J. Bier c.s./Mines de potasse d'Alsace), Jur. 1976, p. 1735, NJ 1977, 494 (JCS).

46. HvJ EG 19 september 1995 (C-364/93, Marinari/Lloyd's Bank c.s.), Jur. 1995, p. I-2719, NJ 1997, 32 (ThMdB).

nis mag nemen van de in deze verdragsluitende Staat toegebrachte schade.⁴⁷

Zijn deze regels bruikbaar voor onrechtmatige gedragingen die via het Internet plaatsvinden, zoals de in casus B en C van hoofdstuk II geschetste gedragingen?

Regel (i) strookt met de in onderdelen B en C van hoofdstuk VII bepleite *lex-protectionisaanknoping* en de daaraan ten grondslag liggende gedachte van slachtofferbescherming. Als het slachtoffer van een Internet-gedraging zich genoodzaakt ziet zijn zaak aan de rechter voor te leggen, dan mag hij kiezen tussen inschakeling van de rechter van het *Handlungsort*, hetgeen doorgaans de woon- of vestigingsplaats van de laedens – de persoon die verantwoordelijk is voor de Internet-gedraging – zal zijn, en inschakeling van de rechter van het *Erfolgsort*, hetgeen vrijwel altijd (mede) tot bevoegdheid van de rechter van de woon- of vestigingsplaats van de gelaedeerde zal leiden.

Regel (ii) acht ik in de Internet-context acceptabel, mits ik hem aldus mag begrijpen dat een Internet-gedraging – in beginsel – in ieder land rechtstreekse (lees: relevante) schade kan veroorzaken en er dus in ieder land een *Erfolgsort* en een bevoegde rechter kunnen worden gevonden. Het lijkt mij van groot belang dat een slachtoffer van een Internet-gedraging in ieder land waar de gedraging inwerkt, een bevoegde rechter kan adiëren. In geen geval zou de regel aldus mogen luiden dat een Internet-gedraging *te allen tijde* slechts in één land, bijvoorbeeld het land waar de aansprakelijk gestelde persoon zich bevindt dan wel het land waar de gelaedeerde woont, relevante schadelijke gevolgen kan hebben en dat de gevolgen in alle andere landen nimmer mogen meetellen in het kader van de vaststelling van de bevoegde rechter.

Regel (iii) verdient heroverweging in de context van het Internet. Ik zie geen reden om de rechter van de plaats vanwaar de gewraakte informatie op het Internet wordt aangeboden een andersoortige (lees: ruimere) bevoegdheid toe te kennen dan de rechter van de plaats waar de informatie via het Internet haar schadelijke inwerking heeft. Beide fora – en zelfs het forum van

47. HvJ EG 7 maart 1995 (C-68/93, *Shevill c.s./Presse Alliance*), Jur. 1995, p. I-415, NJ 1996, 269 (ThMdB), AA 1995, p. 880 (PV).

de woon- of vestigingsplaats van de aansprakelijk gestelde persoon – worden in gelijke mate geconfronteerd met het feit dat een Internet-uiting op hetzelfde moment in vele landen effect sorteert – het in § 38 genoemde wereldwijde bereik van het Internet –, terwijl de vraag naar de aansprakelijkheid daarvoor telkens per land naar het lokale recht zal moeten worden beantwoord, dit laatste op basis van de in onderdelen B en C van hoofdstuk VII bepleite *lex-protectionis*aanknopning. Ik zie slechts twee uitwegen.

Het ene alternatief is hierin gelegen dat de rechter van ieder land – *Handlungsort*, *Erfolgsort* dan wel woon- of vestigingsplaats van de aansprakelijk gestelde persoon – slechts bevoegdheid toekomt ten aanzien van de lokale schadelijke gevolgen. Dit alternatief biedt het voordeel dat iedere rechter zijn eigen recht kan toepassen en zich niet behoeft te buigen over buitenlandse schade en buitenlands recht. Het nadeel is dat de gelaedeerde gedwongen wordt zijn zaak aan diverse nationale rechters voor te leggen en niet de mogelijkheid van concentratie wordt geboden.

Het andere alternatief bestaat hieruit dat de rechter van ieder land – *Handlungsort*, *Erfolgsort* dan wel woon- of vestigingsplaats van de aansprakelijk gestelde persoon – bevoegd wordt verklaard ten aanzien van alle schadelijke gevolgen, waar ook ter wereld gelokaliseerd. In deze benadering, die aansluit bij de rechtspraak van de Hoge Raad,⁴⁸ is het aan de gelaedeerde om zijn zaak te concentreren voor één nationale rechter – doorgaans de rechter van de woon- of vestigingsplaats van de gelaedeerde, mits zich hier ook een *Erfolgsort* bevindt – dan wel zijn zaak te verspreiden over diverse fora. Iedere geadieerde rechter zal vervolgens via de *lex-protectionis*regel aanknopen aan zijn nationaal recht en, naar gelang van de buitenlandse inwerking van de Internet-gedraging en de mate waarin de gelaedeerde ook de buitenlandse schadelijke gevolgen in zijn actie betreft, aan een of meer buitenlandse rechtsstelsels.

Ik opteer voor het laatste alternatief. In de eerste plaats is een

48. HR 24 november 1989 ('Lasdieselaggregaten'), NJ 1992, 404 (DWFV), BIE 1991, 23; HR 21 februari 1992 ('Barbie'), NJ 1993, 164 (JIS), BIE 1993, 65, IER 1992, 24 (AAQ). Zie, over deze rechtspraak, M.V. Polak, *Civiele sancties in het internationale geval voor de Nederlandse rechter*, Studiedrinking 'Prof. Mr. J. Offerhaus', nieuwe reeks nr. 3 (1995) nr. 21.

ruime omvang van de rechterlijke bevoegdheid gunstig voor de gelaedeerde, vooral als deze dicht bij huis een 'wereldwijd' bevoegde rechter kan vinden. Daarnaast meen ik dat de aansprakelijk gestelde persoon, gegeven het voor hem voorzienbare wereldwijde bereik van zijn Internet-gedraging, niet wordt geconfronteerd met een exorbitant forum: hij kan en moet zich realiseren dat hij voor zijn Internet-uiting in ieder land ter wereld voor de civiele rechter ter verantwoording kan worden geroepen. Ten slotte behoeft een ruime omvang van de rechterlijke bevoegdheid geen onoverkomelijke problemen voor de Nederlandse rechter op te werpen. Ik ga ervan uit dat de 'aannemelijkmakingsverplichting' en het 'gelijkheidsvermoeden' (zie § 41) wel de scherpe kantjes van de lex-protectionisregel zullen afslipen en dat de Nederlandse rechter in de praktijk vaak Nederlands recht zal kunnen toepassen. Dit neemt niet weg dat er complicaties kunnen optreden als de Nederlandse rechter een Internet-gedraging (naar Nederlands en/of buitenlands recht) onrechtmatig acht en een sanctie, zoals een gebod tot rectificatie of een verbod op verdere Internet-verspreiding, wil opleggen. Dit laatste aspect komt in hoofdstuk IX aan de orde.

59. Waartoe leidt het vorenstaande in casus B en C? In casus B is de Nederlandse rechter bevoegd op grond van de vestigingsplaats van Stichting S hier te lande. In casus C steunt de bevoegdheid van de Nederlandse rechter op de schadelijke gevolgen van de Internet-gedraging van Maatschappij M die zich rechtstreeks (mede) in Nederland manifesteren. In beide gevallen is de rechterlijke bevoegdheid niet beperkt tot de schadelijke inwerking in Nederland, maar kan zij alle schadelijke gevolgen bestrijken, waar ook ter wereld gelokaliseerd. Voor de buitenlandse rechter geldt, mutatis mutandis, hetzelfde. In ieder land waar de Internet-gedraging rechtstreekse schade veroorzaakt, ontstaat een algemene bevoegdheid voor de plaatselijke rechter. Het is aan de overheid van Satania en Filmbedrijf F, als eisende partijen, om te kiezen in het brede spectrum gelegen tussen – aan het ene uiteinde – concentratie van het wereldwijde geval bij één rechter en – aan het andere uiteinde – inschakeling van telkens een nationale rechter per lokaal onderdeel van het wereldwijde geval.

IX. DE ERKENNING EN TENUITVOERLEGGING

60. In dit hoofdstuk wijd ik een enkel woord aan de derde vraag van IPR die ik in hoofdstuk I opwierp, te weten: welke betekenis heeft een rechterlijke uitspraak in een Internet-geschil in een andere rechtsorde? Zoals ik mij in hoofdstuk VIII beperkte tot de internationale bevoegdheid van de overheidsrechter, concentreer ik mij hier op de erkenning en tenuitvoerlegging van uitspraken van overheidsrechters. De betekenis van arbitrale uitspraken, inclusief de beslissingen van de nog te installeren judex Internet (zie hoofdstuk V), laat ik onbesproken.

Voor de hier centraal staande materie van de erkenning en tenuitvoerlegging gelden, mutatis mutandis, de opmerkingen die ik in het vorige hoofdstuk maakte ten aanzien van de vaststelling van de bevoegde rechter in Internet-geschillen. Uitgangspunt is dat de bestaande regels van IPR, die niet speciaal voor het Internet zijn geschreven, uitkomst zullen moeten bieden. Vervolgens kan worden vastgesteld dat deze regels primair in verdragen, met name de in § 55 genoemde EEX en EVEX, en subsidiair in het nationaal procesrecht – voor Nederland in het Wetboek van Burgerlijke Rechtsvordering – zijn te vinden. Ten slotte valt te verwachten dat deze regels voor een belangrijk deel ook in een Internet-context zullen kunnen functioneren. Zo zal in casus A van hoofdstuk II de (on)mogelijkheid van erkenning en tenuitvoerlegging in Occidentie van een uitspraak van de Nederlandse rechter ten gunste van Burger B kunnen worden onderzocht aan de hand van de 'gewone' IPR-regels inzake erkenning en tenuitvoerlegging van Occidentie. Wederom laat ik dergelijke 'gewone' regels terzijde en concentreer ik mij op de 'Internet-gevoeligheid' van de materie.

61. Op het terrein van de erkenning en tenuitvoerlegging ontwaar ik slechts één 'Internet-gevoeligheid', maar wél een zeer belangrijke. Deze hangt samen met het eerste in § 38 genoemde wezenskenmerk van het Internet, te weten het wereldwijde bereik van het Internet en de onmogelijkheid van compartimentering. In de vorige hoofdstukken bleek al dat dit wezenskenmerk belangrijke gevolgen heeft op het terrein van de delictuele aansprakelijkheid voor Internet-uitingen, zowel voor de kwestie van het toepasselijke recht als voor de vraag naar de bevoegde rech-

ter. Ook voor het onderwerp van de erkenning en tenuitvoerlegging is het wereldwijde bereik en de non-compartmentering van het Internet van betekenis. Zoals een Internet-uiting zich niet tot een land of een groep landen beperkt, blijft een rechterlijke uitspraak over deze uiting niet tot het land van de rechter beperkt. De Nederlandse rechter die zich bevoegd acht om kennis te nemen van een delictuele vordering ten aanzien van een Internet-uiting en deze uiting met toepassing van Nederlands en/of buitenlands recht onrechtmatig acht, spreekt met de sancties die hij in zijn vonnis opneemt – schadevergoeding, gebod tot rectificatie, verbod tot verdere verspreiding van de aangeboden informatie – niet slechts recht binnen en ten behoeve van het Nederlandse rechtssysteem, maar binnen en ten behoeve van alle nationale rechtssystemen. Zijn sancties hebben geen territoriale, maar universele reikwijdte.

Voor beoefenaars van het IPR is de universele reikwijdte van rechterlijke uitspraken geen nieuws. Zij zijn vertrouwd met de idee dat rechterlijke uitspraken in beginsel wereldwijd effect pretenderen, tenzij de rechter zijn uitspraak uitdrukkelijk of stilzwijgend beperkt tot een of meer landen of zo'n beperking voortvloeit uit de aard van de litigieuze materie. Bovendien weten IPR-beoefenaars dat deze wereldwijde geldingspretentie niet in strijd is met de volkenrechtelijke uitgangspunten ten aanzien van de jurisdictie van soevereine Staten. Mijn summiere schets in hoofdstuk IV wees immers uit dat het volkenrecht slechts verbiedt dat een Staat executiemaatregelen op het grondgebied van een andere Staat treft en daarvan is hier geen sprake. De vraag of en, zo ja, in hoeverre een rechterlijke uitspraak gewezen in de ene Staat, voor erkenning en tenuitvoerlegging in de andere Staat in aanmerking komt, is en blijft immers onderworpen aan het IPR van laatstgenoemde Staat. Anders gezegd: de rechter van iedere Staat mag als wereldrechter optreden, maar evenzo mogen alle andere Staten hun grenzen sluiten voor de import van een buitenlandse rechterlijke uitspraak.⁴⁹

Het Internet introduceert op dit punt 'slechts' iets nieuws door zijn 'alles-of-niets'-karakter. Een rechter die wordt geadieerd met een vordering tot rectificatie van een Internet-uiting kan slechts kiezen tussen twee uitersten: afwijzing van het gevorderde – het

49. Zie, in het algemeen, Polak, *supra* noot 48, nr. 21-22.

'niets' – en toewijzing van de gevorderde sanctie, hetgeen per definitie tot wereldwijde gevolgen leidt – het 'alles'. De tussenweg van de geografische beperking van de toewijzende rechterlijke uitspraak tot het land van de rechter en/of enkele andere landen is hier niet begaanbaar, omdat de veroordeelde partij niet bij machte is haar Internet-uiting te compartimenteren. Naleving van het rechterlijk oordeel leidt noodgedwongen tot wereldwijde gedragsaanpassing.

Bij het vorenstaande teken ik aan dat dit alles-of-niets-dilemma uitsluitend praktische consequenties heeft voor rechterlijke uitspraken die een gebod of een verbod inhouden. Immers, naleving van een rechterlijk gebod of verbod door de veroordeelde partij vergt niet slechts aanpassing van de Internet-gedraging binnen het rechtssysteem van de rechter, maar aanpassing van de 'one and only' Internet-gedraging. Bij een rechterlijke uitspraak die tot een schadevergoedingsverplichting leidt, doen dergelijke praktische consequenties zich niet voor. De veroordeelde partij wordt hier niet gedwongen haar wereldwijde gedrag aan te passen, maar kan ervoor kiezen haar Internet-gedraging voort te zetten tegen betaling van schadevergoeding.

De rechter die wordt geadieerd in Internet-zaken, dient zich bewust te zijn van zijn taak als wereldrechter én zich rekenschap te geven van de mogelijke alles-of-niets-gevolgen van zijn bemoeienis met het Internet. Rechtspreken in Internet-geschillen is wereldwijd rechtspreken, hetgeen dwingt tot een zorgvuldige afweging van alle betrokken belangen bij de beantwoording van de vraag of de door de eisende partij gevorderde sancties kunnen worden toegewezen. Aangenomen dat de eisende partij in beginsel in haar recht staat, mag toewijzing van de gevorderde sancties geen automatisme zijn. De rechter dient zich af te vragen of de gevorderde sancties ook passend zijn in de wereldwijde context van het Internet. Voor dit fenomeen heb ik – in het kader van het pre-Internet IPR – de term 'sanctio-non-convenienstoets' geïntroduceerd.⁵⁰ In de Internet-context kan een dergelijke toets tot de slotsom leiden dat sommige sancties – bijvoorbeeld schadevergoeding vanwege belediging of vanwege inbreuk op rechten van intellectuele en industriële eigendom – wél, maar andere sancties – bijvoorbeeld een gebod tot beëindiging van de gewraakte gedraging – níet pas-

50. Polak, *supra* noot 48, nr. 29-30 en 35-36.

send zijn. De internationale context van het Internet vereist dat de rechter een grotere discretionaire bevoegdheid ten aanzien van de door hem op te leggen sancties bezit dan hem in zuiver nationale gevallen toekomt.

62. Het vorenstaande is met name van belang in casus C van hoofdstuk II. In dit geval wordt de Nederlandse rechter, die – zo bleek in hoofdstuk VIII – geacht kan worden internationale bevoegdheid te bezitten, geconfronteerd met een gedraging van Maatschappij M die in sommige rechtssystemen, waaronder Nederland, naar het lokale recht onrechtmatig is, maar in andere rechtssystemen volgens het daar geldende recht rechtmatig is. Aangenomen dat de rechter tot de conclusie komt dat deze gedraging in ieder geval in Nederland onrechtmatig is en derhalve tot aansprakelijkheid van Maatschappij M jegens Filmbedrijf F leidt, dient hij zich te buigen over de op te leggen sancties. Is het passend dat Maatschappij M wordt verboden de film via het Internet aan te bieden? Een dergelijk verbod zou wereldwijd effect sorteren, dus ook in de landen waar Maatschappij M geen inbreuk op het auteursrecht van Filmbedrijf F maakt. De door mij bepleite sanctio-non-convenienstoets zou ertoe kunnen leiden dat deze sanctie niet wordt opgelegd. In plaats daarvan zou de rechter kunnen beslissen dat Filmbedrijf F jegens Maatschappij M 'hooguit' aanspraak kan maken op schadevergoeding voor iedere inbreuk die plaatsvindt in de landen waar de gedraging van Maatschappij M onrechtmatig is.

X. SAMENVATTING EN CONCLUSIE

63. Mits ik alle details en nuances weglaat, kan ik het vorenstaande kort samenvatten en tot een nog kortere conclusie komen.

64. In hoofdstuk I stelde ik dat het Internet voor privatisten eerst en vooral vragen van IPR opwerpt. Het betreft de drie vragen van IPR die ook rijzen in 'gewone' grensoverschrijdende gevallen van privaatrechtelijke aard: welk recht is van toepassing, welke rechter is bevoegd en welke betekenis heeft een rechterlijke uitspraak in een andere rechtsorde?

Deze stelling over IPR en Internet heb ik in hoofdstuk II geïllustreerd aan de hand van drie Internet-casus. Deze casus lagen op het terrein van het overeenkomstenrecht (casus A), het recht inzake de onrechtmatige daad (casus B) respectievelijk het recht inzake de intellectuele en industriële eigendom en de ongeoorloofde mededeling (casus C).

In hoofdstuk III stipte ik de invloed van het publiekrecht op de hier centraal staande materie van privaatrecht aan. Ik sprak over de vrijheid van meningsuiting en de vrijheid van informatievergaring als 'vaste gegevens', die op grond van de functie van het IPR – te weten: de toedeling van grensoverschrijdende casus aan rechtsstelsels – verder onbesproken kunnen blijven.

Vervolgens onderzocht ik in hoofdstuk IV wat het volkenrecht bepaalt omtrent de jurisdictie van Staten ten aanzien van grensoverschrijdende gevallen van privaatrechtelijke aard. Het bleek dat het volkenrecht de Staten op privaatrechtelijk gebied veel vrijheid laat en slechts hun uitvoerende jurisdictie aan banden legt. Het is daarmee aan iedere Staat om te bepalen in hoeverre zijn privaatrecht mede grensoverschrijdende Internet-casus bestrijkt.

In hoofdstuk V liet ik het eenvormig privaatrecht de revue passeren. Op welke premisse berust de roep om een lex en een judex Internet en is deze premisse deugdelijk? En aangenomen dat de premisse deugdelijk wordt bevonden, is de totstandkoming van een lex en een judex Internet dan een haalbare kaart? Ik kwam tot de conclusie dat lex en judex Internet hersenschimmen noch reële voorstellen zijn, maar iets daartussen. Belangrijker was de constatering dat zolang én voor zover zich geen algemeen aanvaarde lex en judex Internet aandienen, het nationaal privaatrecht en de nationale overheidsrechtspraak hun betekenis behouden voor de regulering van Internet-casus.

Om welk nationaal privaatrecht en om welke nationale overheidsrechtspraak gaat het nu bij Internet-casus? Beantwoording van deze vraag is de functie van het IPR. In een wereld van rechtsverscheidenheid is het IPR een noodzakelijk kwaad, bekende ik in hoofdstuk VI. Als onderdeel van het nationaal privaatrecht varieert het IPR van Staat tot Staat, maar de roep om internationale uniformiteit is sterk. Bij de ontwikkeling van IPR-regels voor het Internet dient het streven dan ook gericht te zijn op een resultaat dat in een wereldrecht niet misstaat.

Hoofdstuk VII was gewijd aan de kwestie van het toepasselijke recht. Ik onderzocht of de bestaande verwijzingsregels zonder meer of met enige wijzigingen en aanvullingen geschikt zouden zijn om in de drie Internet-casus tot aanvaardbare resultaten te komen. Voor het terrein van het overeenkomstenrecht bleek het EVO een bruikbaar regelbestand, zij het dat de consumentenovereenkomst die via het Internet tot stand komt, wel om een wijziging lijkt te vragen. Bij de onrechtmatische daad diende zich een keuze aan tussen de *lex originis*- en de *lex protectionis*-aanknoping. Ik koos voor de laatste vanwege haar realistische en slachtofferbeschermende karakter. Op het terrein van de intellectuele en industriële eigendom en de ongeoorloofde mededinging bleek deze *lex protectionis*-aanknoping eveneens bruikbaar.

In hoofdstuk VIII besteedde ik aandacht aan twee gebieden met betrekking tot de internationaal bevoegde rechter waarbinnen de 'gewone' bevoegdheidsregels niet zonder meer functioneren. Voor consumentenovereenkomsten bepleitte ik een beperking van de forumkeuzevrijheid. Op het terrein van de aansprakelijkheid uit onrechtmatige daad en bij inbreuk op rechten van intellectuele en industriële eigendom achtte ik wijziging van de jurisprudentie noodzakelijk, om te bereiken dat de rechter van ieder land, waar zich een Internet-gedraging manifesteert, bevoegd is om zich uit te spreken over alle schadelijke gevolgen, waar ook ter wereld gelokaliseerd.

Ten slotte wijdde ik in hoofdstuk IX een enkel woord aan een kwestie van erkenning en tenuitvoerlegging van rechterlijke uitspraken. De wereldwijde werking van het Internet en de onmogelijkheid om Internet-uitingen te compartimenteren, vergen van de rechter een zorgvuldige afweging alvorens hij sancties oplegt. Welke sanctie wél en welke níet passend is, dient in een *sanctio-non-convenienstoets* te worden bepaald.

65. Kort en klaar. Het Internet creëert nieuwe en ingewikkelde problemen van privaatrechtelijke aard. Bij gebreke van een bruikbaar alternatief, dat noch in het volkenrecht noch in het eenvormig privaatrecht voor het oprapen ligt, zit er weinig anders op dan deze problemen met behulp van het IPR op te vangen. Gelukkig is geen van de problemen die het Internet creëert zo nieuw en zo ingewikkeld dat het bestaande IPR, met hier en

daar een wijziging of aanvulling, er niet mee uit de voeten kan. Het IPR moet én kan blijven dienen als vangnet voor het grensoverschrijdende verkeer, ook in het tijdperk van het Internet.

DEEL III

INTERNET EN STRAFRECHT

preadvies prof. mr. Y. Buruma

INHOUD DEEL III

1	INLEIDING	123
2	BEGRIPPEN	124
	2.1 Statische of dynamische interpretatie van 'informatie'	125
	2.2 Het Internet als publicatiemedium of communicatiemedium	128
	2.3 Het Internet als Cyberspace of als instrument van territoriale gebruikers	130
3	MATERIEEL STRAFRECHT	132
	3.1 Inleiding	132
	3.2 Financiële benadeling van individuele rechts-subjecten	135
	3.3 Aantasting van de informationele privacy en integriteit	140
	3.4 Uitings- en verspreidingsdelicten	151
	3.5 Aantasting van de infrastructuur en de nationale veiligheid	160
4	INTERNATIONAAL STRAFRECHT	163
	4.1 Materieelrechtelijk jurisdictierecht	164
	4.2 Formeelrechtelijke internationale aspecten van het Internet	167
5	FORMEEL STRAFRECHT	171
	5.1 Opsporing van strafbare feiten	172
	5.2 Encryptie en anonimiteit	176
	5.3 Bewijsgaring	181

6	CONCLUSIE	188
7	AANGEHAALDE WETSONTWERPEN	191

Deel III

1 INLEIDING

Toen de eerste atoombom in Alamogordo, New Mexico explodeerde in juli 1945, riep een officier: 'Good God! ... the long haired boys have lost controll!' Hij drukte het vermoeden uit, dat technologie niet langer louter een hulpmiddel of cultuuruiting van de denkende mens is, maar een nauwelijks in de hand te houden systeem dat zich relatief autonoom van de samenleving ontwikkelt. Relatief autonoom: de grenzen van de technologische mogelijkheden worden immers niet (alleen) vanwege een interne logica van de techniek verlegd, maar (ook) vanwege de maatschappelijke vraag.² Uiteraard kunnen we niet steeds de neveneffecten van technologische veranderingen doorzien, of elk alternatief gebruik voorspellen, laat staan dat we precies kunnen voorzien hoe een technologie onze mentale habitus zal veranderen.³ Dat konden we niet toen het gebruik van buskruit en boekdrukkunst werd ontwikkeld; dat kunnen we ook niet in de eerste eeuw van het bestaan van waterstofbom en Internet.

Internet maakt ook een relatief autonome ontwikkeling door: de hier te behandelen vraag is op welke punten het straf- en strafprocesrecht moeten worden aangepast vanwege de komst van het Internet, opdat we voorkomen dat de technische mogelijkheden ongewenste maatschappelijke gevolgen hebben. We denken daarbij nu misschien het eerst aan de problematiek van de computercriminaliteit in enge zin.⁴ We zullen er echter snel aan moeten wennen dat afspraken over afleverplaatsen van

1. Geciteerd in M. Berman, *All that is solid melts into air*, Harmondsworth 1988 (1982): 37.
2. Zie ook H. Achterhuis e.a., *Van stoommachine tot cyborg; denken over techniek in de nieuwe wereld*, Amsterdam 1997.
3. Zie voor Internet de beroemde speculaties van N. Negroponte, *Digitaal leven*, Amsterdam 1996 (1995); en M. Dertouzos, *What will be*, Harper Edge 1997.
4. Daarover in algemene zin II. Franken, H.W.K. Kaspersen en A.H. de Wild (red.), *Recht en computer*, Deventer 1997; Chr. II. van Dijk en →

drugs via het net worden gemaakt, op het net gevestigde casino's worden bezocht en boekhoudingen van criminele groepen ergens in het virtuele domein worden verstopt. Maar niet alleen aan de boeven, ook aan politie en justitie biedt het Internet mogelijkheden die niet noodzakelijk geaccepteerd moeten worden. De uiteindelijke betekenis van het Internet voor het straf- en strafprocesrecht kan op dit moment niet worden overzien, maar geprobeerd zal worden drie principiële vragen te beantwoorden aan de hand van de huidige stand van de techniek. Ten eerste de materieelrechtelijke vraag of het Internet noopt tot nadere strafbaarstellingen; ten tweede of het Internet noopt tot nieuwe internationaal-strafrechtelijke afspraken; ten derde of het Internet noopt tot nadere regeling van de bevoegdheden met het oog op opsporing en vervolging.

De beantwoording van die vragen wordt sterk beïnvloed door de manier waarop tegen het Internet wordt aangekeken – om het wetenschapstheoretisch te zeggen: van het paradigma waarmee over het Internet wordt gedacht. In hoeverre wordt er uitgegaan van een overeenkomst tussen wat in de wereld-*on-line* gebeurt en wat er gebeurt in de wereld-'*off-line*'? Beschouwen we het net primair als communicatiemiddel (denk aan e-mail gebruikers) of primair als publicatiemiddel (denk aan *home-pages*)? Redeneren wij vanuit het territorium-gebonden straf(proces)recht of vanuit de niet door grenzen gebonden '*cyberspace*' – de Mare Liberum van de nieuwste tijd? Deze vragen die de uitgangspositie van ons denken bepalen worden nader uitgewerkt, voordat op de drie eerder genoemde punten wordt ingegaan.

2 BEGRIPPEN

Voordat we zinvol over het Internet kunnen spreken, moeten we stilstaan bij de paradigma's die ons denken erover bepalen. Een paradigma is een geaccepteerd patroon of model van denken, waar theorievorming en probleemoplossing als het ware vanzelf uit voortvloeit. Normale wetenschap houdt zich bezig met die theorievorming en probleemoplossing en het komt zelden voor

→ J.M.J. Keltjens, *Computercriminaliteit*, Zwolle 1995; en Commissie Computercriminaliteit, *Informatietechniek & Strafrecht*, Den Haag 1987.

dat een wetenschapper over het paradigma zelf na hoeft te denken.⁵ Dat neemt niet weg dat ook in het strafrecht het paradigma de agenda beïnvloedt waarmee de verdachte wordt gezien. Beschouwt u de drugsverslaafde als typische verdachte, dan komt u uit op andere vragen dan wanneer de belastingontduiker of de georganiseerde misdaad uw invalshoek bepaalt. Het gaat niet om goed of fout; hooguit is het ene paradigma in de ene context vruchtbaarder te noemen dan het andere.

2.1 *Statische of dynamische interpretatie van 'informatie'*

De neiging bestaat 'informatie' als een statisch begrip op te vatten: als 'iets' dat een zekere waarde vertegenwoordigt en dat als ware het een pakketje wordt doorgegeven van de een aan de ander. Zo kunt u menen dat een foto informatie geeft over een bepaalde gebeurtenis: de foto legt de gebeurtenis vast en die foto wordt vervolgens bijvoorbeeld via het Internet verspreid. In deze opvatting is er slechts in zeer beperkte mate een verschil tussen de 'echte' wereld en de wereld van de informatiestromen; fraude of kinderporno met papier en fraude of kinderporno via het Internet zijn even kwalijk. Zo gezien is het uitgangspunt van de Europese Commissie logisch, dat wat *off-line* illegaal is ook *on-line* illegaal is.⁶ In deze opvatting is het onderscheid tussen gegevens en informatie zinvol. Dat laat zich als volgt toelichten. Een waarnemer ervaart een gegeven dat er zojuist niet was (*bijvoorbeeld u ziet een onverwachte foto van een meisje op het Internet*). Dat gegeven wordt in het waarnemingsapparaat – de hersens, de computer – informatie omdat het bij die waarnemer een (marginale) verandering teweeg brengt: het wordt ingepast in een bestaand kader, het wordt (tijdelijk) opgeslagen in een geheugen en/of leidt tot een reactie. (*De ontvangst van de foto wordt opgeslagen in een stukje geheugen van de computer, en vanuit uw referentiekader besluit u de foto met een bericht te zenden aan de politie zonder dat u daarmee vergeet wat u zag; voor de politie heeft u de foto verrijkt met de toevoeging in het bericht dat u geschokt was door de foto*). Het proces van inpassing,

5. Th. Kuhn, *The Structure of Scientific Revolutions*, Chicago 1970 en 1962.

6. Mededeling van de Commissie van de Europese gemeenschappen van 16 oktober 1996, *Illegale en schadelijke inhoud op het internet*, (COM(96) 487 def. p. 4.

opslag en/of reactie maakt het gegeven tot informatie. Een andere waarnemer ontleent wellicht andere informatie aan hetzelfde gegeven.

Even verrassend als voor de natuurkundigen die licht altijd een deeltjeskarakter hadden toegedicht en die werden geconfronteerd met de idee dat licht ook als golf kan worden beschouwd, is dan de dynamische benadering van informatie.⁷ In belangrijke mate kan in deze opvatting het voorgaande worden gevolgd, maar met dien verstande dat men niet poneert dat er ooit contextloze en historieloze gegevens zijn. Elk gegeven heeft een historie en een context en het besef daarvan onderstreept de mogelijkheid dat een gegeven zelf al betekenisvol is: dat hangt niet alleen van de waarnemer af (zoals een jurkje dat Marilyn Monroe droeg zelf meer waard is dan een ander jurkje van 40 jaar geleden; en zoals een aandeel van een beursgenoteerd bedrijf vandaag in Hong Kong een andere waarde heeft dan gisteren in Amsterdam).⁸ Het onderscheid tussen gegevens en informatie wordt in die zienswijze niet onmogelijk maar minder zinvol. Door de interactie met de ontvanger reproduceert informatie zichzelf tot nieuwe, al dan niet veranderde gegevens die weer in het referentiekader van andere ontvangers als informatie worden gewaardeerd, tenzij de informatiestroom ophoudt. (*De politie legt de foto voor aan de officier van justitie als bewijsmateriaal*). Informatie is zo gezien een relationeel proces dat plaatsvindt in een aaneenschakeling van zenders en ontvangers. Daarbij laat de informatie sporen na bij degene die hem ontvangen en doorgegeven heeft en verandert door de verspreiding van de 'gegevens' de informationele waarde ervan.⁹ Deze benadering van informatie heeft juridisch relevante gevolgen. Een daarvan betreft de mogelijkheid om informatie af te pakken: als bepaalde gegevens worden gekopieerd verliest de oorspronkelijke houder

7. J.P. Barlow, *Selling Wine without Bottles*, in P. Ludlow (ed.), *High Noon on the Electronic Frontier*, MIT Press 1996: 9-34; ook in de *United Nations Manual on the prevention and control of computer-related crime*, *International Review of Criminal Policy*, nr. 43/44 (24 januari 1995) wordt aldus geredeneerd.

8. Uiteindelijk gaat het om een ontologische-cum-epistemologische vraag over de aard en de kenbaarheid van het reël bestaan (bestaat een natuurwet; bestaat informatie – of zijn het slechts concepten?)

9. Ik bedoel het veel algemener, maar de algemene stelling wordt bevestigd door Koers: noot 57, de digitale sporen die het gebruik van Internet nalaat.

niet de feitelijke macht over het gegeven, maar kan dat gegeven wel informatie gaan opleveren voor anderen. Volgens de Hoge Raad is het niet-verliezen van het gegeven reden bij uitstek om gegevens niet als goed te beschouwen.¹⁰ Maar dat roept wel de vraag op, of de oorspronkelijke rechthebbende of degene op wie de gegevens betrekking hebben een eigen – nieuw te formuleren – recht hebben ten aanzien van de informatie die het gegeven uitstraalt of oplevert voor derden.

Dat brengt me op de waarde van informatie. Deze wordt enigszins anders bepaald dan de waarde van een goed: nabijheid in tijd en de mate van verrijking zijn waardebepalend. Ik bedoel daarmee dat een informatieel product doorgaans meer waard is naarmate het dichter bij het moment van het genereren van de informatie ligt (het live concert is meer waard dan de perfecte cd-opname ervan; de eigen waarneming is meer waard dan de *de auditu*). Soms wordt informatie door degenen langs wie ze zich voortbeweegt verrijkt. De primeur van de journalist is doorgaans meer waard dan de achtergrondanalyse, maar soms krijgt de primeur pas zijn waarde door een gedegen beschouwing erover. De waarde van een informatieel pakketje (om de term uit het andere paradigma te gebruiken) is in deze benadering lastig te bepalen: sommige informatie (of eigenlijk: sommige gegevens) zijn voor een persoon van enorme waarde (bijvoorbeeld omdat hij de bron is en ze geheim wil houden); voor ieder ander zijn de gegevens vrijwel waardeloos, tenzij ze door een specifiek referentiekader verrijkt worden (bijvoorbeeld van de zanger die weet dat laatstgenoemde bron chantabel is vanwege die informatie). Dat informatie een relatieve waarde heeft is in dit paradigma begrijpelijker dan in het eerste, waarin toch steeds het gegeven (waarvan informatie wordt afgeleid) als een klomp goud wordt beschouwd; degenen die over patenten onderhandelen kunnen waarschijnlijk goed uit de voeten met het 'pakketjes-paradigma'. Bij de bescherming van gegevens gaat het evenwel niet alleen om het economisch belang van de rechthebbende, maar ook om het belang van de informatiele lading voor degene op wie de gegevens betrekking hebben.

Een derde gevolg van dit paradigmatisch concept van informa-

10. HR 3 december 1996, NJ 1997, 574 m.nt. 't II.

tie, is dat we er het tijd/ruimteprobleem mee kunnen inzichtelijk maken: a) informatie (in bits) bevindt zich niet ergens, zoals goederen zich ergens bevinden; b) informatie past zich aan aan de omgeving en plant zich in belangrijke mate autonoom voort. Strafrechtelijk kunnen we denken aan de vraag waar een strafbaar feit op het net plaatsvindt (zie 4.1). Maar ook aan de vraag wanneer een strafbaar feit plaatsvindt: men dient in dit verband onderscheid te maken tussen *real time* (of: onvertraagde) verwerking van gegevens als een reactie op een buiten het systeem plaatsvindende gebeurtenis in overeenstemming met de door die gebeurtenis opgelegde tijdeisen en vertraagde verwerking. Wanneer een van de vier grote infectiefamilies – de logische bom, een worm, een virus of een trojaans paard – is losgelaten op een computersysteem, doet de schade zich doorgaans pas na geruime tijd voelen. De vraag is dan op welk moment er eigenlijk wordt vernield (art. 350a Sr). Als je de informatie met het trojaanse paard naar binnen brengt of als dat paard bijvoorbeeld reageert op de (externe) prikkel waardoor de schadelijke inhoud vrijkomt? Misschien was het inbrengen een onschuldige grap toen het paard werd binnengebracht, maar blijkt het inmiddels heel schadelijk.

2.2 *Het Internet als publicatiemedium of communicatiemedium*

Het tweede paradigmatisch relevante punt is of het Internet moet worden beschouwd als publicatiemedium of als communicatiemedium. De Europese Commissie zegt hierover: 'Deze constante overschakeling tussen publicatie en privécommunicatie – twee communicatievormen waarop traditioneel zeer verschillende rechtsstelsels van toepassing zijn – vormen een van de grootste uitdagingen voor de Internet-regelgeving.'¹¹ Men hoeft slechts te denken aan de nadruk op enerzijds de (pers)vrijheid en anderzijds de privacy.

Wordt het Internet als publicatiemedium beschouwd dan is belangstelling voor de rol van de *providers* als 'quasi-uitgevers' voor de hand liggend, evenals belangstelling voor de problematiek van de vrije toegang tot en het delen van informatie. Overigens

11. Mededeling van de commissie van 16 oktober 1996, *Illegale en schadelijke inhoud op het Internet*, com(96) 487 def, p. 8 en 9.

is de *provider* ook als quasi-bibliothecaris op te vatten, of als quasi tv-station en dat roept weer andere vragen en oplossingen op. In het paradigma van het Internet als publicatiemedium leveren de uitings- en verspreidingsdelicten vragen op. Wordt het net als communicatiemiddel beschouwd, dan is belangstelling voor de mogelijkheden van bescherming van informatie (bijvoorbeeld via de zgn. *descriptie*) voor de hand liggend. In dit paradigma rijst de vraag of respectievelijk op welke basis communicatie via het Internet kan worden onderschept.

Beide benaderingen zijn legitiem. Een ruwe handreiking wordt geboden door de verschillende gebruiksvormen van het Internet te plaatsen in een matrix:¹²

		Sender	
		public	private
Receiver	public	audience groups bulletin boards mailing lists news groups	target groups in marketing advertising & interactive broadcast
	private	consultation groups in video- & audio-on- demand	discussion lists email-groups mud's; IRC's teleconferencing

Bezien we de matrix dan is dadelijk voorstelbaar dat zich soms conflicten voor zullen doen tussen de benadering vanuit het fundamentele recht van privacy en dat van de vrijheid van meningsuiting. Is er in een *Multi User Dungeon* (MUD), of in een *Inter Relay Chatgroep* (IRC) nu sprake van intieme conversatie waarop vooral art. 8 EVRM van toepassing is, en/of is een daar gedane uitlating tevens op te vatten als een in het openbaar geuite meningsuiting waarop art. 10 EVRM van toepassing is? Vrije me-

12. J.A.G.M. van Dijk, *The Reality of Virtual Communities*, in Jo Groebel (ed), *New Media Developments*, Amsterdam 1997 (TIC 1): 46.

ningsuiting van degene die de tekst plaatst of privacy van degene op wie de tekst betrekking heeft? Uiteraard kunnen zich dergelijke problemen ook voordoen met betrekking tot de (niet-interactieve) massamedia. Het verschil is kwantitatief: als iedereen dit soort zaken die betrekking hebben op het privé-leven van anderen op het net kan zetten, dan wordt de kans groter dat aldus ook zinloze (niet door de gronden van de vrijheid van meningsuiting gelegitimeerde) schade zal ontstaan. Aan de andere kant zou het wonderlijk zijn om alleen de grote uitgevers te laten profiteren van een fundamenteel mensenrecht, juist als het voor iedereen daadwerkelijk mogelijk wordt zijn mening te laten horen.

2.3 Het Internet als Cyberspace of als instrument van territoriale gebruikers

Het derde paradigmatisch relevante punt is of men het Internet beschouwt als een domein dat men vanuit een bepaalde plaats en op een bepaald moment betreedt, of als een welhaast cindeloze ruimte – *cyberspace* – waarin allerlei activiteiten plaatsvinden. In het eerste geval legt men een relatie met territorium; in het tweede geval niet.

Op zich is het opmerkelijk dat we kunnen overwegen de territoriale notie los te laten. Recht en bestuur werden tot dusver in overwegende mate territoriaal gedefinieerd. Door het toenemende individuele bereik om niet alleen kennis te nemen van wat elders gebeurt maar daar ook heen te gaan, of via het Internet daar te handelen, verliest de staat haar karakter als een dwingend territoriaal en vanzelfsprekend kader van beslissingen. Sommigen – in het bijzonder de eerste generaties Internetgebruikers – zien dit met blijdschap aan. Zij beschouwen de gemeenschap die het Internet vormt als een rechtsorde in wording met haar eigen regels; of eigenlijk wordt vooral benadrukt dat het Internet ruimte biedt aan tal van belangengemeenschappen die niet aan geografische grenzen of aan tijd zijn gebonden. Discussie vergt geen eenheid van tijd en plaats. De optimist die vanuit deze paradigmatische invalshoek denkt, drukt vooral de hoop tot zelfregulering binnen het Internet uit (Netiquette e.d.) en wijst op de bescherming die de techniek zelf kan bieden (bijv. cryptografie als feitelijk betere beveiliging tegen inbreuken op de

privacy dan wetgeving;¹³ en filters die bezorgde ouders kunnen aanbrengen om hun kroost de blik op blote lichamen te besparen). De pessimist citeert Hobbes: ... what is life without the state, but solitary, poor, nasty, brutish and short'. Hij vraagt zich af, of het mogelijk is een regelsysteem te ontwikkelen, waardoor bijvoorbeeld moderatoren van nieuws- of discussiegroepen zich bevoegd en in staat weten om hinderlijke deelnemers te straffen en eventueel te verbannen; 'loading' noemt men dat in de kringen van MUD-gebruikers. Wat hier ook van zij, het illustreert dat – om met Donner te spreken – 'de erosie van de structurerende werking van tijd en ruimte' het vermogen tot ordening en zorg van de overheid aantast.¹⁴

Toch kan men ook vanuit het andere paradigma blijven redeneren. Het Internet kan wel worden beschouwd als vrije ruimte – vrije zee –, maar dat neemt niet weg dat de havens territoriaal zijn gebonden. De virtuele ruimte bestaat niet zonder aanknopingspunten in de *real world*. Voor de gebruikers geldt nationaal recht en voor de (vestigingen van) *providers* ook. Evenals in verband met de zee kunnen staten tot afspraken komen en wellicht op enkele kernpunten tot een supranationaal recht. Vooral op het vlak van rechtsmacht en internationale samenwerking zullen (nadere) afspraken moeten worden gemaakt.¹⁵ Daar is nog een extra reden voor.

Op dit moment vindt een proces van economische globalisering plaats: 70% van de wereldhandel is intra-industrie of intra-bedrijf.¹⁶ Activiteiten van bedrijven worden intern, maar internationaal geherstructureerd: in het ene land worden de poorten

13. Cryptografie is de tak van wetenschap die zich bezighoudt met de grondbeginselen, instrumenten en methoden voor het omzetten van gegevens ten einde de inhoud daarvan te verbergen, te voorkomen dat deze inhoud ongemerkt wordt gewijzigd of zonder toestemming wordt gebruikt (ontleend aan het Besluit van de Raad van 19 december 1994, Pb L 367/13). Daarbij wordt vooral gebruik gemaakt van encryptie, de procedure waarbij leesbare gegevens door middel van wiskundige bewerking (algoritmes) worden versleuteld in gecodeerde gegevens.
14. Wetenschappelijke Raad voor het Regeringsbeleid, Informatie en Telecommunicatie: public domain, notitie van 3 juni 1996.
15. Zowel de Organisation for Economic Co-operation and Development (OECD), de Raad van Europa als de Verenigde Naties hebben zich met de computer-gerelateerde misdaad beziggehouden; voor een summier overzicht United Nations Manual (1995).
16. W.H. Reinicke, *Global Public Policy*, Foreign Affairs, vol. 76/6: 127-138.

gesloten en in het andere wordt een nieuwe vestiging geopend. Deze integratie van verschillende nationale dimensies binnen één bedrijf wordt versterkt door het bestaan van allerlei vormen van *teleconferencing*, *intranetten* en wat niet al. De globalisering is haast niet mogelijk zonder geavanceerde vormen van informatie en communicatie; ze vormt een uitdaging met betrekking tot de interne soevereiniteit van staten. Voor zover internationale samenwerking in dit kader niet afdoende is, zou daarom kunnen worden gestreefd naar globale vormen van beleid en bestuur ten dezen, zoals die ook uitgeoefend worden door instellingen als de Wereldbank, het IMF, en (voor een deel van de wereld) de Nato. In een dergelijke samenwerkingsvorm kunnen ook public/private samenwerkingsverbanden worden aangegaan met het oog op de regulering van communicatie; met betrekking tot het Internet zouden staten zo'n verband kunnen aangaan met het *World Wide Web Consortium* (W3C) – dat sinds 1994 de webtechnologie ontwikkelt¹⁷ – en verder met organisaties van *providers*, maar ook met non-gouvernementele organisaties die zich bezig houden met de vrijheid van meningsuiting en/of de privacy, of anders de Internet Society (zie Koers 1.3) een zwaardere rol toedelen.

3 MATERIEEL STRAFRECHT

3.1 Inleiding

De Association Internationale de Droit Pénal greep in 1992 met haar aanbevelingen inzake computercriminaliteit als het ware terug naar het 19e eeuwse gedachtengoed over strafbaarstelling. Ze bepleitte de toepasselijkheid van de subsidiariteitseis, de nadruk op precisie en helderheid, alsmede de beperking tot opzettelijk handelen in dit domein.¹⁸ Met dat in het achterhoofd kun-

17. Zie www.w3.org/consortium; tal van bedrijven (van ABN-AMRO, via France Telecom, Microsoft en Reed-Elsevier tot Xerox Corporation) zijn er lid van; het wordt geleid door MIT Laboratory for Computer Science (USA), National Institute for Research in Computer Science and Control, INRIA (Frankrijk) en Keio University (Japan).

18. *Revue Internationale de Droit Pénal*, 1993 (64): 681-688, aanbevelingen 3-5.

nen we de vraag stellen of het Internet nieuwe vormen van schade, immoraliteit en/of risico oplevert, die niet beter langs andere dan strafrechtelijke weg kunnen worden tegengegaan en waartegen is op te treden zonder al te nadrukkelijk gebruik te maken van vage, gedelegeerde of bestuursafhankelijk geformuleerde bepalingen of 'functionele' manieren van toerekening? Daarbij moet onder ogen worden gezien, dat delicten die via het Internet kunnen worden gepleegd zeer verscheiden zijn. Door de toegenomen gebruikersvriendelijkheid van het Internet, is het profiel van de criminele gebruiker ervan veranderd. Het gaat niet meer louter om hoogbegaafde jongens die beginnen met het uithalen van streken en tenslotte misschien echte delicten plegen; in toenemende mate wordt het gebruik van elektronische bulletin boards en nieuwsgroepen door gewone georganiseerde misdadigers gesignaleerd.¹⁹ Het is m.i. niet zo zinvol om onderscheid te maken tussen gevallen waarin de computer zelf het object is van een delict; die waarin een computer wordt gebruikt; en die welke uitsluitend in de virtuele wereld kunnen plaatsvinden, zoals het zgn. *hacken*.²⁰ Dat onderscheid helpt hooguit eraan te herinneren, dat diefstal van (ram-geheugen)chips en andere onderdelen steeds vaker het object van diefstal worden; ze zijn veel waard en makkelijk te vervoeren en te verkopen.²¹ Maar de delicten waarmee die chips worden gekregen zijn toch gewoon diefstal ('*ram-ripping*'), beroving en zelfs gijzeling.

Bezien we dan wat tot nu toe vooral de nadruk kreeg in verband met computer- en Internetcriminaliteit, dan lag de nadruk aanvankelijk op fraude. Vervolgens ging rond 1990 de aandacht uit naar hackers.²² Behalve in Italië (1994) is het strafrechtelijk optreden tegen *software-piraterij* niet echt van de grond gekomen.

19. United Nations Manual (1995), para 37. Zo ook P. van Eecke, Criminaliteit in Cyberspace, Gent 1997.

20. R.C. MacKinnon, Punishing the Personat: Correctional Strategies for the Virtual Offender, in S.G. Jones, Virtual Culture, London 1997: 206-233.

21. D. Martin, La criminalité informatique, PUF 1997: 36-37 meldt dat in 1996 75 laboratoria alleen in Silicon Valley met dit doel werden beroofd. Zie ook TK 95-96, Aanhangsel 246.

22. Ik herinner aan Operation Sun Devil, waaraan twee jaar lang 150 federale agenten, talrijke andere officials, alsmede allerlei particuliere veiligheidsdiensten werkten om uiteindelijk een aantal jongens op te pakken. Zie J.P. Barlow, Crime and Puzzlement, in Ludlow (1996): 459-486.

Vanaf medio 1995 maakt de wereld zich druk om kinderporno-graphie.²³ En als ik het goed proef neemt inmiddels de zorg toe om spionage en (terroristische) aanvallen op de informatie-infrastructuur.²⁴

Om de aan de orde gestelde vraagstelling te onderzoeken zal nu op een aantal groepen delicten worden ingegaan. Daarbij wordt aangesloten op de hiervoor onderscheiden punten van paradigmatische betekenis en (daarmee op) de aard van de schade die de delicten teweeg brengen. Gaat men uit van informatie als 'pakketje' dan ligt het voor de hand de schade te bezien in termen van de min of meer vaste, economische waarde van dat pakketje: de financiële benadeling van individuele rechthebbende staat dan voorop. Gaat men uit van het meer dynamische beeld van informatie, dan ligt het voor de hand aandacht te besteden aan de betekenis van gegevens voor de bron of degene die het onderwerp ervan is: ik bespreek in dat licht de aantasting van de informationele privacy en integriteit. In beide gevallen gaat het om concreet aanwijsbare individuele benadeelden, die het slachtoffer worden van het 'wegnemen' van gegevens waar zij een recht op hebben. In het derde geval ontstaat de schade juist bij het publiek door de uiting of verspreiding van gegevens; wat er ook zij van de wijze van verkrijging, de openbaarmaking is zelf ontoelaatbaar. In het vierde geval gaat het niet om het wegnemen van economische waarde of informationele waarde, noch om bezwaarlijke verspreiding, maar om aantasting van het communicatiesysteem of andere publiek relevante systemen: hier gaat het om de aantasting van de infrastructuur en de nationale veiligheid. Aldus wordt in iets algemenere termen de ontwikke-

23. Zie *Illegale en schadelijke inhoud op het Internet* (1996), de Green Paper 16 oktober 1996 als Com(96) 483 def; en het rapport van de Working Group on the Protection of Minors and Human Dignity van de EC; European Commission Legal Advisory Board, *Response to the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*, 25 februari 1997, <http://www2.echo.lu/legal/en/internet/gplabreply.html>; zie ook Working Party on illegal and harmful content on the internet, november 1996, <http://www2.echo.lu/legal/en/internet/content/wpen.html>; de VS hadden in 1993 hun Operation Longarm.

24. Zie The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Thinking Differently*, oktober 1997; ook reeds Martin (1997).

ling gevolgd die hiervoor is gesignaleerd van fraude, via *hacken* en kinderporno tot sabotage.

3.2 *Financiële benadeling van individuele rechtssubjecten*

Financieel relevante gegevens zoals saldi en arbeidsuren zijn gebruikelijke objecten van computer-gerelateerde fraude. Maar de soorten fraude zijn oneindig. Een verpleegkundige in Parijs veranderde de gegevens over opiaatbehoeftige patiënten en die van de anesthesie-afdeling om aan dope te komen.²⁵

De dader verandert dergelijke gegevens, of verandert het computerprogramma waarmee die gegevens worden opgeslagen en/of verwerkt (input- respectievelijk programmamanipulatie), teneinde daardoor aanspraak te kunnen maken op aan die gegevens gerelateerde rechten en/of uitkeringen. Een voorbeeld van het eerste is, dat het gegeven dat iemand 5000 per maand verdient wordt veranderd in 15 000; een voorbeeld van het tweede is de salami- of afrondingstechniek waarmee een bankmedewerker door een verborgen computerinstructie in te brengen in het computersysteem van zijn werkgever elke halve cent of minder die moest worden afgerond bij iedere transactie die er plaatsvond liet bijschrijven op zijn eigen rekening. Er wordt van uitgegaan dat het meest voorkomende type computercriminaliteit bestaat in fraude (verduistering, oplichting) door (ex-)werknemers, stagiaires en onderhoudsmensen.²⁶

De toegang tot de computer kan via het Internet verlopen, maar het Internet verandert niet veel wezenlijks aan hetgeen over deze materie is geschreven. Een korte samenvatting volstaat daarom, waarbij eerst op de commune vermogensdelicten wordt ingegaan en vervolgens op vergrijpen tegen de intellectuele eigendom, in het bijzonder het auteursrecht.

3.2.1 *Vermogensdelicten*

Diefstal van computergegevens is een problematisch begrip. Een computergegeven is volgens de Hoge Raad immers geen goed dat

25. Martin (1997): 13.

26. E. Wise, *Computer Crimes and other Crimes against Information Technology in the United States*, RIDP 1993 (64).

kan worden gestolen.²⁷ De rechthebbende verliest het computergegeven niet zelf. Eigenlijk was deze beslissing reeds te voorzien niet alleen door de opvattingen terzake in de literatuur, maar ook door de zaak waarin het afgeven van 'de in de geest opgeslagen bekendheid met de bij zijn betaalpas horende cijfercombinatie' niet werd aangemerkt als een goed in de zin van art. 317 Sr – al ging het daar niet om in een computer opgeslagen gegevens.²⁸ In sommige gevallen zal van dit algemene uitgangspunt moeten worden afgeweken. Giraal geld – ook een computergegeven – kan wel worden gestolen,²⁹ omdat je dat wel kwijt raakt; digitaal geld is nu nog een elektronische cadeaubon, maar een die zodra hij de computer van een detaillist bereikt via *Interpay* (een organisatie van de banken) wordt omgezet in echt, giraal geld – mij lijkt dat het daarom net als gewoon giraal geld 'steelbaar' is. Blijkens een arrest uit 1991 kan het verwerken van computerbestanden onder het bereik van art. 225 Sr komen.³⁰ Een weggeschreven bestand dat bestaat uit met enige duurzaamheid op een magneetschijf vastgelegde gegevens omtrent betalingsopdrachten welke op kennelijk eenvoudige wijze leesbaar kunnen worden gemaakt, is volgens dat arrest een geschrift. De aanpassing van bepaalde in een computer opgeslagen tekst- of cijferbestanden kan dus als valsheid in geschrift worden aangemerkt; of het ook kan worden aangemerkt als vernieling van die bestanden is een vraag die door annotator Corstens terecht is opgeworpen.

Door twee vlak na elkaar gepubliceerde arresten over oplichting (art. 326 Sr) wordt de betekenis van art. 350a Sr ten opzichte van andere strafbepalingen opgehelderd. In het eerste arrest had iemand het functioneren van een mechanisme van een speelautomaat weten te ontregelen, waardoor hem door die automaat ten onrechte geld werd uitgekeerd; dat gold niet als oplichting. In het tweede arrest werd een bank tot afgifte van geld via zijn pinautomaat bewogen door de listige kunstgrepen die bestonden in de toe-eigening van een pasje en het aannemen van de valse hoedanigheid door een onder dwang genoemde pincode in te toetsen;

27. HR 3 december 1996, NJ 1997, 574.

28. IIR 13 juni 1995, NJ 1995, 635.

29. IIR 11 mei 1982, NJ 82, 583. Met de E-cash van Digicash, een soort tegoedbon om te gebruiken op het Internet, ligt het voor zover ik zie, niet anders.

30. HR 15 januari 1991, NJ 1991, 668 m.nt. C.

dat gold wel als oplichting.³¹ In een bijna identiek geval als het laatste had de pashouder onder bedreiging zijn pincode ingetoetst en dat leverde diefstal met bedreiging met geweld van de pashouder op. Dat maakte de stap klein om het gebruik van een pincode door de 'dief' in zo'n geval te kwalificeren als diefstal met een valse sleutel (art. 311 Sr).³² Hieruit kan de conclusie worden getrokken, dat het ontregelen van een mechanisme anders moet worden beoordeeld (geen oplichting), dan het leveren van misleidende input aan een op zich correct werkend mechanisme. Dat laatste kan in het geval een niet-rechthebbende de pinpas gebruikt als oplichting maar eveneens als diefstal met een valse sleutel gelden. Dat sluit aan bij (en bevestigt in zekere zin) het hiervoor gesuggereerde verschil tussen art. 225 Sr en art. 350a Sr. Iets algemener geformuleerd: in geval van inputmanipulatie kunnen de traditionele strafbepalingen van toepassing zijn (art. 225, 311 en 326 Sr) en mogelijk ook – als geval van meerdaadse samenloop, vanwege de verschillende strekking van de artikelen – art. 350a Sr; in geval van programmamanipulatie (of andere verandering van de werking van een informatieverwerkend systeem, zoals het inbrengen van eerder genoemd afrondingsprogramma) is alleen art. 350a Sr een bruikbare vervolgingsgrond. Het voorgaande kan rechtsreeks van toepassing worden geacht voor fraude via het Internet.

Tot slot een opmerking over toekomstige problemen met betrekking tot het daderschap van vermogensdelicten. Wat is eigenlijk de situatie als niet een mens maar een niet op een mens te herleiden virtueel persoon de oplichting verricht? Nu reeds is via het Internet de virtuele popster Kyoko Date te zien, die eigenlijk niet meer te onderscheiden is van een echt mens. De van haar gepubliceerde foto's zijn geen afbeeldingen van een bestaand mens, maar zijn de schepping van een topmodellenbureau; ze heeft cd's op haar naam en een eigen radioprogramma, waar een onbekende haar dagelijks een stem geeft.³³ Gesteld dat u een cd bij deze dame koopt terwijl u niet wist dat ze een virtueel persoon is, en u geeft toestemming een bedrag van uw credit

31. HR 24 september 1991, NJ 1992, 123 en HR 19 november 1991, NJ 1992, 124.

32. HR 28 april 1992, NJ 1992, 657; HR 8 december 1992, NJ 1993, 323; HR 7 mei 1996, NJB 1996, 64.

33. Ine Poppe in NRC Handelsblad 12 december 1997.

card af te laten schrijven. De cd wordt niet geleverd. Normaliter levert deze wanprestatie van de personen achter het virtuele schepsel geen strafbaar feit op. Maar is het enkele feit dat een virtueel persoon geschapen is nu voldoende om te kunnen spreken van het aannemen van een valse hoedanigheid of het aanwenden van een listige kunstgreep als bedoeld in art. 326 Sr? Me dunkt van niet, omdat via een virtueel persoon op zich zeker eenvoudige contracten tot stand moeten kunnen komen (zoals de machines in grootwarenhuizen die bij het leegraken van de schappen automatisch contact leggen met de leverancier). Bovendien zal er voor oplichting in ieder geval het oogmerk van wederrechtelijke bevoordeling moeten worden bewezen – via het functionele daderschap van de geestelijke vader van het programma. Men hoeft geen grote fantasie te hebben om te beseffen dat deze en ingewikkelder problemen gaan komen, maar het is voorbarig daar nu al conclusies in verband met de mogelijke noodzaak van strafbaarstelling uit te trekken.

3.2.2 Intellectueel eigendom en strafrecht

Een tweede groep delicten die financiële benadeling van derden tot gevolg heeft betreft het 'wegnemen' van informatie waarop een ander een exclusief recht heeft in verband met het intellectuele eigendomsrecht. Opzettelijk en culpoos inbreuk maken op eens anders auteursrecht is strafbaar (art. 31 en 32 Auteurswet).³⁴ Eveneens strafbaar is hij die opzettelijk een voorwerp waarin met inbreuk op eens anders auteursrecht een werk is vervat openlijk ter verspreiding aanbiedt; ter verveelvoudiging of ter verspreiding voorhanden heeft; met het oog op de invoer voor handen heeft of bewaart uit winstbejag (art. 31a Auteurswet). Indien dit bedrijfsmatig gebeurt, wordt gesproken van piraterij en is de maximumstraf 4 jaar (art. 31b Auteurswet). In art. 32a Auteurswet is de handel in middelen om kopieerbeveiligingen te doorbreken strafbaar gesteld.³⁵ Het kopiëren van

34. Hetzelfde geldt voor het opzettelijk inbreuk maken op het recht van de octrooihouder (art. 79 Rijksoctrooiwet 1995), waar het om inventieve software-vindingen gaat.

35. Volgens Algemeen Dagblad 19 augustus 1997 gaat de platenindustrie vanaf 1998 alle muziek die op cd verschijnt waarmerken met verborgen →

software – zelfs voor thuis-gebruik – is strafbaar (art. 45n jo art. 16b, eerste lid Auteurswet).³⁶

Ook als degene die het materiaal op het Internet zet, zelf op legale wijze aan het materiaal is gekomen, zonder toestemming van de rechthebbende of maker informatie via het Internet vermenigvuldigt is dat strafbaar (art. 45b jo art. 31 en 32 Auteurswet). Maar wat is dan de positie van degene die het aldus op een bulletinboard vrij toegankelijk gemaakte materiaal daar afhaalt? Is dat een heler? Bij de invocering van de wet computercriminaliteit zijn de gedragingen met betrekking tot door misdrijf verkregen computergegevens bewust beperkt tot die in het gewijzigde art. 273 Sr. Algemene strafbaarheid van heling van computergegevens werd onwenselijk geacht.³⁷ Die gedachte past m.i. bij de benadering dat gegevens niet kunnen worden gestolen of verduisterd. Toch levert dit een ietwat vreemd effect op, als we bedenken dat personen die gepirateerde cd-rom's en muziek-cd's kopen zich wel en personen die dezelfde informatie van het net *downloaden* zich niet aan heling schuldig maken.³⁸ Een cd met informatie is immers wel een goed, al is de informatie sec dat niet.

Art. 273 Sr stelt strafbaar het opzettelijk bekend maken en het uit winstbejag gebruiken van geheime gegevens van een onderneming van handel, nijverheid of dienstverlening welke betrekking hebben op deze onderneming, indien die gegevens niet algemeen bekend waren en daaruit enig nadeel kan ontstaan. Het artikel vergt dus winstoogmerk; dat is anders in de VS gezien het ontslag van rechtsvervolging van de student die voor miljoenen illegaal gekopieerde commerciële software gratis ter beschikking stelde op een voor iedereen toegankelijk bulletin board.³⁹ Wel mag m.i. worden aangenomen dat informatie die

→ codes om intensieve controle mogelijk te maken op onder meer illegale verkoop via het Internet.

36. Zie uitgebreider Van Dijk & Keltjens (1995), hoofdstuk 4.

37. T&G Sr (Van Woensel), aant. 11 bij art. 416 onder verwijzing naar TK 1989-1990, 21 565, 6: 37-38; toch is heling van kinderporno op een gegevensdrager (voor de wijziging van art. 240b Sr) geaccepteerd door Rb Zutphen 5 december 1995, Computerrecht 1996.

38. HR 2 maart 1982, NJ 1982, 446 nam heling aan bij de verkoop van grammofoonplaten waarvoor geen auteursrechten waren betaald.

39. M. Godwin, Cops on the I-way, Time, special issue, vol. 145 (1995), nr. 12; M.D. Rasch, Computer security, Security Management april 1996: 59-67 wijst erop dat het Amerikaanse strafrecht op dit punt van het civiele recht verschilt, omdat voor een civielrechtelijke veroordeling geen voordeel is vereist.

is verkregen van een publiek domein, bijv. een bulletin board of een nieuwsgroep, kan worden gebruikt en men hoeft dan niet meer bang te zijn voor vervolging wegens heling. Alleen al het feit dat de gegevens niet meer geheim zijn, leidt tot de niet-toepasbaarheid van art. 273 Sr. Maar betekent dit ook dat openbare documenten – bijvoorbeeld door de rechter voorgelezen getuigenverklaringen – uit een rechtszaak zonder toestemming op het Internet kunnen worden gezet? Bij de beantwoording van die vraag (in 3.3) komen we bij een ander type benadeling.

3.3 Aantasting van de informationele privacy en integriteit

Niet alleen de waarde van gegevens in het vrije economische verkeer, maar ook de waarde van gegevens voor degene op wie deze betrekking hebben, is strafrechtelijk relevant (zie 2.1). Hebben deze personen een substantieel recht op bescherming van hun privacy of op het behoud van de integriteit van de gegevens? Het gaat wat betreft die privacy niet om een academische vraag, maar om een problematiek waarover blijkens een recent onderzoek 30% van de 10.000 onderzochte Internetgebruikers zich zorgen maakt; van 24% gaan de grootste zorgen uit naar de censuur.⁴⁰ Twee concrete voorbeelden: mag een echtgenoot na de echtscheiding de blootfoto's van zijn vrouw zonder haar toestemming op het Internet plaatsen; of mogen legaal verkregen processtukken inzake een procedure op het Internet worden gezet? Die voorbeelden illustreren dat in verband met het Internet zal moeten worden gezien of het recht op privacy (of enig ander recht) niet alleen het recht betreft om met rust gelaten te worden, maar ook het recht op een soort controle: 'the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others.'⁴¹ Zo dit controlerecht bestaat is de volgende vraag of het genot van dit recht is of zou moeten worden verzekerd door het strafrecht. Zelfs indien uit art. 8 EVRM de positieve verplichting wordt afgeleid dat de burger moet worden beschermd tegen de inbreuken op het ge-

40. Gvu 8th www user survey, 10.10.1997-16.11.1997 op www.gvu.gatech.edu/user_surveys/survey_1997_10/.

41. Alan Westin, geciteerd in E.M. Wise, *Computer Crimes and Other Crimes against Information Technology in the United States*, *Revue Internationale de Droit Pénal* (64) 1993: 663.

not van het in dat artikel neergelegde recht⁴², zegt dit uiteraard nog niet dat er een juridische plicht tot strafbaarstelling is. Maar rechtspolitiek kan wellicht worden gesteld, dat de komst van het Internet de bescherming tegen malicieuze acties van (eventueel anonieme) personen via het civiel recht veel moeilijker heeft gemaakt dan voorheen. Tegen een identificeerbare krant of omroep kan wegens een publicatie een onrechtmatige-daadsactie worden gestart, maar nu is wellicht eerder strafrechtelijk overheidsoptreden nodig omdat adequate juridische bescherming tegen anoniemi moeilijker is te verwezenlijken.

Wat ligt er op dit moment ter strafrechtelijke bescherming van de privacy? In de eerste plaats is het verboden zomaar binnen te dringen in iemands computer; een tweede punt betreft het vernielen van gegevens of het kopiëren ervan; aan het slot van deze paragraaf kom ik terug op het derde punt, het verspreiden van die privé-gegevens.

3.3.1 *Binnendringing en vernieling*

Via het Internet is het mogelijk om ongeautoriseerd binnen te dringen in een computersysteem van een ander. Dit '*hacken*' is strafbaar gesteld in art. 138a (computervredebreuk). De hacker doet zich voor als legitieme gebruiker door een *password* te gebruiken of door het systeem via een 'achteringang' die gemaakt is voor onderhoudsdoeleinden te betreden. Het doel van *hackers* kan zeer verschillend zijn. Er zijn er die optreden als dieven van privé-gegevens, vernielers ('*crushers*'), of als facilitair bedrijf van criminelen. Er zijn ook 'uitvinders' die geïnteresseerd zijn in de vraag 'what makes it tick' en die kunnen rekenen op gemengde gevoelens van onbegrip en sympathie. De digitale burgerrechtenactivisten kunnen zelfs van de zijde van sommige politieambtenaren op enige sympathie rekenen, daar iedereen die zich met de materie bezig houdt met enige zorg kijkt naar de aanleg van dataverzamelingen die zowel bij het particuliere bedrijfsleven als de diverse overheden plaatsvindt.⁴³ Deze verschillende doelein-

42. EHRM 26 maart 1985, NJ 1985, 525 (X en Y tegen Nederland), para 32; om deze reden is art. 165a Sv in 1985 opgenomen.

43. Een spectaculair voorbeeld van activisme is de kraak van 54 000 wachtwoorden van alle World Online-abonnees, Telegraaf 9 december 1997.

den illustreren dat het zinvol is onderscheid te maken tussen ongeautoriseerde toegang en ongeautoriseerde toegang met culpoze schade, en/of met ongeautoriseerd gebruik, en/of met ongeautoriseerd kopiëren, en/of met opzettelijke vernieling.

Voor de computervredebreuk (art. 138a Sr) is een vereiste dat de hacker enige beveiliging doorbreekt of de toegang verwerft tot een geautomatiseerd werk door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid. 'Het gaat erom dat degeen die de computer binnendringt door het doorbreken van de beveiliging, heeft blij gegeven de wetenschap te hebben gehad dat hij een beveiligd systeem binnendringt en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken'.⁴⁴ Het zal dikwijls niet gaan om het binnendringen in een computer, maar in een netwerk, of in een discussiegroep, of wellicht in de toekomst in een teleconferentie. In al deze gevallen kan dunkt me wel worden gesproken van het in art. 138a Sr gebruikte woord geautomatiseerd werk, dat in art. 80sexies Sr wordt gedefinieerd als 'een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken'. Het enkele bericht dat personen jonger dan 18 jaar niet binnen mogen, of dat politie-ambtenaren dat niet mogen, is niet voldoende om als beveiliging te gelden. Of de hacker nu binnenkomt door een met behulp van een daartoe bestemd programma het password te omzeilen, door het password van de rechthebbende te gebruiken of door zich voor te doen als onderhoudsmedewerker – het is allemaal strafbaar. Met name van de *providers* mogen de nodige inspanningen tot beveiliging worden verwacht; of het feit dat die inspanningen niet steeds geweldig zijn, reden tot strafbaarstelling is laat ik nu maar in het midden.

Indien de hacker na binnendringen gegevens kopieert is dat een strafverzwarende omstandigheid (art. 138, tweede lid Sr). Hackt men niet bij de eigen werkgever of netwerkbeheerder, maar via de telecommunicatie – dat zal in geval van gebruik van het Internet steeds het geval zijn – dan is dat eveneens reden voor een hogere straf, indien de computervredebreuk geschiedt met het oogmerk van wederrechtelijke bevoordeling. Daarbij is aan de betekenis van laatstgenoemde term zoals gebruikt in art. 326 Sr

44. Aldus de veel geciteerde MvT TK 1989-90, 21 551, 3: 15.

gedacht.⁴⁵ Dat impliceert onder meer dat niet afdoet aan strafbaarheid het feit dat de hacker ook een eigen recht op de informatie heeft (bijvoorbeeld omdat de informatie op hemzelf betrekking heeft). Het oogmerk van bevoordeling is een strafverzwarringsgrond. Opmerkelijk is dat deze strafverzwarringsgrond niet bovenop die van het kopiëren van aangetroffen informatie komt (de delicten van art. 138a, tweede en derde lid hebben beide een maximale bedreiging van 4 jaar), als we bedenken dat er al personen zijn die tegen betaling *hackenderwijs* diverse elektronisch verkrijgbare gegevens over bepaalde personen verzamelen en koppelen. Het is ietwat verwonderlijk dat het *hoppen* via het ene binnengedrongen netwerk, naar een ander (bijvoorbeeld van de regionale politie naar de CRI) even zwaar wordt bestraft.

Is de hacker eenmaal binnengedrongen dan rijst de vraag, wat hij heeft gedaan. Het is niet alleen niet vast te stellen wat hij heeft gezien en/of wat hij heeft gekopieerd, maar ook niet wat hij heeft veranderd, gewist of toegevoegd. Zelfs onbedoelde en/of niet dadelijk waarneembare schade kan zijn aangericht. De al eerder aan de orde gestelde art. 350a en 350b Sr stellen het dodelijke respectievelijk culpoze wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens, dan wel het toevoegen van andere gegevens daaraan strafbaar. Doordat – anders dan met betrekking tot vernieling in de *real world* zoals strafbaar gesteld in art. 350 Sr – ook culpoos vernielen strafbaar is, mits daardoor ernstige schade met betrekking tot de gegevens is veroorzaakt, zal de hacker die door zijn binnentreden dergelijke schade heeft veroorzaakt, al snel strafbaar zijn. De kans is overigens groot dat de hacker in dat geval ter zake van (voorwaardelijk) opzet zal worden vervolgd.

Uiteraard kunnen via het Internet allerlei ongewenste programma's worden meegezonden. In art. 350a, derde lid wordt op het verspreiden en ter beschikking stellen van virussen die bedoeld zijn om schade aan te richten door zichzelf te vermeerderen een hogere strafbedreiging gesteld dan op de gewone 'computervernieling'. Ik beschouw dit als een gevaarzettingsdelict: de daad-

45. T&C (Buitting), aant. 4 bij art. 138a met verwijzing naar de Tweede nota van wijziging.

werkelijke schade hoeft niet te zijn aangericht, terwijl juist de vermeerdering naar andere computers cruciaal is.

Lastiger is de in art. 350a, eerste lid strafbaar gestelde opzettelijke en wederrechtelijke toevoeging van andere gegevens. Het artikel zal vooral zien op bijvoorbeeld het heimelijk plaatsen van een tijdbom. Wellicht wordt de tijdbom nog niet eens gebruikt om iemand af te persen, maar heeft een programmeur/werknemer zich slechts op malicieuze wijze willen verzekeren (zonder dat anderen dat weten) tegen een ooit komend ontslag, teneinde dan (bijvoorbeeld doordat de bom zal afgaan x maanden nadat de werknemer van de loonlijst wordt geschrapt) de mogelijkheid tot wraakneming door vernieling en/of afpersing te hebben. Maar wat te denken van de tegenwoordig veel gebruikte *cookies* en *applets*? Een *cookie* is een klein stukje informatie dat een server (bijv. vanaf een *home page*) stuurt naar een *browser* (bijv. die waarmee u over het net surft); aanvankelijk diende het er vooral voor dat die server bij een later bezoek de gebruiker zou herkennen en deze zich niet opnieuw zou hoeven te identificeren of financiële verplichtingen aangaan.⁴⁶ De cookies bieden de gebruikers veel gemak; vooral voor interactieve communicatie zijn ze haast onontbeerlijk. U hebt echter niet uitdrukkelijk voor het sturen van de cookie toestemming gegeven. Strikt genomen valt het zenden ervan dus onder art. 350a Sr. Sinds kort zijn er browsers waardoor het mogelijk is om cookies te weren of pas na uitdrukkelijke toestemming te ontvangen en dan rijst de vraag naar de invloed van de 'eigen schuld' van de ontvanger van de cookies. Dankzij de flexibiliteit van ons strafprocessuele opportuniteitsbeginsel lijkt er wellicht nauwelijks een probleem. Maar dan wordt miskend, dat de cookies veel meer toepassingen hebben gekregen. De server kan er mee zien wie zijn site heeft bezocht. Een cookie kan zelfs worden geplaatst en vervolgens teruggeroepen opdat de server die de cookie heeft geplaatst kan nalczen welke *sites* door de gebruiker (bij wie de cookie is geplaatst) heeft bezocht; deze toepassing – die in feite op het digitaal volgen neerkomt – wordt vooral in de sfeer van de marketing gebruikt. Juridisch onbeantwoord zijn nog diverse vragen met betrekking tot het beheer, gebruik en verkopen van via cookies verkregen informatie. De *applets* werken globaal op dezelfde manier. Ook de applet zal nor-

46. Meer hierover op www.cookiecentral.com.

maliter worden opgedaan als men een bepaalde site bezoekt. De applet is zelf een klein programmaatje dat kan reageren op gebeurtenissen (toetsaanslagen, het bewaren van een file) en kan communiceren met de browser van de bezoeker. Het is niet noodzakelijk dat de applet stopt te werken als de bezoeker de pagina verlaat; de applet kan ook communiceren met andere applets. Vanuit veiligheidsoverwegingen is echter het meest bijzonder dat het technisch mogelijk is dat applets in bestanden lezen of schrijven van de gebruiker die hem in werking heeft gezet door zijn bezoek aan de applet-leverende site. De *HotBot search engine* heeft geteld dat op meer dan 400 000 webpagina's een of meer *Java-applets* worden geplaatst. Het lijkt me zeker dat – op het vlak van privacy en dat van security – misbruik voor de hand ligt. Maar het is onzinnig om elk gebruik van cookies strafbaar volgens art. 350a Sr te achten.

Het gaat in art. 350a en 350b Sr zowel om gegevens die worden verwerkt als die worden overgedragen. Dat betekent dat het niet uitmaakt of men een e-mailbericht dat (nog) in de mailbox van een gebruiker rust ontoegankelijk maakt of dat men datacommunicatie onderschept en valse commando's of antwoorden genereert. Een spectaculair voorbeeld van dat laatste is het eerste gedocumenteerde geval van elektronische verkrachting. De dader nam deel aan een MUD en fabriceerde een programma, waardoor het leek of een andere deelneemster aan die MUD de door de dader geschreven (obscene) teksten had verzonden.⁴⁷ Het is natuurlijk heel vervelend als je woorden in de mond gelegd krijgt die je geheel niet passen. Waar het in dat geval nog om (door de deelnemers zeer serieus genomen) verstrooiing ging, is de betekenis van de casus groot als we denken aan nieuws- en discussiegroepen. Vergelijkbaar hiermee is ook het veranderen van homepages e.d. door derden. Op 18 december 1995 stond op de homepage van een Griekse krant het sensationele, maar onware bericht dat Papandreou dood was.⁴⁸ Nog weer anders, maar ongetwijfeld ook op grond van art. 350a strafbaar, is het bewust wegblazen van een deelnemer aan een *teleconference* door een *zgn. kill file* in een systeem te plaatsen waardoor berich-

47. J. Dibbell, A rape in cyberspace, in Ludlow (1996): 375-397.

48. I.E. Vassilaki, Multimediale Kriminalität, Computer und Recht 1997: 297-302.

ten afkomstig van een bepaald adres automatisch onzichtbaar worden.

Onder het opzettelijk vernielen valt ongetwijfeld ook het kidnappen van gegevens door er een voor de rechthebbende niet te verbreken *encryptie*-programma op los te laten (*'bit-napping'*), bijvoorbeeld teneinde de rechthebbende af te persen. Volgens het voorontwerp Computercriminaliteit II krijgt de OvJ en tijdens het gerechtelijk vooronderzoek de RC de bevoegdheid te bepalen dat onrechtmatige gegevens, waarvoor onttrekking aan het verkeer kan worden bevolen, ontoegankelijk gemaakt worden; als strafrechtelijke maatregel wordt in 36b Sr het ontoegankelijk maken van gegevens opgenomen. Ontoegankelijk maken zal neerkomen op hetgeen hiervoor als *'bitnapping'* werd aangeduid; versleuteling (*encryptie*) zonder dat de oorspronkelijke gebruiker over de sleutel beschikt. Dat de gegevens zelf een strafbare aard moeten hebben, betekent dat men kan denken aan opruiende informatie of kinderporno; overigens blijkt hier de ontoereikendheid van het pakket-paradigma, omdat contextloze gegevens niet kunnen opruien en informatie wel.

3.3.2 *Strafbare interceptie*

Naast de inbreuken op (en het 'afpakken van') in het computersysteem opgeslagen gegevens, zijn ook inbreuken op de privacy mogelijk doordat de dader zich richt op het gegevensverkeer van het slachtoffer. Dat bleek eigenlijk al toen het onderscheid tussen het vernielen (het verhinderen of veranderen) van e-mail in en buiten de *mail-box* werd gerelativeerd. Op het tappen en/of vastleggen van die e-mail is echter nog niet ingegaan. Illegale interceptie van gegevensverkeer is strafbaar gesteld in art. 139a-e Sr. Het gaat niet alleen om privacy-gevoelige e-mail. De term gegevensverkeer duidt niet alleen op tekst, maar ook op beeld, geluid en wat niet al; men denke ook aan het onderscheppen van teleconferenties via Internet. Voorts behoeven de gegevens niets met de privacy van doen te hebben. Men denke bijvoorbeeld aan het (semafoon)signaal dat een geldautomaat afgeeft als deze weer gevuld moet worden.

In art. 139a gaat het om het opzettelijk aftappen of opnemen van gegevens die in een woning, besloten lokaal of erf door mid-

del van de computer worden overgedragen met een technisch hulpmiddel zonder dat de tapper daartoe is gerechtigd. Daarbij kan worden gedacht aan het plaatsen van een 'bug', het inbrengen van een chip in een toetsenbord, en wellicht in de nabije toekomst het toezenden van een '*applet*' (een soort Trojaans paardje dat naar iedereen die van het Internet gebruik maakt kan worden gezonden) om alle aanslagen op een toetsenbord te sturen naar een vast adres. De kwaadwillende kan aan dergelijke vormen van interceptie behoefte hebben, als hij weet dat zijn slachtoffer hetzij van een niet op het Internet aangesloten computer gebruik maakt, dan wel via het Internet geëncrypteerde berichten verzendt; op het moment waarop de vingers het toetsenbord raken is er nog niets versleuteld.

Art. 139c Sr heeft betrekking op het aftappen of opnemen van gegevens die niet voor de tapper, niet mede voor hem noch voor zijn opdrachtgever zijn bestemd, waar die gegevens worden verzonden via de telecommunicatie-infrastructuur⁴⁹, of voor een telecommunicatie-inrichting die wordt aangewend voor dienstverlening aan het publiek (bijvoorbeeld bij mobiele telecommunicatie), of door middel van daarop aangesloten randapparatuur (bijvoorbeeld een intranet binnen een groot bedrijf of een ambtelijke dienst). De terminologie wordt volgens de ontwerp Telecommunicatiewet vereenvoudigd, zodanig dat ook het aftappen van gegevensstromen bij access-providers onder de werking van de strafbepaling zal vallen. Het is twijfelachtig of het inzien (bijvoorbeeld door een provider) van iemands mailbox op dit moment onder de strafbepaling is te rekenen. In het kader van de aangekondigde grondwetsherziening is strafbaarstelling daarvan aangekondigd.⁵⁰ Het lijkt niet uit te sluiten, dat het zonder toestemming van de rechthebbende plaatsen van een 'zendprogramma' bij een *access-provider* (waardoor men Internetverkeer van die rechthebbende naar zichzelf toeleidt) onder het bereik van dit artikel valt (zie 5.3). Met betrekking tot het plaat-

49. Volgens art. 1f Wet Telecommunicatievoorzieningen is een telecommunicatie-infrastructuur een stelsel van inrichtingen met daarbij behorende middelen die, geheel of gedeeltelijk, openbare gronden overschrijdt, welk stelsel is begrensd door daartoe behorende aansluitpunten met inbegrip van de telecommunicatie-inrichtingen buitenslands.

50. TK 1996-97, 25 533, 1-3 (Telecommunicatiewet); TK 1997-98, 25 443, 5, p. 5 (herziening art. 13 Grondwet).

sen en terughalen van een cookie waarmee kan worden nagegaan welke sites iemand heeft bezocht geldt in verband met art. 139c Sr hetzelfde als in 3.3.1 met betrekking tot art. 350a Sr is geschreven. Strikt genomen is het zenden van het geschetste type cookie aan te merken als een overtreding van art. 139c Sr. Het kan niet de bedoeling zijn om al het gebruik van cookies strafbaar te stellen en het is strafrechtelijk niet fraai om de dogmatische vraag met betrekking tot een grote categorie gevallen (pragmatisch) op te lossen door elke cookie-zending strafbaar te stellen en verder te rekenen op het door het OM te hanteren opportuniteitsbeginsel (zie 3.3.1).

Tot slot zij gewezen op de strafuitsluitingsgronden van art. 139c, tweede lid. Kort gezegd is voor zover gegevensverkeer met een gewone ontvanger kan worden opgevangen dit 'afluisteren' niet strafbaar: de ether is vrij. Het afluisteren ten behoeve van de strafvordering of de staatsveiligheid komt in 5.3 aan de orde. De werkgever/abbonementhouder kan in het bijzonder om misbruik van het systeem op te sporen de communicatie van een werknemer afluisteren 'behoudens in geval van kennelijk misbruik'. Overigens zal de werkgever daarbij wel moeten onderkennen, dat ook in de werkomgeving een door art. 8 EVRM beschermde privé-sfeer wordt erkend.⁵¹

3.3.3 *Verstreking of verspreiding met informationeel nadeel*

De hacker die gegevens overneemt, is strafbaar. Toch lijkt het onder omstandigheden nog erger als voor betrokkenen gevoelige gegevens vervolgens in de openbaarheid worden gebracht. Extreem was het geval dat zich recentelijk in Nederland heeft voorgedaan, waarbij een *provider* werd *gehackt* en alle e-mail van de bedrijven die via die *provider* toegang tot het net kregen op het net is gegooid. Die *hackers* zijn nu reeds vervolgbaar. Maar wat is de huidige stand van het recht ten aanzien van het plaatsen op het net van legaal verkregen informatie?

Op zich is de vrijheid van meningsuiting niet voldoende rechtvaardiging om alles op het net te zetten. In art. 10, tweede lid EVRM is uitdrukkelijk als uitzonderingsgrond op die vrijheid het 'voorkomen van verspreiding van vertrouwelijke mededelingen'

51. EHRM 25 juni 1997, NJCM-bulletin 1997: 765-767 en 1088-1092 (Halford).

opgenomen. In dat verband kennen wij ook een strafbaarstelling, die van toepassing kan zijn bij plaatsing van gegevens op het net. In art. 272 Sr is strafbaar gesteld het schenden van geheimhoudingsplichten die uit hoofde van ambt, beroep of (vaak: en) wettelijk voorschrift bestaan. Onder omstandigheden wordt een doorbreking van de geheimhoudingsplicht aanvaard. Te denken is aan de plicht om aangifte te doen (art. 160 en 162 Sv) of de plicht om – daartoe geroepen – te getuigen (art. 289 Sv), welke plichten op hun beurt worden doorbroken voor wat de verschoningsgerechtigden betreft (art. 217-219a Sv). De voornaamste categorie gevallen waarin een niet-wettelijk gelegiti-meerde doorbreking gerechtvaardigd zou kunnen zijn is die van de 'klokkenluiders', de (ex-)leden van een organisatie die zonder daartoe opdracht of toestemming te hebben gekregen van hun superieuren informatie onthullen met de bedoeling de aandacht te vestigen op een misstand waarvan ze door hun werk binnen de organisatie kennis hadden gekregen. Die klokkenluiders schijnen in de VS door wetgeving te worden beschermd.⁵² Ook de bescherming van de goede naam of de rechten van anderen biedt een grond om uitzondering te maken op het in art. 10 EVRM gewaarborgde recht van vrije meningsuiting. Strafbarestellingen – buiten de in de volgende paragraaf te behandelen belediging – zijn er nauwelijks. Wel is het openbaarmaken van een portret zonder daartoe gerechtigd te zijn een met geldboete te bestraffen overtreding (art. 35 Auteurswet). De details daargelaten, komen art. 20 en 21 Auteurswet erop neer dat openbaarmaking van een in opdracht gemaakt portret alleen mag met toestemming van de geportretteerde; openbaarmaking van een zonder opdracht vervaardigd portret is niet geoorloofd voor zover een redelijk belang van de geportretteerde zich daartegen verzet. Openbaarmaking van persoonsgegevens die worden beschermd door de Wet Persoonregistraties is niet strafbaar – behoudens het geval dat deze geschiedt aan een buitenlandse (bij amvb aangewezen) persoonsregistratie (art. 50 jo 49 WPR).⁵³ Verder is er geen materieel strafrechtelijke bescherming tegen

52. M.A.P. Bovens, *Verantwoordelijkheid en organisatie*, Zwolle 1990: hoofdstuk 12.

53. Deze wet zal worden gewijzigd met de op stapel staande Wet bescherming persoonsgegevens.

ongcautoriscerde verspreiding van gegevens die op een persoon betrekking hebben. Het is m.i. niet goed te verteren dat het wel strafbaar is om zonder toestemming compromitterende foto's te plaatsen (indien ze kunnen worden aangemerkt als 'portretten' in de zin van de Auteurswet), maar niet om zonder toestemming even compromitterende dagboekfragmenten op het Internet of andere door de benadeelde vervaardigde niet voor publicatie (laat staan als werk van letterkunde, wetenschap of kunst waar het auteursrecht op toepasselijk is) bedoelde teksten. Ook het feit dat ik bepaalde medicijnen aanschaf bij de apotheek, kan een ander zien (de apotheker zelf is tot geheimhouding verplicht) en op het Internet plaatsen en ook die openbaarmaking is niet strafbaar. Dat is het zelfs niet als die ander systematisch informatie over mij inwint en daarvan vervolgens gebruik maakt, tenzij de dader daarmee de registratiewetgeving heeft overtreden. Kortom: het is een beetje vreemd dat de op geld waardeerbare in een geautomatiseerd werk opgeslagen bedrijfsgeheimen wel (art. 273 Sr) en de op de persoonlijke levenssfeer betrekking hebbende gegevens niet als zodanig strafrechtelijk worden beschermd tegen niet door betrokkene geautoriseerde bekendmaking.

Omdat strafbepalingen de verboden handelingen precies behoren te beschrijven, en in dit verband ook de vrije nieuwsgaring een rol kan spelen, is het opstellen van een dergelijke strafbepaling geen sinecure.⁵⁴ Wellicht zou het feit dat de betreffende persoon van wie de persoonlijke levenssfeer wordt geschonden zelf de vervaardiger van de gegevens is (het dagboek) of de omstandigheid dat een andere persoon ten aanzien van het gerelateerde onderwerp een geheimhoudingsplicht heeft (zoals de apotheker) een handvat kunnen bieden. Ook de wenselijkheid van strafbaarstelling van het op het Internet zetten van op aanwijsbare personen betrokken verzonnen informatie zou daarbij moeten worden onderzocht. Berucht is de Baker-zaak, waarbij een student zijn obscene verzinsels over een klasgenote (gedetailleerd uitgewerkte wensen haar te verkrachten etc.) op het Internet zette.⁵⁵ Hij deed haar niets en richtte zich ook niet tot

54. United Nations Manual (1995): para 140 met verwijzing naar the Select Committee of Experts on Computer-Related Crime van de Raad van Europa en de daardoor voorbereide Recommendation No. R(89)9, die door de Raad op 13 september 1989 is aanvaard.

55. Zie MacKinnon (1997): 213-214.

haar in de 'real world'. Een strafbare bedreiging zie ik er niet in; misschien kan het wel als belediging worden aangemerkt (art. 266 Sr). Als beledigend is ook de wraakactie aan te merken die bestond in het massaal verspreiden van (valselijk) ondertekende e-mailberichten met kinderpornografische inhoud, waarbij de persoon die zou hebben ondertekend niets met het bericht te maken had maar het object was van de wraakactie.⁵⁶

3.4 *Uitings- en verspreidingsdelicten*

Bij de hiervoor besproken delicten was het 'afpakken' van informatie van aanwijsbare rechtssubjecten aan de orde, waarbij zoals op het eind van die paragraaf aan de orde kwam ook de wijze waarop die informatie wordt gebruikt van belang bleek. In deze paragraaf ligt de nadruk op de verspreiding. De slachtoffers – zo die al aanwijsbaar zijn – wordt misschien wel leed, afschuw of ontzetting toegebracht, maar zij raken geen bezit of informatieel controlerecht (zoals in de vorige paragraaf besproken) kwijt. Het verspreiden van opruiende teksten (art. 131 Sr), racistische praat (art. 137c-e Sr), kinderporno (art. 240b Sr), en belediging van een individu (art. 266-271 Sr) betreft dogmatisch nogal verschillende onderwerpen. In al deze gevallen gaat het echter om vanwege de inhoud strafbaar gestelde uitingen, dat wil zeggen uitlatingen en/of beelden die bij geschrift en/of afbeelding worden verspreid. Het gaat steeds om formele, dus niet door het gevolg gekwalificeerde delicten, waarbij normatieve beoordelingen een grote rol spelen bij de bewijsvraag. Onder meer door de Europese Commissie is onderscheid gemaakt tussen illegale en schadelijke inhoud.⁵⁷ Met dat laatste wordt bedoeld op het feit dat kinderen ongewenst toegang kunnen krijgen tot bepaalde uitingen op het Internet die wellicht voor hen schadelijk zijn maar niet verboden voor volwassenen. Tot nu toe is schade of gevaar voor schade evenwel nog niet van belang gebleken bij de strafbaarstelling van uitingsdelicten. Ik ga op deze vanuit het perspectief van het strafrecht niet-relevante problematiek daarom verder niet in. Wel illustreert dit punt het klemmende karakter van de kernvraag: waarom stellen we uitingsdelicten strafbaar. Het belang van

56. Zie het eerste jaarverslag van het Internet Meldpunt Kinderporno.

57. European Commission Legal Advisory Board (1997).

die kernvraag wordt ook onderstreept door het bijzondere geval van de virtuele porno: na manipulatie van bestaande foto's, waarbij geen (nieuwe) fysieke slachtoffers behoeven te zijn gevallen, ontstaat een afbeelding die niet van een echte afbeelding is te onderscheiden. Bij de totstandkoming van art. 240b Sr realiseerden Parlement en minister zich reeds, dat hetgeen op een afbeelding te zien is niet noodzakelijk ook in werkelijkheid heeft plaatsgevonden. Minister Sorgdrager achtte in 1995 vervolging in dergelijke gevallen minder gewenst, omdat niet een werkelijk bestaand kind was beschadigd, maar de wet sluit succesvolle vervolging in dat geval niet uit. Die eist dat bewezen wordt dat de *afbeelding inhoudt* dat bij het seksuele gebeuren een kind is betrokken.⁵⁸ Als men schade als enig criterium voor strafbaarstelling aanvaardt, is de wettelijke strafbaarheid van het verspreiden van virtuele porno een moeizaam te accepteren gegeven. Acht men ook obsceniteit (oftewel de oorzaak van morele of esthetische walging) voldoende grond voor strafbaarstelling, dan is het een stuk eenvoudiger. Maar dan raakt men wel de problematiek van de vrijheid van meningsuiting in het hart. Dan zal men moeten beseffen dat censurerende autoriteiten die impliciet of expliciet bestaan bij een beperking van de vrije meningsuiting historisch gezien geen goede papieren hebben.⁵⁹ Toch lijkt deze tweede benadering het geldend recht weer te geven: uitingsdelicten hebben op dit moment niet noodzakelijk met schade te maken. De uitingsdelicten hebben enkele andere in het oog springende overeenkomsten: in verband met het ouderschap de problematiek van de positie van de *provider*, de betekenis van het begrip openbaar of openlijk, alsmede de problematiek van de vrijheid van meningsuiting. Hoewel alleen in art. 240b Sr uitdrukkelijk sprake is van een 'afbeelding – of een gegevensdrager, bevattende een afbeelding –' waarmee aanvankelijk vooral aan videobanden werd gedacht, acht ik het schrift en/of afbeeldingsbegrip in alle gevallen mede te omvatten de uitlatingen en/of beelden die via het Internet worden verspreid. De conclusie van De Roos, Schuijt en Wissink dat de bestaande delictomschrijvingen van uitingsdelicten – misschien op een enkele uitzonde-

58. NLR art. 240b, aant. 3 en 7.

59. Zie J.M. Coetzee, *Giving Offence: essays on censorship*, Chicago 1996; en uiteraard het veel besproken Hart-Devlin-debat.

ring na – ook toepasbaar zijn op gedragingen op het Internet lijkt plausibel.⁶⁰ In zoverre kunnen we op dit terrein wel stellen dat wat *off-line* verboden is ook *on-line* verboden is.

Dat neemt niet weg dat er steeds weer vragen kunnen rijzen als gevolg van het feit dat uitingen via het Internet worden gedaan. Bijvoorbeeld: is het enkele oppikken van kinderporno van het Internet en *downloaden* naar de eigen harde schijf al te beschouwen als strafbaar 'vervaardigen, invoeren of doorvoeren'? Dat zou dan neerkomen op het strafbaarstellen van het kale bezit van kinderporno, of van heling van computergegevens die kinderporno bevatten en dat zou weer niet overeenstemmen met het algemene idee dat computergegevens normaliter niet geheel kunnen worden. Op dergelijke, voor de praktijk relevante, punten kan ik hier niet verder ingaan en ik beperk me tot de eerder genoemde gemeenschappelijke punten met betrekking tot de uitingsdelicten.

3.4.1 *Het ouderschap*

In eerste aanleg is het strafrecht gericht op degenen die de hiervoor bedoelde ongewenste uitingen op het net plaatsen. In hoeverre bestaat er echter strafrechtelijke medeverantwoordelijkheid voor anderen? De PTT en kabelnetbeheerders zullen zich meestal kunnen beroepen op het ontbreken van opzet ten aanzien van de verboden uiting, maar ook de *provider* langs wie een e-mailbericht gaat weet in beginsel van niets. Doorgaans zal zo'n *provider* dan ook niet een 'doen', maar hooguit een 'laten' zijn tegen te werpen. Strafrechtelijk relevant nalaten vergt evenwel altijd een plicht om te handelen, een Garantenstelling. Is zo'n plicht te construeren? Sieber gaat ervan uit dat het gelet op de huidige stand van de techniek te veel gevraagd is om in het algemeen echte controle ter zake van de inhoud van de berichten van een *provider* te verwachten.⁶¹ Dat zal in het bijzonder gelden

60. Th de Roos, G. Schuijt en L. Wissink, Smaad, laster, discriminatie en porno op het Internet, Alphen 1996 – zij aarzelen nog over het smaadschrift, maar neigen tot extensieve interpretatie naar het Internet; zie ook het onder 3.2 behandelde IIR 15 januari 1991, NJ 1991, 668 m.nt. C.

61. U. Sieber, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, Juristen Zeitung 1996: 429-442 en 494-507, i.h.b. 506.

voor de aanbieders van Internet-toegang en netwerk-exploitanten; aanbieders van *host-diensten* hebben soms meer zicht. Dat laatste geldt bijvoorbeeld voor de organisatoren van bepaalde discussiegroepen, die de ingekomen post sorteren.

Een plicht om te handelen kan ook ontstaan als de *provider* door eigen toedoen of door tussenkomst van derden ervan op de hoogte is geraakt dat er op het Internet strafbare feiten worden gepleegd en vervolgens niet ingrijpt. De Legal Advisory Board van de Europese Commissie schreef hierover:

*'The Legal Advisory Board considers that Internet service providers are responsible for their own content which they make available for use; they are responsible for third-party content which they make available for use if they can reasonably be said to have had knowledge about the contents and its possibly illegal or harmful content and blocking its use is both technically possible and can reasonably be expected; they are not responsible for third-party content to which they merely provide access for use.'*⁶²

Ook de Europese ministers waren het erover eens dat de beheerders van *on-line* diensten niet strafbaar behoren te zijn, tenzij ze op de hoogte zijn van de inhoud van het bericht.⁶³ De strafbaarheid van de *provider* is dan op diverse manieren te construeren. Aan de zgn. IJzerdraadcriteria (macht en aanvaarding) waarmee het functioneel ouderschap wordt bepaald, voldoet de *provider* in het door de LAB omschreven geval.⁶⁴ Ook vervolging voor gelijktijdige medepllichtigheid, voor voorafgaande medepllichtigheid (naar analogie van het opzettelijk de deur open laten staan, waarna een inbraak volgt) en volgens Harteveld en Van der Neut ook voor medeplegen is denkbaar.⁶⁵

Het is derhalve zinnig om de vraag te stellen of de Internetproviders ook als uitgevers ex 53 Sr niet vervolgbaar zijn. Me dunkt dat eigenlijk verschil zou moeten worden gemaakt tussen diverse soorten *providers*. Een *listowner* of een redacteur die een nieuwsgroep modereert (door bijvoorbeeld discussies te leiden en te controleren of de bijdragen niet de inhoudelijke of formele ka-

62. European Commission Legal Advisory Board (1997).

63. M. de Waard, Regeringen geven Internet volledig vrij baan, NRC Handelsblad 9 juli 1997.

64. HR 23 februari 1954, NJ 1954, 378 m.nt. B.V.A. Röling.

65. A.E. Harteveld en J.J. van der Neut, Internet-providers in de strafrechtelijke gevarenczone, DD 1996: 426-439.

ders van de betreffende groep te buiten gaan) heeft een inhoudelijke betrokkenheid – misschien nog meer dan een krantenuitgever. Menig *access-provider* staat evenwel heel ver van de inhoud af en is veeleer als *relais-station* te beschouwen dan als drukker of uitgever. In het voorontwerp Computercriminaliteit II wordt een aan de uitgever analoge situatie geschapen voor de *provider* zonder dat het hiervoor geschetste verschil een rol speelt. De tussenpersoon die a) bij de openbaarmaking of verspreiding zijn naam/adres bekend maakt, b) de dader bekend maakt terwijl c) die dader vervolgbaar en in Nederland gevestigd is, wordt zelf niet vervolgd.

3.4.2 Wat is openbaar?

Openbaarheid en dergelijke termen komen in diverse artikelen in het wetboek voor. Daarbij is onderscheid te maken in twee hoofdgroepen. Er zijn delicten waarbij de waarneming en de waarneembaarheid door het publiek of door derden beslissend is. Dat werd vroeger aangenomen t.a.v. de openbaarheid in verband met art. 239 Sr (exhibitionisme) en nog steeds in art. 141 (openlijke geweldpleging). Openbare plaatsen, maar ook algemeen toegankelijk gestelde plaatsen, onverschillig of de toegankelijkheid aan enige voorwaarde is gebonden vallen hieronder. In deze opvatting wees de Hoge Raad in 1931 zelfs een arrest volgens welk een plaats ook dan openbaar is, wanneer zij feitelijk voor het publiek toegankelijk is, ook al is de toegang verboden.⁶⁶ Voor de tweede groep delicten is de enkele waarneembaarheid niet genoeg, maar impliceert openbaarheid een zich wenden tot het publiek. In verband met art. 131 (opruiming tegen het openbaar gezag) gaat het dus weliswaar ook om de omstandigheid dat het feit gepleegd wordt in het publiek, 'd.i. wordt waargenomen door personen wier toevallige tegenwoordigheid mocht worden vermoed'. Maar als men zich tijdens een openbare bijeenkomst heimelijk tot een andere bezoeker wendt – op het gevaar van waarneembaarheid af – dan mist dat de voor opruiming vereiste publiciteit. Kort gezegd: de dader moet zich wenden tot het publiek – tot ieder die het zien of horen wil – zoals ook het geval is in art. 113 (verspreiding beledigend geschrift), eenvoudige be-

66. NLR art. 239, aant. 7; IIR 30 maart 1931, NJ 1931, 1030.

lediging (art. 266) en volgens R Emmelink ook in art. 240b (kinderporno).⁶⁷ Ook voor het openbaar maken in de zin van art. 137e Sr kan m.i. een zich wenden tot het publiek nodig worden geacht.⁶⁸

Het onderscheid tussen beide betekenisinhouden is van belang met het oog op de uitingsdelicten op het Internet. Benadrukt men de eis dat betrokkene zich tot het publiek wendt, dan zal mijns inziens zorgvuldig moeten worden onderscheiden tussen verschillende soorten verspreiding. Bij de racistische opmerkingen die hetzij om politieke dan wel om pervers-aanstootgevende redenen op het Internet worden gezet, wordt alleszins openbaar gemaakt. Maar juist in verband met obsceniteiten zoals kinderporno is volledig openlijke publicatie vrijwel non-existent.⁶⁹ Men zal daarom moeten bezien of de verzender een (beperkt) publiek wil bereiken, of niet. Dat lijkt de beste vervanging van het criterium dat men meer dan één exemplaar van een geschrift moet ronddelen, welk criterium voor zover het het Internet betreft obsoleet is geworden. Zo zal men in het bijzonder niet van verspreiding kunnen spreken als een privé-zender een e-mailbericht stuurt naar één privé-ontvanger. Dan wendt de zender zich niet tot een publiek, en men zal hem niet (analoog aan het genoemde arrest uit 1931) mogen aanrekenen dat e-mail op zich vrij gemakkelijk kan worden gelezen door derden. De man die kinderpornografische films in Manilla maakt, ze daar e-mailt naar zijn huisadres in Nijmegen en ze thuis *downloadt*, waarbij hij het risico van betrapting door de douane tot nul reduceert voert wel in (als bedoeld in art. 240b Sr), maar verspreidt niet en stelt niet openlijk tentoon. Men zal om hem te straffen ook het oogmerk van latere verspreiding of openlijke tentoonstelling moeten bewijzen. Dat betekent niet dat niet 'in het openbaar' wordt gehandeld, zodra men een e-mail verzendt. Degene die een campagne begint tegen zijn voormalige werkgever door per e-mail allerlei beledigende mededelingen te verspreiden onder een bestand aan geadresseerden, lijkt zich wel degelijk strafbaar te maken aan het delict van art. 266 Sr evenals degene die zijn bericht naar een nieuws- of discussie- of *Inter Relay Chatgroep* stuurt.

67. NLR art. 131, aant. 4; NLR art. 240b, aant. 5.

68. Anders J.L. van der Neut, *Discriminatie en strafrecht*, Arnhem 1986, 63-65.

69. A. Stange, *Pornographie im Internet, Computer und Recht* 1996: 424-428.

Naast verspreiding van bepaalde geschriften is ook het in voorraad hebben ervan onder omstandigheden strafbaar (art. 113, 132, 137e Sr). Het lijkt mij niet bezwaarlijk onder 'in voorraad hebben' ook te verstaan, het in een opslagplaats op de computer bewaren. Ingewikkelder ligt het of onder 'in voorraad hebben' ook gerekend kan worden het 'in de brievenbus' hebben. In de wereld *off-line* zal niemand een voorraad in de brievenbus bewaren. *On-line* is dat minder abnormaal: de ruimte in mijn 'mail-box' is onuitputtelijk. Bovendien zou elke kinderporno-ruil, indien een uitzondering voor de mail-box gemaakt zou worden, zijn materiaal daar bewaren.

3.4.3 *De vrijheid van meningsuiting e.d.*

Met betrekking tot de uitingsdelicten is de vrijheid van meningsuiting zoals neergelegd in art. 10 EVRM uiteraard van groot gewicht. Deze vrijheid heeft niet alleen betrekking op informatie en ideeën die als gunstig of als onschuldig worden ontvangen, maar ook op die welke 'offend, shock or disturb the state or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society"'.⁷⁰ De bescherming van deze vrijheid betreft spraak, drukwerk, radio en televisie, artistieke scheppingen, film en vermoedelijk (want anders dan de voorgaande nog niet verzekerd door een uitspraak van het Europese Hof voor de Rechten van de Mens) elektronische informatiesystemen.⁷¹ Het belang van dit grondrecht blijkt als we in herinnering roepen, dat het Internet tijdens de coup in de Sovjet Unie, tijdens de *sit-in* op het Tianaminplein en tijdens de oorlog in Bosnie (de zgn. *Peacelink*) werd gebruikt door democratische groepen om contact te houden met de vrije wereld.

Hiertegenover staat dat het Internet ook wordt gebruikt om bomrecepten en kinderporno te verspreiden, en berichten van voetbalvandalen die met elkaar willen vechten, of van niet altijd volstrekt nobele guerilla-groepen. Alleen al het (principeel bezien) geringe verschil tussen het aan dissidenten stem gevende

70. Sedert EHRM 7 december 1976, A24, NJ 1978, 236 (Handyside) constante jurisprudentie.

71. D.J. Harris, M. O'Boyle, C. Warbrick, *Law of the European Convention on Human Rights*, London 1995: 379.

Peacelink en het aan guerrilla's stem gevende Conflictnet illustreert overigens hoe moeilijk het is om de mogelijkheid van inbreuken op de vrijheid van meningsuiting te legitimeren.

Natuurlijk maakt art. 10, tweede lid EVRM beperking mogelijk, maar de toelaatbaarheid daarvan moet onderwerp worden van nauwgezet onderzoek, waarbij zowel specifieke aspecten van het medium als de hoedschap worden betrokken. In het bijzonder zal met culturele verschillen tussen de lidstaten moeten worden rekening gehouden, hetgeen het EVRM ook toelaat. Maar die nationale '*margin of appreciation*' is niet absoluut. Bij het beoordelen van inbreuken beziet het Hof steeds of de inbreuk noodzakelijk was, hetgeen dikwijls neerkomt op een proportionaliteitsafweging. Daarbij wordt in het bijzonder rekening gehouden met de eventuele omstandigheid dat op alternatieve wijze aan dezelfde informatie kon worden gekomen.⁷² Verder lijkt er in de rechtspraak van het Hof ook verschil te zijn ten aanzien van de aard van de uitlating. Het beperken van politieke uitlatingen vergt (terecht!) een zware bewijslast bij de staat om de '*pressing social need*' aan te tonen; maar de lidstaten hebben nogal wat ruimte om een op de uitingenvrijheid gebaseerd verweer te verwerpen ('*for the protection of morals*') als het gaat om een artistieke expressie die het publieke debat niet of nauwelijks raakt.⁷³ In verhouding tot politieke expressie kan – op het gevaar van misverstand af – worden gesteld dat ten aanzien van artistieke expressie iets meer en ten aanzien van commerciële expressie de meeste ruimte wordt geboden aan de nationale cultuur en/of de censor.⁷⁴

Zo bezien behoeft een staat een fractie minder behoedzaam te zijn bij het aanpakken van kinderporno op het Internet dan van racistische propaganda. Daar is nog een argument voor. Het valt op dat bijvoorbeeld op racistische nieuwsgroepen zeer regelmatig berichten van anti-racisten verschijnen.⁷⁵ Het open karakter van het Internet en de interactieve mogelijkheden ervan maken

72. EHRM 26 november 1991, NJ 1992, 457 (Observer and Guardian/Spycatcher); EHRM 29 oktober 1992, NJ 1993, 544 (Open Door).

73. EHRM 24 mei 1988, NJ 1991, 685 (Müller); EHRM 20 september 1994, NJ 1995, 366 (Otto-Preminger-Institut).

74. D.J. Harris, M. O'Boyle, C. Warbrick, *Law of the European Convention on Human Rights*, London 1995: 414.

75. S. Zickmund, *Approaching the radical other: the discursive culture of cyberhate*, in S.G. Jones (ed.), *Virtual culture*, London 1997: 185-205.

het voor de racisten niet alleen gemakkelijker elkaar te bereiken (zoals meestal wordt benadrukt), maar ook moeilijker om zich geheel te isoleren in een immer radicaler wordend eigen kringetje. Juist de hermetische geïsoleerdheid die sommige radicale groepen eigen is, brengt de leden ervan tot daadwerkelijk niets ontziend optreden. Zo bezien kan het Internet ook een bondgenoot zijn in de strijd tegen verkondigers van obscene opvattingen.

Bij het denken over strafrechtelijke aansprakelijkstelling in het licht van art. 10 EVRM hoeft niet alleen aan de rechten van degene die illegaal via het net zou hebben gecommuniceerd te worden gedacht. Het optreden tegen *providers* heeft een ook voor de vrije meningsvorming van derden enorme invloed. Toen de Duitse *provider* DFN daartoe genoot door het Duitse OM de toegang tot de *provider* XS4All blokkeerde ('stroomopwaarts blokkeren') wegens de aanwezigheid van het linkse blad 'Radikal' in september 1996 en april 1997 betekende dit dat in Duitsland XS4all nauwelijks meer kon worden bekeken, hetgeen schade opleverde aan de 20.000 andere XS4all-abonnees. Aardig in verband met het eerder aangehaalde criterium van het EHRM – of op alternatieve manier aan dezelfde informatic kan worden gekomen – was dat het blad daarna via 43 andere *WWW-sites* en twee nieuwsgroepen op het Net verscheen en bovendien was het te verkrijgen bij een e-mail listserver.⁷⁶ De gevolgen van stroomopwaartse blokkades zijn dus groot. Als bepaalde groepen (bijvoorbeeld kinderen, studenten) beschermd moeten worden, dan dient dat liever stroomafwaarts te gebeuren, dat wil zeggen met behulp van technologieën die de rechthebbenden (bijvoorbeeld ouders, universiteiten) in staat stellen om de Internet-inhoud die hun woning binnenkomt te controleren. Dat levert dan overigens wel nieuwe problemen op: bijvoorbeeld in hoeverre een werkgever, universiteit of andere (particuliere) netwerkbeheerder censuur mag uitoefenen of inbreuk mag maken op de privé-sfeer van de gebruikers met wie hij een relatie onderhoudt die de verhouding tussen netwerkbeheerder en klant te boven gaat.⁷⁷

76. Illegale en schadelijke inhoud op het Internet, COM(96) 487 def. p. 17.

77. C. Kadie, Computer and academic freedom news's list of banned computer material on college campuses, in Ludlow (1996): 301-310. Zie ook EHRM 25 juni 1997, NJCM-bulletin 1997: 765-767 en 1088-1092 (Halford).

3.5 Aantasting van de infrastructuur en de nationale veiligheid

Een laatste aparte categorie van schade waarbij het Internet een bijzondere betekenis heeft, betreft de schade aan de infrastructuur zelf. Dat betreft niet alleen de telecommunicatieve infrastructuur, maar ook de bancaire sector, de energievoorziening, kwesties van ruimtelijke ordening en vervoer (waterkeringen, spoorwegen), en vitale dienstverlening bijvoorbeeld op het vlak van de gezondheidszorg. Een voorbeeld van dat laatste leveren de Italiaanse hackers ('*crushers*') die de codes van bloedzakjes bij een bloedbank verwisselden. Een recent Amerikaans rapport overdrijft niet, als wordt gesteld: 'Our security, economy, way of life and perhaps even survival are now dependent on the inter-related trio of electrical energy, communications and computers.'⁷⁸

In militaire kring wordt reeds in termen van aanval en verdediging met betrekking tot de informatiekkanalen gedacht, te meer daar militaire en civiele infrastructuren steeds minder onderscheiden van elkaar raken. John Deutsch, directeur van de CIA, liet in dit verband in juni 1996 voor een Senaatscommissie al de term elektronische Pearl Harbour vallen.⁷⁹ Oceanen en bevrindende buurlanden bieden geen garantie meer voor de veiligheid. Dat betekent dat de Amerikanen van oordeel zijn dat dreigingen die via het Internet verlopen niet alleen een verantwoordelijkheid zijn voor de politic, maar tevens voor binnenlandse veiligheidsdiensten en de krijgsmacht. Het is namelijk op het moment dat het bestaan van een saboteur of een spion blijkt, niet te zien of het gaat om een industriële spion van een concurrerend bedrijf (art. 273 Sr), een individuele misdadiger, een politiek gemotiveerde terrorist, dan wel een spion van een vreemde mogendheid (art. 98-98c Sr). Het net biedt hen allen snelheid, relatieve anonimiteit en het vermogen grote hoeveelheden gegevens te vernielen of te kopiëren. Het is in dit licht van bijzonder belang dat eventuele bedrijven die dit aangaat gevoelig worden gemaakt voor deze strategische aanleggenheid en niet zwijgen – zoals i.v.m. fraude – omdat ze menen dat ze anders hun goede naam te grabbel gooien.

78. The President's Commission on Critical Infrastructure Protection, *Critical Foundations – Thinking Differently*, oktober 1997.

79. Martin (1997): 51.

In het Nederlandse materiële strafrecht worden in art. 161 sexies en septies speciale gevallen van vernieling van geautomatiseerde werken voor telecommunicatie strafbaar gesteld, indien storing ontstaat, gemeen gevaar voor goederen, levensgevaar te duchten is en/of het feit iemands dood ten gevolge heeft. In andere gevaarzettingsdelicten wordt onder specifieke omstandigheden strafbaar gesteld het 'vernielen, beschadigen, of onbruikbaar maken' van waterstaatswerken, elektriciteitswerken, (lucht)verkeerswerken, spoorwegen, veiligheidstekens voor lucht- en scheepvaart, (lucht)vaartuigen en gebouwen, terwijl aparte strafbaarstellingen betrekking hebben op gevaarlijk gedrag met betrekking tot waterreservoirs, het milieu, en radioactief materiaal (zie boek II, titel VII, Sr). Het is denkbaar dat ook via het Internet de aldus beschermde publieke goederen in gevaar worden gebracht. Het komt mij voor dat bij het onbruikbaar maken ook kan worden gedacht aan een via het Internet uitgevoerd bombardement met duizenden berichten tegelijk om de ontvanger aldus te overbelasten of om diens computergeheugen te laten vollopen door duizenden verzoeken om automatische reacties te verzenden zonder deze van een retouradres te voorzien. Niettemin is een terminologische wetswijziging van deze artikelen nodig geacht in het ontwerp Telecommunicatiewet.⁸⁰ Ook de (op zich het eigendomsrecht beschermende) artikelen 351 en 351bis Sr zijn in dit verband van belang. Strafbbaar volgens deze artikelen is het opzettelijk en wederrechtelijk (resp. culpoos) beschadigen (etc.) van spoorweg- of elektriciteitswerken, geautomatiseerde werken voor opslag of verwerking van gegevens of werken voor telecommunicatie, werken dienend tot waterkering, waterlozing, gas- of waterleiding of riolering, voor zover deze werken ten algemene nutte gebezigd worden, dan wel goederen of werken ten behoeve van de landsverdediging. In de praktijk worden op het Internet ook bomrecepten en 'crash-programma's' geplaatst zoals door het vernielzuchtige type hacker worden gehantcerd. Mij lijkt dit strafbaar te achten krachtens art. 133 Sr; het (voorwaardelijk) opzet gericht op het plegen van een strafbaar feit zal in de genoemde voorbeelden dikwijls aannemelijk zijn. Art. 10, tweede lid EVRM laat inbreu-

80. TK 1996-97, 25 533, 3, p. 143.

ken op de uitingsvrijheid toe ter voorkoming van strafbare feiten en juist met het oog daarop is art. 133 Sr geschreven.

In de praktijk ligt de grootste kwetsbaarheid die betrekking heeft op het Internet zelf in de sfeer van het krijgen van niet-geautoriseerde toegang, m.n. doordat via het binnendringen bij *access providers* vervolgens programma's worden geïnstalleerd waardoor *log-in* informatie van de gebruikers (inclusief hun paswoorden e.d.) wordt verkregen.⁸¹ Men dient zich daarbij te realiseren dat dit '*password sniffing*' vooral van belang is omdat dikwijls via de ongeautoriseerde toegang tot een eerste netwerk een door-gang naar een tweede netwerk wordt gevonden. In feite gaat het hierbij niet om een kwetsbaarheid van het Internet zelf, als wel om kwetsbaarheden van access-systemen die met het Internet zijn verbonden. De *providers* kunnen zich wat mij betreft als een postbode opstellen, in die zin dat zij zich niet hoeven te bekommeren om de inhoud van de post, maar ze hebben wel meer verantwoordelijkheden dan de postbode om beveiligingen aan te brengen. Terecht worden daarom ook in de Wet op de Telecommunicatievoorzieningen eisen aan de exploitanten gesteld voor de technische veiligheid en betrouwbaarheid.

Tot slot verdient in verband met de nationale veiligheid nog melding het op grond van de In- en uitvoerwet uitgevaardigde Uitvoerbesluit strategische goederen 1963. Volgens art. 2 van dit besluit is uitvoer van bepaalde goederen zonder vergunning verboden en strafbaar als zwaarste soort economisch delict (art. 1 onder 1e WED). Het herhaaldelijk gewijzigde besluit kent onder meer als uitwerking de Vrijstellingsregeling strategische goederen 1992. Daaruit blijkt dat voor goederen die in het vrije verkeer van een aantal bevriende staten worden gebracht, geen vergunning nodig is, tenzij het gaat om (in een bijlage opgesomde) bijzondere goederen. Op die bijlage staan onder meer supercomputers alsmede (programmatuur voor) informatica-beveiliging (m.u.v. toegangscontroleapparatuur voor PIN-codes, apparatuur voor het bevestigen van authenticiteit van gegevens en cryptografische apparatuur speciaal ontworpen voor gebruik in

81. F. Lynn McNulty, Security on the Internet, statement before the subcommittee on Science, US House of Representatives 22 maart 1994.

apparaten voor bank- of geldtransacties).⁸² Daaruit is af te leiden dat andere middelen en functies ter verzekering van de toegankelijkheid, geheimhouding of integriteit van gegevens of communicatie (m.u.v. storingsbeveiliging) nimmer zonder vergunning mogen worden uitgevoerd.

Gaat het dan om het plaatsen van cryptografische programmatuur op het Internet, dan rijst de vraag of het enkele op het Internet plaatsen reeds als uitvoer kan worden beschouwd: me dunkt van wel. Misschien kijken wij in Nederland met enige verbazing aan tegen de vergeefse pogingen van de Amerikaanse autoriteiten om Phil Zimmerman die op ideële grondslag (gratis) het door hemzelf ontwikkelde sterke encryptieprogramma '*Pretty Good Privacy*' (zie ook 5.2) op het Internet zette, strafrechtelijk aansprakelijk te stellen.⁸³ Maar als het feit in Nederland of door een Nederlander was gepleegd had deze tot 6 jaar gevangenisstraf kunnen worden veroordeeld.

4 INTERNATIONAAL STRAFRECHT

Een van de meest in het oog springende problemen met betrekking tot Internet en strafrecht is het vraagstuk van de mondialiteit – of men het Internet nu definieert in termen van '*Cyberspace*' of in termen van territoriaal gebonden havens van waaruit de Internet-zee wordt bevaren. Er kan toegang gezocht zijn in het ene land, data gemanipuleerd in het tweede en de consequenties ervaren in het derde. Deze mondialiteit levert vragen op van materiële rechtsmacht: welke staat is bevoegd verdachten van een delict te vervolgen. Maar ook vragen van formele rechtsmacht: is het bewijs aangetroffen op een server in Nederland, of is het neergelegd op een hard disk van een *provider* in een andere staat?

82. Uitvoerbesluit strategische goederen 1963, Stb. 128 met de 21ste wijziging van maart 1996, Stb. 223; deze laatste wijziging diende ter incorporering van het J3-Besluit van de Raad van 19 december 1994, en Vo 3381/94, PbEG L 367 beide inzake 'dual use' goederen; Vrijstellingsregeling strategische goederen 1992, Stcrt. 233, gewijzigd Stcrt. 1994, 50.

83. Omdat Zimmerman zijn programma niet verkocht had – en alleen daarom – kon hij niet (zoals de overheid had gewild) vervolgd worden ter zake van illegale export van strategisch materiaal.

4.1 Materieelrechtelijk jurisdictierecht

Uitgangspunt in het rechtsmachtrecht is het recht van de *locus delicti*, het territorialiteitsbeginsel van art. 2 Sr. Dat artikel levert twee vragen op: wat betekent 'in Nederland' en wat is het 'zich in Nederland aan een strafbaar feit schuldig maken'. Die eerste vraag betreft het feit dat niet alleen het grondgebied het antwoord oplevert of in Nederland is gehandeld, maar dat ook bepaalde territorialiteitsficties bestaan. Men denke aan de territoriale wateren, de luchtkolom boven Nederland en installaties die bestendig verblijven op volle zee (boorinstallaties, kunstmatige havens). Ik meld deze territorialiteitsficties omdat denkbaar is dat we ze ook zouden laten gelden voor de laagbanige of in elk geval voor de geostationaire satellieten die over enkele jaren de telecommunicatie en daarmee ook de Internetcommunicatie in overwegende mate zullen beheersen.⁸⁴

De tweede vraag, waar de *locus delicti* is, is een vraag die bij formeel omschreven delicten niet moeilijk is te beantwoorden – de plaats van handelen. Bij delicten met een materiële omschrijving is de vraag of het gaat om de plaats van handeling of de plaats waar het gevolg intreedt. We lijken nog uit te gaan van de lichamelijke gedraging, maar deze leer is geamendeerd tot de leer van het instrument – of die van de verlengde arm van de dader.⁸⁵ De leer van het instrument is in het Singapore-arrest nog verder opgerekt:⁸⁶ als plaats van een bewezenverklarde oplichting was mede aan te merken de plaats waar het slachtoffer tot het gewenste gedrag werd bewogen. Men duidt dit aan als ubiquiteitstheorie: één delict kan op meer plaatsen rechtsmacht op grond van het territorialiteitsbeginsel opleveren. Recent werd in een arrest over de verspreiding van de ontkenning van de Holocaust overwogen: 'Als plaats waar het in art. 137e, eerste lid aanhef en onder 2 Sr strafbaar gestelde feit wordt begaan heeft mede te gelden de plaats waar de desbetreffende voorwerpen zijn ontvangen.'⁸⁷ Hoe dicht deze interpretatie ook aan mag

84. M. Hegener, Een telefoongids in 0,002 seconden thuis, NRC Handelsblad 23 december 1997 meldt dat er 40 satellietvloten (bij elkaar 1100 satellieten) daadwerkelijk in voorbereiding zijn.

85. HR 6 april 1915, NJ 1915, 427 (Azewijnse paard).

86. HR 6 april 1954, NJ 1954, 368.

87. HR 25 november 1997, nr. 105.393.

zitten tegen de leer van het gevolg, er wordt van uitgegaan dat de laatstbedoelde leer nog niet is aanvaard: het is immers te gek als Zwitserland via het territorialiteitsbeginsel rechtsmacht kan claimen, omdat iemand in Nederland een klap op het hoofd kreeg, waaraan hij in een Zwitsers ziekenhuis overlijdt.

Hoewel de ubiquiteitstheorie diverse jurisdicties mogelijk maakt zijn daarmee nog niet alle problemen de wereld uit en dat komt doordat het Internet niet alleen de ruimtelijke dimensies doorbreekt, maar ook de tijd. Spectaculair is het voorbeeld van dr. Philip Nitschke die een via het Internet te downloaden euthanasie-softwareprogramma heeft ontwikkeld met een bijbehorende injectiespuit (die werkt als een soort printer) en dodelijk 'medicijn', waarmee vier Australiërs zich inmiddels van het leven hebben beroofd.⁸⁸ Maakt Nitschke zich nu schuldig aan hulp bij zelfdoding in Nederland, wanneer hier iemand dit programma daadwerkelijk gebruikt, wanneer iemand het *downloads*, of vindt het strafbare feit plaats als hij de software in Australië op het net zet? Op zich is het al interessant welk delict het meest in aanmerking komt en de beantwoording van die vraag beïnvloedt vermoedelijk ook die over de gestelde vraag, maar het gaat me er nu alleen om te illustreren dat wat in *real life* doorgaans op één moment plaatsvindt dankzij het Internet in preciezer af te bakenen deelbeslissingen uiteenvalt.

De leer van het instrument schept in verband met Internet territorialiteitsaanspraken ten aanzien van elke gedraging die waar ook ter wereld plaatsvindt en waardoor een bericht op het net terechtkomt. Het gaat mij nu niet om het juristenprobleem van de zgn. positieve rechtsmachtconflicten; daar komen de diverse landen wel uit. Belangrijker acht ik dat uiteindelijk deze interpretatie ertoe leidt dat bijvoorbeeld de Nederlandse uitings- en verspreidingsdelicten universele gelding krijgen.⁸⁹ Maar dezelfde redenering kunnen andere staten hanteren. Dat merkte het echtpaar Thomas – dat in het liberale Californië een '*Amateur Action Bulletin Board System*' beheerde – toen ze door iemand van de postale recherche uit het preutser Tennessee werden ver-

88. www.taunet.net.au/deliverance/default.html.

89. Zo ook C.B. van der Net, Locus delicti op het Internet, Computerrecht 1996/3: 90-94; idem, Strafrechtelijke jurisdictie in een digitale omgeving, bijlage bij ITeR workshop 5 maart 1997.

volgd. De rechter stelde dat ('anders dan het Internet'?!), een BBS onder controle is van een operator. Als iemand uit Memphis zich aanmeldt, aanvaardt de operator de verplichting zich te houden aan de standaard van Memphis.⁹⁰ En in 1995 oordeelde het Duitse OM dat 200 nieuws- en discussiegroepen vanwege hun pornografische of rechtsradicale inhoud niet in overeenstemming met het Duitse recht waren; *on-line* aanbieder CompuServe werd verzocht de toegang tot die nieuwsgroepen te blokkeren. Omdat het eerst niet lukte onderscheid te maken tussen Duitse en andere abonnees, schorste CompuServe voor alle 5,8 miljoen abonnees uit de hele wereld de toegang tot die groepen, hetgeen het protest uitlokte dat de Duitse zedelijkheidsnormen werden geëxporteerd.⁹¹

Mensen, zoals het echtpaar Thomas, worden vervolgd voor feiten waar ze niet op rekenen en voor feiten die hun landgenoten wellicht ook helemaal niet strafwaardig vinden. En staten met de meest stringente wetgeving kunnen, zoals Duitsland deed, hun stempel op het Internet drukken, terwijl het voor de gebruiker natuurlijk ook onmogelijk is het recht van alle aangesloten landen te kennen. Nederland zal overigens geen rechtsmacht claimen wanneer het gaat om uitingen op het Internet die niet duidelijk op Nederland zijn gericht.⁹² Maar dat Nederland terughoudend is, betekent niet dat het buitenland dat dan ook is.

Nu zou men kunnen streven naar een inperking van deze vergaande rechtsmacht. Daarbij kan voor zover het gronddelict op het Internet wordt gepleegd (zoals bij uitingsdelicten) aansluiting worden gezocht bij het actieve nationaliteitsbeginsel: de nationaliteit – of in een aangepaste versie het domicilie – van de verdachte geeft dan de doorslag voor de vervolgbaarheid. Dat is niet nodig als het gronddelict niets met Internet te maken heeft (bijv. drugssmokkel). Het is dan uiteraard van belang te kunnen weten welke nationaliteit een bepaalde gebruiker van het Internet heeft. Daarom is de suggestie gedaan om analoog aan de

90. *US v. Thomas*, 6th Circuit 29 januari 1996, onder meer aangehaald in Rasch, o.c.

91. Illegale en schadelijke inhoud op het Internet, GOM(96) 487 def. p. 17; zie ook U. Jäger & M. Collardin, *Die Inhaltsverantwortlichkeit von Online-Diensten*, Computer und Recht 1996: 236-240.

92. Aldus A. Patijn in: I. van den Berg, H. Hymans en A. Schmidt (red.), *Regulering van het Internet*, Alphen/Diegem 1997 (IteR 9), p. 71.

situatie op zee elke homepage een nationaliteitsvlag te laten dragen.⁹³ Wat daar ook van zij, er is ook nog het rechtspolitieke probleem dat bij de hegemonie van het nationaliteits- of eventueel het domiciliebeginsel de lidstaat waar een inbreuk op de rechtsorde is gemaakt, erop moet kunnen vertrouwen dat de betreffende andere staat – zo mogelijk – optreedt. Dat zal alleen het geval zijn bij (gekwaliceerde) dubbele strafbaarheid (art. 5, eerste lid ten tweede Sr). Dit laatste levert het aardige inzicht dat het nationaliteitsbeginsel precies het tegengestelde bezwaar heeft aan dat van het territorialiteitsbeginsel. Uiteindelijk leggen landen met de meest liberale wetgeving (vanwege de eis van dubbele strafbaarheid) hun stempel op het Internet op. We moeten echter niet vergeten dat een staat er een voordeel in behoort te zien, dat een onderdaan niet gestraft wordt voor iets wat in het eigen land toelaatbaar is. Dat voordeel lijkt mij zwaarder te wegen dan de wens om een vanuit het buitenland opererende niet-nationaal te kunnen straffen op grond van het territorialiteitsbeginsel voor iets wat hier (waar het instrument zijn werking heeft) strafbaar is; om van de uitleveringsproblemen in dat laatste geval nog maar te zwijgen. Zo bezien is er veel te zeggen voor de hegemonie van het nationaliteitsbeginsel. Omdat het ondenkbaar is dat staten bij verdrag afstand zullen doen van hun aanspraken op grond van het territorialiteitsbeginsel, men ik dat ten dezen gestreefd zou moeten worden naar een beleidsmatige afspraak inzake de goede rechtsbedeling, bijvoorbeeld middels een orgaan als in 2.3 bedoeld, om alleen op grond van het actieve nationaliteitsbeginsel of het domiciliebeginsel te vervolgen. Indien zo'n afspraak onmogelijk is, dan zou op de lange duur in Nederland toch een informatiepunt moeten komen waar gebruikers van het Internet de vraag kunnen voorleggen, wat in het buitenland wel of niet strafbaar is.⁹⁴

4.2 *Formeelrechtelijke internationale aspecten van het Internet*

Niet alleen het materiële recht levert jurisdictieproblemen op, maar ook het formele. Op zichzelf lijkt er geen enkel bezwaar

93. Onder meer door J. Boek in: I. van den Berg e.a. (1997), p. 66 e.v.

94. Zie ook G.G.Th. Wierda, Een slot op de deur, *Computerrecht* 1996/6: 233-235.

als Nederlandse opsporingsambtenaren zich via het Internet be-geven naar open toegankelijke sites die – laten we nu maar zeg-gen – een natuurlijke band met een vreemde staat hebben.⁹⁵ De stelling in de memorie van antwoord bij de wet computercriminaliteit dat geen onderzoek mag worden verricht in computer-gegevens die zich fysiek op het grondgebied van andere staten bevinden, gaat ten onrechte uit van een ‘pakketjes-paradigma’ – alsof een buitenlandse ‘home page’ niet zou mogen worden bekeken!⁹⁶ Ook omgekeerd is er dunkt me geen probleem met een Amerikaans onderzoek dat zich niet verder strekt dan het werpen van een blik op een Nederlandse home page. Die situatie is wellicht het best te vergelijken met die waarin tijdens een Amerikaanse telefoontap op een Amerikaanse telefoon, een Neder-lander opbelt: het feit dat een buitenlander belt hoeft de Ame-rikanen niet te nopen tot het uitzetten van de tap.⁹⁷

Het is iets anders, of de Nederlandse opsporingsambtenaren ook zo’n buitenlandse site of discussiegroep zouden mogen betre-den als daarvoor een identificatie of betaling nodig is. In het nationale recht zie ik ook daarin geen probleem – al lijkt dit wel een soort handeling om ex art. 152 Sv vast te leggen. Maar in het internationale verkeer rijst dan de vraag of de Nederlandse amb-tenaar zijn optreden niet zou moeten melden aan de nationale autoriteiten van het ‘ontvangende’ land. In de *United Nations Manual* staat hierover: ... ‘the direct penetration by prosecuting authorities of foreign data banks generally constitutes an infrin-gement of the sovereignty of the State of storage (and often in a punishable offence); however, there might be some specific exceptions that could be developed internationally in which di-rect access to foreign data banks via telecommunication net-works could be permissible and the lengthy procedure of mutual assistance avoided.’⁹⁸ De Amerikaanse justitie wenst in elk geval van benadering van Amerikaanse *providers* op de hoogte te wor-den gesteld. Nog weer een stap verder gaat de in de volgende paragraaf te bespreken vragen of de Nederlandse opsporings-

95. Zo ook P. de Hert en K. Bodard, Internetmisdaad: een uitdaging, A.J.T.-dos- sier 1996-97 nr. 7, p. 111.

96. TK 21 551, 6, p. 22.

97. M. Soiné, Fahndung via Internet, Neue Zeitschrift für Strafrecht, 1997 (4): 166-169; en (7): 321-325.

98. United Nations Manual (1995): para 153.

ambtenaar daarbij een valse naam mag opgeven, of in het buitenland zonder toestemming in een bestand mag grasduinen (*hacking*).

Ook omgekeerd zullen wij het niet juist achten als bijvoorbeeld de Amerikaanse autoriteiten zelfs zonder dat de Nederlandse autoriteiten dit weten een Nederlandse *access-provider* 'hacken'. Dergelijke vormen van opsporing van Internet-gerelateerde delicten vergen tenminste verzoeken om kleine rechtshulp. Overigens zijn in verband met de kleine rechtshulp de internationale verschillen ten aanzien van de strafbaarheid van computercriminaliteit een minder groot probleem dan wel wordt gesuggereerd.⁹⁹ Een hoofdgregel van het kleine rechtshulprecht is immers – anders dan van het uitleveringsrecht – dat dubbele strafbaarheid niet is vereist.¹⁰⁰

Misschien is het echter wel zinnig om internationaal af te spreken dat in afwachting van een rechtshulpverzoek de politie uit de ene staat aan collega's in een andere staat kan vragen voorlopig vast te leggen welk communicatieverkeer er is geweest via een bepaalde *provider*. De kleine rechtshulpprocedure is immers in sommige gevallen te omslachtig: als een Belg via *providers* van een Griekse universiteit en een Amerikaanse kerk een Nederlandse *provider* hackt en berooft, moet omwille van de spoedige voortgang van het onderzoek niet te veel tijd verloren gaan met verzoeken aan Griekenland en de VS. Het bewijsmateriaal zal uit België en Nederland komen en daartoe zullen formele rechtshulpverzoeken nodig zijn; maar de sturingsinformatie uit Griekenland en de VS zou wellicht achteraf kunnen worden gelegitimeerd door een melding aan de justitiële autoriteiten aldaar. Nadere internationale afspraken met het oog op Internet lijken in ieder geval nuttig en er zijn vermoedelijk wel meer onderwerpen ten aanzien waarvan een zekere globalisering van de opsporing gewenst is.¹⁰¹ Daarbij zal evenwel enige voorzichtigheid

99. Zie voor die suggestie de Beleidsadviesgroep computercriminaliteit, Digitaal rechercheren, juni 1996: 9; ook relativerend zijn De Hert en Bodard (1996-97).

100. Zie bijvoorbeeld art. 1 en 2 Europees Rechtshulpverdrag.

101. Zie de in 1995 door het ministercomité van de Raad van Europa aangenomen Recommendation R(95) 13 concerning problems of criminal procedure law connected with information technology; H. Kaspersen, Aanbeveling Raad van Europa inzake de opsporing van strafbare feiten in een geautomatiseerde omgeving, Computercrrecht 1995: 289-291.

moeten worden betracht, al was het maar met het oog op de nationale soevereiniteit. Zo vind ik het toch een ietwat zorgwekkende bevinding dat de Raad van de Europese Unie en de Amerikaanse FBI sinds november 1993 samenwerken aan een plan 'to introduce a global telecommunications tapping system'.¹⁰² Deze samenwerking is moeilijk te doorzien. Een resolutie van de Raad van Europa van 17 januari 1995 (die pas twee jaar later werd gepubliceerd!) stelt onder meer:

'De wetshandhavingsdiensten moeten kunnen beschikken over real-time, continue controle mogelijkheden voor de interceptie van telecommunicatieverkeer: (...)

De netwerkexploitanten/dienstenverstrekkers zouden de wetshandhavingsdiensten één of meer interfaces moeten verschaffen van waaruit de geïntercipieerde communicatie naar de bewakingspost van de wetshandhavingsdienst kan worden gezonden. (...) Voor de wetshandhavingsdiensten is het noodzakelijk dat de intercepties zo worden uitgevoerd dat noch het doelwit van de interceptie noch andere onbevoegde personen eventuele veranderingen opmerken die zijn aangebracht om te voldoen aan de interceptieopdracht'.¹⁰³

Op 23 november 1995 werd vervolgens een Memorandum of Understanding getekend door 15 EU-lidstaten voor uitbreiding van de werking van deze resolutie naar derde landen. Er waren twee contactadressen: het secretariaat-generaal van de Raad van de Europese Unie en de directeur van de FBI in Washington. De relatie met de FBI is daarom zo opmerkelijk, omdat de Amerikanen samen met het Verenigd Koninkrijk, Canada, Australië en Nieuw Zeeland het wereldwijde – op Intelsat en *non-Intelsat* communicatiesatellieten gerichte – ECHELON-interceptiesysteem hanteren. Uit alle individuele, zakelijke en overheidscommunicatie die via satellieten verloopt worden op grond van een *'Dictionary-programma'* berichten geselecteerd en aan de betref-

¹⁰² Statewatch report, European Union and FBI launch global surveillance system (www.privacy.org/pi/activities/tapping/statewatch_tap_297.html) met verwijzing naar 'Interception of communications, report to COREPER, ENFOPOL 40, 10090/93, Confidential, Brussels, 16.11.1993; Memorandum of Understanding concerning the lawful interception of telecommunications, ENFOPOL 112, 10037/95, Limite, Brussels 25.11.95.

¹⁰³ Resolutie van de Raad van 17 januari 1995, PbEG 4 november 1996, C 329/1-6.

fende veiligheidsdiensten doorgegeven (zie over dergelijke surveillancemogelijkheden ook 5.3).¹⁰⁴ Tegen die achtergrond van het bestaan van een telecommunicatief surveillancesysteem, waarbij het niet gaat om het gericht af luisteren van aansluitingen, maar om het scannen van tekstinhouden, krijgt de frase '*real-time*, continue controlemogelijkheden voor de interceptie' uit de resolutie een wat mij betreft onverwachte betekenis. Met het oog op het toenemend gebruik van satellieten bij telecommunicatie lijkt meer duidelijkheid over deze materie geboden.¹⁰⁵

5 FORMEEL STRAFRECHT

Strafvorderlijke vragen kunnen vanwege het Internet rijzen bij de opsporing van allerlei soorten delicten. Te denken is aan het achterhalen van afspraken die via het Internet werden gemaakt over de plaats van import van een lading heroïne. In een gedocumenteerd geval wisten betrokkenen dat hun telefoon werd afgeluisterd, en daarom zond een Oekraïense godfather via het Internet een bruiloftsfoto van zijn dochter aan zijn Italiaanse collega: in een moedervlekje op de wang van de bruid zat een brief verstopt met alle relevante gegevens.¹⁰⁶ Een ander voorbeeld is het snel integraal verplaatsen van boekhoudingen van criminele organisaties, waardoor het buitengewoon lastig wordt die boekhoudingen ooit terug te vinden.

Op dit moment houden wat de politie betreft zowel de interregionale bureaus computercriminaliteit, als de superspecialisten van de Centrale Recherche Informatiedienst (CRI) en de Dienst Technologie en Operationele Ondersteuning zich bezig met het

104. N. Hager, *Secret Power*, New Zealand's role in the International Spy Network, 1996; idem, *Exposing the global surveillance system*, *Covert Action Quarterly* winter 1996-97 (nr. 59).

105. Zie ik het goed dan hebben noch de Nieuw Zeelandse, noch de Australische of de Britse autoriteiten hier meer helderheid over willen verschaffen; *New Zealand Herald* 21 juli 1997 inzake de aanpassing van de Nieuw Zeelandse Crimes Act; vraag van senator Bourne aan de Australische minister van defensie op 19 maart 1997, www.democrats.org.au/democrats/parliament/1997/0507/avbgou.html; (Britse) Correspondence with Ministers, 9th Session 1995-96, HL 74, pages 26-29.

106. Martin (1997): 42-43.

Internet, terwijl in dit verband ook wordt samengewerkt met het Gerechtelijk Laboratorium. In de praktijk, zo werd mij in gesprekken duidelijk, houden deze specialisten zich echter voor meer dan 90% bezig met het bieden van ondersteuning in gevallen waarin een verdachte een gewoon strafbaar feit heeft gepleegd, maar daarbij een computer heeft gebruikt.¹⁰⁷ Het toegankelijk maken van digitaal bewijsmateriaal lijkt voor hen op dit moment een hogere prioriteit dan het opsporen op het Internet. Zo zijn inmiddels technieken ontwikkeld om bewijsmateriaal dat in een computer wordt aangetroffen op verantwoorde wijze veilig te stellen (zgn. *full image* kopieën van de schijf); voor verdediging en rechter kan nu welhaast bewezen worden dat niet met het materiaal is geknoeid door de politie.

Achtereenvolgens zal worden ingegaan op het opsporen van strafbare feiten, de moeilijkheden die encryptie en anonimiteit opleveren, en de bewijsgaring in het bijzonder met betrekking tot gegevens over verdachten althans het wettelijk geregelde onderzoek in geautomatiseerde werken (art. 125i-125n Sv).

5.1 Opsporing van strafbare feiten

In de meeste gevallen waarin bij het plegen van strafbare feiten van het Internet gebruik wordt gemaakt, zal het delict in de *real world* worden vastgesteld: de drugs waarover per Internet werd bericht worden daadwerkelijk vervoerd. Ten aanzien van dit type vaststelling is te vermelden dat de Raad van Hoofdcommissarissen aangifte via het Internet mogelijk wil maken.¹⁰⁸ Aannemelijk is dat ook (meer) van het Internet zal worden gebruik gemaakt bij het zoeken van vermiste personen en bij het vragen om informatie over gepleegde strafbare feiten.¹⁰⁹

Vooralsindien geen aanwijsbare slachtoffers vallen (in het bijzonder bij sommige verspreidingsdelicten), is de vraag hoe opsporingsambtenaren van een delict op de hoogte raken.

107. Twee hoofden en een medewerker van Interregionale Bureau's Computercriminaliteit, het hoofd van het DTOO, het Hoofd van de Afdeling Computeronderzoek van het Gerechtelijk Laboratorium en de coördinerend AG op het vlak van de computercriminaliteit, waren zo vriendelijk mij over hun werk ten aanzien van het Internet te vertellen.

108. Volkskrant 8 april 1997.

109. Zie Soiné (1997) en W. Bär, Öffentlichkeitsfahndung im Internet, Computer und Recht 1997: 422-431.

Een eerste manier is de melding van particulieren. Interessant is in dit verband het initiatief van een aantal *Internet-providers* tot de oprichting van een meldpunt kinderporno. Iemand richt zich dan tot het meldpunt; van daaruit wordt contact gezocht met de *provider*; deze wendt zich tot de gebruiker met de mededeling dat men van de betreffende data niet is gediend. Doorgaans haalt de gebruiker de porno dan van het Internet. Het delict is beëindigd, aangifte blijft uit en het bewijsmateriaal van kinderporno is verloren gegaan. Nu het meldpunt is ondergebracht bij de CRI is de geschetste werkwijze aan te merken, als een soort politiesepot. In de gevallen waarin de CRI vindt dat er strafrechtelijk moet worden opgetreden, is deze politiedienst in staat de beslissing terzake te nemen. Wat de rol van particulieren in verband met fraude betreft moet vastgesteld, dat de slachtoffers (banken, telecommunicatiemaatschappijen etc.) doorgaans geen belang zien in het erbij halen van de politie: wat is een telefoonfraude van fl. 86.000 op de 3,5 mld \$ jaaromzet van AT&T ten opzichte van het verlies van vertrouwen van beleggers en consumenten als die fraude bekend wordt? Die verklaring voor het feit dat de politie soms slechts bij toeval van zeer grote fraudes verneemt die bij het slachtoffer maar al te bekend zijn, stemt cynisch.

Een tweede manier waarop de politie op de hoogte raakt van delicten is de *data-surveillance*. Voor zover dit kijken op het Internet of een strafbaar feit wordt gepleegd, geschiedt door het surfen over publiek toegankelijke *web sites* lijkt er (zoals ook in 4.2 opgemerkt) niets aan de hand. Het is verdedigbaar, dat het bevragen van een of meer *web sites*, BBS'en of wat dan ook naar aanleiding van een tip moet worden beschouwd als opsporing, maar dat is het rijden in een auto naar een bepaalde plaats vanwege een tip ook. Dat dit als opsporingshandeling is aan te duiden, heeft dus voor de strafvordering verder geen betekenis. Er zijn ten aanzien van data surveillance echter twee bijzondere aspecten. Eerst wordt ingegaan op het probleem van legitimatie. Dan wordt teruggekomen op de surveillance op *provider* niveau. Tijdens het surfen over het Internet, het bezoek aan nieuwsgroepen e.d. wordt de gebruiker soms gevraagd zich te identificeren. Dan rijst de vraag of het toelaatbaar is dat politieambtenaren zich op het net van een alias bedienen. Hierbij dient onderscheid gemaakt te worden tussen het geval waarin een

politie-ambtenaar naar publieke gedeeltes van het Internet surft en daar waar hij particuliere één-op-één contacten via het net legt. De laatsbedoelde situatie doet zich voor, als een politie pseudo-klant contact legt met een verdachte. Dan zal de verdachte zonder dat hij het weet (en zonder cautie) via het Internet verklaringen afleggen tegen een opsporingsambtenaar. Dit is een vorm van informatie-inwinning en/of infiltratie. Van politie informatie-inwinning in de zin van art. 126j wetsontwerp Bijzondere opsporingsbevoegdheden zal sprake zijn, als een opsporingsambtenaar zonder dat kenbaar is dat hij als zodanig optreedt, stelselmatig informatie inwint over de verdachte, bijvoorbeeld door deel te nemen aan een *newsgroup*.¹¹⁰ Van infiltratie (art. 126h en p Wetsontwerp Bob) is sprake, als wordt deelgenomen aan de criminele groep: dat lijkt het geval wanneer een politieambtenaar bijvoorbeeld om toegang te krijgen tot een uitwisselingsplaats van kinderporno zelf enkele kinderpornoplaatjes verstrekt. Op dit moment zal daarvoor ook het Talloncriterium (niet uitlokken) gelden en is een dergelijke operatie slechts toelaatbaar na toetsing door de Centrale Toetsingscommissie van het openbaar ministerie (CTC). Verdergaande 'sting'-operaties op het Internet zijn uiteraard mogelijk, maar daarmee nog niet rechtmatig. In de Sisson-zaak reageerde een 45-jarige man op een Internet-bericht van Jessica, die zei dat ze 14 jaar was en dat 'older guys treat you grown-up'. Na 9 maanden ook seksueel expliciete correspondentie reisde Sisson naar een motel om haar te ontmoeten, waar hij werd gearresteerd wegens 'travelling across state lines for the purpose of engaging in a sexual act with a minor'. Jessica was een virtuele persoon van wie de teksten werden geschreven door een Amerikaanse politie-agente.¹¹¹

Het surfen op het Internet mag m.i. wel vanuit een gemaskeerde computer gebeuren. Dit is van belang omdat de informatie-*provider* (met cookies) kan zien wie zijn web-pagina bezoekt, zoals bleek toen de Amsterdamse politie onderzoek deed naar de confrontatie tussen Ajax/Feyenoord hooligans; en bij berichtenverkeer kan de ontvanger zien van welke account een bericht werd

110. Aldus uitdrukkelijk TK 1996-97, 25 403, 3, p. 34.

111. M.L. Cadell en S.E. Lucas, Accidents on the Information Superhighway: On-Line Liability and Regulation, *Richmond Journal of Law & Technology* 1996/2.

verzonden. Bij het bekijken van publiek domein op het Internet geldt wat mij betreft de mogelijkheid van anonimiteit als groot goed (zie 5.2), maar dat impliceert dat ik ook geen bezwaren zie tegen anoniem lezende agenten. Ook gaat het me te ver om van de politieambtenaren te vergen, dat ze als ze om ergens binnen te komen hun naam moeten opgeven, dan ook verplicht zouden zijn hun functie te vermelden. Twijfelachtig vind ik het of evenveel terughoudendheid mocht worden betracht ten aanzien van het eenmalig negeren van een mededeling bij een *site* of *newsgroup*, waarbij expliciet de toegang wordt geweigerd aan politie- en douane-ambtenaren (zoals porno-sites doorgaans aan minderjarigen). Het is wat mij betreft dan nog niet zeker dat er van de zojuist bedoelde politieke informatie-inwinning sprake is; dan is er immers geen stelselmatige informatie-inwinning en zolang de betreffende opsporingsambtenaar niet zelf handelingen verricht (bijvoorbeeld ter valsc identificatie of om deelnemers uit te horen) kan van misleiding door een overheidsfunctionaris ook nog geen sprake zijn.

Voor de beoordeling van de surveillance op *provider*-niveau is een korte technische uiteenzetting noodzakelijk. Wanneer gebruiker A via een *provider* met gebruiker B communiceert, dan is over deze communicatie op verschillende manieren iets te weten te komen. In de eerste plaats kan technisch bezien een tap het verkeer van A naar de *provider* onderscheppen. In de tweede plaats kan bij de *provider* een programma worden aangebracht, dat zodra een bepaald signaal doorkomt, aan een derde (bijvoorbeeld de politie) daarover bericht geeft. Het bepaalde signaal kan zijn het feit dat er een bericht van A komt; het kan zijn dat er een bericht naar B gaat (of naar een bepaald land); en het kan zijn dat er in het bericht een bepaald woord, beeld, 'geëncrypteerde *string*' (die misschien niet decodeerbaar is, maar wel herkenbaar doordat dezelfde zender deze *string* ook gebruikte in contact met een drugshandelaar) of wat dan ook is opgenomen. Het is praktisch mogelijk om al het verkeer op deze wijze te filteren dat langs een bepaalde *provider* loopt.¹¹² Indien de politie zonder zelf te *hacken* – wat naar verluidt in de VS wel gebeurt – een dergelijk programma wil aanbrengen, is meewerking van de *provider* nodig. Het is niet aannemelijk dat de *provider* zonder meer

112. Een andere indruk wekt nog TK 1996-1997, Aanhangsel 1370.

tot toestemming bereid is, al was het maar omdat deze vreest voor een civiele vordering van zijn cliënt op grond van de mogelijkheid aan te nemen inspanningsverplichting om de privacy van de gebruikers te beveiligen.

Het juridisch relevante verschil tussen surveillance en op een persoon gerichte opsporing, is aldus technisch bezien niet voor de hand liggend. Wil men alle communicatie van afzender A vernemen, dan is art. 8 EVRM zonder twijfel in het geding.¹¹³ Maar ook kan – zoals in het Echelonstelsel – op woorden worden gesurveilleerd: zodra het woord ‘bom’ in een bericht zit, kan automatisch een signaal worden verzonden aan de politie dat dit bericht langs kwam, van wie het afkomstig was en aan wie het gestuurd wordt; mutatis mutandis geldt hetzelfde voor het woord Colombia in het adres.

Hoewel dergelijke niet op verdachten gerichte surveillance die mijzelf doet denken aan totalitaire staten, misschien niet eens is op te vatten als inbreuk op de privacy, is zij dunkt me wel een ontoelaatbare inbreuk op de ook door art. 8 EVRM beschermde ‘correspondence’. Dat het niet gaat om het stelsmatig observeren van een aanwijsbare individu doet daar niet aan af, omdat correspondentie nu eenmaal per se wordt beschermd door art. 8 EVRM. Niet met zekerheid weerlegbaar is het tegenargument, dat bij gebrek aan surveillancebevoegdheden vaker gegrepen zal moeten worden naar het zwaardere middel van volledige interceptie jegens bepaalde personen. Maar ik schat nu eenmaal in dat het eerder om het een *en* het ander, dan het een *of* het ander gaat. Ik heb overigens geen aanwijzingen dat de Nederlandse politie reeds nu van de geschetste surveillancevorm gebruik maakt, maar de belangstelling ervoor bestaat en de programmatuur is, als ik goed ben ingelicht, relatief eenvoudig te verkrijgen.

5.2 Encryptie en anonimiteit

De inhoud van een van het Internet geplukt bericht zal dikwijls niet te lezen zijn, vanwege het gebruik van encryptie – maar dat

113. Ook telefoongesprekken vallen onder ‘correspondence’ volgens EIIRM 6 september 1978, AAc 1979, 327 en EIIRM 2 augustus 1984 (A-83); zie ook Hand. NJV 1988-I, p. 25 c.v. (A. Patijn) en Hand. NJV 1990-I, p. 50 c.v. (J. de Boer), welke auteurs ook communicatie tussen computers tot ‘correspondence’ rekenen.

betekent niet dat het feit dat er communicatie is geweest niet interessant kan zijn voor de opsporingsinstanties; de naam van de zender kan problemen opleveren als gebruik is gemaakt van een anonieme *re-mailer*. Op beide punten wordt ingegaan.

Als het om versleuteling gaat, lijken de VS en de Europese Unie tegenover elkaar te staan. Sinds Phil Zimmerman in juni 1991 het versleutelingssysteem '*Pretty Good Privacy*' op het net zette, is vooral de FBI een lobby begonnen om iedereen ervan te overtuigen dat vooral drugshandelaren, spionnen, terroristen en gewelddadige gangs bij dergelijke systemen baat hebben.¹¹⁴ Minder spectaculair, maar ook van belang is het feit dat encryptie ook het vermijden van belastingen en het witwassen van criminele verdiensten zal vergemakkelijken.

Hier tegenover staat de benadering die de dubbele betekenis van encryptie – voor versluiering en voor authenticatie – onderstreept. Positieve vormen van versluiering door encryptie blijken nu reeds bij het mobiele (GSM-) telefoonverkeer en bij het semafoonverkeer (zoals bijvoorbeeld om de noodzaak tot navulling van PIN-automaten te melden aan de bank). Willen andere nuttige communicatiestromen tot bloei komen – men denke aan het handels- en bankverkeer, maar ook aan berichtenuitwisseling in de sfeer van de gezondheidszorg – dan zal encryptie niet gemist kunnen worden. Daarnaast heeft encryptie nog aparte betekenis voor authenticatie, digitale handtekeningen en de zekerheid dat er niet geknoeid is met berichten.

In de discussie draait het bovenal om de vraag of versleutelde data (het kan zowel om communicatie als om opslag gaan) te decoderen moeten zijn voor de overheid.¹¹⁵ Volgens degenen die deze vraag positief beantwoorden, kunnen encryptiemiddelen alleen toelaatbaar zijn als de sleutel ergens is gedeponeerd. In de VS is wat dit betreft de zgn. Clipper Chip ontwikkeld, die de Internetgebruikers dwingt gebruik te maken van deze hardware, omdat de overheid ervan gebruik maakt en de chip voorkomt dat andere geëncrypteerde berichten worden geaccepteerd. Dit systeem of welk ander systeem dat een '*masterkey*' nocr-

114. Zie bijvoorbeeld de Statement of Louis J. Freeh, directeur FBI voor de Senate Judiciary Committee Hearing on Encryption, 9 juli 1997.

115. Zie het rechtsvergelijkende overzicht van A-M Kemna en A. Tuinder, *Regulering van encryptie*, Alphen/Diegem 1996; en de discussies in Ludlow (1996): 173-249.

legt bij de regering, een *trusted third party*, of een serie 'key recovery agents' die elk toestemming moeten geven, komt er op neer dat op grond van een rechterlijk bevel een versleuteld gegeven kan worden gedecodeerd met behulp van een bij een ander dan betrokkenen neergelegde ('in escrow gegeven') sleutel. Bezwaren hiertegen zijn dat de hoogst gevoelige geheime (verzameling) sleutel(s) voor langere duur moet worden veiliggesteld. De concentratie van decryptie-informatie is uiteraard op zich gevaarlijk zowel met het oog op 'foute' overheden, als met het oog op criminele of andere aanvallen.¹¹⁶

De andere benadering stelt dat versleuteling een defensief mechanisme is, waarmee je op zich geen kwaad kunt berokkenen weshalve de overheid vanwege de risico's voor privacy en briefgeheim niet zover mag gaan dat ze decodeerbaarheid eist. Bovendien ontwikkelen niet alleen de versleutelingstechnieken zich snel, maar ook de decodeerprogramma's en dat betekent dat het vastleggen van een bepaald programma eventuele belanghebbenden de mogelijkheid op een veiliger programma onthoudt. De slimme boef zal bovendien toch zijn eigen encryptieprogramma gebruiken, of een steganografie-programma, waarmee bijvoorbeeld door extreme verkleining tekst in een neutraal plaatje of een plaatje in neutrale tekst wordt verborgen. De discussie doet enigszins denken aan de problemen met de invoering van GSM-telefonie, die met opzet werd vertraagd teneinde het wettelijk af luisteren mogelijk te maken. Als ik het goed zie hebben wij in Nederland met een op grond van een rechterlijke machtiging aftapbaar en dan ook leesbaar te maken systeem niet veel problemen. Het van bovenaf regelen van encryptie-programma's heeft bovendien het voordeel, dat het veel eenvoudiger is standaardversleuteling te bewerktstellen (zoals reeds gebeurt bij GSM-telefonie). De kans op fouten neemt toe zodra versleuteling afhangt van handmatige activiteiten van degene met wie je communiceren wilt. Als we de nu bestaande situatie waarin e-mail door iedere derde die even z'n best doet kan worden gelezen, willen veranderen – en ook als we video-contacten

116. H. Abelson (en 10 andere cryptografiespecialisten uit het Amerikaanse en Engelse universitaire en bedrijfsleven), *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, World Wide Web Journal summer 1997 (www.w3j.com).

via 'secure tunnels' willen doen toenemen (teleconferenties) – is een dergelijk automatisch gebruik van encryptie onmisbaar. Tot decryptie van opgeslagen gegevens kan verplicht worden op grond van art. 125k Sv in geval van huiszocking of van het in 5.3 te bespreken art. 125j Sv. In het voorontwerp computercriminaliteit II wordt een vergelijkbare verplichting (van bijvoorbeeld beheerders van computersystemen) geïntroduceerd voor stromende gegevens, dat wil zeggen voor telecommunicatie. Aan de verdachte mag het bevel niet worden gegeven en de verschooningsgerechtigden hoeven het niet na te komen (art. 125m Sv). Dat de verdachte het bevel niet kan worden gegeven is een m.i. rijkelijk vergaande erkenning van het nemo teneturbeginsel. In het Saunders-arrest heeft het Europese Hof immers als grens van toelaatbare dwang gesteld de dwang om 'non-testimonial evidence' te geven.¹¹⁷ De wet mag een verdachte verplichten iets te verstrekken wat onafhankelijk van zijn wil bestaat: normaliter wordt dan gedacht aan vingerafdrukken of aan een administratie, maar waarom ook niet aan de sleutel op een encryptieprogramma? De wetgever is in dit verband niet te bekrompen geweest en heeft aansluiting gezocht bij de traditie in het commune strafprocesrecht om zelfs de uitlevering van goederen aan de verdachte niet af te dwingen. Mijn politieke informanten hadden anders dan de Beleidsadviesgroep computercriminaliteit geen probleem met art. 125k en 125m Sv.¹¹⁸

De mogelijkheid om je als een ander voor te doen op het Internet zorgt voor problemen. In het privaatrecht hebben de gebruikers zelf het probleem dat ze moeten kunnen bewijzen dat ze iemand zijn (en dat ze goed zijn voor hun woord); in het strafrecht ligt de moeilijkheid bij de politie om te bewijzen dat een bepaalde persoon op het net dezelfde is als de persoon met dezelfde naam in de *real world*. Toch moeten die problemen ons niet dadelijk op het spoor zetten van een mogelijk verbod op anonimiteit. Ook *off line* is er niets mis mee als u in Yab Yum of bij de boekwinkel een virtuele naam opgeeft zo lang u maar betaalt. Iets dergelijks zal zich ook op het Internet voordoen.

117. EHRM 17 december 1996, NJCM-bulletin 1997, p. 298-314 m.nt. E. Myjer (Saunders).

118. Beleidsadviesgroep Computercriminaliteit, Op weg naar ... digitaal rechercheren, 1996, p. 12.

Dat betekent, dat zelfs in het geval er een adequate oplossing komt om een digitale handtekening te plaatsen en/of de identiteit van een contractpartij vast te stellen, dit niet in de weg staat aan de mogelijkheid dat men in sommige (andere) gevallen als anonus wil optreden. Er valt in dit verband te denken aan de nieuws- en praatgroepen waar HIV-positieven, drugverslaafden of slachtoffers van een seksueel delict ervaringen uitwisselen. En er is toch ook weinig op tegen als personen in *Inter Relay Chatgroepen* – virtuele caf  s – onder aangenomen persoonlijkheid met elkaar communiceren; sommigen waarderen de experimenten waarbij deelnemers drastische rolwisselingen ondergaan ten opzichte van hun *real life*-persona (bijvoorbeeld de man die zich als vrouw voordoet) als verrijkend en stimulerend.¹¹⁹ David Chaum, de directeur van Digicash gaat zelfs nog verder en betreft het recht op anonimiteit ook op gewone, simpele contracten: 'The fundamental question is, do you as a payer have a right of control over your identity when you make a payment? If someone tells you when you make a purchase that you always have to identify yourself, you'd wonder what kind of country you're living in.'¹²⁰

Al deze, onderling verscheiden, toepassingen van anonimiteit maken het begrijpelijk dat de *Legal Advisory Board* van de Europese Commissie stelt: 'The LAB recognises that anonus communication poses difficulties to law enforcement purposes. Not unlike traditional media in the context of the Internet services will develop supporting anonus speech, while others will require identification. The right of anonymity and effective technical means to protect this right should be ensured for users.'¹²¹ Overigens laat de vraag zich stellen of het hier gepostuleerde recht aan art. 8 EVRM is te ontleen.

Uiteraard onderkent de LAB dat anonieme betalingen ook gedaan kunnen worden voor drugtransacties en huurmoorden.¹²²

119. Zie bijvoorbeeld A.S. Bruckman, *Gender Swapping on the Internet*, in Ludlow (1996): 317-325.

120. K. Kleiner, *Banking on electronic*, New Scientist (146) 8 april 1995.

121. European Commission Legal Advisory Board (1997).

122. F. Kuitenbrouwer, *Internet: de vrijheid voorop*, in C.H. Brands e.a., *Er is meer* (Swart-bundel), Deventer 1996: 301 herinnert in dit verband aan het verbod op anonieme muurkranten, welk verbod door HR 24 juni 1980, NJ 1981, 689 werd toegelaten. Hij acht het kennelijk aannemelijk dat een dergelijk verbod achterhaald is al was het maar vanwege de acceptatie →

Het strafprocesrecht zal daarom regels moeten bevatten om tot identificatie van gebruikers over te kunnen gaan. Dat valt in het bijzonder niet mee, als gebruik is gemaakt van zgn. anonieme *remailers*. Zo'n *remailer* wordt normaliter gebruikt om een afzender verborgen te houden voor de ontvanger; Amnesty International schijnt ervan te hebben gebruik gemaakt om informatieverzoeken aan (Turkse) dissidenten te kunnen afschermen. Als het de bedoeling is dat de zender post terugkrijgt van de ontvanger, dan wordt bij de anonieme *re-mail*-instelling een uniek nummer toegekend aan de verder onherkenbare afzender. Dan zal de (wellicht in een vreemd land gezetelde) *provider* (al dan niet onder dwang) moeten meewerken, wil men erachter kunnen komen wie de anonieme verzender is. Met het oog op de criminaliteitsbestrijding is ervoor gepleit het beginsel van wettelijke naspoorbaarheid in nationale en Europese gedragscodes voor *re-mailing*-activiteiten op te nemen, bijvoorbeeld ertoe strekkend dat deze instellingen identiteitsgegevens registreren.¹²³

5.3 Bewijsgeving

Is eenmaal vastgesteld dat een bepaald feit is gepleegd, dan moet vervolgens worden onderzocht wie het feit heeft gepleegd en welk bewijs daarvoor te vinden is.

Wat betreft de identificatie van verdachten die van het Internet gebruik maken of gebruik hebben gemaakt ligt er niet alleen een probleem bij de anonieme *remailers*. Art. 125f Sv – dat het vorderen van zgn. printgegevens mogelijk maakt met betrekking tot de vraag wie op een bepaald moment deelneemt aan het telecommunicatieverkeer – is op dit moment niet steeds bruikbaar, zie ik het goed, dan kan de PTT hooguit melden dat er met de telefoon van verdachte is gecommuniceerd met een *provider*, maar niet aan wie de *provider* het bericht heeft doorgezonden. De *provider* hoeft anders dan de PTT Telecom niets te bewaren en is een doorgeefluik (nog even los van de vraag of de *provider*

→ van het verschoningsrecht sedert EHRM 27 maart 1996, NJ 1996, 577 en HR 10 mei 1996, NJ 1996, 578.

123. Illegale en schadelijke inhoud op het Internet, COM(96) 487 def. p. 18; een Finse anonieme *remailer* (anon.penet.fi) is gedwongen openheid van zaken te geven in een Scientology-proces.

verplicht is mee te werken).¹²⁴ Met de Telecommunicatiewet zal dit veranderen.¹²⁵

Volgens art. 125i kan de RC tijdens het gvo het bevel geven dat degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die kunnen dienen om de waarheid aan de dag te brengen, deze gegevens, voor zover deze zijn opgeslagen, worden verwerkt of overgedragen met gebruikmaking van een geautomatiseerd werk, zal vastleggen, hem daartoe toegang zal verlenen etc. Met enige regelmaat wordt op grond hiervan aan *providers* gevraagd om aan de hand van het e-mailadres gegevens te verstrekken waardoor een bijbehorende persoon kan worden geïdentificeerd. In sommige gevallen – waaronder spionage en kinderpornografie – kunnen opsporingsambtenaren wellicht ook art. 551 Sv gebruiken (zonder tussenkomst van de rechter-commissaris).¹²⁶ Wat betreft de meewerking ter identificatie wijs ik op de mogelijke complicatie die zou kunnen ontstaan als een bulletin board operator om nadere informatie wordt gevraagd. Dan rijst de vraag of het verschoningsrecht van de journalist ook voor zo'n operator geldt, aangezien deze per slot van rekening een publicatiemedium verzorgt.

Overigens kan technisch gezien via de 'cookies' in de computer van gebruikers dikwijls worden achterhaald welke plaatsen op het Internet zijn bezocht (zie 3.3.1); het plaatsen van een cookie door de opsporingsautoriteiten met dat doel lijkt mij echter niet zonder meer toelaatbaar. Het lijkt op een soort peilzender. Het Wetsontwerp bijzondere opsporingsbevoegdheden dat wel over observatie van een persoon met een technisch hulpmiddel dat over een kortere of langere periode signalen registreert (wat moet gelden als stelselmatige observatie) spreekt,¹²⁷ rept (terwijl in het ontwerp wel rekening is gehouden met de noden van het digitaal rechercheren) nergens uitdrukkelijk van de mogelijkheid tot politieel gebruik van cookies over te gaan. Toch lijken mij de betreffende artikelen 126g en 126o ontwerp Sv toe-

¹²⁴ Kaspersen in Franken, Kaspersen, De Wildt (1997): 410 pleit voor een uitbreiding van art. 125f Sv tot service providers onder verwijzing naar Recommendation R(95)13 van de Raad van Europa.

¹²⁵ TK 1996-97, 25 533, 1-3.

¹²⁶ Volgens Utrechts Nieuwsblad 11 juli 1997 is deze weg een keer bewandeld.

¹²⁷ TK 1996-97, 25 403, 3: 27.

passelijk, want ook dit gebruik van een cookie komt neer op observatie met een technisch hulpmiddel.

Ik ben daarom niet gelukkig met de ontwikkeling dat particuliere rechercheurs met cookies de verkooppunten op het Internet van in strijd met het auteursrecht vervaardigde cd-roms nalopen op de personen die daar een bestelling hebben geplaatst. Naar verluidt worden deze kopers met een bezoek vereerd en wordt hen (met vermelding van art. 36b Auteurswet dat binnentreding in de woning ter inbeslagneming door een opsporingsambtenaar op last van de officier van justitie mogelijk maakt) verzocht of men de gekochte waar kan ophalen.¹²⁸

Naast informatie ter identificatie van personen is ook de inhoud van communicatie van belang voor het opsporingsonderzoek. Er is een aantal mogelijkheden om communicatie via het Internet te onderscheppen. Afgezien van de met de Wet computercriminaliteit geïntroduceerde nieuwe dwangmiddelen spelen daarbij zowel het tappen van telecommunicatie, het onderscheppen van brieven, de reikwijdte van de bevoegdheden tijdens huiszoeking en het z.g. direct af luisteren een rol. Het doet eigenlijk wonderlijk aan dat deze verschillende methoden verschillende eisen stellen al naar gelang de techniek van interceptie. Ik deel de mening van het DTOO dat juist in verband met Internet de maatvoering (de hoeveelheid en gedetailleerdheid) van informatiegaring van groot belang is. Logischer ware in dat perspectief m.i. een onderscheid naar de mate van inbreuk op de privacy in die zin dat bijvoorbeeld het inkijken in een e-mailbox aan hogere eisen zou moeten voldoen dan het bekijken van een gezonden bericht aan een (publiek bedoeld) bulletin board. Dat sluit ook aan bij de techniek-onafhankelijke benadering in het voorstel tot wijziging van art. 13 Grondwet, volgens welk alle vormen van 'vertrouwelijke communicatie' in beginsel grondwettelijke bescherming genieten. 'Bij het verzenden van gegevensdragers in gesloten verpakkingen, het verzenden van beveiligde computerberichten over het datanetwerk en het verzenden van gesloten faxen (sealfax) is in objectieve termen sprake van een wil die

128. Aldus werd mij door een medewerkster van het VARA-Consumentenprogramma Kassa verteld.

gericht is op geheimhouding van de communicatie' – vertrouwelijke communicatie dus.¹²⁹

Blijkens de memorie van toelichting bij art. 125g Sv (dat met de Wet computercriminaliteit werd aangepast) gaat het bij het aftappen van telecommunicatie om overdracht van gegevens op afstand tussen personen onderling, tussen personen en computers en tussen computers onderling.¹³⁰ Er is zo bezien geen twijfel over dat e-mail onder de aftapbevoegdheid valt. Toch zijn er nog twijfelaars: zij stellen de vraag of e-mail berichten worden beschermd door het briefgeheim. Me dunkt van niet. Bij de wet computercriminaliteit is er immers wel rekening met computerverkeer gehouden en is niettemin aan e-mail (dat halverwege de jaren 80 met SURF-Net en Geo-Net bekend was) niet de status van 'brief' gegeven. Achteraf is wel verdedigbaar dat voor die status misschien enige aanleiding had bestaan: een e-mail bericht wordt immers niet alleen gecommuniceerd, maar kan ook worden opgeslagen en dat doet denken aan een brief.¹³¹ De mogelijkheid tot opslag bestaat echter nu ook voor gesproken communicatie via antwoord-apparaten en voice-mail: toch is een telefoongesprek nog geen brief. Nu de wetgever ervoor kiest het e-mail tappen onder art. 125g Sv te brengen en dus in gevallen in de wet bepaald op last van een rechter mogelijk te maken, is het onuist het briefgeheim op te voeren als reden om e-mail niet te kunnen aftappen. Terecht is al eerder besloten dat zo'n redenering ook niet opgaat voor fax-post.¹³²

De in de mailbox of elders opgeslagen e-mail berichten kunnen worden verkregen tijdens de huiszoeking in welk kader men immers ook in – in de doorzochte plaats aanwezige – computers mag grasduinen.¹³³ Is het beperkende art. 113 Sv van toepassing als de opsporingsambtenaren nu in het kader van de huiszoeking proberen de inhoud van een mailbox aan een onderzoek te onderwerpen en eventueel de daar aanwezige e-mail te lezen? Gesteld dat die mailbox niet zodanig beveiligd is dat derden er niet gemakkelijk in kunnen kijken (en dat is doorgaans het ge-

129. TK 1996-97, 25 443, 3, p. 2-3.

130. TK 1989-90, 21 551, 3, p. 7.

131. Zie ook J. Verbeek, E-mail moet vallen onder het briefgeheim, NRC Handelsblad 21 juli 1997.

132. HR 26 mei 1992, NJ 1992, 753 m.nt. ThWvV.

133. G.J.M. Corstens, het Nederlands strafprocesrecht, Arnhem 1995, 446.

val), dan is de opmerking van de minister dat e-mail als briefkaart is op te vatten relevant.¹³⁴ Dan valt te redeneren: kennelijk had de mail-boxhouder geen behoefte aan privacy en is het geen inbreuk op het briefgeheim om te lezen wat er gemakkelijk te lezen is. Er kan echter ook worden gesteld dat de gemiddelde e-mailgebruiker als *reasonable expectation of privacy* heeft dat de inhoud van zijn geautomatiseerde brievenbus niet wordt bekeken; de vergelijking met een brief lijkt dan redelijker dan vergelijking met een briefkaart. De vergelijking met de briefkaart is bovendien hoogst theoretisch. In het normale postverkeer overheerst de gesloten enveloppe; waarom zou dan in het geautomatiseerde postverkeer de briefkaart overheersen? En voorts is er sprake van een overgangssituatie: zodra iedereen zijn post (automatisch) versleutelt, kan er niet eens meer geautomatiseerd worden ingekeken op deze manier.¹³⁵ Het lijkt mij daarom juist tijdens de huiszoeking de e-mailbox wel als een brievenbus met brieven op te vatten, waarop art. 113 Sv van toepassing is. Dit doet overigens niet af aan het feit dat de wetgever een inkijkoperatie in die mailbox heeft mogelijk gemaakt in art. 1251 Sv. Op grond van dat artikel bestaat buiten het kader van een huiszoeking tijdens een gerechtelijk vooronderzoek de mogelijkheid dat een provider wordt gevraagd een mailbox in te zien en e-mailgegevens aan de rechter-commissaris mee te delen.

In het Wetsontwerp bijzondere opsporingsbevoegdheden is rekening gehouden met een aanvullende interceptiemanager op het niveau van de gebruiker. Die is van belang, omdat er zulke sterke encryptietechnieken bestaan dat het geheel niet zinvol hoeft te zijn om via art. 125g Sv te tappen. Die aanvullende weg is het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (art. 1261 en s Sv). Volgens de MvT impliceert de bevoegdheid communicatie op te nemen 'dat als bijvoorbeeld in een kantoor een bug wordt geplaatst op een toetsenbord en de muis van een computer, alle toetsaanslagen en muisklikken van de computer worden geregistreerd. Zodoende kan deze communicatie worden onderschept alvorens de tekst wordt encrypted'. 'De bevoegdheid opent de mogelijkheid', aldus de

134. TK 1996-1997, Aanhangsel 1370; zie ook TK 1996-97, 25 443, 3, p. 2.

135. Hierover ook J. Bock, Th. Derksen en R. Vrijsde, Verslag Studiedag CRI: digitaal Rechercheren in de praktijk 1 april 1997, Beleidsadviesgroep Computercriminaliteit 1997, p. 18.

MvT, 'gegevensinvoer te onderscheppen nog voor er gecommuniceerd wordt. (...) Onbedoeld kunnen aldus meer gegevens worden verkregen dan waartoe de bevoegdheid strekt. (...) Indien vooraf redelijkerwijs bekend kan zijn dat door de plaatsing van een technisch hulpmiddel geen communicatie, maar alleen andere uitingen worden opgenomen, mag het technisch hulpmiddel niet worden geplaatst. Het is dus niet toegestaan een bug te plaatsen op een toetsenbord van een PC die niet op een netwerk is aangesloten'.¹³⁶ Het lijkt aannemelijk dat ook het in 3.3.2 genoemde gebruik van *applets* (voor zover die als de computer van de afgeluisterde over een microfoon beschikt ook als bugs zijn te programmeren) hieronder zal worden gerekend.

Kan er nu (zonder dat de politie tot *hacking* overgaat) ook worden geïnterceptieerd op het niveau van de *provider*? Actueel is in dit verband de problematiek met betrekking tot een opdracht van de RC ex art. 125i Sv aan de Nederlandse *provider* XS4All om gedurende een maand het Internetverkeer van een van de cliënten van die *provider* te tappen. Volgens de *provider* is die vordering onrechtmatig omdat art. 125i niet toekomstgericht zou zijn. Dit verweer is in het verleden ook gedaan met betrekking tot toekomstgerichte telefoontaps. De gesprekken betroffen dan dikwijls andere feiten dan die ter zake waarvan het gerechtelijk vooronderzoek was gevorderd; dergelijke gesprekken mogen voor het bewijs voor die andere feiten worden gebruikt.¹³⁷ In het licht van die jurisprudentie heeft de telefoontap zich bij uitstek tot een pro-actief opsporingsmiddel kunnen ontwikkelen; wel was steeds een verdenking van een strafbaar feit nodig, al was dat maar ter zake van art. 140 Sr (deelneming criminele organisatie). Omdat art. 125i Sv alleen gebruikt kan worden tijdens een gerechtelijk vooronderzoek, moet er ook dan sprake zijn van een verdenking, maar dat neemt niet weg dat de tap dan ook met het oog op toekomstige delicten wordt gebruikt.

Hiertegen in te brengen is, dat de wetgever het krachtens art. 125i Sv bedoelde bevel tot uitlevering van gegevens uit een geautomatiseerd werk heeft afgeleid van het in art. 105 Sv opgeno-

¹³⁶ TK 1996-97, 25 493, 3, p. 35-36.

¹³⁷ HR 17 mei 1983, NJ 1983, 636; HR 14 april 1987, NJ 1988, 515; HR 24 november 1992, NJ 1993, 307. Zie voor toekomstgerichte toepassing van art. 125f Sv Corstens (1995): 413 en Van Dijk & Keltjens (1995): 194-197.

men bevel tot uitlevering.¹³⁸ De *access provider* wordt niet als een *relais-station* beschouwd, maar als een elders aanwezig geautomatiseerd werk waar pakketjes gegevens zijn opgeslagen. Een bevel tot uitlevering van toekomstige gegevens is evenals een bevel tot uitlevering van 'pakjes' moeilijk denkbaar. In dit perspectief past dat art. 125i Sv voorkomt dat van de drastischer huiszoekingsbevoegdheid ex art. 125j gebruik moet worden gemaakt. Laatstbedoeld artikel is niet bedoeld het onderzoek in netwerken in andere situaties dan in die van huiszoeking toe te laten.¹³⁹

Er is wat mij betreft niets mis met een ook op toekomstige feiten gerichte gegevenstap bij de *access-provider*, maar dan moet de tap wel geschieden op bevel van een Rechter Commissaris in geval van een concrete verdenking (en dus niet in geval van gewenste surveillance). Zojuist bleek dat art. 125i Sv voor zo'n tap echter gezien de wetsgeschiedenis een ietwat vreemde basis is. Art. 125g Sv levert een logischer basis op om toe te passen in zaken als de lopende XS4All zaak. Op dit moment is een provider nog niet verplicht mee te werken. Blijkens art. 13.1 ontwerp Telecommunicatiewet komt daar verandering in. Volgens dat artikel stellen aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hun aanbod uitsluitend beschikbaar als dat aanbod aftapbaar is. Als aanbieders van telecommunicatiediensten worden in de memorie van toelichting ook genoemd *Internet access providers* en *Trusted Third Parties*.¹⁴⁰ Zij zijn op grond van art. 13.2 ontwerp Telecommunicatiewet verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last tot het aftappen of opnemen van door hen verzorgde telecommunicatie.

Dat laatste is misschien zo wie so nodig als wordt bedacht dat in de toekomst de telecommunicatie waarschijnlijk vooral via de laagbanige (en geostationaire) satellieten zal lopen, waarbij het tevens vaker zal voorkomen dat Nederlandse ingezetenen bellen met een buitenlands abonnement. De verschillende bedrijven die de satellieten de ruimte inschieten mochten weliswaar tapbaarheid garanderen, maar het is de vraag of eenzelfde soort

138. TK 1989-90, 21 551, 3, p. 26.

139. Van Dijk & Keltjens (1995): 235, jo 266 en TK 21 551, 3, p. 10 en TK 21 551, 11, p. 11.

140. TK 1996-97, 25 533, 3, p. 71.

contact zal ontstaan als nu met PTT Telecom. En voorzover het gaat om abonnementen via buitenlandse bedrijven is het de vraag of die tot tappen bereid zijn op grond van een bevel van een RC uit een voor hen vreemd land.

6 CONCLUSIE

Op welke punten zullen we het straf- en strafprocesrecht moeten aanpassen vanwege de komst van het Internet, opdat we voorkomen dat de technische mogelijkheden ongewenste maatschappelijke gevolgen hebben? Die vraag lag achter de in dit preadvies behandelde problemen. Ik recapituleer de belangrijkste bevindingen.

Op het vlak van het materiële strafrecht is wat de traditionele vermogensdelicten betreft, niet veel bijzonders te melden. Hooguit verdient enige aandacht het verschijnsel dat virtuele personen contracten gaan sluiten. Als we een recht op anonimiteit op het net postuleren, zullen mensen niet te gemakkelijk mogen worden beschouwd als oplichters als zij met een identiteit opereren die niet overeenkomt met die welke zij in de *real world* hebben. Wellicht mag dan wel van hen worden verwacht dat zij kenbaar maken dat zij onder een alias optreden.

Wat de intellectuele vermogensdelicten betreft is de vraag gesteld of het juist is dat iemand die gepirateerde cd's koopt wel en iemand die dezelfde gepirateerde informatie *downloadt* niet als heler kan worden aangemerkt. Zelf ben ik van oordeel dat de schade, de immoraliteit of het risico dat degene die *downloadt* teweeg brengt niet zodanig is dat strafbaarstelling is geïndiceerd vanwege de informationele lading van bepaalde gegevens.

Wat betreft de bescherming van op personen betrekking hebbende gegevens is de vraag gesteld of er een strafrechtelijke bescherming tegen ongeautoriseerde verspreiding van die gegevens zou moeten komen. Onder omstandigheden lijkt strafbaarstelling hiervan mij wel geïndiceerd.

Zowel met het oog op de bescherming van individuele netgebruikers als met het oog op de bescherming van de infrastructuur is het belang van aan de *providers* te stellen eisen van veiligheid en betrouwbaarheid aan de orde gesteld. Het ligt daarbij voor de hand de verschillen tussen diverse soorten *providers* meer

dan in de in voorbereiding zijnde wetgeving (Computercriminaliteit II) bij de beoordeling te betrekken.

Nadere aandacht verdient het meezenden van *cookies* en *applets*. Aan de ene kant lijkt elk meezenden van cookies nu te vallen onder de strafbepaling van art. 350a Sr, hetgeen onzinnig is; aan de andere kant lijkt ongewenste interceptie via deze programmaatjes mogelijk en daarin kan dus wel reden tot strafbaarstelling bestaan.

Op het vlak van het internationale strafrecht is ingegaan op het probleem dat in de huidige opvattingen met betrekking tot het territorialiteitsbeginsel mensen worden vervolgd voor feiten die ze zelf niet voor strafbaar houden. Dit heeft ook als effect dat stringente staten hun normen exporteren. Internationale afspraken om de nationaliteit (of eventueel het domicilie) van de verdachten van gepleegde gronddelicten op het Internet de doorslag te laten geven, lijken met het oog hierop gewenst.

Wat betreft het internationale formele recht is opgemerkt dat nadere afspraken nuttig lijken in verband met de kleine rechtshulp, de internationale politiesamenwerking en het grasduinen op 'buitenlandse' Internetlocaties. Internationale samenwerking mag echter niet tekort doen aan rechtstatelijke waarborgen. Daarbij is met enige zorg gewezen op de kennelijke (en heimelijke) samenwerking van de Raad van Europa met de Amerikaanse autoriteiten bij het (met het oog op surveillance) tapen van alle telecommunicatie die per satelliet plaatsvindt. Ook die samenwerking lijkt reden om een internationaal orgaan gericht op telecommunicatie waaraan ook op mensenrechten gerichte non-gouvernementele organisaties deelnemen in het leven te roepen.

Op het vlak van het formele strafrecht is ingegaan op het gemaskeerde gebruik van het Internet door politie-ambtenaren. Daarbij is onderscheid gemaakt tussen echte '*sting*'-operaties – die als 'gewone' infiltratie kunnen gelden – en activiteiten waarbij geen contact wordt gelegd met verdachten (of andere subjecten), maar de politie niet onmiddellijk wil opvallen. Dat laatste moet m.i. kunnen zonder dat in al dergelijke gevallen de voor undercover-operaties geldende eisen worden gesteld.

Data surveillance op het niveau van *providers* – door op grond

van het gebruik van bepaalde woorden automatisch een bericht aan de politie te zenden – lijkt vanwege het recht op bescherming van de ‘correspondence’ in art. 8 EVRM niet toelaatbaar.

Wat betreft het achterhalen van namen van Internetgebruikers is vastgesteld dat zulks nog niet mogelijk is op grond van art. 125f Sv, maar wel door de rechter-commissaris op grond van art. 125i Sv. De technische mogelijkheid om dit doel te bewerkstelligen door het gebruik van cookies, lijkt onder voorwaarden te kunnen worden gelegitimeerd door de artikelen inzake stelselmatige observatie uit het wetontwerp bijzondere opsporingsmethoden.

Wat betreft het achterhalen van de inhoud van de communicatie via het Internet zijn tal van artikelen toepasselijk. Op grond van art. 125g Sv kan een bewegende informatiestroom via de telecommunicatielijnen worden afgetapt; op grond van een huiszoekingsbevel kan een e-mailbox worden onderzocht, waarbij het briefgeheim een rol speelt en zo’n box kan in andere gevallen worden ingekeken op grond van art. 125i Sv; op grond van het wetontwerp bijzondere opsporingsbevoegdheden kunnen de aanslagen op het toetsenbord direct worden afgeluisterd (wat van belang is in verband met het gebruik van encryptie). Een en ander wordt wellicht nog aangevuld met de mogelijkheid om krachtens art. 125i Sv een medewerkingsplicht aan het toekomstgericht tappen door *providers* te construeren, al lijkt de aanpassing van de Telecommunicatiewet een betere basis op te leveren. Opgemerkt is dat het eigenlijk niet bevredigend is dat deze methoden naast elkaar bestaan terwijl daarmee eerder een toevallige wettelijke opbouw van kracht is dan één die doordacht is gebaseerd op de diverse gradaties van inmenging in de privacy op het Internet.

Als in 2020 een vervolg verschijnt op ‘Tussen droom en daad’ zal men zich misschien verbazen over het soort vragen waarover de NJV in 1998 in verband met het Internet debatteerde.¹⁴¹ Maar we mogen hopen dat dan nog niet is gezwicht voor een technologisch fatalisme: ‘wat kan mag en wat nodig is moet’. Sinds de industriële revolutie heeft het proces van modernise-

141. J.H.A. Lokin en C.J.H. Jansen, *Tussen droom en daad; de Nederlandse Juristen-Vereeniging, 1870-1995*, Zwolle 1995.

ring – dat ons steeds weer onzeker en verontrust maakt – onze energie en verbeelding steeds weer tot leven gebracht, omdat we greep willen houden op onze wereld. De rechtsgeleerdheid als vakgebied waar instrumentaliteit en rechtsbescherming elkaars keerzijde vormen heeft juist daarbij de taak om ons te herinneren dat ‘wat kan niet hoeft’ en ‘wat nodig is door onszelf wordt bepaald’. Verzaakt de rechtsgeleerdheid de taak de technologische veranderingen bij te sturen, dan zullen we ons snel niet meer thuis voelen in een wereld waarin de technologische verandering op zich onafwendbaar is. ‘I believe that we and those who come after us will go on fighting to make ourselves at home in this world, even as the homes we have made, the modern street, the modern spirit, go on melting into air.’¹⁴²

7 AANGEHAALDE WETSONTWERPEN

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 (Kamerstukken I 1997/98, 25 443, p. 232)

Artikel 13

1. Het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken zijn onschendbaar. Het geheim van de gegevens met betrekking tot communicatie als bedoeld in de eerste volzin is eveneens onschendbaar.
2. De geheimen, bedoeld in het eerste lid, kunnen worden beperkt in de gevallen bij de wet bepaald. Beperking van de geheimen, bedoeld in de eerste volzin van het eerste lid, kan slechts plaatsvinden op last van de rechter, of, indien de beperking in het belang van de nationale veiligheid plaatsvindt, met machtiging van een bij wet aangewezen minister. Beperking van het geheim, bedoeld in de tweede volzin van het eerste lid, kan slechts plaatsvinden door of met machtiging van hen die daartoe bij de wet zijn aangewezen.
3. De wet stelt regels ter bescherming van de geheimen, bedoeld in het eerste lid.

¹⁴² Berman (1988/1982): 348.

4. Degene van wie een geheim als bedoeld in het eerste lid, eerste volzin, is beperkt, wordt van die beperking zo spoedig mogelijk in kennis gesteld. Indien de beperking in het belang van de nationale veiligheid of het belang van de strafvordering heeft plaatsgevonden, kan volgens bij de wet te stellen regels de kennisgeving worden uitgesteld. In de bij de wet te bepalen gevallen kan de kennisgeving achterwege worden gelaten, indien het belang van de nationale veiligheid zich tegen kennisgeving blijvend verzet.

Telecommunicatiewet (Kamerstukken II 1996/97, 25 533, p. 2)

Artikel 13.1

1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten stellen hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn.
2. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de technische aftapbaarheid van openbare telecommunicatienetwerken en openbare telecommunicatiediensten.

Artikel 13.2

1. Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld.
2. Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last tot het aftappen of opnemen van door hen verzorgde telecommunicatie.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen organisatorische en personele maatregelen en te treffen voorzieningen met betrekking tot aftappen.

Artikel 13.7

Onze Minister kan in belang van de veiligheid van de staat of de handhaving van de strafrechtelijke rechtsorde bij beschikking bepalen dat een of meer artikelen van dit hoofdstuk van over-

eenkomstige toepassing zijn op aanbieders van een niet openbaar telecommunicatienetwerk, een niet openbare telecommunicatiedienst of aanbieders van huurlijnen indien het netwerk, de dienst of een huurlijn feitelijk opstaat voor derden.

Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden); (Kamerstukken II 1996/97, 25 403, p. 2)

Artikel 126h

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een opsporingsambtenaar als bedoeld in artikel 141, onderdeel b, deelneemt of medewerking verleent aan een groep van personen waarbinnen naar redelijkerwijs kan worden vermoed misdrijven worden beraamd of gepleegd.

2. De opsporingsambtenaar mag bij de tenuitvoerlegging van het bevel een persoon niet brengen tot andere strafbare feiten dan waarop diens opzet reeds tevoren was gericht.

Artikel 126j

1. In geval van verdenking van een misdrijf kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar als bedoeld in artikel 141, onderdeel b, zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar, stelselmatig informatie inwint over de verdachte.

2. Het bevel wordt gegeven voor een periode van ten hoogste drie maanden. De geldigheidsduur kan telkens voor een periode van ten hoogste drie maanden worden verlengd.

Artikel 126l

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een op-

sporingsambtenaar als bedoeld in artikel 141, onderdeel b, vertrouwelijke communicatie opneemt met een technisch hulpmiddel.

2. De officier van justitie kan in het belang van het onderzoek bepalen dat ter uitvoering van het bevel een besloten plaats, niet zijnde een woning, wordt betreden zonder toestemming van de rechthebbende.

Artikel 126m

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard op de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een opsporingsambtenaar telecommunicatie opneemt met een technisch hulpmiddel.

Artikel 126n

1. In geval van ontdekking op heterdaad, verdenking van een misdrijf als omschreven in artikel 67, eerste lid, of het misdrijf, bedoeld in artikel 138a van het Wetboek van Strafrecht kan de officier van justitie in het belang van het onderzoek een vordering doen inlichtingen te verstrekken terzake van alle verkeer dat over de telecommunicatie-infrastructuur of over een telecommunicatie-inrichting die wordt aangewend voor dienstverlening aan het publiek, heeft plaatsgevonden en ten aanzien waarvan het vermoeden bestaat, dat de verdachte eraan heeft deelgenomen.

Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II); voorontwerp januari 1998

Artikel 53

1. Bij misdrijven gepleegd door middel van de drukpers of door enig ander middel voor de openbaarmaking of verspreiding van uitingen in gesproken woord, beeld of geschrift, wordt de tussenpersoon als zodanig niet vervolgd, indien:

- a. hij bij de openbaarmaking of verspreiding zijn identiteit heeft bekendgemaakt;
 - b. de dader bekend is of op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door de tussenpersoon is bekendgemaakt, en
 - c. de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle handelingen heeft verricht die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van verdere verspreiding.
2. Onder de tussenpersoon, bedoeld in het eerste lid, wordt verstaan: een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in gesproken woord, beeld of geschrift afkomstig van derden.

Aan artikel 126m worden vier nieuwe leden toegevoegd, die luiden:

- 5. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij gelegenheid van de toepassing van het eerste lid tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in het eerste lid bedoelde telecommunicatie, het bevel worden gericht medewerking te verlenen aan het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken.
- 6. Het bevel, bedoeld in het vijfde lid, kan slechts aan de verdachte worden gegeven indien uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte en indien het onderzoek dringend noodzakelijk is voor het aan de dag brengen van de waarheid.
- 7. De personen, bedoeld in artikel 96a, derde lid, kunnen zich verschonen van de nakoming van dit bevel.

DEEL IV

HET INTERNET: HET
AUTEURSRECHT VOORBIJ?

preadvies mr. P.B. Hugenholtz

INHOUD DEEL IV

I.	INLEIDING	201
II.	DE ELEKTRONISCHE KOPIE	206
	Probleemgevallen: browsen en hyperlink	
	211	
	Wettelijke beperkingen	214
III.	HET EINDE VAN DE TERRITORIALITEIT	216
IV.	AANSPRAKELIJKHEID VAN INTERMEDIAIRS	223
	Toerekenbare inbreuk?	225
	Onzorgvuldigheid: bevorderen van inbreuk	
	228	
	Risico-aansprakelijkheid?	231
	Horizontale oplossing	233
V.	ALTERNATIEVEN VOOR HET AUTEURSRECHT	235
	V.1 Overeenkomstenrecht	236
	V.2 Technische maatregelen	243
	V.3 Lex Informatica	253
VI.	CONCLUSIE	258

Deel IV

INLEIDING

Slechts eenmaal eerder in de illustere geschiedenis van de Nederlandse Juristen-Vereeniging stond het auteursrecht op de agenda van de jaarvergadering. Dat was in 1877; de jonge vereniging vierde toen haar achtste verjaardag. Advocaten schreven hun memoranda nog eigenhandig met pen, papier en inkt. Brieven werden besteld per postkoets en ijlhode. De *courant* en het *magazijn* waren de enige massamedia van betekenis. En de Auteurswet 1912, die tot op de dag van vandaag – zij het in gewijzigde vorm – van kracht is gebleven, was nog ver weg. Sterker: zelfs haar voorganger, de Wet van 1880, stond nog in de steigers.

Toch was in 1877 de kiem van het Internet in feite al gelegd. In 1847 was de eerste openbare telegraafverbinding in Nederland door de Hollandsche IJzeren Spoorwegmaatschappij in gebruik genomen. In 1877 was het telegraafnet uitgegroeid tot een wereldomspannend communicatienetwerk. Openbare telefonie werd korte tijd later (in 1880) in Nederland geïntroduceerd.²

Dat het Internet in 1877 reeds in statu nascendi verkeerde, ging aan de illustere leden der Vereeniging echter voorbij. Een jaar eerder hadden zij nog gedelibereerd over de prangende *quaestie* of het ‘wenschelijk (is) dat dames-regentessen de absolute voogdij over kinderen, die onder haar toezicht verpleegd worden verkrijgen? Zijn zij geëmancipeerd genoeg om haar die voogdij zonder gevaar te kunnen geven?’³

Thans, in 1877, stond de emancipatie opnieuw centraal, en wel die van een betrekkelijk nieuw, zich ontluikend rechtsgebied. De

1. De tekst van dit preadvies werd afgesloten op 15 januari 1998.

2. A.A.M. Enserinck, *De Nederlandsche Radio-Wetgeving geschiedkundig ontwikkeld*, diss. Leiden, Alphen aan den Rijn 1993, p. 20.

3. *Handelingen NJV* 1876 II, p. 12.

beide *praeadviseurs*, mrs. Fresemann Viëtor en De Ridder, bogen zich tezamen met de leden ter vergadering verenigd over de vraag: 'Naar welk hoofdbeginsel moet de Staat de rechten van schrijvers en kunstenaars op het product van hun arbeid regelen?'⁴ Anders geformuleerd: welke rechtsbeginselen liggen er ten grondslag aan het auteursrecht? De preadviseurs vonden dit geen moeilijke vraag; dergelijke rechtsbeginselen zijn er niet: '... er is geen rechtsbeginsel dat de Staat kan nopen schrijvers en kunstenaars de rechten van hun arbeid te verzekeren.'⁵ Noch het leerstuk van de letterkundige of intellectuele eigendom, noch de leer 'dat de arbeider recht heeft op het loon van zijn arbeid', noch de opvatting dat de koper van een boek zich stilzwijgend verplicht zich van nadruk te onthouden vermocht de preadviseurs te vermurwen. Als er al gronden zijn tot bescherming van schrijvers en kunstenaars, dan zijn die slechts gelegen in het *algemeen belang*. De vergadering was het hiermee eens, met 36 stemmen voor en 10 tegen.⁶

Over de ratio van het auteursrecht valt 121 jaar na dato gelukkig meer te zeggen, zeker in het licht van de communicatierevolutie die sedertdien heeft plaatsgevonden. Het auteursrecht heeft zich in de afgelopen eeuw geëmancipeerd tot een volwaardig en volwassen rechtsgebied. Auteursrechtelijke beginselen zijn inmiddels diep in het rechtsbewustzijn van de gemiddelde justitiabele verankerd. Ironisch genoeg is het juist het Internet waardoor de grondslagen van het auteursrecht opnieuw ter discussie komen te staan.

Over de bescherming van niet-openbare gedigitaliseerde gegevens heeft de Vereniging zich nog betrekkelijk recent (in 1988) gebogen. In zijn preadvies over privaatrechtelijke middelen van gegevensbescherming wijdde Verkade tien bladzijden aan de intellectuele eigendom, vooral aan het lelijke zusje van het auteursrecht, de *geschriftenbescherming*.⁷ Het Internet kwam in de pread-

4. Handelingen NJV 1877 I, p. 33.

5. J. Fresemann Viëtor, Handelingen NJV 1877 I, p. 44.

6. Handelingen NJV 1877 II, p. 70-71. Zie de kritiek op het votum bij H.L. de Beaufort, Het auteursrecht in het Nederlandsche en internationale recht (diss. Utrecht), Utrecht: Den Boer 1909, p. 73 e.v.

7. Handelingen NJV 1988 I, p. 43-53.

viezen van 1988 nog niet voor, zelfs niet in het algemeen gedeelte waar de integratie van informatica en telecommunicatie waaruit het Internet is voortgekomen, beschreven werd.⁸

Sinds de doorbraak van het World Wide Web, enkele jaren geleden, is het Internet uit de auteursrechtelijke literatuur niet meer weg te denken. De communicatierevolutie die het Internet te weeg heeft gebracht, wordt in deze literatuur weerspiegeld. 'Almost everything we think we know about intellectual property is wrong', schrijft Internet-goeroe John Perry Barlow.⁹ Het auteursrecht is ontstaan in een analoge wereld van tastbare kopieën (de drukpers). 'To assume that systems of law based in the physical world will serve in an environment that is as fundamentally different as Cyberspace is a folly for which everyone doing business in the future will pay.'¹⁰ Ook in de meer serieuze rechtswetenschappelijke literatuur wordt de noodklok over het auteursrecht geluid. In het spraakmakende artikel van Dommering is sprake van een ware *crisis van het auteursrecht*; 'het auteursrecht spoelt weg door het elektronische vergiet.'¹¹

Tegenover deze doemdenkers staan optimisten die menen dat het met de auteursrechtelijke gevolgen van het Internet wel meevalt. In deze opvatting behoeft aan het auteursrechtelijke systeem in wezen weinig te veranderen. Misschien moeten enkele begrippen in het licht van het Internet wat worden opgefrist, bijgevild of 'verduidelijkt', grosso modo kan het auteursrecht zo blijven als het altijd (dat wil zeggen: sinds het begin van deze eeuw) is geweest. Het auteursrecht heeft in het verleden vele media-stormen (fonograaf, radio en televisie, kabel, informati-

8. Handelingen NJV 1988 I, p. 11.

9. John Perry Barlow, *Selling Wine without Bottles. The Economy of Mind on the Global Net*, in: P. Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment*, Den Haag: Kluwer Law International, p. 187.

10. Barlow, a.w., p. 174, waarover *kritisch* P.B. Hugenholtz, *Het auteursrecht gaat langer mee dan Barlow denkt*, *Zeno* 1996-1, p. 8.

11. E.J. Dommering, *Het auteursrecht spoelt weg door het elektronisch vergiet. Enige gedachten over de naderende crisis van het auteursrecht*, *Computerrecht* 1994-3, p. 109.

ca) doorstaan; waarom zou het aan het Internet ineens bezwijken?¹²

Over de toekomst van het auteursrecht in een digitale netwerk-omgeving gaat dit preadvies. In hoofdstuk II wordt de eerste van vier rode draden, die de infrastructuur vormen van dit preadvies, geïntroduceerd: de actuele kwestie van de *elektronische kopie* en daaraan verwante problemen als de 'hyperlink', 'caching' en 'browsing'. Ook de reikwijdte van de wettelijke beperkingen zal in dit kader aan de orde komen.

De tweede rode draad is *de territorialiteit*, of liever: het einde daarvan. In hoofdstuk III zal worden geschetst hoe het wegvallen van territoriale grenzen voor het auteursrecht ernstige consequenties heeft. Het IPR, waarover Polak preadviseert, vormt daartegen geen adequate remedie, zelfs niet als vangnet.

De derde rode draad is de *aansprakelijkheid* van de Internet-provider. Dient de intermediair te 'bloeden' voor iedere inbreuk die via zijn computers plaatsvindt? Dit vraagstuk, dat centraal staat in hoofdstuk IV, lijkt zich te ontwikkelen tot een 'horizontaal' leerstuk, dat het auteursrecht ruimschoots overstijgt.

De vierde rode draad, tenslotte, wordt afgewikkeld in hoofdstuk V. Hier worden enkele *alternatieven* voor auteursrechtelijke bescherming beschreven. Aanbieders van informatie-diensten zullen hun toevlucht zoeken tot contractuele en technische maatregelen om onbevoegd gebruik te verhinderen. De vraag rijst of deze maatregelen voldoende ruimte laten voor de informatievrijheid van de gebruiker. Wellicht wordt het tijd voor dwingendrechtelijke bepalingen die deze vrijheid ook in de toekomst zullen waarborgen. Aan het slot van dit hoofdstuk wordt een somber scenario geschetst: rechtsregels zullen door informaticaregels buitenspel worden gezet, het publieke domein zal achter een ondoordringbare encryptielaag verdwijnen.

12. Vgl. Paul Goldstein, *Copyright's Highway: The Law and Lore of Copyright from Gutenberg to the Celestial Jukebox*, New York: Hill & Wang 1994, p. 205: 'Copyright law has a youthful capacity to self-correct'.

Deze inhoudsopgave maakt duidelijk dat dit preadvies over (veel) meer gaat dan het auteursrecht in enge zin. Aldus kom ik enigszins tegemoet aan de wens van het NJV-bestuur mij ook met *mediarechtelijke* kwesties in te laten. Over de (on)rechtmatigheid van publicaties op het Internet in brede zin gaat dit preadvies echter niet. Daarvoor zijn, afgezien van plaatsgebrek, twee redenen aan te voeren. Allereerst roept dit onderwerp naar mijn voorlopig oordeel geen belangwekkende nieuwe vragen van materieel civielrecht op. Een belediging in druk is ook op het Internet geen compliment. Interessant en belangrijk is natuurlijk wel het IPR-probleem dat samenhangt met het onvermijdelijk wereldwijde effect van de uiting. Medepreadviser Polak gaat op deze complicatie uitvoerig in.

De tweede reden is het feit dat de NJV zich nog betrekkelijk recent met de bescherming van het individu tegen onrechtmatige uitingen in de media heeft bezig gehouden; ik verwijs naar de preadviezen van Diemer¹³ en Mout¹⁴ uit 1978. Voor uitvoerige beschouwingen over de digitale communicatie- en informatievrijheid vanuit staatsrechtelijk perspectief wijs ik op de preadviezen van Kalkman, Hins en Jurgens, die in 1995 werden uitgebracht aan de Vereniging voor Media- en Communicatierecht en de Staatsrechtkring.¹⁵

Dit preadvies biedt evenmin ruimte voor een aantal verwante auteursrechtelijke kwesties: de allocatie van rechten (aan wie behoren de 'elektronische rechten'?)¹⁶ en het complexe karakter van multimedialicenties¹⁷. Buiten beschouwing blijft eveneens het object van auteursrechtelijke bescherming, een onderwerp waarover in de afgelopen jaren meer dan genoeg geschreven

13. Handelingen NJV 1978 I, p. 7-79.

14. Handelingen NJV 1978 I, p. 81-165.

15. Communicatie- en informatievrijheid in het digitale tijdperk, Publikaties van de Staatsrechtkring nr. 11, Zwolle: Tjeenk Willink 1995.

16. K.J. Koelman, De overdracht overdacht, te verschijnen in: Informatierecht/AMI 1998-5.

17. K.J. Koelman, Multimedialicenties, enkele juridische en praktische knelpunten, ITeR-reeks nr. 10, Alphen aan den Rijn: Samsom 1998; J.M.B. Scignette, Beheer en clearance van intellectuele eigendomsrechten in de digitale informatiemaatschappij, ITeR-reeks nr. 10, Alphen aan den Rijn: Samsom 1998.

is.¹⁸ Evenmin wordt aandacht besteed aan de morele rechten van de auteur.

Tot slot van deze inleiding past een waarschuwing: *dit preadvies bevat bederfelijke waar*. Wij weten veel te weinig van de nieuwe digitale wereld om definitieve standpunten in te nemen. Gedreven door een mengeling van *horror vacui* en verlatingsangst (en aangevuurd door lobbies), kiezen nationale en internationale wetgevers voor de vlucht vooruit. Het Internet dreigt overspoeld te worden door premature wetgevende initiatieven. Laten wij, rechtsgelcerden en praktizijns, het goede voorbeeld geven en het hoofd koel houden.

II. DE ELEKTRONISCHE KOPIE

Auteursrechthebbenden plegen het Internet te beschouwen als een wereldomspannend kopieerapparaat, bediend door een miljoenenleger van gevaarlijke en anonieme piraten. Dat schrikbeeld is, hoe karikaturaal ook, niet eens zo ver bezijden de waarheid. Anders dan in de goede oude tijd van de drukpers, waarin het auteursrecht is ontstaan, beschikt tegenwoordig vrijwel iedere informatieconsument over zijn eigen, hoogwaardige reproductie- en distributie-apparaat: zijn *personal computer*. Via het digitale net kunnen perfecte kopieën van auteursrechtelijk beschermde werken in een oogwenk naar alle uithoeken van de aarde worden verspreid. Geen wonder dat vanuit het kamp van de rechthebbenden de roep om versterking van het auteursrecht de afgelopen jaren oorverdovend is geweest.

De campagne van de rechthebbenden heeft, veel sneller dan op internationaal niveau gebruikelijk, geresulteerd in een verdrag dat beoogt de rechten van auteurs en auteursrechthebben-

18. F.W. Grosheide, *Auteursrecht op maat* (diss. Utrecht), Deventer: Kluwer 1986; A.A. Quaadvlieg, *Auteursrecht op techniek* (diss. Nijmegen), Zwolle: W.E.J. Tjeenk Willink 1987; P.B. Hugenholtz, *Auteursrecht op informatic* (diss. Amsterdam UvA), Deventer: Kluwer 1989; J.F. Haeck, *Idee en programmaformule in het auteursrecht* (diss. Amsterdam UvA), Deventer: Kluwer 1998.

den op het Internet veilig te stellen. Het Auteursrechtverdrag¹⁹, dat in december 1997 in het kader van de World Intellectual Property Organization tot stand is gekomen (WIPO-verdrag), voorziet allereerst in een ruim geformuleerd 'right of communication to the public' (art. 8). Art. 8 stelt buiten twijfel dat de beschikbaarstelling van werken via het Internet aan de auteursrechthebbende exclusief is voorbehouden. In Nederland heeft daaromtrent overigens nimmer serieuze twijfel bestaan. Het 'media-neutraal' geformuleerde recht van openbaarmaking (art. 1 jo. 12 Auteurswet 1912) is flexibel genoeg ook de verspreiding van werken via het Internet (al dan niet op individueel verzoek) te omvatten. Sterker: het openbaarmakingsrecht is daarvoor bij uitstek geschikt, veel beter dan het reproductierecht.²⁰

Het Verdrag bevat voorts enige 'flankerende' bepalingen, zoals een verbod op het verwijderen van 'rights management information' (informatie over de auteursrechtelijke status van een werk) en een verbod op het omzeilen van technische beschermingsmaatregelen; zie p. 242 e.v. *infra*.

Een poging om ook het reproductierecht in het WIPO-Verdrag een plaats te geven is op het laatste nippertje stukgelopen op taai verzet van een 'ad hoc' coalitie van intermediairs, telecommunicatiebedrijven en eindgebruikers. Het WIPO-ontwerp bevatte aanvankelijk (in art. 7) een zeer ruim geformuleerd reproductierecht, inhoudende de 'direct and indirect reproduction (...), whether permanent or temporarily, in any manner or form'. Ook de *tijdelijke* kopie zou aldus onder het reproductierecht worden gebracht.

19. F.J. Arkenbout, Nieuwe verdragen over auteursrecht en naburige rechten, Informatierecht/AMI 1997-4, p. 67; F.W. Grosheide, Enkele kanttekeningen bij het WIPO Copyright Treaty 1996, Informatierecht/AMI 1997-4, p. 74. Het WIPO-Auteursrechtverdrag is afgedrukt in Informatierecht/AMI 1997-4 (bijlage).

20. P.B. Hugenholtz, Auteursrecht en information retrieval, Deventer: Kluwer 1982, p. 44; idem, Adapting copyright to the information superhighway, in: P. Bernt Hugenholtz (ed.), The Future of Copyright in a Digital Environment, Den Haag: Kluwer Law International 1996, p. 101; D.J.G. Visser, Auteursrecht op toegang (diss. Leiden), Den Haag: VUGA 1997, *passim*.

Aanvaarding van het voorstel zou vergaande consequenties hebben gehad. Doordat in een digitale omgeving iedere verzending, ieder transport, iedere ontvangst en ieder gebruik van informatie met enige vorm van tijdelijk kopiëren gepaard gaan, zou het auteursrechtelijke exploitatierecht ver buiten zijn traditionele oevers zijn getreden.²¹ Normale gebruikshandelingen die in de 'analoge' wereld altijd vrij van auteursrechtelijke aanspraken hebben kunnen plaatsvinden (het lezen van een boek, het draaien van een plaat, het kijken naar de televisie), zouden op het Internet auteursrechtelijk belast worden. Het auteursrecht zou eensklaps met een (digitaal) *gebruiksrecht*, een 'exclusive right to read', worden uitgebreid.²² Aldus zou de ratio van het reproductierecht, het beschermen tegen ongeoorloofde vormen van exploitatie, geheel uit het oog worden verloren.²³

In zijn artikel in Computerrecht²⁴ noemt Dommering de 'elektronische kopie' een 'spook uit het papieren tijdperk'. Hij nodigt ons uit het 'repro-denken', waarvan de traditionele auteursrechtleer is doortrokken, te verlaten en op zoek te gaan naar auteursrechtelijke concepten die beter passen bij de digitale omgeving. In zijn dissertatie van 1997 neemt Visser de uitnodiging van Dommering, misschien wat al te gretig, aan. Volgens Visser kan het reproductierecht, van oudsher de harde kern van het auteursrecht (het 'copyright'), beter helemaal worden afgeschaft. Een ruim geformuleerd recht van openbaarmaking (een 'auteursrecht op toegang') is alles wat de rechthebbende in de toekomst nodig heeft.²⁵

Volgens het Legal Advisory Board, een adviescollege van de Europese Commissie, verdient een normatieve benadering van de exploitatierechten de voorkeur. Verveelvoudiging is een rechts-

21. P.B. Hugenholtz, Het auteursrecht, het Internet en de informatiesnelweg, NJB 1995, p. 513-519; Visser, a.w., p. 61-82.

22. Jessica Litman, The Exclusive Right to Read, Cardozo Arts and Entertainment Law Journal (13) 1994, p. 29.

23. I. Cherpillod, Droit d'auteur et droits voisins en relation avec les autoroutes de l'information: le contenu des droits et leurs limitations, in: Reto M. Hilty (red.), Information Highway, Bern: Stämpfli 1996, p. 264.

24. Noot 11.

25. D.J.G. Visser, Auteursrecht op toegang (diss. Leiden), Den Haag: VUGA 1997, besproken door E.J. Arkenbout, Informatierecht/AMI 1997-8, p. 172.

begrip, geen louter technisch bepaalde notie. Niet de (toevallige) stand van de techniek, maar het recht (de norm) dient de reikwijdte van de bescherming te bepalen.²⁶

Onder druk van de 'ad hoc' coalitie is art. 7 van het WIPO-voorstel uiteindelijk geschrapt.²⁷ Daarbij speelden, toegegeven, rechtswetenschappelijke bezwaren nauwelijks een rol. Gevreesd werd dat een ruim geformuleerd reproductierecht zou leiden tot (ongewenste) verruiming van de aansprakelijkheid van Internet-providers; zie p. 219 c.v. *infra*.

De discussie over het digitale reproductierecht is daarmee echter niet gesloten. Het richtlijnvoorstel dat de Europese Commissie eind december 1997 openbaar maakte, voorziet eveneens in een uitgebreid reproductierecht (art. 2), dat ook de tijdelijke elektronische kopie omvat.²⁸ Het voorstel sluit aan bij gelijksoortige bepalingen in de Softwarerichtlijn²⁹ en de Databankrichtlijn³⁰.

De bepaling in het richtlijnvoorstel reikt echter minder ver dan de verongelukte WIPO-bepaling. Tijdelijke reproductiehandelingen 'which are integral to a technological process made for the sole purpose of enabling a use of a work or other subject matter and have no separate economic significance' (art. 5 lid

26. Legal Advisory Board, Reply to the Green Paper on Copyright in the Information Society, <http://www2.echo.lu/legal/en/labhome>. In gelijke zin F.W. Grosheide, Enkele kanttekeningen bij het WIPO Copyright Treaty 1996, Informatierecht/AMI 1997-4, p. 75 r.k.

27. Wel is bij wijze van compromis het volgende *Agreed Statement* bij het WIPO-Auteursrechtverdrag aangenomen: 'The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention.'

28. Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society, COM (97) 628.

29. Richtlijn 91/250/EEG van de Raad van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's, Pb EG 1991 L 122/42.

30. Richtlijn 96/9/EG van het Europees Parlement en de Raad van 27 maart 1996 betreffende de rechtsbescherming van databanken, Pb EG 1996 L 77/20.

1) moeten door de nationale wetgever worden vrijgesteld. De Toelichting noemt als (enig) voorbeeld van zo'n vrijgestelde reproductiehandeling het transport van een film vanuit een databank in Duitsland naar de personal computer (PC) van een gebruiker in Portugal. Onderweg op het netwerk zullen talloze tijdelijke kopieën van (gedeelten van) de film worden gemaakt, aldus de Commissie. Dergelijke 'transport-kopieën' vallen volgens het voorstel niet onder het auteursrecht.

Een ander voorbeeld is *caching*. Teneinde de wachttijden op het WWW (de 'World Wide Wait') binnen de perken te houden, zijn veel providers ertoe overgegaan kopieën van recent opgevraagde web-pagina's tijdelijk op hun eigen servers (computers) te bewaren, zodat zij door gebruikers sneller geraadpleegd kunnen worden ('proxy-caching'). Ook de gebruiker maakt zich, ongetwijfeld zonder het te beseffen, regelmatig schuldig aan caching. De bij het browsen gebruikte navigatiesoftware zorgt ervoor dat recent opgevraagde webpagina's in het werkgeheugen of op de harde schijf van de PC van de gebruiker tijdelijk beschikbaar blijven. Het gaat hier in beide gevallen om technisch geïndiceerde reproductiehandelingen zonder zelfstandige economische betekenis, die op grond van het richtlijnvoorstel zijn toegestaan.³¹

Verwant aan caching, maar daarvan wel te onderscheiden, is *mirroring*, het 'spiegelen' van een web site. In dit geval wordt een (populaire) web site door een service provider in zijn geheel gekopieerd en via zijn eigen server aan het publiek beschikbaar gesteld. Ook hier is het primaire doel de toegankelijkheid van de web site te verbeteren. Amerikaanse sites die op Europese servers worden gespiegeld zijn vanuit Europa veel sneller te bereiken. Zo bezien zou ook mirroring onder het regime van het richtlijnvoorstel een vrijgestelde handeling moeten zijn. Dikwijls dient mirroring echter ook een ander doel: het vergroten van de aantrekkingskracht (met bijbehorende advertentie-revenuen) van de

31. Zie Overweging 23 van de considerans. Denkbaar is overigens dat morele rechten wel een rol spelen, bijvoorbeeld indien 'gecachte' webpagina's door de provider niet vaak genoeg ververs worden; gebruikers worden in zo'n geval naar verouderde pagina's verwezen.

'spiegelende' provider. In zo'n geval kan uiteraard niet worden volgehouden dat het reproduceren geen zelfstandig economische betekenis heeft.

Overigens gaat mirroring niet alleen met reproduceren, maar ook met openbaarmaken gepaard. De analogie met secundaire kabeldistributie, waarvoor afzonderlijke toestemming van de rechthebbenden vereist is, ligt hier voor de hand.³² In de praktijk pleegt voor mirroring eveneens toestemming (van de beheerder van de gespiegelde site) te worden gevraagd.

Probleemgevallen: browsen en hyperlink

Het richtlijnvoorstel laat zich niet met zoveel woorden uit over de status van een tweetal gedragingen die op het World Wide Web evenzeer gemeengoed zijn, maar in auteursrechtelijke kringen voor veel controverse hebben gezorgd: het *browsen* (het 'bladeren' door web-pagina's) en de *hyperlink* (de 'aanklikbare' elektronische doorverwijzing).

Het browsen gaat ongetwijfeld met kopiëren (in technische zin) gepaard. Wie een web-pagina opvraagt, laadt de inhoud daarvan tijdelijk in het werkgeheugen van zijn computer. Is hier voldaan aan de beide criteria van art. 5 lid 1 van het richtlijnvoorstel?³³

Om met het laatste te beginnen: is browsen een economisch relevante exploitatiehandeling? De vergelijking met het bladeren in een encyclopedie dringt zich op. De 'bladeraar' verricht een typische gebruikshandeling. Hij exploiteert de encyclopedie niet, zelfs niet als hij hem van A tot Z leest en uit zijn hoofd leert. Dat wordt niet anders als de encyclopedie niet toebehoort aan de 'bladeraar', maar bijvoorbeeld aan een bibliotheek.

Zo is ook het browsen bij uitstek een consumptieve handeling. Het feit dat de gebruikers van commerciële databanken voor gebruikshandelingen afzonderlijk ('per use') plegen te betalen,

32. HR 30 oktober 1981, nr. 11 739, NJ 1982, 435 (CAI Amstelveen).

33. Overweging 23 van de considerans suggereert dat browsen onder art. 5 lid 1 begrepen wordt.

doet daar niet aan af. Wie zijn tijdschriften bij de kiosk betreft, betaalt eveneens per gebruikte eenheid. Maar daarmee is het lezen van de Panorama nog geen auteursrechtelijk relevante handeling geworden.

Niet iedere transactie waarmee auteursrechtelijk beschermde werken zijn gemoeid, behoort – kortom – een afzonderlijke auteursrechtelijke aanspraak te genereren. In de materiële wereld stelt onder meer de *uitputtingsregel* paal en perk aan de ongebreidelde opeenstapeling van auteursrechtelijke claims. De verkrijger van een exemplaar dat met toestemming van de rechthebbende op de markt is gebracht, kan daarmee doen en laten wat hij wil. In de virtuele wereld van het Internet bestaat behoefte aan een vergelijkbare begrenzing,³⁴ zeker als het (door de Commissie gepropageerde) uitgebreide reproductierecht regel zou worden.

Op de keper beschouwd, is de kwestie van het browsen niet het *hot issue* dat sommige Internet-scribenten er graag van maken. Zelfs als het reproductierecht zich tot iedere tijdelijk gekopieerde bit zou uitstrekken, zou browsen op het World Wide Web zijn toegestaan. Wie informatie via het web beschikbaar stelt, moet immers geacht worden het goed te vinden dat daarvan normaal gebruik wordt gemaakt. Browsen op het World Wide Web mag dus, al was het maar op grond van een stilzwijgende licentie.³⁵

Ook over de auteursrechtelijke status van de *hyperlink* woeden discussies een betere zaak waardig. Volgens sommigen is het aanbrengen van een 'link' naar auteursrechtelijk beschermde informatie mogelijk een vorm van (secundaire) openbaarmaking.³⁶ Anderen zien in de hyperlink slechts het elektronische equivalent van een voetnoot, die auteursrechtelijk buiten schot be-

34. Jerome H. Reichman, *Electronic Information Tools – The Outer Edge of World Intellectual Property Law*, IIC (24) 1993, p. 463; E.J. Dommering, a.w. noot 11, p. 110; David Nimmer, *Brains and Other Paraphernalia of the Digital Age*, Harvard Journal of Law and Technology (10) 1996, p. 33.

35. Nimmer, a.w., p. 20.

36. G. Brunt en M.H.M. Schellekens, *Auteursrecht in DigiWorld*, in: S.J.H. Gijrath e.a. (red.), *Intellectueel eigendom in digitaal perspectief*, Alphen aan den Rijn: Samsom 1996, p. 35-36.

hoort te blijven.³⁷ Ik sluit mij graag aan bij laatstgenoemde opvatting, maar doe dat hier zonder argumenten. Evenals het browsen, is het maken van hyperlinks een verschijnsel dat inherent is aan het World Wide Web. De mogelijkheid naar iedere pagina op het web een link te leggen ('hypertext') is een wezenlijk onderdeel van de programmeertaal waarmee webpagina's worden opgemaakt. Wie informatie via het web beschikbaar stelt, moet dan ook niet klagen als van die mogelijkheid daadwerkelijk gebruik wordt gemaakt.

Dat neemt niet weg dat zich situaties kunnen voordoen, dat tegen het leggen van een link legitiem bezwaar wordt gemaakt. Uit de praktijk bekend is het voorbeeld van de web site die zonder dat de bezoeker er erg in heeft, linkt naar pagina's van een concurrerende site. De bezoeker wordt in de waan gelaten dat de gepresenteerde pagina's deel uitmaken van de bezochte site ('framing'). Dergelijke gevallen van misleiding zijn op basis van het recht van ongeoorloofde mededinging (en eventueel het merkenrecht) gemakkelijk te bestrijden.³⁸

De rechthebbende zal evenzeer willen kunnen optreden tegen wie welbewust linkt naar een inbreukmakende publicatie op het web. Ook in dat geval biedt het gemene recht voldoende aanknopingspunten voor rechtshandhaving. De 'linker' handelt in zo'n geval niet minder onrechtmatig dan wie welbewust adverteert voor een gepirateerd product en dusdoende inbreuk bevordert.³⁹ Aan een auteursrechtelijk verbodsrecht ter zake van de hyperlink bestaat met dat al naar mijn oordeel geen enkele behoefte.

37. D.J.G. Visser, *The Economic Rights Involved. Report on the Netherlands*, in: M. Dellebeke (ed.), *Copyright in cyberspace, AIAI Study Days*, Amsterdam, Amsterdam: Otto Cramwinckel 1997, p. 127.

38. Th. Hoeren, *Cybermanners und Wettbewerbsrecht – Einige Überlegungen zum Lauterkeitsrecht im Internet*, *Wettbewerb in Recht und Praxis* 1997-11, p. 996.

39. Spoor/Verkade, p. 342; Pres. Rb Amsterdam 25 juni 1981, *Auteursrecht* 1981, p. 85 (NBB/De Piraat).

Wettelijke beperkingen

Het Internet dwingt niet alleen tot heroverweging van de exploitatierechten, maar ook tot herijking van het stelsel van wettelijke beperkingen dat daarvan de limiet bepaalt. Veel bestaande beperkingen zijn, in tegenstelling tot de abstract geformuleerde rechten van verveelvoudiging en openbaarmaking, in 'media-specifieke' termen gesteld. Sommige gelden alleen voor de gedrukte media, andere alleen voor film of omroep. Om deze regels aan te passen aan de multimediale context van het Internet is een majeure 'operatie stofkam' noodzakelijk. Visser heeft daarvoor in zijn recente ITeR-studie belangrijk voorwerk verricht.⁴⁰

Deze herijkingsoperatie dient verder te gaan dan het actualiseren van de bewoordingen van bestaande wetteksten, het 'multimedia-bestendig' maken van de wet. Wie beweert dat alles dat in de 'papieren wereld' thans is toegestaan, ook op het Internet 'moet kunnen', redeneert eendimensionaal. Evenals bij de uitleg van de exploitatierechten, dient de ratio van de beperkingen bij deze operatie leidraad te zijn. Deze ratio verschilt van beperking tot beperking; in sommige gevallen heeft een beperking meerdere rechtsgronden. Ik onderscheid een drietal categorieën:

Belangrijke wettelijke beperkingen als art. 15 Aw (vrije nieuwsvoorziening), art. 15a (citaatrecht) en art. 16b (eigen oefening, studie of gebruik) hebben hun rechtsgrond (mede) in constitutioneel gewaarborgde vrijheden, zoals de informatievrijheid (art. 10 EVRM en art. 7 Grondwet) en de bescherming van de persoonlijke levenssfeer (art. 8 EVRM en art. 10 Grondwet). Het spreekt vanzelf dat deze grondrechtelijk geïnspireerde beperkingen ook op het Internet onverkort van kracht dienen te blijven. Waar de bewoordingen van de huidige wet tekort schieten, is wetswijziging noodzakelijk.

Een tweede categorie wettelijke beperkingen komt voort uit overwegingen van algemeen belang, zonder dat daarvoor direct

40. D.J.G. Visser, Naar een multimedia-bestendig auteursrecht, ITeR-reeks nr. 10, Alphen aan den Rijn: Samsom 1998.

een grondrechtelijke grondslag valt aan te wijzen. Men denke hierbij aan wettelijke beperkingen ten behoeve van het onderwijs en de bibliotheken.⁴¹ Vergelijkbare beperkingen gelden in andere landen voor archieven en musea. Dienen dergelijke beperkingen in een digitale omgeving in stand te blijven? Hier is het oppassen geblazen. Het gevaar bestaat dat deze beperkingen, eenmaal omgezet in 'multimedia-bestendige' bewoordingen, alle perken te buiten gaan.

Nemen wij als voorbeeld de bibliotheek. Naar huidig auteursrecht geldt een aantal 'bibliotheek-privileges', die de bibliotheken de ruimte bieden hun belangrijke maatschappelijke taak gevrijwaard van auteursrechtelijke besognes te vervullen. Boeken mogen zonder toestemming worden geraadpleegd en uitgeleend; kopieën mogen in opdracht van gebruikers worden gemaakt en afgegeven. Dienen deze privileges ook te gelden voor de digitale bibliotheek van de toekomst?

Het probleem is: niemand weet hoe de digitale bibliotheek er uit zal zien. De fysieke beperking van de traditionele bibliotheek – met zijn voordeur, zijn boekenvoorraad en zijn vier muren – vormt een natuurlijke begrenzing aan het bibliotheekprivilege. In de digitale omgeving vallen deze grenzen weg; de digitale bibliotheek is (potentieel) altijd geopend, voor de gehele wereld toegankelijk en alom aanwezig. Vrij van auteursrechtelijke beslommeringen zou de digitale bibliotheek vrij spel hebben.⁴² Vergelijkbare problemen spelen ten aanzien van onderwijsinstellingen en musea. Van onderwijs-op-afstand naar online exploitatie is maar een kleine stap.

De derde categorie beperkingen levert de minste problemen op. Het gaat hier om de beperkingen die hun plaats in de wet slechts aan falende marktwerking hebben te danken. Een voorbeeld is het reprorecht, het stelsel van wettelijke beperkingen dat (institutionele) gebruikers de vrijheid laat op grote schaal – tegen betaling van 'reprodubbeltjes' – fotokopieën van auteursrechte-

41. Uiteraard zijn deze beperkingen wel tot bepaald *sociale* grondrechten te herleiden.

42. Dirk Visser, De auteursrechtelijke bibliotheek-exceptie van morgen, *Informatic Professional* 1997-2, p. 26.

lijk beschermde geschriften te maken. Mede door het enorme aantal gebruikers en rechthebbenden is een contractuele regeling van het fotokopiëren nooit van de grond gekomen.

Beperkingen als deze dienen niet blindelings naar de digitale omgeving te worden overgeplant. Zoals elders in dit preadvies (§ V.1) nader zal blijken, vormt het Internet een ideale voedingsbodem voor complexe contractuele exploitatiemodellen. Het staat zonder (proefondervindelijk) onderzoek geenszins vast dat op het Internet aan een 'reprorecht-model' behoefte bestaat. Terecht strekken de voorstellen van de Commissie Reprorecht en de minister van Justitie voor een vernieuwd reprorecht zich niet uit tot de elektronische kopie.⁴³

In haar voorstel voor een Auteursrechtrichtlijn doet de Europese Commissie een ambitieuze poging tot harmonisatie van de wettelijke beperkingen. Art. 5, leden 2 en 3, bevat daartoe een limitatieve opsomming van toegestane beperkingen, onder meer ten behoeve van bibliotheken, onderwijs en wetenschap, de actuele nieuwsvoorziening, het citeren en het voeren van gerechtelijke procedures. Aanvaarding van het voorstel zou betekenen dat een groot aantal andere, thans geldende nationale beperkingen mocht worden geschrapt of aangepast.⁴⁴ Gezien de grote culturele verschillen tussen de lidstaten, die zich vertalen in een scala van beperkingen die van land tot land verschillen, lijkt deze poging tot harmonisatie tot mislukken gedoemd.

III. HET EINDE VAN DE TERRITORIALITEIT

De tweede rode draad in dit verhaal loopt door in de preadviezen van Polak en Buruma. In cyberspace ('the space without a space') zijn de grenzen van de fysieke ruimte ('meatspace') volledig weggevallen. Het Internet kent en ondersteunt geen geografische territorialiteit. Het net is een zelf-routerend systeem:

43. Commissie Auteursrecht, Eindrapport over het Reprorecht, Informatierecht/AMI 1997-5, p. 95; brief van de minister van Justitie aan de Voorzitter van de Tweede Kamer, Kamerstukken TK, 1996-1997, 25 528, nr. 1.

44. Zie de voorbeelden genoemd door D.J.G. Visser, Staatscourant 1997, 246, p. 6.

de bits en bytes zoeken hun eigen weg van zender naar ontvanger. Fysieke lokatie heeft op het net vrijwel iedere betekenis verloren. Wie veelvuldig van het Internet gebruik maakt, ervaart dat als het ware aan den lijve. Zijn vaste e-mail-correspondent in Los Angeles is hem nader dan zijn Internetloze collega proximus uit Amsterdam.

Voor de theorie en de praktijk van het auteursrecht vormt het wegvallen van geografische territorialiteit een ernstig probleem. Het auteursrechtelijke bouwwerk rust immers op een solide territoriaal fundament. Alle internationale verdragen en harmonisatie-richtlijnen ten spijt, het auteursrecht bestaat nog steeds uit een lappendeken van nationale, territoriaal begrensde rechten. De overgang van lappendeken naar netwerk ('from patchwork to network'⁴⁵) roept ingewikkelde auteursrechtelijke vragen op, die door het IPR slechts ten dele kunnen worden beantwoord.

De Berner Conventie, die sedert 1886 wereldwijde auteursrechtelijke bescherming waarborgt, heeft deze lappendeken goeddeels in stand gehouden. De inhoud van het auteursrecht wordt autonoom bepaald door iedere conventiestaat (art. 5 lid 2 BC). De minimumrechten van de conventie doen daar – alleen voor buitenlanders⁴⁶ – nog een klein schepje bovenop. Het gelijkheidsbeginsel van de Conventie houdt in dat buitenlanders met 'binnenlanders' gelijk worden gesteld: een Fransman wordt in Nederland als een Nederlander beschermd (en omgekeerd). Aldus beschikt de maker van een werk over een bundel van (inmiddels meer dan honderd⁴⁷) nationale auteursrechten, die hij in ieder conventieland volgens het lokale recht beschermd weet.

De exploitatie van auteursrechtelijk beschermde werken heeft in de praktijk het patroon van de lappendeken grotendeels gevolgd. Uitgaverrechten (voor boeken en andere gedrukte publicaties) worden per territoire verleend en geëxploiteerd. De ex-

45. Paul Edward Geller, *From Patchwork to Network: Strategies for International Intellectual Property in Flux*, te verschijnen in: *IIC* (28) 1998.

46. W.J.M. Diekman, *TRIPs, WIPO en de Nederlanders*, *Informatierecht/AMI* 1997-10, p. 207.

47. Bij de Berner Conventie zijn 128 staten aangesloten (stand per 1 januari 1998).

exploitatie van bioscoopfilms geschiedt eveneens op geografische grondslag. Territoriale afbakening van markten fungeert hierbij onder meer als instrument van prijsdiscriminatie en gedifferentieerde marketing.⁴⁸ Nationale (quasi-)monopolies op het collectieve beheer van auteursrechten (BUMA, STEMRA, Stichting Reprorecht, enzovoorts) versterken deze 'nationalistische' tendens.

Deze licentiepraktijk werkt goed zolang het medium in kwestie territoriale exclusiviteit daadwerkelijk toelaat. Hierbij speelt de mogelijkheid van rechtshandhaving uiteraard een belangrijke rol. De lappendeken gaat scheuren zodra het medium niet langer effectief aan de rechtsmacht van een nationale staat (met bijbehorend geweldmonopolie) kan worden onderworpen.⁴⁹ Gepirateerde boeken en video's kunnen aan de grenzen worden tegengehouden.⁵⁰ Fabrieken van illegale CD's kunnen, desnoods met de sterke arm, gesloten worden. Maar wat te doen tegen de (geenszins denkbeeldige) web site op de Kaaiman Eilanden, waar de nieuwste hits tegen een habbekrats wereldwijd verkrijgbaar zijn?

Helemaal nieuw is dit probleem overigens niet. Het auteursrecht heeft al eerder kennis gemaakt met een medium dat zich van staatsgrenzen weinig aantrekt: de etheromroep. De ether laat zich, evenmin als het Internet, gemakkelijk in het keurslijf wringen van een territoriaal licentiemodel. Geen wonder dat de introductie van de omroepsatelliet destijds voor grote verwarring onder rechthebbenden heeft gezorgd. Moest voor een uitzending per omroepsatelliet de toestemming worden verkregen van alle rechthebbenden die zich binnen de 'footprint' (het zenderbereik) van de satelliet bevinden, of kon met licenties in het land van 'opstraling' worden volstaan?

48. John H. Barton, *The Balance Between Intellectual Property Rights and Competition: Paradigms in the Information Sector*, *European Competition Law Review* 1997, p. 441.

49. David R. Johnson en David Post, *Law and Borders – The Rise of Law in Cyberspace*, *Stanford Law Review* (48) 1996-5, p. 1369.

50. Verordening nr. 3295/94 van de Raad tot vaststelling van maatregelen om het in het vrije verkeer brengen, de uitvoer, de wederuitvoer en de plaatsing onder een schorsingsregeling van nagemaakte of door piraterij verkregen goederen te verbieden van 22 december 1994, Pb EG L 341/8.

De Europese Richtlijn satellietomroep en kabeldoorgifte⁵¹ heeft aan deze verwarring voor de landen van de Europese Economische Ruimte een einde gemaakt. De Richtlijn bepaalt dat een uitzending per satelliet slechts als openbaarmaking is aan te merken in de lidstaat waar de 'injectie' van het programmadrage signaal plaatsvindt. Plaatselijke rechthebbenden (filmdistributeurs, omroepen, enz.) kunnen zich tegen een satellietuitzending vanuit een andere lidstaat derhalve niet langer met auteursrechtelijke middelen verzetten. Voor satellietuitzending behoeft voortaan slechts in het land van oorsprong toestemming van rechthebbenden te worden verkregen.

Hoewel op het eerste gezicht geschikt om ook voor het Internet soelaas te bieden, heeft de constructie van een 'injectierecht' voorlopig geen navolging gekregen.⁵² Het reduceren van een veelheid van nationale rechten tot één digitaal injectierecht moge voor exploitanten een uitkomst zijn, voor rechthebbenden is het een nachtmerrie. Deze nachtmerrie heet *delocalatie*, de verplaatsing van exploitatie-activiteiten naar landen met een laag beschermingsniveau, de zogeheten 'copyright havens' (niet: 'heavens'). De angst voor delocalatie verklaart in belangrijke mate waarom rechthebbenden zoveel belang hechten aan aansprakelijkheid van de service provider, de laatste 'fysieke' schakel tussen de tastbare en de virtuele wereld. Zolang de wereldkaart van het auteursrecht nog een groot aantal witte plekken vertoont, lijkt toepassing van het lex-originismodel op het Internet uitgesloten.

In afwachting van een globale oplossing moet het Internet onder de lappendeken van de territorialiteit een plaatsje krijgen. Dat is geen gemakkelijke opgave. Zoals Polak in zijn preadvies beschrijft, is de IPR-regel van de lex protectionis naar huidig recht de enige verwijzingsregel die redelijkerwijs in aanmerking komt. De vraag of een gedraging op het Internet als een inbreuk op

51. Richtlijn 93/83/EEG van de Raad van 27 september 1993 tot coördinatie van bepaalde voorschriften betreffende het auteursrecht en naburige rechten op het gebied van de satellietomroep en de doorgifte via de kabel, Pb EG 1993 L 248/15, waarover P.B. Hugenholtz, De Europese richtlijn inzake satellietomroep en kabeldoorgifte, Informatierecht/AMI 1994-5, p. 87.

52. Zie het preadvies van Polak, § 50.

een recht van intellectuele eigendom valt aan te merken, wordt derhalve beheerst door het recht van het land waar de gedraging haar 'schadelijke inwerking' heeft.⁵³ Die inwerking, zo schrijft Polak elders, is voorzienbaar wereldwijd.⁵⁴ Dat betekent dat iedere publicatie op het Internet potentieel naar het (auteurs)recht van meer dan 100 soevereine staten moet worden beoordeeld.⁵⁵ De aanbieder van informatie loopt daardoor een groot aansprakelijkheidsrisico.⁵⁶ Hij dient van ieder auteursrechtelijk beschermd werk dat hij 'op het net zet' voor meer dan 100 staten de nodige rechten te verwerven.

Een extra complicerende factor vormt hierbij de inhoud van het auteursrecht die van land tot land verschilt. De bestaande rechts-onzekerheid over de reikwijdte van het auteursrecht op het Internet accentueert deze verschillen. Wie het probleem van de tijdelijke kopie naar Nederlands recht al ingewikkeld vindt, wil er niet aan denken wat rechtens is in, laten we zeggen, Burkina Faso. Toch dwingt toepassing van de lex-protectionisregel op het Internet de bona fide exploitant tot dergelijke hersengymnastiek. Zo heeft iedere actor op het Internet zijn eigen auteursrechtelijke nachtmerrie.

Prille initiatieven uit de hoek van het collectieve rechtenbeheer om exploitanten de helpende hand te bieden, geven weinig reden tot optimisme. De Internet-licentie die BUMA/STEMRA (op grond van een 'Tijdelijke regeling muziekgebruik op Internet'⁵⁷) voor Nederlandse site-beheerders in petto heeft, is goed bedoeld, maar weinig meer dan een wassen neus. De licentie heeft slechts betrekking op het gebruik van muziekwerken (tekst en bladmuziek), niet op uitvoeringen of opnamen daarvan. Daarover waakt niet BUMA of STEMRA, maar de Stichting

53. Polak, § 53.

54. Polak, § 50.

55. Jane C. Ginsburg, Global Use/Territorial Rights: Private International Law Questions of the Global Information Infrastructure, *Journal of the Copyright Society of the U.S.A.* (12) 1995, p. 320.

56. C.E. Drion en J.J. Linnemann, Aansprakelijkheidskwesties en andere uitdagingen van het Internet aan de nationale rechtsorde, *NJB* 1996-41, p. 1739.

57. J. Jonkers, Buma/Stemra en het Internet, *Informatierecht/AMI* 1997-3, p. 54; Tijdelijke regeling muziekgebruik op Internet, <http://www.buma.nl>.

SENA, die belast is met het collectieve beheer van naburige rechten. SENNA doet aan de Tijdelijke Regeling niet mee.

Het is overigens maar de vraag of de rechtenorganisaties over de vereiste bevoegdheden beschikken namens alle door hen vertegenwoordigde rechthebbenden Internet-licenties af te sluiten. Een generieke rechtenoverdracht of licentie pleegt onder de vigeur van art. 2 lid 2 Auteurswet beperkt (ten gunste van de auteur) te worden uitgelegd.⁵⁸ Of de thans door de rechtenorganisaties gehanteerde aansluitcontracten ook de 'elektronische rechten' omvatten, is betwist.⁵⁹

Het gebrekkige mandaat van de rechtenorganisaties en de stammenstrijd tussen de organisaties onderling maken een collectieve oplossing op korte termijn illusoir. Ook op langere termijn biedt deze benadering weinig perspectief.⁶⁰ In veel rechtenorganisaties zijn het niet de individuele auteurs, maar de grote rechthebbenden (uitgevers, filmproducenten) die het voor het zeggen hebben. Deze *major players* zullen er de voorkeur aan geven de elektronische rechten zelf te beheren. Internet-rechten zijn zolangzamerhand geen 'nevenrechten' meer, maar primaire exploitatierechten die door de rechthebbenden niet graag uit handen worden gegeven. Het Internet schept voor uitgevers en producenten nieuwe kansen die zij graag zelf zonder tussenkomst van een rechtenorganisatie willen benutten.

De conclusie dringt zich op dat rechtmatige exploitatie van auteursrechtelijk beschermde werken via het Internet voorshands vrijwel *onmogelijk* is. Alleen in het uitzonderlijke geval dat vast staat dat geen rechtenoverdracht heeft plaatsgevonden en er geen reden is te twijfelen aan het makerschap van de auteur, kan

58. Vgl. Rb Amsterdam 24 september 1997, Mediaforum 1997-11/12, p. B159 (NVJ/Volkskrant); K.J. Koelman, noot 16.

59. H.W. Wefers Bettink, Muziek op Internet: de BUMA-regeling, Computerrecht 1997-2, p. 55.

60. Er zijn meer redenen waarom collectief rechtenbeheer op het Internet gedoemd is te falen. Stel dat website-beheerders of providers door een 'super-BUMA' in de gelegenheid werden gesteld een Internet-licentie voor alle mogelijke werken te verwerven. Aan wie zouden de royalties moeten worden uitgekeerd? Aan eenieder van wie werken via het Internet openbaar worden gemaakt: bij benadering de gehele Internet-bevolking.

de Internet-exploitant erop vertrouwen dat het 'auteursrechtelijk wel goed zit'. Het komt er in de praktijk op neer dat het alleen de auteur zelf is die zonder auteursrechtelijke risico's zijn gedachtengoed in cyberspace de vrije loop kan laten.

De vraag rijst of het IPR geen alternatief zou moeten bieden. De lex-protectionisregel moge een elegant en intellectueel bevredigend resultaat opleveren, wie meer wil met het Internet dan het uiten van zijn eigen hoogstpersoonlijke gevoelens wordt er ernstig door belemmerd. Hoe deze impasse te doorbreken? Door het ontwerpen van een regel die de exploitant niet dwingt rekening te houden met de auteurswetten van meer dan honderd soevereine staten. In contractuele verhoudingen voorkomt de vrijwillige rechtskeuze door partijen veel IPR-ellende. Een mogelijke oplossing voor het Internet zou zijn auteurs(rechthebbenden) bij eerste publicatie van hun werk tot een rechtskeuze te verplichten, zodat a priori zekerheid bestaat over het op exploitatie en inbreuk toepasselijke recht. Een verplichte rechtskeuze zou een homogene beschermingsomvang van het werk over het gehele Internet (en daarbuiten) waarborgen; rechthebbenden en gebruikers zouden met lokaal afwijkende regimes voortaan geen rekening meer hebben te houden.⁶¹ De rechtskeuze zou als onderdeel van de 'rights management information' onverbrekkelijk met het werk verbonden blijven. Het spreekt vanzelf dat een dergelijke (of andere) IPR-oplossing bij voorkur in een internationaal verdrag haar beslag zou moeten krijgen.⁶²

Uiteraard zijn alle problemen hiermee nog lang niet uit de wereld. Het lijkt moeilijk voorstelbaar de inhoud van het auteursrecht geheel door het recht van het land van oorsprong te laten

61. Ik ontleen het idee van de verplichte rechtskeuze aan de doctoraalscriptie van UvA-student M.P.Th. Steyn, *Internationaal auteursrecht in de informatiemaatschappij* (Amsterdam UvA 1998). Het idee impliceert herinvoering van een (thans door de Berner Conventie verboden) formaliteitseis; bij publicatie ware behalve de naam van de rechthebbende ook het land van verplichte rechtskeuze te vermelden. Vgl. het vlaggebeginsel in het zeerecht, waarover J. Boek, in: Ingrid van den Berg e.a. (red.), *Regulering van het Internet*, ITeR-reeks nr. 9, Alphen aan den Rijn: Samsom 1997, p. 63.

62. A.A. Quaadvlieg, *Een multiple personality syndroom in het i.p.r.: wie is auteursrechthebbende?*, *Informatierecht/AMI* 1997-8, p. 161-162.

bepalen.⁶³ In elk geval zullen *ordre publique*-regels, zoals beperkingen ter bescherming van de informatievrijheid, roet in het eten blijven gooien⁶⁴, zeker als rechthebbenden ertoe zouden overgaan en masse het recht van een al te auteursrechtvriendelijke staat te kiezen.

Welke IPR-regel men ook verkiest, het territorialiteitsbeginsel van het nationale en internationale auteursrecht blijft het belangrijkste obstakel. Veruit de beste oplossing is dan ook het materiële auteursrecht op mondiaal niveau geheel gelijk te schakelen. Als de voortekenen ons niet bedriegen, zal het Internet aan de mondiale unificatie van het auteursrecht een beslissende impuls geven. De contouren van een *wereldauteursrecht* (lange tijd een *fata morgana*) beginnen zich af te tekenen. Het WIPO-Auteursrechtverdrag dat eind 1996 tot stand kwam, moge een mislukking heten, het verbijsterende tempo waarmee het verdrag tot stand is gekomen, is veelzeggend.

IV. AANSPRAKELIJKHEID VAN INTERMEDIARIS

Zelfs met een wereldauteursrecht in de hand blijft de handhaving van het auteursrecht op het Internet een *mer à boire*. In een oceaan van potentiële inbreukmakers lijkt effectieve rechtshandhaving een illusie. Geen wonder dat rechthebbenden hun pijlen elders richten: op de intermediairs die de schakel vormen tussen de virtuele en de 'echte' wereld. Anders dan de digitale wereldburger die zich kan verschuilen achter een masker van anonimiteit of zich door delocatie aan handhaving kan onttrekken, zijn de providers relatief gemakkelijke prooien. De aansprakelijkheid van de provider is een van de meest controversiële juridische vraagstukken die het Internet te bieden heeft.⁶⁵

63. Vgl. Quaadvlieg, a.w., p. 160.

64. Vgl. Cour de Cassation 28 mei 1982, RIDA 1991, nr. 149, p. 197 (Asphalt jungle).

65. Zie o.m. G. Spindler, Deliktsrechtliche Haftung im Internet – nationale und internationale Rechtsprobleme, ZUM 1996-7, p. 533; N. Bortloff, Die Verantwortlichkeit von online Diensten, GRUR Int 1997-5, p. 387; Instituut voor Informatierecht (K.J. Koelman), Liability for On-line Intermediaries, Amsterdam: Instituut voor Informatierecht 1997.

De aansprakelijkheidsvraag vergt een nauwkeurige analyse van de maatschappelijke rol en functie van de Internet-providers.⁶⁶ Problematisch is vooral de hybride positie van de *service provider*, die derden in de gelegenheid stelt informatie via het net te verspreiden. De service provider stelt daartoe capaciteit op zijn servers ter beschikking. In sommige gevallen is hij ook inhoudelijk bij het informatie-aanbod betrokken. Daarnaast biedt de service provider andere communicatiediensten aan, zoals e-mail en nieuwsgroepen.

Van de service provider te onderscheiden is de *access provider*; deze biedt gebruikers toegang tot het Internet door het aanbieden van inbelfaciliteiten. De access provider heeft met het informatie-aanbod op het Internet niets van doen; tot blokkeren of afsluiten van inbreukmakende sites is hij evenmin in staat. Complicerende factor is de dubbelrol die veel providers in de praktijk vervullen: zij zijn access en service provider in één. Deze dubbelrol verklaart ten dele de verwarring die over de aansprakelijkheid van de provider inmiddels is ontstaan.

De variabele rol van de provider maakt het moeilijk algemene uitspraken over de aansprakelijkheid te doen. Om dezelfde reden dienen vergelijkingen met tussenpersonen uit de 'analoge' wereld, zoals uitgevers, drukkers, kabelexploitanten en PTT's, met de nodige voorzichtigheid te worden gemaakt.

Een favoriete analogie onder de providers zelf is die van de 'common carrier', die (volgens een oude PTT-slogan) 'geen boodschap aan de boodschap' heeft, en voor de vervoerde boodschappen nimmer aansprakelijk kan worden gesteld. Deze vergelijking is misplaatst. De bijzondere status van de common carrier vloeit voort uit de universele leveringsplicht die hem als (quasi-)monopolist bij wet is opgelegd. Deze verplichting impliceert een exoneratie of rechtvaardigingsgrond ten aanzien van de inhoud van de vervoerde boodschappen. Voorts kan de common carrier zich ten aanzien van de door hem geleverde niet-openbare diensten (tele-

66. Zie het preadvies van Koers, § 1.3.

fonie, dataverkeer, huurlijnen) beroepen op het telecommunicatiegeheim (art. 13 Gw⁶⁷) en daarop gebaseerde strafbepalingen.

Anders dan de common carrier geldt voor Internet-providers geen wettelijke leveringsplicht; er is (voorshands) geen sprake van dominante marktpartijen, maar van een levendige concurrentie. Het telecommunicatiegeheim kan door de providers alleen worden ingeroepen voor diensten met een besloten karakter (e-mail bijvoorbeeld).⁶⁸

Toerekenbare inbreuk?

Zijn providers aansprakelijk voor de inbreukmakende bits en bytes die hun servers passeren? Oudere rechtspraak inzake 'analoge' intermediairs werpt enig licht op deze vraag. Geen twijfel bestaat over de aansprakelijkheid van drukkers en uitgever⁶⁹ of handelaars in gepirateerde producten.⁷⁰ Deze intermediairs pleegen rechtstreeks inbreuk op een uitsluitend recht (van verveelvoudiging of openbaarmaking) en zijn daarvoor aansprakelijk. De omstandigheid dat de intermediair bij de gepubliceerde inhoud op geen enkele wijze betrokken is geweest, doet aan de toerekenbaarheid niet af.⁷¹ Op de intermediair rust normaliter een onderzoeksplicht; door die te verzaken neemt hij het risico van auteursrechtinbreuk voor zijn rekening. Het absolute karakter van het auteursrecht brengt mee dat de intermediair eerder voor door derden gepleegde auteursrechtinbreuk dan voor anderszins onrechtmatige uitingen van derden aansprakelijk zal

67. Een weinig doordacht voorstel tot wijziging van art. 13 Gw heeft aanleiding gegeven tot pittige discussies: Kamerstukken TK 1996-1997, 25 443, nr. 1-2, waarover *kritisch* N.A.N.M. van Eijk, (G)een recht op vertrouwelijke communicatie: fax en email vogelvrij, NJB 1997, p. 1554, en Egbert Dommering, Geen telefoongheim op de elektronische snelweg, Mediaforum 1997-10, p. 142.

68. Kamerstukken TK 1997-1998, 25 443, nr. 5, p. 19.

69. Rb Amsterdam 13 december 1930, NJ 1931, 938.

70. Pres. Rb Amsterdam 5 augustus 1982, KG 1982, 139; zie Onrechtmatige Daad, Art. 162, lid 3, aant. 16 en aldaar aangehaalde jurisprudentie.

71. HR 10 november 1989, NJ 1990, 113 (Mary Daly/Kardinaal Simonis); Spoor/Verkade, p. 404-405. Overigens is voor toewijzing van een verbod of een verklaring voor recht geen toerekenbaarheid vereist.

zijn.⁷² Hierbij speelt de 'ideële' uitingsvrijheid van de media uiteraard een rol.⁷³

Geen auteursrechtinbreuk pleegt de organisator van een evenement (bijvoorbeeld een muziekconcours⁷⁴) of degene die in zijn lokaliteit (bijvoorbeeld een horecagelegenheid⁷⁵) de gelegenheid schept tot openbaarmaken. De organisator of zaaleigenaar is niet degene die feitelijk openbaarmaakt.⁷⁶ Wel kan onder omstandigheden sprake zijn van (onrechtmatig) 'bevorderen' van inbreuk; zie hierna. Het is moeilijk een scherpe grens te trekken tussen activiteiten die rechtstreeks auteursrechtinbreuk opleveren en vormen van inbreuk 'bevorderend' handelen of nalaten. Gerbrandy merkt hierover op: 'Hoc verder de gewraakte handelingen (van hem in wiens inrichting de uitvoering plaats had) van de feitelijke uitvoering af staan, des te meer dringt zich de schuld-vraag naar voren en vereist deze een afzonderlijk onderzoek.'⁷⁷

Evenmin als inbreukmakers aan te merken zijn leveranciers van hulpgoederen en -diensten of andere ondersteunende faciliteiten, zoals kaartverkopers, zettters en elektriciteitsmaatschappijen.⁷⁸ Ook de producent of leverancier van kopieerapparatuur is voor daarmee gepleegde verveelvoudigingen niet auteursrechtelijk aansprakelijk; zie *infra* § V.2.

Een grensgeval is de kabelexploitant. In de zaak *KTA/Columbia* moest de Hoge Raad oordelen over de vraag of de kabelexploitant die uitzendingen van zogenoemde kabelpiraten (nolens vo-

72. Vgl. Pres. Rb Amsterdam 11 januari 1993, Mediaforum 1993-3, p. B38 (Dit-corp/Heertje); Pres. Rb Amsterdam 24 februari 1993, KG 1993, 115 (Sonja op zaterdag); zie Onrechtmatige Daad, VII, aant. 44, 47 en 167 en aldaar aangehaalde jurisprudentie.

73. EHRM 23 september 1994, NJ 1995, 387, Mediaforum 1994-11/12, p. B101 (Jersild).

74. HR 11 februari 1926, NJ 1926, p. 354.

75. HR 8 maart 1957, NJ 1957, 271 (BUMA/De Vries); S. Gerbrandy, Kort commentaar op de Auteurswet 1912, Arnhem: Gouda Quint 1988, p. 125 en p. 327, met uitvoerige verwijzingen naar jurisprudentie.

76. HR 4 juni 1920, NJ 1920, 720; HR 11 februari 1926, NJ 1926, 354; Gerbrandy, i.a.p.

77. Gerbrandy, a.w., p. 317.

78. Vgl. voor Duitsland: G. Schricker (red.), Urheberrecht. Kommentar, München: Beck 1987, p. 1115.

lens) doorgaf als openbaarmaker was aan te merken. In eerdere arresten had de Hoge Raad al uitgemaakt dat kabeldoorgifte van omroepprogramma's in beginsel als (secundaire) openbaarmaking is aan te merken.⁷⁹ In de KTA-zaak beriep de kabelexploitant zich vergeefs op zijn passieve rol van 'doorgeefluik'. Vast stond dat KTA door het nemen van technische maatregelen (het 's nachts afschakelen van haar antennes) aan de piraterij een einde kon maken. De Hoge Raad baseerde mede hierop zijn oordeel dat de kabelexploitant wel degelijk openbaarmaakte. Reeds het enkele 'in werking doen zijn van haar apparatuur – die meebrengt dat haar abonnees de films op hun scherm ontvangen' werd door de Hoge Raad beschouwd als openbaarmaking waarvoor het kabelnet aansprakelijk is.⁸⁰ Eerder had de Hoge Raad in het *Draadomroeparrest* beslist dat de PTT als exploitant van de draadomroep voor openbaarmaking aansprakelijk was en 'dat daaraan niet kan afdoen dat ... de PTT geen invloed heeft op de samenstelling van de programma's, welke zij op deze wijze openbaar maakt'.⁸¹

In de eerste (en tot op heden enige) procedure over de auteursrechtelijke aansprakelijkheid van Internet service providers, de geruchtmakende zaak *Scientology/XS4All e.a.*, overwoog de President van de Rechtbank Den Haag:

'dat zij (providers) niet meer doen dan gelegenheid geven tot openbaarmaking en dat zij in beginsel geen invloed kunnen uitoefenen of zelfs maar kennis dragen van datgene wat diegene die via hen toegang tot Internet hebben gekregen daarop uitdragen. In beginsel is er daarom geen aanleiding hen aansprakelijk te houden voor onrechtmatige – bijvoorbeeld op auteursrechten van derden inbreuk makende – handelingen van gebruikers.'⁸²

79. HR 30 oktober 1981, zaak 11 739, NJ 1982, 435 en IIR 30 oktober 1981, zaak 11 740, AA 1982, 79; in gelijke zin HR 25 mei 1984, zaak 12 281, NJ 1984, 697 en IIR 25 mei 1984, zaak 12 282, AA 1986, 628; G.J.H.M. Mom, Kabeltelevisie en auteursrecht (diss. Amsterdam UvA), Lelystad: Vermande 1990.

80. IIR 14 januari 1983, NJ 1984, 696.

81. IIR 27 juni 1958, NJ 1958, 405.

82. Pres. Rb Den Haag 12 maart 1996, Mediaforum 1996/4, p. B59, met commentaar D.J.G. Visser op p. 61. De in het vonnis gebruikte terminologie is verwarrend; service providers worden door de President ten onrechte als 'access providers' aangeduid.

Volgens de President is de activiteit van de service providers derhalve niet als 'openbaarmaken' te kwalificeren. Het Scientology-vonnis lijkt op het eerste gezicht moeilijk te rijmen met het arrest in de zaak KTA/Columbia.⁸³ Een relevant verschil is wellicht de mate van inhoudelijke betrokkenheid van de intermediair. De rol van de kabelexploitant in het communicatieproces is minder passief dan die van de Internet-provider. De kabelexploitant heeft weliswaar met de inhoud van de doorgegeven programma's geen bemoeienis, voor de selectie van de programma's is hij, behoudens bindende aanwijzingen door de wetgever, programmeraden of het Commissariaat voor de Media (art. 81h-81l Mediawet), wel degelijk verantwoordelijk. Een belangrijk verschil is voorts gelegen in de praktische mogelijkheid controle uit te oefenen. Het in de gaten houden van enkele tientallen kabelkanalen is wellicht (nog net) 'te doen', dat geldt niet voor het bewaken van de vele duizenden web sites die iedere provider onder zijn hoede heeft.

Tijdens de Diplomatieke Conferentie in Genève is door de verdragsluitende landen een *Agreed Statement* bij art. 8 van het WIPO Auteursrechtverdrag aangenomen, dat naadloos aansluit bij het oordeel van de President:

'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.'

Onzorgvuldigheid: bevorderen van inbreuk

Handelingen die niet rechtstreeks in strijd zijn met de exclusieve rechten van auteursrechthebbenden, maar aan de inbreuk hebben bijgedragen, kunnen op grond van art. 6:162 BW wegens strijd met de maatschappelijke zorgvuldigheid toch onrechtmatig worden bevonden. Gerbrandy spreekt in dit verband van het 'bevorderen' van auteursrechtinbreuk.⁸⁴ Zo werd in de zaak

83. C.E. Drion en J.J. Linnemann, Aansprakelijkheidskwesties en andere uitdagingen van het Internet aan de nationale rechtsorde, NJB 1996-41, p. 1738.

84. Gerbrandy, a.w., p. 327; Spoor/Verkadé, p. 341.

Buma/De Vries het stilzitten van de eigenaars van een café-bedrijf waar muziek ten gehore werd gebracht in strijd met art. 1401 BW (oud) geoordeeld.⁸⁵ Bij het oordeel van de Hoge Raad speelde een rol dat de eigenaars feitelijke zeggenschap hadden over het musicerende personeel en dat zij hadden behoren te weten dat in het café-bedrijf auteursrechtelijk beschermde werken ten gehore zouden worden gebracht.

Toepassing van de beide door de Hoge Raad gehanteerde criteria (wetenschap en feitelijke controle) leidt ten aanzien van de Internet providers tot het volgende resultaat. De *access* provider is een 'bloot vervoerder'; hij heeft geen kennis van de getransporteerde informatie en zelfs geen mogelijkheid inbreukmakend handelen te voorkomen of, bij gebleken inbreuk, in te grijpen. De *access* provider kan inbreukend materiaal niet van het Internet verwijderen; het materiaal bevindt zich immers niet op zijn eigen servers. Technisch mogelijk is wel het compleet 'afsnijden' van de toegang tot de service provider die de inbreukmakende site faciliteert. Een dergelijke ingreep kan van de provider echter onmogelijk gevergd worden; alle 'onschuldige' informatie-aanbieders die van dezelfde service provider gebruik maken, zouden eveneens worden getroffen. Geconcludeerd kan worden dat de *access* provider voor inbreuk niet aansprakelijk gesteld kan worden.

De *service* provider bezit evenmin a priori kennis van de vervoerde 'content', tenzij hij bij het informatie-aanbod op enigerlei wijze betrokken is (bijvoorbeeld door het verkopen van advertentieruimte of het actief ondersteunen van aantrekkelijke sites). Deze situatie doet zich met name voor bij 'besloten' service providers, zoals CompuServe. Het informatie-aanbod van deze providers wordt in belangrijke mate door de providers zelf samengesteld en geselecteerd.

Behoort de service provider van eventuele inbreuk te weten? Dat er via zijn servers zo nu en dan beschermde werken worden openbaargemaakt, zal hem in abstracto zeker bekend zijn c.q. behoren te zijn. In de praktijk is inbreuk echter eerder uitzondering dan regel; veruit de meeste informatie die via het Inter-

85. HR 8 maart 1957, NJ 1957, 271.

net wordt verzonden is 'eigen werk', waaraan auteursrechtelijk geen vuiltje kleeft. In zoverre verschilt de positie van de service provider wezenlijk van die van de zaaleigenaar, drukker of handelaar in videocassetten. Het lijkt daarom onjuist van de (subjectieve) wetenschap van de provider al te zeer te abstraheren.

Beschikt de service provider over de mogelijkheid feitelijke controle uit te oefenen? Niet a priori; het vooraf op inbreuk 'screenen' van de vele tienduizenden webpagina's die via zijn server(s) worden aangeboden, is naar de huidige stand van de techniek⁸⁶ ondoenlijk.⁸⁷ Na op de inbreuk te zijn gewezen, is ingrijpen door de provider daarentegen alleszins mogelijk. Het inbreukmaken van de materiaa kan, desnoods tegen de wil van de beheerder van de web site, van de server worden gewist.

Afgezien van gevallen van evidente inbreuk is notificatie van de service provider een sine qua non voor aansprakelijkheid. Het vonnis in de zaak *Scientology/XS4ALL c.s.* onderschrijft deze conclusie; de President overweegt dat van aansprakelijkheid eerst sprake zou kunnen zijn 'in een situatie waarin onmiskenbaar duidelijk is dat een publicatie van een gebruiker onrechtmatig is en waarin redelijkerwijs mag worden aangenomen dat zulks ook bij de access (bedoeld is: service, PBII) provider bekend is, bijvoorbeeld doordat deze op een en ander is geattendeerd'.

Het vonnis roept de vraag op wanneer 'onmiskenbaar duidelijk' is dat een publicatie van een gebruiker onrechtmatig is'. Is iedere boze brief van een advocaat voldoende of dient de onrechtmatigheid eerst in rechte te worden vastgesteld? Naar mijn oordeel zal de provider in geval van gemotiveerde ontkenning door

86. In de toekomst is dat mogelijk anders. Zogenaamde *electronic copyright management systems* zullen in staat zijn de auteursrechtelijke status van gedistribueerde werken automatisch te verifiëren; zie § V.2 infra. De vraag rijst of de maatschappelijke zorgvuldigheid meebrengt dat providers dergelijke maatregelen moeten toepassen; zie Instituut voor Informatierecht, *Liability for On-line Intermediaries*, Amsterdam: Instituut voor Informatierecht 1997, p. 80-81.

87. Op dit punt wijkt de positie van de service provider af van die van de beheerder van een elektronisch bulletin board (BBS), die uit het informatie-aanbod de rotte appels nog betrekkelijk gemakkelijk kan verwijderen; Rb. Rotterdam 24 augustus 1995, *Informatierecht/AMI* 1996-5, p. 101 (Bridge-soft/Lenior).

de beheerder van de web site de status quo voorlopig mogen handhaven, in afwachting van een gerechtelijk oordeel. De provider dient immers ook jegens zijn contractspartij zorgvuldig te handelen; zijn contractuele verplichtingen dienen bij het zorgvuldigheidsoordeel te worden meegewogen. Enige kennis van het auteursrecht mag echter wel van de provider worden gevergd. Ten aanzien van web sites waarop complete muziekwerken of romans worden aangeboden, zal hij zijn handen – in elk geval na notificatie door rechthebbenden – niet in onschuld kunnen wassen.

Risico-aansprakelijkheid?

Vooraf onder rechthebbenden bestaat de (begrijpelijke) wens service providers met een vorm van risico-aansprakelijkheid te belasten.⁸⁸ Gezien het gesloten wettelijke systeem van risico-aansprakelijkheden⁸⁹, is hiervoor wetswijziging noodzakelijk, tenzij zou worden aangenomen dat art. 162 lid 3, slotzinsnede (toerekening volgens verkeersopvattingen) hiervoor een voldoende grondslag biedt. De wetsgeschiedenis lijkt een extensieve uitleg van deze bepaling echter in de weg te staan.⁹⁰

De vraag rijst of voor risico-aansprakelijkheid valide gronden bestaan. Vóór risico-aansprakelijkheid pleit ongetwijfeld het *culpa in causa*-beginsel dat aan iedere aansprakelijkheid uiteindelijk ten grondslag ligt. De providers hebben de condities gecreëerd, waardoor (grootscheepse en wereldwijde) inbreuk op auteursrechten mogelijk is geworden. Sterker, de providers plukken daarvan dagelijks de vruchten.

Een tweede argument voor risico-aansprakelijkheid is de eis van rechtszekerheid. Toepassing van het criterium van wetenschap is in hoge mate subjectief; aansprakelijkheid is in concreto moci-

88. Vgl. F.J. Dommering, Internet: een juridische plaatsbepaling van een nieuw communicatieproces, in: M.F. Gelok en W.M. de Jong (red.), *Volatilisering in de Economie*, Wetenschappelijke Raad voor het Regeringsbeleid, Vg8, Den Haag: SDU Uitgevers 1997, p. 146.

89. Mon. Nieuw BW B-45 (Jansen), p. 11.

90. Asser-Hartkamp III, nr. 91-92; Mon. Nieuw BW B-45 (Jansen), p. 12 en p. 36.

lijk te voorspellen. Dit argument werkt overigens ook in omgekeerde richting; een wettelijke exoneration biedt evenzeer rechtszekerheid.

Een belangrijk argument contra risico-aansprakelijkheid is gelegen in de informatievrijheid die door art. 10 EVRM wordt gewaarborgd. Op deze vrijheid kunnen Internet-providers zich ongetwijfeld beroepen.⁹¹ Indirect speelt ook de uitingsvrijheid van de informatieveranciers een rol. Risico-aansprakelijkheid dwingt de provider tot inhoudelijke bemoeienis en het nemen van preventieve voorzorgsmaatregelen. Dat hiervan een *chilling effect* op de uitingsvrijheid via het Internet zal uitgaan, behoeft geen betoog. Providers zullen voortaan alleen met 'nette' informatie-aanbieders in zee gaan.

Rechthebbenden stellen zich op het standpunt dat uit auteursrechtelijke aansprakelijkheid geen bloed vloeit. Het verbodsrecht van de rechthebbenden zal zich, zoals in de analoge praktijk gebruikelijk, oplossen in een vergoedingsaanspraak. De providers betalen een paar centen royalties aan de rechthebbenden, en berekenen deze door aan hun abonnees. Daarmee komen de rechthebbenden aan hun trekken, en blijft de informatievrijheid gesauveerd.

Dit argument overtuigt niet. Zoals hiervoor (p. 216-217) geschetst, ontbreekt voor een dergelijke collectieve oplossing de contractuele infrastructuur. Rechthebbenden zijn er tot op heden niet in geslaagd voor het gebruik van beschermde werken op het Internet collectieve licenties aan te bieden, die de licentienemer enige vorm van zekerheid verschaffen. Anders dan zijn 'analoge' collega de kabelexploitant is de service provider niet in staat zich contractueel tegen auteursrechtelijke claims in te dekken. Mede in dit licht bezien, zou invoering van risico-aansprakelijkheid een disproportionele maatregel zijn.

91. A.W. Hins, Gedachten en gevoelens over de elektronische snelweg, in: Communicatie- en informatievrijheid in het digitale tijdperk, Publikaties van de Staatsrechtkring nr. 11, Zwolle: Tjeenk Willink 1995, p. 35, onder verwijzing naar EHRM 22 mei 1990, Publ. ECIR, Series A, Vol. 178 (Autronic).

Horizontale oplossing

De aansprakelijkheid van Internet-providers is ook buiten het terrein van het auteursrecht een 'hot issue'. In het concept-wetsvoorstel Computercriminaliteit II wordt voorgesteld de (voor uitgevers en drukkers geschreven) 'cascaderegels' van art. 53 en 54 Sr zodanig te verruimen dat ook Internet-providers en andere 'tussenpersonen' van deze vervolgingsuitsluitingsgrond kunnen profiteren.⁹² De provider zou aan aansprakelijkheid kunnen ontsnappen door zich bekend te maken, de dader aan te wijzen en verdere verspreiding van de uiting te voorkomen.

Het voorstel biedt ook voor civielrechtelijke verhoudingen een interessant model. Door de getrapte aansprakelijkheid wordt de service provider gestimuleerd in zijn contracten met informaticaleveranciers verplichtingen over (het opheffen van) anonimiteit en (het verwijderen van) inbreukmakend materiaal op te nemen. Onder een civielrechtelijke cascaderegels zullen gelaedeerden altijd over een verhaalsmogelijkheid beschikken. Anders dan onder het huidige recht zullen zij echter niet langer de keuze hebben tussen de 'deep pocket' van de provider en de smalle beurs van de kleine inbreukmaker.⁹³

Ook uit een oogpunt van rechtszekerheid en -transparantie lijkt het zinvol op zoek te gaan naar een *horizontale* aansprakelijkheidsregel, die voor alle rechtsgebieden gelijke gelding heeft. Een horizontale benadering zou goed aansluiten bij het Scienology-vonnis; de door de President ontwikkelde aansprakelijkheidsmaatstaf geldt voor alle (civielrechtelijk) onrechtmatige uitingen.

Het Duitse *Informations- und Kommunikationsdienste-Gesetz*,⁹⁴ dat

92. Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met nieuwe ontwikkelingen in de informatietechnologie, concept-wetsvoorstel 10 november 1997; A.W. Hins, a.w., p. 52-54; Theo de Roos, Gerard Schuijt en Louisa Wissink, Smaad, laster, discriminatie en porno op het Internet, ITeR-reeks nr. 3, Alphen aan de Rijn: Samsom 1996, p. 154 e.v.

93. Hins, a.w., p. 57.

94. BT-Drucksache 13/7934, <http://www.iid.de/rahmen/iukdgbt.html>.

op 1 augustus 1997 in werking is getreden, bevat in art. 1 (het *Teledienstegesetz*) een voorbeeld van een horizontale wettelijke regeling.⁹⁵ De wet geldt als *lex specialis* voor alle vormen van civiel- of strafrechtelijke aansprakelijkheid.⁹⁶ Informatieleveranciers zijn voor 'eigen inhoud' normaal aansprakelijk. Service providers kunnen voor 'vreemde inhoud' alleen aansprakelijk worden gesteld als zij daarvan kennis dragen en redelijkerwijs technisch in staat zijn verder gebruik te verhinderen. Access providers zijn nimmer aansprakelijk, ook niet voor gevallen van 'proxy-caching'. De nieuwe wet laat blokkeringsverplichtingen voortvloeiend uit het gemeene recht, voorzover deze technisch uitvoerbaar zijn, onverlet.

Het recente voorstel voor een Europese Auteursrechtrichtlijn bevat geen regels over de aansprakelijkheid van intermediairs. In de Toelichting wordt een afzonderlijke richtlijn, waarin deze kwestie horizontaal – naast andere aspecten van 'electronic commerce' – geregeld wordt, in het vooruitzicht gesteld. Ongetwijfeld zal de Duitse wet daarbij als inspiratiebron dienen.

Voor de praktijk heeft een horizontale regel ongetwijfeld voordelen; gelaedeerden en providers weten ongeveer waar zij aan toe zijn. De bestaande divergentie tussen de verschillende aansprakelijkheidsregimes heeft merkwaardige consequenties. Om aan auteursrechtelijke aansprakelijkheid te ontsnappen, zal de provider geneigd zijn 'verdachte' web sites te controleren en af te sluiten. Door dergelijke inhoudelijke bemoeienissen wordt de provider, geheel in strijd met zijn gedroomde rol van common carrier, gaandeweg in de rol van uitgever gedwongen, waardoor hij ook voor anderszins onrechtmatige uitingen aansprakelijk zal zijn.⁹⁷

95. De wet creëert geen uniforme maatstaf van aansprakelijkheid, maar een horizontale wettelijke exoneratie. Van civiel-, straf- of bestuursrechtelijke aansprakelijkheid kan in een concreet geval eerst sprake zijn als het 'filter' van het *Teledienstegesetz* gepasseerd is; S. Engel-Flehsig, *Das neue Informations- und Kommunikationsdienstes-Gesetz*, NJW 1997-45, p. 2984.

96. F.W. Bulst, *Hear No Evil, See No Evil, Answer for No Evil: Internet Service Providers and Intellectual Property – The New German Teleservices Act*, EIPR 1997-13, p. 33.

97. Vgl. de Amerikaanse *Prodigy*-zaak, beschreven door Q.R. Kroes, *Internet, aansprakelijkheid in het Amerikaanse recht*, Computerrecht 1996-1, p. 7.

Nadeel is dat een horizontale benadering weinig recht doet aan het verschil in rechtsgrond van de betrokken regimes. Aansprakelijkheid voor onrechtmatige uitingen heeft, mede onder invloed van de uitingsvrijheid, een sterk culpoos karakter. In gevallen van auteursrechtinbreuk speelt het risico-element een grotere rol. Het is in dit licht bezien de vraag of het verstandig is al deze regimes over één aansprakelijkheidskam te scheren.⁹⁸

In elk geval dienen technologiespecifieke oplossingen te worden voorkomen. Door de voortgaande convergentie van telecommunicatie-, informatic- en omroepdiensten zal de rol van de Internet service provider in de toekomst met die van de kabelexploitant, omroepinstelling en elektronische uitgever vervloeien. Eventuele wetgeving zal daarom niet te nauw mogen aansluiten bij de huidige stand van de techniek. De door het concept-wetsvoorstel Computercriminaliteit II geïntroduceerde, technologieneutrale 'tussenpersoon'⁹⁹ is een novum dat navolging verdient.

V. ALTERNATIEVEN VOOR HET AUTEURSRECHT

Gedreven door twijfels over de effectiviteit van het auteursrecht in een digitale omgeving zijn rechthebbenden op zoek gegaan naar alternatieve beschermingsregimes of strategieën. In dit hoofdstuk zal een tweetal substituten voor auteursrechtelijke bescherming worden beschreven: het overeenkomstenrecht (§ V.1) en technische maatregelen, inclusief de daarbij behorende juridische bescherming (§ V.2). Vooral de combinatie van beide instrumenten belooft in de toekomst een serieuze en vervaarlijke concurrent van het auteursrecht te worden (§ V.3).

98. Instituut voor Informatierecht, *Liability for On-line Intermediaries*, Amsterdam: Instituut voor Informatierecht 1997, p. 82-83.

99. Art. 53 lid 2 van het concept-wetsvoorstel Computercriminaliteit II definieert deze 'tussenpersoon' als volgt: 'een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in gesproken woord, beeld of geschrift afkomstig van derden ...'.

V.1 Overeenkomstenrecht

Het overeenkomstenrecht is in veel opzichten een volwaardig alternatief voor auteursrechtelijke bescherming op het Internet. De structuur van het net maakt het mogelijk dat informatieproducenten rechtstreeks of door tussenkomst van intermediairs een veelheid van contractuele relaties aangaan en onderhouden met hun eindgebruikers. Sterker: het Internet (en het World Wide Web in het bijzonder) is daarvoor geknipt. De 'textuele' context en het interactieve karakter van het medium zijn ideale randvoorwaarden voor het ontstaan van een contractuele cultuur.¹⁰⁰

Het contractenrecht lijkt het instrument bij uitstek om het rechtsvacuüm waarin het Internet zich thans bevindt, te vullen. Informatieproducenten, intermediairs en eindgebruikers kunnen zonder inmenging van de alom gevreesde overheden hun eigen regels kiezen, en daarmee naar hartelust experimenteren. Idealiter kunnen uit deze zich ontwikkelende contractuele praktijk nieuwe rechtsnormen ontstaan die op de nieuwe omgeving van het net beter zijn toegesneden.

Contractuele zelfregulering oogt aantrekkelijk, maar heeft een keerzijde. Anders dan de mythe van het Internet het wil, is cyberspace geen egalitaire samenleving met gelijke kansen voor iedere 'netizen'. In een wereld die geheel door contracten wordt geregeerd, delven zwakkere partijen het onderspit en komen fundamentele vrijheden in het gedrang.

Buiten het Internet zijn rechtstreekse contractuele relaties tussen informatieproducent en -consument betrekkelijk uitzonderlijk. De koper van een boek contracteert niet met de auteur of uitgever. Wie een CD aanschaft, doet met de platenmaatschappij of musicus geen zaken. Een uitzondering vormt de afnemer van computersoftware, die zich door middel van zogeheten *gebruikslicenties* dikwijls rechtstreeks aan de software-

100. Robert P. Merges, The End of Friction? Property Rights and Contract in the 'Newtonian' World of On-Line Commerce, Berkeley Technology Law Journal (12) 1997-1, p. 118.

producent gebonden weet. Ook kopers van CD-ROMs worden in toenemende mate met dergelijke (standaard)contracten geconfronteerd.

De opmars van de gebruikslicentie staat in direct verband met de (in hoofdstuk II beschreven) uitdijning van het reproductierecht. Waren gebruikshandelingen in het papieren tijdperk vrij van auteursrechtelijke aanspraken, in een digitale omgeving valt ieder gebruik in beginsel onder het verbodsrecht van de rechthebbende. Dit verbodsrecht vormt de grondslag van de gebruikslicentie.

Gebruikslicenties zijn, evenals de 'garanties' die fabrikanten van huishoudelijke elektronica zo graag hanteren, veelal eufemismen voor hun tegendeel. Gebruikslicenties staan in de praktijk (anders dan het 'licere' suggereert) de arme consument bijzonder weinig toe. De software mag gebruikt worden (gelukkig maar!), maar meer zit er voor de gebruiker niet in. Het programma mag maar op één machine tegelijk worden gebruikt; behalve een enkele reservekopie mogen geen kopieën worden gemaakt; de software mag niet worden uitgeleend of doorverkocht; enzovoorts.

Naar verwachting zal de gebruikslicentie op het gecommercialiseerde Internet van de nabije toekomst eerder regel dan uitzondering zijn. Wie regelmatig over het net surft, stuit nu reeds bij tijd en wijle op allerhande 'click-through' of 'mouse-click' contracten. Over enkele jaren zullen de meeste reguliere informatieproducten via het Internet gelicentieerd worden: kranten, tijdschriften, boeken, muziek, computersoftware, enzovoorts. De relatie tussen informatieproducent en -consument zal aldus in toenemende mate door het contractenrecht worden beheerst. De technische maatregelen die in § V.2 worden besproken, zullen in dat proces een belangrijke rol spelen. Zonder acceptatie van de licentievoorwaarden zal het informatieproduct, dat de consument op het net wordt aangeboden, achter een ondoordringbare encryptielaag verborgen blijven.

Over de rechtsgeldigheid van dergelijke contracten gaat dit preadvies niet. Uiteraard zijn daarbij, mede in het licht van Afde-

ling 6.5.3 BW (Algemene voorwaarden), vraagtekens te plaatsen.¹⁰¹ In de zaak *Coss/IM Data* achtte de Amsterdamse rechtbank de koper van computersoftware niet gebonden aan de bepalingen van de gebruikslicentie die zich in de cellofaanverpakking van het programma bevond, een zogenaamde *shrinkwrap*- of krimpfolielicentie.¹⁰² Terecht oordeelde de Rechtbank dat het enkele openen van de verpakking geen licentie-overeenkomst tussen de producent van het programma en de gebruiker deed ontstaan.

Ervan uitgaande dat via het Internet afgesloten (licentie)contracten in beginsel gewoon geldig zijn, rijst de vraag in hoeverre de wettelijke beperkingen van het auteursrecht daardoor genegeerd kunnen worden. Staat het de producent vrij de gebruiker contractueel aan gebruiks- en kopieerbeperkingen te onderwerpen die verder gaan dan de Auteurswet voorschrijft? Mag, bijvoorbeeld, in een gebruikslicentie de consument worden verboden een werk voor eigen gebruik te kopiëren (art. 16b Aw), te citeren (art. 15a Aw) of voor educatieve doeleinden te 'readeren' (art. 16 Aw)? Vragen die steeds belangrijker zullen worden naarmate het aanbod aan licentievrije informaticaproducten zal afnemen.

Uit het *Leesportefeuille-arrest* uit 1952¹⁰³ zou met enige goede wil een aanwijzing voor een antwoord gelezen kunnen worden. Spaarnestad, uitgever van onder meer *Libelle* en *Panorama*, had op de voorpagina van haar bladen de volgende clausule afgedrukt:

'dat de uitgeefster dit tijdschrift slechts ter beschikking stelt onder de uitdrukkelijke voorwaarde, dat iedere verkrijger door het enkele feit van zijn verkrijging jegens haar (...) de verplichting op zich neemt het tijdschrift niet ter beschikking te stellen of te doen stellen van een leesportefeuille ...'

101. J.E.J. Prins, *Contracting in an On-line Marketplace*, in: V. Bekkers e.a. (eds.), *Emerging Electronic Highways*, Den Haag: Kluwer Law International 1996, p. 144-148.

102. Rb Amsterdam 24 mei 1995, *Computerrecht* 1997-2, p. 63; zie K.J. Koelman, *Multimedialicenties, enkele juridische en praktische knelpunten*, ITeR-reeks nr. 10, Alphen aan den Rijn: Samsom 1998, § 4.2.

103. HR 23 januari 1952, NJ 1952, 95.

Kon deze clause de uitputting van het verspreidingsrecht voorkomen? De Hoge Raad meende van niet en oordeelde dat het beding 'het beoogde gevolg niet kon brengen, daar de Spaarne-stad niet aan zich kon houden een recht, dat haar, nadat de uitgaven in druk waren verschenen, niet toekwam'.¹⁰⁴

Zijn de wettelijke beperkingen van het auteursrecht van regerend of dwingend recht? Deze vraag heeft in de Verenigde Staten, vooral in de context van het Internet, inmiddels tot uitgebreide literatuur¹⁰⁵, rechtspraak¹⁰⁶ en zelfs wetgevendende initiatieven¹⁰⁷ geleid. De discussie staat daar vooral in het teken van het constitutionele leerstuk van de 'preemption'; het statelijke contractenrecht mag het federale auteursrecht niet ondermijnen.

In Nederland is de discussie eerst recent op gang gekomen.¹⁰⁸ De wettelijke beperking van het auteursrecht blijkt zich in een complex krachtenveld te bevinden. Het beginsel van de contractsvrijheid in combinatie met het 'eigendomsrechtelijke' karakter van het auteursrecht biedt op het eerste gezicht alle ruimte voor contractuele beperkingen die verder gaan.¹⁰⁹ Het grondrechtelijke karakter van diverse wettelijke beperkingen wijst daarentegen in omgekeerde richting; zie p. 210 *supra*.

104. In gelijke zin HR 20 november 1987, NJ 1988, 280 (Stemra/Free Record Shop).

105. Jerome H. Reichman, *Electronic Information Tools – The Outer Edge of World Intellectual Property Law*, IIC (24) 1993, p. 462; Paul Goldstein, *Summary of Discussion*, in: P. Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment*, Den Haag: Kluwer Law International 1996, p. 245-246; Maureen A. O'Rourke, *Copyright Preemption After the ProCD Case: A Market-Based Approach*, Berkeley Technology Law Journal (12) 1997-1, p. 53; Niva Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, Berkeley Technology Law Journal (12) 1997-1, p. 93.

106. *ProCD v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

107. *Digital Era Copyright Enhancement Act*, H.R. 3048; het voorstel verklaart ongeldig bepalingen in een standaard-licentieovereenkomst die (a) betrekking hebben op onbeschermde informatie of (b) bestaande wettelijke beperkingen inperken.

108. Instituut voor Informatierecht (J. Guibault), *Contracts and Copyright Exemptions*, Amsterdam: Instituut voor Informatierecht 1997.

109. P.C. van Schelven en H. Struik, *Software-recht*, Deventer: Kluwer 1995, p. 121.

Dat de grondrechten rechtstreeks, indirect of gehuld in het kleed van de algemene rechtsbeginselen kunnen doorwerken in (horizontale) contractuele rechtsverhoudingen is inmiddels algemeen aanvaard.¹¹⁰ Voor horizontale werking lijkt des te meer alle aanleiding te bestaan, nu het hier gaat om contractuele relaties tussen partijen waarvan er één, de producent/rechthebbende, welhaast per definitie een machtspositie inneemt.¹¹¹ Deze machtspositie manifesteert zich onder meer in het gebruik van standaard-adhesiecontracten.¹¹²

Ook vanuit een oogpunt van consumentenbescherming zijn er goede gronden aan de partijautonomie paal en perk te stellen. Het BW bevat een uitvoerige regeling van de koopovereenkomst, die ten aanzien van de consumentenkoop grotendeels van dwingend recht is (art. 7:6 BW). De beperkte omschrijving van 'koop' (art. 7:1 BW) c.q. 'consumentenkoop' (art. 7:5 BW) laat echter niet toe deze regeling zonder meer toe te passen op de 'koop' van informatie anders dan op fysieke dragers, bijvoorbeeld via het Internet. Elektronisch afgenomen informatiediensten vallen buiten de definitie; het verdient aanbeveling het BW op dit punt aan te passen.¹¹³

Tenslotte kan het nationale of Europese mededingingsrecht een licentie eveneens op losse schroeven zetten.¹¹⁴ De machtspositie die ieder recht van intellectuele eigendom in feite schept, maakt

110. A.G. Maris en J.M. Polak, *Handelingen NJV 1969-I*; A.K. Kockkoek, *De betekenis van grondrechten voor het privaatrecht*, WPNR 1985, nr. 5742, p. 385.

111. E.J. Dommering, *Algemene belangen in het burgerlijk recht*, Mon. Nieuw BW A-7, Deventer: Kluwer 1982, p. 17-20.

112. Zie echter J.E.J. Prins, *Contracting in an On-line Marketplace*, in: V. Bekkers e.a. (eds.), *Emerging Electronic Highways*, Den Haag: Kluwer Law International 1996, p. 148 (in een netwerkomgeving zullen contracten 'op maat' voor adhesiecontracten in de plaats komen).

113. C.J. Sander, *De consument op de elektronische snelweg: een inleiding naar Nederlands en Duits recht*, *Tijdschrift voor Consumentenrecht* 1997-3, p. 195.

114. Per 1 januari 1998 is ook in zuiver nationale verhoudingen een beroep op het mededingingsrecht ten overstaan van de gewone rechter mogelijk; Wet van 22 mei 1997, houdende nieuwe regels omtrent de economische mededinging (*Mededingingswet*), Stb. 1997, 242.

dat het opleggen van gebruiksbeperkingen die verder gaan dan het uitsluitend recht mededingingsrechtelijk riskant is.¹¹⁵

In de huidige Auteurswet valt niet te lezen of bestaande wettelijke beperkingen van reglend of dwingend recht zijn. In het arrest *Dior-Evora* heeft de Hoge Raad overwogen dat de wettelijke beperkingen in het algemeen belang gecodificeerd zijn.¹¹⁶ Of daarmee ook bedoeld is dat zij – op straffe van strijd met de wet of de openbare orde (art. 3:40 BW) – nimmer contractueel opzij mogen worden gezet, is echter de vraag.¹¹⁷

Aan de Europese wetgever komt de eer toe de eerste uitdrukkelijk dwingendrechtelijke beperkingen te hebben gecodificeerd. De Softwarerichtlijn van 1991 bevat er een viertal. Op grond van art. 5 lid 2 kan 'het maken van een reservekopie door een rechtmatige gebruiker van het programma (...) niet bij overeenkomst worden verhinderd ...' Ook het 'observeren' (bestuderen) van de werking van een programma mag contractueel niet worden uitgesloten (art. 9 lid 1 jo. art. 5 lid 3). Blijkens Overweging 17 van de considerans geldt dat ook voor het 'runnen' van het programma en het corrigeren van fouten (art. 5 lid 1). Van dwingend recht zijn eveneens de hoogst ingewikkelde decompilatiebepalingen (art. 9 lid 1 jo. art. 6).

Over de rechtsgrond van deze beperkingen is verschil van mening mogelijk. De decompilatieregels zijn sterk mededingingsrechtelijk gekleurd; de overige bepalingen lijken (mede) te zijn ingegeven door overwegingen van consumentenbescherming. De informatievrijheid heeft bij de Softwarerichtlijn, gezien de aard van het product, nauwelijks een rol gespeeld. Bij de Databankrichtlijn, die van een aanzienlijk wijdere strekking is, lijkt dat wel het geval te zijn geweest. Ook deze richtlijn bevat enkele beperkingen van dwingend recht (art. 15): de rechtmatige gebruiker mag normale gebruikshandelingen verrichten (art. 6 lid

115. Vgl. Verordening (EC) nr. 240/96, Pb EG 1996 I. 31/2 (Vrijstellingsverordening Technologielicenties), waarover H.W. Wefers Bettink, NTER 1996-5, p. 103.

116. HR 20 oktober 1996, Informatierecht/AMI 1996-3, p. 43.

117. K.J. Koelman, *Multimedialicenties, enkele juridische en praktische knelpunten*. ITeR-reeks nr. 10, Alphen aan den Rijn: Samsom 1998, § 4.3.

1); hergebruik van niet-substantiële gedeelten van een databank is toegelaten (art. 8).

Hoewel de bewoordingen van de Softwarerichtlijn over het dwingendrechtelijk karakter van deze bepalingen geen misverstand laten bestaan, heeft de Nederlandse wetgever bij de implementatie nagelaten de Richtlijn op dit punt te volgen. Bij de totstandkoming van de implementatiewet stelde de staatssecretaris van Justitie zich op het standpunt dat uitwerking in de wet niet nodig was, omdat reeds op grond van de 'algemene regels van het vermogensrecht' afwijking bij contractueel beding nietig zou zijn.¹¹⁸ Kennelijk ging de staatssecretaris er van uit dat de beperkingen van het auteursrecht in beginsel (op grond van art. 3:40 BW?) dwingendrechtelijk van aard zijn.¹¹⁹

Geconcludeerd kan worden dat reeds naar huidig recht de licentievrijheid van de rechthebbende niet onbeperkt is. Wettelijke beperkingen die hun rechtsgrond hebben in constitutionele vrijheden mogen mijns inziens in een licentie-overeenkomst niet zomaar opzij worden gezet; voor beperkingen op mededingings- of consumentenrechtelijke grondslag geldt mogelijk hetzelfde.

Deze conclusie roept opnieuw de vraag op wat de rechtsgronden van de wettelijke beperkingen nu eigenlijk zijn¹²⁰; zie p. 210-211 *supra*. Om discussies hierover te vermijden verdient het aanbeveling het dwingendrechtelijke karakter van de beperkingen die deze status in elk geval verdienen (art. 15 en 15a Aw, alsmede de privé-kopie van art. 16b) in de wet vast te leggen. Op termijn zal de wetgever wellicht nog een stap verder moeten gaan. Het (contracten)recht zal ook buiten de context van het auteursrecht dwingendrechtelijke waarborgen moeten bieden aan de informatieconsument, bijvoorbeeld in de vorm van onvervreemdbare gebruiksrechten.¹²¹

118. Kamerstukken TK 1991-1992, 22 531, nr. 3, p. 7 en nr. 5, p. 17-18.

119. Zie de kritiek op dit standpunt bij D.W.F. Verkade, Computerprogramma's in de Auteurswet: het vierde regime, Computerrecht 1992-3, p. 95 l.k.; en Van Schelven/Struik, a.w. (noot 109), p. 122.

120. Guibault, a.w. (noot 108), p. 24-28.

121. Elkin-Koren, a.w. (noot 105), p. 105-106.

Geheel zonder precedent zou een dergelijke regeling niet zijn. In tal van landen, waaronder Frankrijk, België en Duitsland, bestaat sinds jaar en dag een wettelijke regeling van de uitgeefovereenkomst. 'Zwakke' auteurs worden tegen 'sterke' uitgevers, ten dele met dwingendrechtelijke bepalingen, in bescherming genomen.¹²² Daarvoor worden argumenten gehanteerd die ook aan het consumentenrecht ten grondslag liggen.¹²³ Alle reden dus om ook de informatieconsument een wettelijke hand toe te steken.¹²⁴

V.2 Technische mautregelen

Dat de handhaving van het auteursrecht op het Internet geen sinecure is, moge inmiddels wel duidelijk zijn. Het wereldomspannende kopieerapparaat roept handhavingsproblemen op van duizelingwekkende proporties. Zolang deze problemen niet zijn opgelost, verbaast het niet dat veel producenten ervoor terugschrikken hun werken elektronisch aan te bieden. De relatieve schraalheid van het huidige informatie-aanbod op het Internet is hiermee ten dele verklaard.

Overigens is het *opsporen* van inbreuk, vergeleken met de analoge wereld, een peulenschil. Met behulp van de geavanceerde zoekmachines die op het World Wide Web gratis beschikbaar zijn (Alta Vista, Excite, Yahoo!, enz.) zijn inbreukmakende sites in een oogwenk te vinden. Daarnaast maken sommige rechthebbenden gebruik van gespecialiseerde zoekprogramma's, zogeheten 'web crawlers', om piraten volautomatisch op te sporen.¹²⁵

122. Reichman, a.w. (noot 105), p. 467.

123. N. Knittler, Die Wertungsgrundsätze des Konsumentenschutzgesetzes und ihre sinngemässe Anwendung auf das Urhebervertragsrecht, in: R. Dittich, Urhebervertragsrecht. Stand – Entwicklung, Wenen: Manz 1986, p. 46.

124. Het is in dit verband betreurenswaardig dat de Consumentenbond zich uitsluitend voor de consument van materiële goederen lijkt in te zetten. Is het de Bond ontgaan dat wij inmiddels ruimschoots het informatietijdperk zijn binnengetreden?

125. Copyright owners learning to police online sales, performance of musical works, BNA Electronic Information Policy and Law Report (3) 1998-1, p. 4.

Wat te doen als bestaande wettelijke instrumenten ontbreken of onvoldoende functioneren om eigendomsaanspraken te beschermen? Mackaay geeft het antwoord: 'build your own fence!'¹²⁶ Zoals in het Wilde Westen (een populaire Internet-metafoor) eigendomsrechten door palen en prikkeldraad werden gevestigd, zo kunnen in cyberspace door het optrekken van digitale hekwerken uiteindelijk nieuwe 'property rights' ontstaan.

Het digitale prikkeldraad heet *encryptie*: het versleutelen van informatie. Door toepassing van encryptie kunnen commerciële informatieleveranciers voorkomen dat ongeautoriseerde (niet-betalende) gebruikers toegang krijgen tot een informatiedienst of -product. Alleen wie over de juiste sleutel beschikt, kan over de informatie(dienst) beschikken.

Naast encryptie staat een heel scala aan technische beschermingsmaatregelen ter beschikking van de informatie-exploitant of -producent die zijn aanbod wil beveiligen: het gebruik van wachtwoorden en andere login-procedures, combinaties van hardware en software, antikopieerprogrammatuur, elektronische 'watermerken', enzovoorts. Al deze technieken culminerend in het *Electronic Copyright Management System* (ECMS), een volautomatisch systeem van beveiligde distributie, rechtenbeheer, controle en afrekening. Met dergelijke systemen wordt thans op diverse fronten geëxperimenteerd, o.a. in het kader van het Europese ESPRIT-project IMPRIMATUR.¹²⁷

Zelfs al ligt volgens sommigen het antwoord op machine in de machine¹²⁸, het toepassen van technische beschermingsmaatregelen gebeurt in de praktijk nog niet op grote schaal. Wie op het World Wide Web rondkijkt, stuit maar zelden op een gesloten deur. Voorlopig zijn het vooral de aanbieders van digitale *sex* die van wachtwoorden en/of encryptie gebruik maken. Selectieve

126. E. Mackaay, *The Economics of Emergent Property Rights on the Internet*, in: P. Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment*, Den Haag: Kluwer Law International, p. 20.

127. Zie <http://www.imprimatur.alcs.co.uk>.

128. Ch. Clark, *The Answer to the Machine is in the Machine*, in: P. Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment*, Den Haag: Kluwer Law International, p. 139.

toegang past ook slecht bij de open-deurcultuur die voor het Internet tot op heden zo kenmerkend is geweest. Met de verwachte commercialisering van het net zullen gebruikers echter in toenemende mate met digitale wegversperringen te maken krijgen.

Technische maatregelen zullen veelal in combinatie met contractuele middelen worden toegepast. De technische maatregel vormt het begin- en eindpunt van de contractuele relatie tussen producent en eindgebruiker. Wie geen contractpartij (meer) is, wordt af- of uitgesloten.

Diverse functies

Technische maatregelen kunnen verschillende functies vervullen. Bekend uit de 'analoge' wereld zijn de *conditional access* (voorwaardelijke toegang) systemen. Deze dienen ertoe de toegang tot een informatiedienst te controleren; de abonnees van Filmnet/Canal+ en de gebruikers van de online databank van Kluwer Datalex zijn hiermee inmiddels vertrouwd.

Een tweede categorie vormen de maatregelen die ongeoorloofd reproduceren en (verder) gebruik van informatieproducten aan banden leggen. Bekend uit de jaren '80 zijn de *kopieersloten* waarmee sommige softwareproducenten hun programma's trachtten te beveiligen. Voor 'hackers' vormde het kraken van deze sloten een ware sport. Reguliere gebruikers voelden zich echter bekocht; reservekopieën moesten worden nabesteld, de software kon niet op een andere PC worden geïnstalleerd. Beveiligde computersoftware is inmiddels vrijwel uit de schappen van de computerwinkels verdwenen. Een voorbeeld uit de jaren '90 is de antikopieer-chip die in sommige digitale audiorecorders wordt ingebouwd. De chip voorkomt het maken van 'seriële' (meer dan één) kopieën.¹²⁹ Ook de digitale audiorecorder is inmiddels 'geflopt'.

¹²⁹ In de Verenigde Staten zijn fabrikanten van digitale audiorecorders op grond van de *Audio Home Recording Act* (1992) wettelijk verplicht tot toepassing van dergelijke chips.

Een derde categorie maatregelen dient ertoe auteursrechtelijk beschermde werken te identificeren en de rechthebbenden te traceren. Een werk wordt voorzien van een moeilijk te verwijderen digitale code, die informatie verschaft over de identiteit en het adres van de maker of rechthebbende, het land van oorsprong van het werk, het jaar van eerste publicatie, enzovoorts. Een vergelijkbare code wordt in de wereld van het gedrukte boek al jaren toegepast: het ISBN. Het digitale equivalent, waarover uitgevers recent overeenstemming hebben bereikt, heet 'Digital Object Identifier' (DOI).¹³⁰ Dergelijke codes vormen een onmisbare schakel in ieder electronic copyright management system. Zowel in het WIPO-verdrag (art. 12) als in het richtlijnvoorstel (art. 7) worden maatregelen tegen het verwijderen van deze 'rights management information' in het vooruitzicht gesteld.¹³¹

Tot de vierde categorie behoren maatregelen die de *authenticiteit* van de getransporteerde informatie waarborgen. Elektronische documenten worden voorzien van een 'digitale handtekening', 'vingerafdruk' of 'watermerk'. Alleen gewaarmerkte informatie is authentiek.

Het nieuwe regime: bescherming van technische bescherming

Technische beschermingsmaatregelen vormen met dat al een belangrijke uitbreiding van het auteursrechtelijke wapenarsenaal. Bovenop de auteursrechtelijke beschermingslaag fungeren de technische maatregelen als een extra pantser. Voor rechthebbenden schijnt deze tweede laag echter nog niet genoeg te zijn. Een derde laag is inmiddels in de maak: de *juridische* bescherming van technische bescherming van auteursrechtelijk beschermde werken.

Op grond van art. 11 van het WIPO-Auteursrechtverdrag zijn de verdragstaten verplicht '(to) provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connec-

130. <http://www.doi.org>.

131. P.B. Hugenholtz, De WIPO-Verdragen: ongeregeld goed, Informatierecht/AMI 1997-4, p. 80.

tion with the exercise of their rights (...) and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.¹³² In het voorstel voor een Auteursrechtlijn van de Europese Commissie, dat ten dele strekt tot implementatie van het WIPO-Verdrag, komt eveneens een anti-kraakbepaling voor. Deze gaat echter aanzienlijk verder dan de WIPO-bepaling; niet alleen het 'kraken' zelf, maar ook het produceren en verhandelen van apparatuur die daarvoor geschikt is, vallen onder het richtlijnvoorstel.¹³³ De Software-richtlijn bevat een vroege voorloper van deze bepaling in art. 7 lid 1 onder c (art. 32a Auteurswet).

Dit nieuwe regime roept tal van vragen op. Vragen, allereerst, over de reikwijdte van het nieuwe recht. Richten de bepalingen zich alleen tegen handelingen die auteursrechtinbreuk faciliteren of reiken zij verder? Een complicatie vormt met name het stelsel van wettelijke beperkingen van het auteursrecht, dat kopiëren voor bepaalde 'goede doelen' uitdrukkelijk toelaat. Is het kraken van een kopieerbeveiliging in het kader van dergelijk legitiem gebruik toegestaan? De zinsnede 'permitted by law' aan het slot van de WIPO-bepaling suggereert van wel. Maar hoe te oordelen over het richtlijnvoorstel dat ook de productie en verhandeling van antikraakapparatuur verbiedt? Bedenk hierbij dat veel technisch beschermde informatie tot het publieke domein behoort, bijvoorbeeld wetsteksten en jurisprudentie.¹³⁴

132. Zie voor kritiek op eerdere voorstellen Thomas C. Vinje, *A Brave New World of Technical Protection Systems: Will There Be Room For Copyright?*, *EIPR* (19) 1996-8, p. 431; F.W. Grosheide, *Enkele kanttekeningen bij het WIPO Copyright Treaty 1996*, *Informatierecht/AMI* 1997-4, p. 78.

133. Art. 6 lid 1 van het richtlijnvoorstel luidt: 'Member States shall provide adequate legal protection against any activities, including manufacture or distribution of devices or the performance of services, which have only limited commercially significant purpose or use other than to circumvent and are carried out knowingly or with reasonable grounds to know that they will enable or facilitate without authority the circumvention of any effective technological measure designed to protect any copyright or any rights related to copyrights as provided by law or the sui generis rights provided for in Chapter III of Directive 95/9/EC.'

134. Vinje, a.w., p. 434: 'technical protection does not follow the contours of copyright'.

Als het kraken in het kader van legitieme kopieerhandelingen is toegestaan, kan het produceren van daartoe benodigde apparatuur mijns inziens moeilijk worden verboden. Juist omdat bestaande kopieerapparatuur, zoals fotokopieermachines, videorecorders en personal computers, niet alleen voor inbreukmakende doeleinden (kan) worden aangewend, maar ook voor 'substantial non-infringing uses'¹³⁵ geschikt is, is naar Nederlands recht de fabricage of verhandeling van dergelijke apparatuur nimmer onrechtmatig verklaard.¹³⁶

Het nieuwe regime roept, in de tweede plaats, vragen op ten aanzien van de proportionaliteit. Is er naast het arsenaal aan auteursrechtelijke en technische middelen waarover informatieproducenten thans kunnen beschikken nu werkelijk behoefte aan nog meer? De informatie-industrie is groot geworden met 'maar' één laag bescherming: het auteursrecht. *Drie lagen bescherming* (met de nog te implementeren Databank-richtlijn erbij zelfs *vier*) lijkt in dat licht bezien wat overdreven. Waar zijn de tijden gebleven dat het verlenen van rechten van intellectuele eigendom een goed gemotiveerde uitzondering op de regel van vrije mededinging was?¹³⁷

Van een aantoonbare behoefte is al helemaal geen sprake geweest.¹³⁸ In de praktijk wordt van technische beschermingsmaatregelen nog maar mondjesmaat gebruik gemaakt. Een nuchtere wetgever had eerst, zoals het hoort, de kat uit de boom gekeken. Uit rechtseconomisch oogpunt valt de haastige spoed waarmee het nieuwe regime tot stand is gekomen eveneens te betreuren. Volgens Mackaay mochten nieuwe 'fences' niet te snel door wettelijke maatregelen worden gevolgd; het rijpingsproces van nieuwe rechten in wording wordt erdoor verstoord.¹³⁹

135. De term is van het Amerikaanse Supreme Court in de Betamax-zaak, waarover P.B. Hugenholz, *Betamax: geen happy end voor Hollywood*, Auteursrecht/AMR 1984, p. 47.

136. Spoor/Verkade, p. 342; vgl. Gerbrandy, a.w. (noot 75), p. 328-329.

137. T. Koopmans, *Intellectuele eigendom, economie en politiek*, Informatierecht/AMI 1994-6, p. 107; in gelijke zin Laddie, *Copyright: Over-Strength, Over-Regulated, Over-Rated?*, EIPR 1996-5, p. 260: 'We should not be handing out monopolies like confetti while muttering "this won't hurt" '.

138. Vinje, a.w. (noot 132), p. 439.

139. Mackaay, a.w. (noot 126), p. 22.

Ook het rechtskarakter van het nieuwe regime roept vragen op. Opneming in het WIPO-Auteursrechtverdrag resp. het richtlijnvoorstel suggereert dat het auteursrechtelijk van aard is; de bewoordingen van beide bepalingen wijzen in dezelfde richting. Toch is gerede twijfel op zijn plaats. Technische maatregelen hebben lang niet altijd tot doel de bescherming van auteurs of auteursrechthebbenden veilig te stellen. Veel maatregelen dienen, integendeel, in de eerste plaats de belangen van de aanbieders van informatiediensten.¹⁴⁰ Zo geschiedt het coderen van een abonneetelevisiedienst niet primair ter bescherming van de rechten van de filmproducenten, maar om ongeautoriseerd gebruik van de *dienst* te verhinderen. De enigszins gekunstelde relatie met het auteursrechtelijke regime vormt een welkome legitiematie voor verbodsbepalingen en strafrechtelijke sancties.¹⁴¹ Door het nieuwe regime de jas van het auteursrecht aan te trekken kan het meeliften met de bestaande internationale instrumenten.

Het nieuwe regime valt daarenboven moeilijk te rijmen met een der belangrijkste rechtsgronden van het auteursrechtelijke systeem, het bevorderen van de spreiding van cultuur en kennis in de samenleving.¹⁴² Het auteursrecht beloont de auteur die zijn gedachtengoed uit (dat wil zeggen: in de openbaarheid brengt) met een uitsluitend recht van exploitatie. Het nieuwe regime heeft een omgekeerd effect. Het beloont het ontoegankelijk maken van informatie met een aanvullend recht, met behoud van auteursrechtelijke bescherming.¹⁴³

Voorwaardelijke toegang

Om de verwarring compleet te maken heeft de Europese Commissie in juli 1997 een voorstel ingediend voor een afzonderlijke

140. A. Lucas, Le droit d'auteur et protections techniques. Rapport Général, in: M. Dellebeke (ed.), Copyright in cyberspace, ALAI Study Days, Amsterdam, Amsterdam: Otto Cramwinckel 1997, p. 344.

141. Lucas, a.w., p. 352.

142. F.W. Grosheide, Auteursrecht op maat, Deventer: Kluwer 1986, p. 139-143.

143. Pamela Samuelson, Copyright, Digital Data, and Fair Use in Digital Networked Environments, in: Ejan Mackaay e.a. (eds.), The Electronic Superhighway, Den Haag: Kluwer Law International 1995, p. 126.

richtlijn 'betreffende de rechtsbescherming van diensten gebaseerd op, of bestaande uit, voorwaardelijke toegang'.¹⁴⁴ Hoewel het daaraan ten grondslag liggende Groenboek¹⁴⁵ alleen het oog had op de bescherming van geëncrypteerde televisiediensten, is het richtlijnvoorstel ook van toepassing op zogenoemde 'diensten van de informatiemaatschappij', een verschrikkelijke term waarmee diensten worden bedoeld 'die op individueel verzoek van de ontvanger van de dienst op afstand langs elektronische weg worden verricht' (aldus de considerans). Informatiediensten via het Internet vallen hier uiteraard ook onder.

Het richtlijnvoorstel richt zich tegen de productie, invoer, verhandeling en het bezit van 'illegale uitrusting', dat wil zeggen soft- of hardware die bedoeld is om ongeautoriseerde toegang tot een beschermde dienst te verschaffen. Anders dan de WIPO-bepaling en haar pendant in de voorgestelde Auteursrechtrichtlijn maakt het voor de toepassing van dit voorstel niet uit of de beschermde dienst auteursrechtelijk beschermd materiaal bevat.

Beide richtlijnvoorstellen laten de lidstaten vrij in de wijze waarop de rechtsbescherming gestalte krijgt. De wetgever heeft derhalve de keuze uit een strafrechtelijke of civielrechtelijke oplossing. Met betrekking tot het verhandelen van kraakmiddelen voor computerprogramma's heeft de Nederlandse wetgever gekozen voor een strafrechtelijke aanpak (art. 32a Auteurswet) ter implementatie van de Softwarerichtlijn. Uiteraard kan implementatiewetgeving achterwege blijven, indien zou blijken dat het bestaande recht reeds in voldoende mate bescherming biedt.

¹⁴⁴ Voorstel voor een richtlijn van het Europees Parlement en de raad betreffende de rechtsbescherming van diensten gebaseerd op, of bestaande uit, voorwaardelijke toegang, COM (97) 356 def, Pb EG C 314/7; hierover: H.M.H. Speyart, *Décodeurs de Dijon: een communautair beschermingsregime voor technische inhoudsbeveiliging*, NTER 1997-9, p. 190.

¹⁴⁵ Europese Commissie, Groenboek rechtsbescherming van geëncrypteerde diensten op de interne markt, COM(96) def. van 6 maart 1996.

Kraken naar Nederlands recht

Hiermee rijst de vraag hoe het kraken en verhandelen van kraakmiddelen zich verhouden tot het bestaande Nederlandse recht.¹⁴⁶ Is het verwijderen van een technische beschermingslaag van een informaticaproduct of -dienst jegens de producent of dienstverlener onrechtmatig? In de materiële wereld wordt het plaatsen van een hek niet onmiddellijk met een eigendomsaanspraak beloond. Het enkele feit dat ergens in het veld een hek staat, impliceert nog geen verbod over het hek te springen¹⁴⁷, laat staan erover heen te kijken.

Tegen bepaalde vormen van kraken biedt het strafrecht een remedie. De Wet op de Computercriminaliteit verklaart computervredebreuk tot een misdrijf (art. 138a Sr); het 'vernietigen' van gegevens opgeslagen in een computer is eveneens strafbaar (art. 350a-b Sr). Indien het kraken geschiedt door het aftappen van een versleuteld signaal biedt het verbod van art. 139c Sr tevens een strafrechtelijke grondslag. Tenslotte kan ook art. 441 Sr (doorgifte van een vertrouwelijk radiobericht) een rol spelen.

Het verwijderen van een encryptielaag rondom een informatieproduct 'in ruste' is echter naar huidig recht, behoudens bijkomende (bijvoorbeeld contractuele) omstandigheden, niet onrechtmatig, en zou dat naar mijn mening ook niet moeten worden.¹⁴⁸ Zoals het de eigenaar van een gesloten koffer is toegestaan deze desnoods met geweld te openen, zo staat het de eigenaar van een beveiligde CD-ROM vrij deze naar hartelust te kraken. Voorzover in dat proces (delen van) de CD-ROM tijdelijk worden gekopieerd, dient dat op grond van art. 16b Auteurswet te zijn toegelaten.

146. F.W. Grosheide, Copyright and Technical Protection Devices. Report on the Netherlands, in: M. Dellebeke (ed.), Copyright in cyberspace, ALAI Study Days, Amsterdam, Amsterdam: Otto Cramwinckel 1997, p. 400-411.

147. Geller, a.w. (noot 43).

148. In gelijke zin Julie E. Cohen, Some Reflections on Copyright Management Systems and Laws Designed to Protect Them, Berkeley Technology Law Journal (12) 1997-1, p. 178.

Over de (on)rechtmatigheid van de fabricage of verhandeling van kraakmiddelen bestaat grote onduidelijkheid. Het huidige auteursrecht biedt, afgezien van art. 32a Auteurswet, weinig soelaas. De civielrechtelijke omweg van het 'bevorderen van inbreuk' (zie p. 224 *supra*) biedt onder omstandigheden wellicht enig perspectief. Hierbij moet echter bedacht worden dat kraaken en kopiëren verschillende handelingen zijn, en dat het een niet noodzakelijk tot het ander leidt.

De jurisprudentie op basis van het recht van ongeoorloofde mededeling is verdeeld. In het arrest *Decca/Holland Nautic*¹⁴⁹ oordeelde de Hoge Raad de verhandeling door Holland Nautic van radio-ontvangers waarmee navigatiesignalen afkomstig van het Decca-systeem konden worden ontvangen jegens Decca niet onrechtmatig. Het enkel profiteren van het Decca-systeem kon door de beugel, nu Decca zich niet op enig recht van intellectuele eigendom kon beroepen. Voor aanvullende bescherming op grond van het gemene recht zou slechts ruimte bestaan indien de prestatie van Decca zodanig is 'dat zij op één lijn valt te stellen met die welke toekenning van een dergelijk recht rechtvaardigen'. Daarvan was naar het oordeel van de Hoge Raad geen sprake. Het risico van aanhaken was, gelet op het beginsel van vrijheid van handel en bedrijf, inherent aan de wijze waarop Decca haar bedrijf had ingericht.

In scherp contrast met het Decca-arrest staat de uitkomst van de zaak *Ten Electronics/Esselte*, die helaas niet tot de Hoge Raad is doorgezet. Het Amsterdamse Hof achtte de verkoop van decoders waarmee de abonneeprogramma's van Filmnet zonder toestemming konden worden genoten, jegens Esselte (destijds exploitant van FilmNet) wél onrechtmatig.¹⁵⁰ Volgens het Hof was de prestatie van Esselte als 'éénlijnsprestatie' aan te merken.

In de zaak *Groeneveld/TDS* kon de Hoge Raad wegens het ontbreken van een daartoe strekkend cassatiemiddel geen antwoord

149. HR 27 juni 1986, NJ 1987, 191.

150. Hof Amsterdam 2 mei 1991, Mediaforum 1991, p. B73; vgl. Pres. Rb Den Haag 20 januari 1986, KG 1986, 92 (Filmnet/Planken); Th.C.J.A. van Engelen, Prestatiebescherming en ongeschreven intellectuele eigendomsrechten (diss. Leiden), Zwolle: W.E.J. Tjeenk Willink 1994, p. 244.

geven op de vraag of de exploitant van een abonneetelevisiesysteem deze bescherming daadwerkelijk verdiende. Het gemak waarmee de Hoge Raad het beroep op de ontvangstvrijheid (art. 10 EVRM) verwierp, doet echter een bevestigend antwoord vermoeden.¹⁵¹

V.3 *Lex Informatica*

De combinatie van technische beschermingsmaatregelen en *on-line* licenties roept een duister toekomstbeeld op. Gaan wij toe naar een wereld waarin ieder gebruik van informatie volledig gedictieerd wordt door volautomatische systemen? Een wereld waarin ieder informaticaproduct zijn eigen licentievoorwaarden in de vorm van onuitwisbare computerprogramma's met zich meedraagt? Waarin wat mag en niet mag niet langer bepaald wordt door het recht, maar is *voorgeprogrammeerd*?

Zullen 'programmaregels' voor echt recht in de plaats komen? De ware technocraat ziet het liever vandaag dan morgen gebeuren. Zo zingt de Amerikaan Reidenberg de lof van de 'Lex Informatica' in alle toonaarden.¹⁵² Het informaticaregime biedt vele voordelen boven het recht van intellectuele eigendom en andere juridische instrumenten. Aantrekkelijk is vooral de volautomatische handhaving, die niet *ex post* maar onmiddellijk en automatisch plaatsvindt. Het programma dwingt de gebruiker zich aan de regels te houden: (goedkope en snelle) 'self-enforcement' in plaats van (dure en trage) handhaving in rechte. In de cynische woorden van Lessig: 'In the well implemented system, there is no civil disobedience. Law as code is a start to the perfect technology of justice.'¹⁵³

151. HR 17 december 1993, NJ 1994, 274 met kritische noot EAA. De Hoge Raad overwoog dat 'de door het verdragsartikel gewaarborgde ontvangstvrijheid zich niet uitstrekt tot het ontvangen van televisiebeelden die door de verspreider ervan zijn gecodeerd met het oogmerk aldus de toegankelijkheid van deze beelden te beperken tot de kring van personen die hem, als tegenprestatie voor de verspreiding, abonnementsgelden betalen'.

152. Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, *Texas Law Review* (76) 1998, p. 553.

153. Lawrence Lessig, *The Zones of Cyberspace*, *Stanford Law Review* (48) 1996, p. 1408.

Van de vrijheid van het Internet naar de dictatuur van de Lex Informatica, het is maar een kleine stap. Het net zal van een open en anarchistische ruimte in een gesloten en gecontroleerd systeem veranderen. De regels van deze 'gecodeerde' wereld zullen niet langs democratische weg, maar door ingenieurs worden bepaald, zo waarschuwt Lessig.¹⁵⁴

In zijn preadvies van 1988 bespreekt Verkade een eerste symptoom van het nieuwe schrikbewind: de 'logische bom'. Het computerprogramma dat niet regelmatig door de leverancier wordt onderhouden, blaast zichzelf op.¹⁵⁵ Verkade noemt in zijn preadvies een scala van rechtsgrondslagen op grond waarvan tegen dergelijk maatregelen kan worden geageerd: wanprestatie, ongeoorloofde oorzaak, redelijkheid en billijkheid, enzovoorts. Tegen extreme vormen van technologische eigenrichting kan ook het strafrecht een remedie bieden, zo heeft het legendarische *Palingfuiken*-arrest ons geleerd.¹⁵⁶

Maar hoe te oordelen als het de informatieconsument a priori duidelijk is dat het door hem gekochte computerspel maar X maal gespeeld kan worden; het boek maar Ymaal gekopieerd kan worden; de muziek maar Z maal beluisterd kan worden? Is het onrechtmatig een gloeilamp op de markt te brengen die sneller stuk gaat dan de stand van de techniek, strikt genomen, voorschrijft? Hebben wij onze welvaart niet juist te danken aan de productie van consumptiegoederen die ab initio defectueus zijn?

De vraag rijst of hier voor de wetgever een taak ligt. Mogelijk zal de onzichtbare hand van het marktmechanisme hier corrigerend werken. Ik roep in herinnering het fiasco van de 'copy protected' software, die niemand lustte. Boeken die zichzelf na eerste lezing verbranden; dat worden, hoop ik, ook geen bestsellers.

Het afkalvende publieke domein

Voor het auteursrecht zal de Lex Informatica hoe dan ook verrei-

154. Lessig, a.w., p. 1410.

155. Handelingen NJV 1988 I, p. 54.

156. IIR 25 juni 1934, NJ 1934, 1261.

kende consequenties hebben. Het auteursrecht zal door de informatieproducent worden vervangen 'with a new, private regime of his own making that admits no exceptions and pays no heed to the public domain', voorspelt Vinje.¹⁵⁷ Volgens Samuelson zal er op den duur voor het auteursrecht hooguit een ceremoniële rol overblijven: 'there may be nothing for copyright to do, except perhaps to serve as a kind of *deus ex machina* justifying the use of technological and contractual means for protecting works in digital form'.¹⁵⁸

'Moet het mooie stelsel van beperkingen dat we hebben dan in het Museum voor Auteursrecht worden bijgezet?', vraagt wetgever Arkenbout zich bezorgd af.¹⁵⁹ Als de techniek zijn kans grijpt, inderdaad. Ook de rest van de Auteurswet kan dan naar het archief. In een volledig gecontroleerd systeem bestaat aan bescherming erga omnes immers geen behoefte meer.

Grootschalige toepassing van contracten en technische maatregelen zal het delicate evenwicht tussen informatiebescherming en informatievrijheid, waarin het huidige auteursrecht tracht te voorzien, verstoren. Het gevaar bestaat dat allerhande informatie die tot het publiek domein behoort (onbeschermde gegevens, wetten, rechtspraak, overheidsinformatie, 'verjaarde' werken) door middel van encryptie en contract aan de openbaarheid onttrokken wordt.¹⁶⁰ Mede in het licht van de nog immer voortgaande proliferatie van het recht van intellectuele eigendom, waarvoor onder meer Spoor¹⁶¹ en Verkade¹⁶² hebben gewaarschuwd, is dat een zorgwekkend vooruitzicht.

¹⁵⁷ Vinje, a.w. (noot 132), p. 437.

¹⁵⁸ Pamela Samuelson, Copyright, Digital Data, and Fair Use in Digital Networked Environments, in: Ejan Mackaay e.a. (eds.), *The Electronic Superhighway*, Den Haag: Kluwer Law International 1995, p. 125; Visser, diss. (noot 20), p. 208.

¹⁵⁹ E.J. Arkenbout, *Informatierecht/AMI* 1997-8, p. 174.

¹⁶⁰ W. Sorgdrager, Ook in Cyberspace zijn afspraken nodig, *NRC Handelsblad* 6 juni 1996, p. 8.

¹⁶¹ J.H. Spoor, *De gestage groei van merk, werk en uitvinding* (oratie Amsterdam VU), Zwolle: W.E.J. Tjeenk Willink 1990.

¹⁶² D.W.F. Verkade, *Intellectuele eigendom, mededinging en informatievrijheid* (oratie Leiden), Deventer: Kluwer 1990, p. 11-15; idem, →

Het publieke domein kalft af, zo waarschuwt Phillips. 'Look at every aspect of intellectual property and the evidence is plain: the public domain, like the mighty rainforests of South-America, is being whittled away almost while we watch it.'¹⁶³

Recht op informatie

Tegen de voorspelde 'versleuteling' van het publieke domein kan zelfs een met dwingendrechtelijke beperkingen uitgerust auteursrecht geen remedie bieden. Met auteursrechtelijke middelen valt immers geen *toegang* tot informatie te forceren. Ook elders in het recht zijn regels die de toegang van de burger tot specifieke (voor de samenleving essentiële) informatie waarborgen, uiterst schaars. Een uitzondering vormt het recht op informatie dat iedere burger ingevolge de Wet Openbaarheid van Bestuur jegens de overheid kan invoeren. In horizontale verhoudingen heeft een vergelijkbaar, op de informatievrijheid geïnspireerd recht (ook wel 'garingsrecht' of 'garingsvrijheid' geheten) tot op heden niet¹⁶⁴ of nauwelijks¹⁶⁵ erkenning gevonden.

Het mededingingsrecht lijkt vooralsnog de enige rechtsgrond voor een horizontaal recht op informatie te bieden, althans voor het spiegelbeeld daarvan: een leveringsplicht. In het *Magill*-arrest¹⁶⁶ oordeelde het Hof van Justitie dat de weigering van de Britse omroepen om uitgever Magill een licentie te verstrekken voor het gebruik van de programmeergegevens misbruik van machtspositie opleverde. Deze machtspositie was volgens het

→ Intellectuele eigendom: wetenschaps-stimulator, Mededelingen KNAW, Deel 60, 1997-6, met venijnige kritiek op art. 450 Auteurswet (het nieuwe auteursrecht op 'gevonden voorwerpen').

163. Jeremy Phillips, *The Diminishing Domain*, EIPR 1996-8, p. 429; zie tevens Jessica Litman, *The Public Domain*, Emory Law Journal (39) 1990, p. 965.

164. HR 25 juni 1965 nr. 9836, NJ 1966, 115 (Televisier I); Europese Commissie voor de Rechten van de Mens 6 juli 1976, NJ 1978, 237 (De Geïllustreerde Pers vs. Nederland).

165. HR 23 oktober 1987, NJ 1988, 310 (NOS/KNVB); zie met name de noot van G.A.I. Schuijt, *Informatierecht/AMI* 1988, p. 35; E.J. Dommering, *Informatie-monopolies*, in: De Maris-bundel, Deventer: Kluwer 1989, p. 150-153.

166. Hof van Justitie EG 6 april 1995, Mediaforum 1995, p. B65-71; vgl. Hof Arnhem 5 augustus 1997, *Informatierecht/AMI* 1997, p. 214 (Denda/KPN).

Hof gegeven door het feitelijke monopolie op de gegevens; de omroepen zijn hiervan immers de enige bron.

Interessant is dat het Hof de casus ook vanuit het perspectief van de levering van de gegevens beoordeelde. Onder verwijzing naar oude jurisprudentie van het Hof over de levering van grondstoffen overwoog het Hof, dat de omroepen elke mededinging op de markt (voor wekelijkse programmagidsen) hadden uitgesloten, 'aangezien (de omroepen) eenieder de toegang tot de basisgegevens, het onontbeerlijke materiaal voor de productie van een dergelijke gids, ontzegden'. Waar art. 10 EVRM geen horizontale informatierechten en -plichten schept, doet art. 86 EG-Verdrag onder omstandigheden wél een plicht tot levering van informatie ontstaan. Mede in het licht van de recent in werking getreden Mededingingswet, waarin het Europese normenstelsel is overgenomen, is dat een belangrijke constatering.

Ook in het publiekrechtelijke omroeprecht zijn symptomen van een recht op informatie (in het algemeen belang) waar te nemen.¹⁶⁷ De recente discussies over de exclusiviteit van sportuitzendingen en de verslaggeving van (andere) belangrijke evenementen illustreren deze tendens.¹⁶⁸ Inmiddels zijn op nationaal en Europees niveau wettelijke maatregelen genomen om de toegang van het publiek tot dergelijke uitzendingen te waarborgen.¹⁶⁹ Teneinde de afkalving van het publieke domein te stuiten, ware vergelijkbare wetgeving buiten het domein van de omroep te overwegen. Te denken valt aan een recht van toegang tot belangrijk wetenschappelijk bronnenmateriaal, kunstvoorwerpen e.d. Ook maatregelen om het openbare aanbod van informatiediensten te stimuleren, bijvoorbeeld in de vorm van subsidies, lijken als middel tot instandhouding van het publiek domein gewenst.¹⁷⁰

¹⁶⁷ E.J. Dommering, *Informatiemonopolies*, in: *De Maris-bundel*, Deventer: Kluwer 1989, p. 152-153; vgl. J.W. Kalkman, *Versleutelde informatie*, Mediaforum 1994-6, p. 70.

¹⁶⁸ Vgl. J. van den Beukel, *De noodzaak van voetbal in een democratische samenleving*, Mediaforum 1997-5, p. 75.

¹⁶⁹ Art. 71j en 73 lid 7 Mediawet; art. 9 Europese Conventie voor Grensoverschrijdende Televisie, Trb. 1989, 103; art. 3bis Televisierichtlijn.

¹⁷⁰ Dommering, a.w. (noot 88), p. 150.

VI. CONCLUSIES

Tot besluit van dit preadvies zet ik, met een schuin oog naar de wetgever, mijn voornaamste bevindingen kort op een rij.

In hoofdstuk II bleek dat de bestaande auteursrechtelijke exploitatierechten met het Internet best uit de voeten kunnen. Het recht van openbaarmaking lijkt voor de netwerkomgeving geknipt. Het recht van verveelvoudiging behoeft, mits 'normatief' geïnterpreteerd, evenmin aanpassing. Daarentegen vormt de door de Europese Commissie geprogageerde technocratische uitleg van het reproductierecht, die ook iedere tijdelijke kopie omvat, een bedreiging voor de informatie vrijheid. Controversiële kwesties zoals het browsen, caching, mirroring en de hyperlink lijken bij nuchtere analyse zonder wetswijziging oplosbaar. Wijziging behoeven wel een aantal wettelijke beperkingen in de Auteurswet, die al te zeer op 'analoge' media zijn toegeschreven (zoals art. 15). Bij het 'multimediabebestendig' maken van de wet dient de ratio van de beperkingen goed in het oog gehouden te worden. Niet iedere bestaande beperking verdient het naar het Internet te worden overgeplant.

Een veel groter probleem voor het auteursrecht vormt het wegvallen van de geografische grenzen. Zoals in hoofdstuk III beschreven, is het auteursrechtelijke systeem op territoriale leest geschoeid; bestaande licentiepraktijken sluiten hierbij aan. De *lex protectionis*-regel maakt dat iedere publicatie op het Internet naar het (auteurs)recht van meer dan 100 soevereine staten moet worden beoordeeld. De exploitant van auteursrechtelijk materiaal loopt daardoor onaanvaardbare aansprakelijkheidsrisico's. De conclusie is dat rechtmatige openbaarmaking van auteursrechtelijk beschermde werken op het Internet alleen voor de auteur zelf is weggelegd. Dit probleem vraagt om een radicale oplossing: de gelijkschakeling van het auteursrecht op mondiaal (niet: Europees) niveau. Het einde van de territorialiteit is het begin van het wereldatauteursrecht.

Hoofdstuk IV handelde over een van de moeilijkste vraagstukken die het Internet te bieden heeft, de aansprakelijkheid van de provider. Geconstateerd werd dat de variabele en hybride rol

die de provider in de praktijk vervult, het onmogelijk maakt in algemene termen hierop een antwoord te geven. Met enige slagen om de arm werd geconcludeerd dat de access provider auteursrechtelijk buiten schot blijft, terwijl de service provider slechts via de omweg van de onrechtmatige daad valt aan te pakken. Van de provider kan niet gevergd worden dat hij het materiaal dat via zijn server wordt aangeboden, tevoren op inbreuk controleert. Aansprakelijkheid zal eerst ontstaan nadat de provider van de inbreuk kennis heeft genomen, en de inbreuk redelijkerwijs vaststaat. Invoering bij wet van een vorm van risico-aansprakelijkheid werd, mede in het licht van de informatievrijheid, een disproportionele maatregel bevonden. Een eventuele 'horizontale' regeling, een voor alle rechtsgebieden gelijk geldend aansprakelijkheidsregime, heeft het voordeel van de rechtszekerheid, maar het nadeel dat met de ratio van het materiële recht geen rekening gehouden wordt.

In hoofdstuk V, tenslotte, passeerde een tweetal alternatieven voor auteursrechtelijke bescherming de revue, het contractenrecht en de techniek. De niet-hiërarchische architectuur van het Internet lijkt een ideale voedingsbodem voor een bloeiende contractuele cultuur. Om de informaticaconsument te beschermen ontstaat behoefte aan wettelijke beperkingen die niet kunnen worden 'weggecontracteerd'. De combinatie van contractuele en technische bescherming (encryptie) zal de behoefte aan juridische bescherming erga omnes op den duur doen afnemen. De aanhoudende roep om versterking van het auteursrecht dient, in dit licht bezien, te worden gerelativeerd. Waar in elk geval geen behoefte aan bestaat is invoering van een derde beschermingslaag: juridische bescherming van technische bescherming van auteursrechtelijke bescherming. Naar verwachting zal het Internet in de nabije toekomst in snel tempo 'op slot' gaan. Versleutelde informatieproducten en -diensten zullen hun eigen voorgeprogrammeerde gebruiksregels automatisch afdwingen. De 'Lex Informatica' zal het Internet met onwrikbare logica regeren. Voor het *informatierecht*, waarin het auteursrecht gaandeweg zal opgaan, ligt hier de schone taak het afkalvende publieke domein te redden.

Tot slot enige bemoedigende woorden voor de Nederlandse (au-

teurs)wetgever. Hoewel de logica gebiedt dat hij zich met het Internet niet inlaat, is er voor de wetgever toch een (bescheiden) rol weggelegd. Het internationale recht, waar eventuele regulering van het Internet haar beslag zou moeten krijgen, wordt niet in diplomatieke conferenties geboren, maar geschapen naar het beeld van bestaande nationale regelingen. Willen wij meespelen in het internationale spel, dan zullen wij eerst ons eigen, digitale Poldermodel moeten ontwerpen. Nationale wetgeving blijft dus zinvol, niet als panacee, maar als proeftuin voor een internationale oplossing.

Hiermee is niet gezegd, dat de nationale wetgever hals-over-kop aan de slag moet. Integendeel, als er één advies uit dit procdvies onthouden wordt, dan dit: laten we er nog een jaartje over slapen. Na het jaar 2000 zien we wel weer verder.