

Aansprakelijkheid en Internet: de provider

Mr. P. Kleve
Erasmus Universiteit Rotterdam

1. Inleiding: waarom geeft Internet juridische problemen?

Deze congresbundel staat in het teken van 'IT en recht' waarbij een groot aantal bijdragen de nadruk legt op Internet¹. Een belangrijke vraag lijkt derhalve: waarom geeft Internet juridische problemen? De nieuwe juridische vraagstukken komen voort uit nieuwe maatschappelijke ontwikkelingen, die worden aangestuurd door nieuwe technologie. De invoering op grote schaal van de pc heeft geleid en leidt nog steeds tot allerlei veranderingen in de manier waarop wij gewend waren met elkaar om te gaan. Zo wordt thans een groot deel van de handelstransacties tussen bedrijven geautomatiseerd - soms zelfs zonder enige menselijke tussenkomst - afgewerkt door toepassing van EDI - electronic data interchange, de geautomatiseerde uitwisseling van gegevens volgens bepaalde vooraf afgesproken standaarden. En in het kielzog van de bedrijven blijken ook steeds meer consumenten de weg te vinden naar de elektronische markt. In dit verband spreekt men wel van 'ecommerce', waaronder alle commerciële handelstransacties worden begrepen, zowel de bedrijfsmatige EDI transacties die over een meer besloten netwerk passeren, als de transacties die in de meer open omgeving van Internet plaats vinden. Tengevolge van deze door de technologie mogelijk geworden bestelprocedures komen juridische vragen naar boven, zoals die naar de rechtsgeldigheid van 'elektronische transacties' en de bewijskracht van 'elektronische documenten', de vraag op welke wijze een bevestiging van de wilsuiting kan plaats vinden waaraan juridische gebondenheid kan worden toegekend overeenkomstig het plaatsen van een handtekening en de vraag bij voorbeeld hoe algemene voorwaarden in elektronische vorm op bindende wijze van toepassing kunnen worden verklaard. Naast en in de plaats van het 'papier regime' ontstaat een 'elektronisch regime', met nieuwe vraagstukken voor juristen. En anders dan dat juristen, vooral in het privaatrecht, gewend waren, kunnen deze nieuwe juridische vragen niet steeds door middel van a contrario dan wel per analogiam redeneren beantwoord worden.

Computers worden evenwel gebruikt sinds 1960. Hoe komt het dan, zo kan men zich afvragen, dat er eerst thans zo'n aandacht is voor juridische vraagstukken? Als voor de hand liggende verklaringen worden wel genoemd het internationale aspect, de schaalvergroting en het toegenomen thuisgebruik. Zonder te willen ontkennen dat deze drie factoren ieder op zich van enige invloed kunnen zijn, lijkt het toch niet goed mogelijk hiermee een afdoende verklaring te geven. Internationale transacties zijn natuurlijk niet nieuw. Ook in het voor-

computertijdperk kenden we een bloeiende internationale handel, waarbinnen omgegaan diende te worden met vraagstukken tengevolge van verschillen in rechtssystemen. En schaalvergroting en thuisgebruik dragen er wel toe bij dat problemen als hier bedoeld vaker zullen optreden, doch veroorzaken ze niet. Nee, de verklaring lijkt veeleer samen te hangen met de functionaliteit van computers. Hoewel computers heden ten dage als onmisbaar gezien worden voor het geordend functioneren van de samenleving - men denke slechts aan de doemscenario's die vanwege de 'millenniumbug' worden voorspeld - is de functionaliteit daarvan beperkt. Naast de functies van invoer en uitvoer van gegevens wordt de functionaliteit van computers onderscheiden in rekenen (processorcapaciteit), onthouden (opslagcapaciteit) en communiceren. Indien we kijken naar de hieraan verbonden kosten, dan zien we dat rekenen altijd het goedkoopst is geweest, gevolgd door de opslagcapaciteit, en dat de kosten van telecommunicatie het hoogst zijn. En hoewel alledrie de functies in de loop der tijd steeds goedkoper zijn geworden, nemen de verschillen onderling nog steeds toe. Zo bezien, lijkt de huidige populariteit van Internet niet een toevallige, maar een logisch uitvloeisel van inmiddels kosteneffectievere telecommunicatie. Op grond van dit model is voorspelbaar dat computerprogramma's die gebruik maken van compressietechnieken steeds aantrekkelijker zullen worden. Immers, de processorcapaciteit die nodig is om de compressie te berekenen is goedkoper dan de opslagcapaciteit van niet-gecomprimeerde data, terwijl ook de telecommunicatie van gecomprimeerde data goedkoper is. Een andere voorspelling zou kunnen zijn dat de invoering van niet-intelligente computers zonder opslagmedium, die gebruik maken van centraal beschikbare programmatuur en databestanden, minder kansrijk zal zijn, omdat de daaruit volgende toegenomen telecommunicatie nu eenmaal duurder is dan lokale verwerking en opslag.

Internet is dus niet toevallig, maar verklaarbaar op grond van afgenomen kosten voor telecommunicatie. Niettemin blijken compressietechnieken aantrekkelijk, zowel ter reductie van de kosten voor opslagcapaciteit als die voor telecommunicatie. Er is echter nog een tweede reden waarom het gebruik van compressieprogramma's aantrekkelijk is, namelijk beveiliging. Compressie van databestanden geschiedt volgens bepaalde algoritmen. Om een gecomprimeerd bestand weer leesbaar te maken, zal er wederom een algoritme gebruikt moeten worden om de data terug te zetten in de eigenlijke vorm. Zonder beschikking over, of kennis van het gebruikte algoritme zijn gecomprimeerde bestanden dus voor 'derden' onleesbaar. En naast de hierboven opgeworpen vraag naar de juridische status van elektronische gegevensbestanden belanden we hiermee op het tweede majeure vraagstuk in het internettijdperk, dat van de cryptografie.

2. Probleemgebied met uitstraling: cryptografie

Voor een veilig en betrouwbaar gegevensverkeer over Internet is het gebruik van cryptografische technieken onontbeerlijk. Het elektronisch betalingsverkeer bij voorbeeld zou niet van de grond gekomen zijn zonder betrouwbare encryptie ('versleuteling') van de betalingstransacties. Versleuteling van berichten zal voor niemand echt onbekend terrein zijn, of dat nu gecodeerde berichten in oorlogstijd zijn, in spannende spionagefilms, of het 'geheimschrift' dat we zelf in onze jeugd wel eens bedacht hebben. Wat we daarvan ook hebben 'meegekregen' is dat gecodeerde berichten gekraakt kunnen worden, door 'de vijand', computer whizz kids of in het algemeen door personen waarvoor de inhoud van het bericht niet bestemd was. Als we maar lang genoeg proberen, dan zou iedere code te kraken zijn. Toch is dat niet helemaal waar. Bij de zogenoemde 'single pad' versleuteling, een codeermethode waarbij voor ieder bericht afzonderlijk een codeersleutel wordt afgesproken en dus ook éénmalig wordt gebruikt, is de code praktisch gesproken niet te herleiden. Bij frequente communicatie is het natuurlijk wel erg lastig en omslachtig om steeds een nieuwe codeersleutel af te spreken, die dan ook nog eens iedere keer vertrouwelijk aan de wederpartij ter beschikking moet worden gesteld. Dan wordt het handiger om één keer een codeersleutel af te spreken, en die gedurende enige tijd te hanteren. Zodra de kans groter wordt dat de sleutel niet meer uitsluitend aan partijen beschikbaar staat, wordt een nieuwe sleutel afgesproken. Het nadeel van deze vormen van symmetrische versleuteling, waarbij voor het versleutelen dezelfde codeersleutel wordt gebruikt als voor het ontsleutelen, is dat het in de praktijk niet zo gemakkelijk blijkt te zijn de sleutel vertrouwelijk te houden. Een derde manier om berichten te versleutelen, die enerzijds kenmerken van de betrouwbaarheid van de single pad encryptie herbergt en anderzijds het gemak van de symmetrische versleuteling, bestaat uit de zogenoemde 'asymmetrische encryptie'.

De uitgangspunten van asymmetrische versleuteling zijn dat voor ieder bericht steeds twee (verschillende) sleutels nodig zijn, één om het bericht te versleutelen en één (andere) om het bericht te ontsleutelen. Een bericht dat met de ene sleutel is versleuteld, kan niet met dezelfde sleutel worden ontsleuteld. Daarvoor is de andere sleutel van het sleutelpaar noodzakelijk. Zo kan evenmin een sleutel waarmee een bericht is ontsleuteld, worden gebruikt om het bericht opnieuw te versleutelen. Deze, op een wiskundig algoritme gebaseerde, cryptografische techniek blijkt uitermate geschikt om de juridische vraagstukken in verband met internetcommunicatie op te lossen. Bij internetcommunicatie komen steeds dezelfde juridische vraagstukken aan de orde: hoe kunnen partijen bereiken dat berichten vertrouwelijk blijven zodat alleen de ontvanger daarvan kennis kan nemen? (i), hoe kunnen partijen bereiken dat berichten onweerlegbaar de afzender identificeren? (ii) en hoe kunnen partijen bereiken dat de inhoud van de berichten aantoonbaar authentiek (ongewijzigd) is? Indien

partijen zich bedienen van asymmetrische encryptie, wordt bereikt dat de hier geschetste CIA-problematiek (confidentiality, identity en authenticity) adequaat wordt opgelost. Beide partijen beschikken ieder over een sleutelpaar. Zowel de afzender als de ontvanger houden beiden van hun sleutelpaar één sleutel geheim (de privé-sleutel). De andere sleutel van ieders sleutelpaar mag publiekelijk bekend zijn (de publieke sleutel). Indien de afzender het bericht versleuteld met zijn privé-sleutel kan het bericht uitsluitend worden ontsleuteld met zijn publieke sleutel. Als de wederpartij nog niet de beschikking heeft over de publieke sleutel van de afzender, stuurt de afzender zijn publieke sleutel gewoon mee met het bericht. Publieke sleutels mogen immers algemeen bekend zijn. Uit dit systeem van asymmetrische versleuteling volgt dat berichten die met iemands publieke sleutel óntsluteld kunnen worden, dus vérsleuteld moeten zijn geweest met diens privé-sleutel. En omdat niemand behalve de afzender de beschikking heeft over die (wel geheim gehouden) privé-sleutel moet het bericht dus wel door de afzender zijn gemaakt en van hem afkomstig zijn. Dit gebruik is dus de oplossing voor het vraagstuk van identificatie. Het probleem is echter dat nog steeds iedereen die het bericht - toevallig - ontvangt of als intermediair het bericht doorgeeft, het bericht ook kan ontsleutelen en vervolgens kan lezen. Wat die derde overigens níet kan is het bericht wijzigen en als zijnde het authentieke bericht van de afzender doorsturen. Hij kan het (gewijzigde) bericht immers niet versleutelen met de privé-sleutel van de afzender omdat hij daarover niet beschikt. De authenticiteit, de integriteit van de inhoud van het bericht, is door deze methodiek derhalve ook gewaarborgd. Resteert de vertrouwelijkheid, het voorkomen dat derden voor wie het bericht niet is bestemd kennis nemen van het bericht. Ook dit is oplosbaar door middel van dezelfde asymmetrische encryptie. De afzender kan het bericht nadat hij dit heeft versleuteld met zijn privé-sleutel namelijk nóg een keer versleutelen, maar nu met de publieke sleutel van de ontvanger. Daaruit volgt dan weer dat een bericht dat is versleuteld met de publieke sleutel van de ontvanger uitsluitend door die ene ontvanger kan worden ontsleuteld, en wel met diens privé-sleutel. Dus, door twee maal te versleutelen, één maal met de privé-sleutel van de afzender en vervolgens één maal met de publieke sleutel van de ontvanger, wordt zowel identificatie als vertrouwelijkheid gewaarborgd. De authenticiteit volgt uit de onmogelijkheid een eenmaal ontsleuteld bericht opnieuw te versleutelen met de privé-sleutel van de afzender. Voor bewijsdoeleinden dient dan ook altijd het bericht *in versleutelde vorm zoals ontvangen* te worden bewaard.

Voor diegenen die met het lezen van deze bijdrage voor het eerst kennis nemen van deze vorm van asymmetrische encryptie, kan wellicht de indruk ontstaan dat het hier om bijzondere computerprogramma's handelt. Dat is maar ten dele waar. Een computerprogramma dat op basis van deze technologie werkt is bij voorbeeld Pretty Good Privacy, dat vrij beschikbaar van Internet te downloaden

is, en waarvan bovendien de broncode vrij beschikbaar is. Maar ook de moderne versies van de internetbrowsers Netscape Navigator en Internet Explorer beschikken tegenwoordig standaard over met deze techniek verwante 'beveiligingsknoppen'. Adequate beveiligingstechniek is derhalve voor iedere internetgebruiker zonder technische know how gemakkelijk beschikbaar en toepasbaar. Wel is het zo, dat verschillende landen wettelijke regelingen kennen voor software met cryptografie know how². Zo valt in de Verenigde Staten cryptografie met sleutels langer dan 40 bits onder de werking van de Export Administration Act. Onder export valt ook het ter beschikking stellen op Internet. Dit heeft overigens niet tot gevolg dat de rest van de wereld het zonder zware cryptografie moet stellen. Bezwaren die wel worden vernomen van de zijde van het Amerikaanse bedrijfsleven zijn eerder de handelsbelemmerende werking daarvan en dat de (internationale) markt voor zware encryptie in handen komt van andere (buitenlandse) aanbieders. Voor de toekomst beoogt men daarom in het kader van het Wassenaar Arrangement³ te bereiken dat de uitvoer van sterke encryptie met sleutels van meer dan 56 bits niet meer zonder vergunning mogelijk wordt. Daarbij dient de gebruiker in te stemmen met de voorwaarden van de Amerikaanse overheid voor toegang tot de sleutels, teneinde desgewenst berichten te kunnen ontsleutelen.

3. De beveiliging doorbroken

Hierboven is gesteld dat beveiliging, en dan met name een vrij en onbelemmerd gebruik van cryptografie, onontbeerlijk is voor een betrouwbaar handels- en betalingsverkeer. Maar niet alleen daarvoor. Ook vraagstukken met betrekking tot privacy op Internet of afrekenmechanismen met betrekking tot de elektronische beschikbaarstelling van auteursrechtelijk beschermde werken zijn daarmee gebaat. En bij voorbeeld eerbiediging van het grondrecht op het briefgeheim kan op Internet door betrokkenen zelf geëffectueerd worden met behulp van cryptografie. Hoewel nut en noodzaak van de door de Commissie Computercriminaliteit voorbereide Wet Computercriminaliteit te betwijfelen valt, is het zeker de verdienste van deze commissie onder voorzitterschap van Franken waar zij als een van de eersten in de juridische literatuur de aandacht vestigde op het belang van beveiliging van computersystemen⁴. Informatiebeveiliging past ook helemaal in de lijn van de overheid waar zij voor Nederland een prominente plaats opeist in de ontwikkeling van internetdienstverlening. Op zijn minst gezegd is het dan ook vreemd, maar in ieder geval tegenstrijdig aan de hiervoor geschetste beleidsuitgangspunten, te merken dat diezelfde overheid keer op keer initiatieven onderneemt voor de regulering van encryptie. Ach, het aanknopingspunt voor het belang van de overheid is natuurlijk gauw gevonden. Als informatie-uitwisseling thans zo goed beveiligd kan plaatsvinden zodat derden van de inhoud van de communicatie geen kennis kunnen nemen, geldt dit natuurlijk zowel de communicatie van de bovenwereld als die van de

onderwereld. En het is nu eenmaal ook de taak van de overheid om criminaliteit te bestrijden. En dan zou het wel gemakkelijker zijn voor die overheid als zij vrije toegang zou verkrijgen tot communicatie tussen verdachte personen met betrekking tot verdachte transacties⁵.

De eerste poging van justitie vat te krijgen op de informatie-uitwisseling dateert al weer uit 1994, in de vorm van een voorontwerp van wet uitgaande van een algemeen verbod op het gebruik van encryptie. Op dit verbod zouden natuurlijk uitzonderingen nodig zijn voor overheidsdiensten. Voorts zou voor particuliere ondernemingen een vergunningenstelsel gaan gelden. Aan die vergunningen zouden dan weer voorwaarden kunnen worden gekoppeld met betrekking tot het sleutelbeheer en de toegang daartoe voor justitie. Dit voorontwerp is ten onder gegaan aan de hevige maatschappelijke kritiek, onder meer vanuit het bedrijfsleven, maar ook vanuit de juridische wereld⁶. Dat het ontwerp het daglicht niet heeft mogen aanschouwen, is begrijpelijk; regulering van encryptie werkt niet. Al is het alleen maar omdat criminelen zich er niet aan houden. Criminelen vragen geen vergunning aan, maar nemen eerder het risico van overtreding van een vergunningsregeling dan dat zij het risico lopen dat informatie omtrent hun handel en wandel ter beschikking van justitie komt. De 'last' wordt derhalve uitsluitend gedragen door bona fide organisaties die wel een vergunning moeten aanvragen, en voorts ongemerkt het risico lopen dat inzage in hun communicatie noodzakelijk wordt geacht in het kader van een opsporingsonderzoek. Al is men wellicht zelf niet verdacht, men kan immers communiceren met personen die dat wel zijn. Voorts lijkt justitie met zulke wetsvoorstellen er van uit te gaan dat telecommunicatie noodzakelijkerwijs in traceerbare en identificeerbare pakketjes moet plaatsvinden. En ook dat is onjuist. Zo is er het voorbeeld van de zogeheten 'steganografie', de versluisde versleuteling. Het is zeer eenvoudig om in een onschuldig uitziend plaatje een tekst te verstoppen die voor niemand kenbaar is behalve de ontvanger. Bovendien valt in een plaatje van 50 Kb 2 Kb aan tekst te verwaarlozen. Het oog ziet slechts een stipje met een andere kleur grijs. Als men die plaatjes dan ook nog eens in een willekeurige serie uploadt in een willekeurige nieuwsgroep en alleen de beoogd ontvanger weet over welke plaatje het gaat en in welke nieuwsgroep, dan wordt helemaal duidelijk dat justitie het nakijken heeft. Een laatste bezwaar tenslotte is de wetenschap vanuit beveiligingsmanagement van het verhoogd risico dat men loopt indien derden - waaronder zeker de overheid - toegang krijgen tot beveiligingsmaatregelen.

De hardnekkigheid waarmee de overheid haar zinnen heeft gezet op toegang tot informatie is echter groot, en het wekt dan ook geen verbazing om nieuwe voorstellen omtrent encryptie tegen te komen in het voorontwerp Wetsvoorstel Computercriminaliteit II dat hieronder nog aan de orde zal komen.

4. Strafrechtelijke aspecten: de (bijzondere?) positie van de provider

Hierboven is in de inleiding uiteengezet dat de afgenomen kosten van telecommunicatie de aanzet hebben gegeven tot de huidige ontwikkeling van Internet. Daarbij is in paragraaf 2 aandacht besteed aan het belang van cryptografie voor diezelfde ontwikkeling. In de vorige paragraaf is voorts geschetst dat vrij gebruik van cryptografie en de daaruit voortvloeiende vertrouwelijkheid van gegevensuitwisseling niet past binnen de opvatting van de overheid ten aanzien van criminaliteitsbestrijding. Ook komt uit de vorige paragraaf naar voren dat regulering van cryptografie nauwelijks effectief zal blijken te zijn ter beteugeling van met name de georganiseerde misdaad. Het is echter niet louter de communicatie over Internet van criminelen die justitiële aspecten in zich draagt. Ook de inhoud op zich van de communicatie kan strafrechtelijk relevant zijn. Men denke hier vooral aan de verspreiding van kinderpornografie, racisme op Internet alsmede de (ongoorloofde) openbaarmaking van auteursrechtelijk beschermde werken. En bij al deze problematiek is de provider de spin in het web. Immers, hij is met zijn intermediaire dienstverlening onmisbaar voor al deze vormen van communicatie. Zonder de ingang van een provider, zonder diens medewerking aan het transport van de data en zonder diens beschikbaarstelling van opslagcapaciteit voor email en webpagina's zou geen van deze verboden handelingen kunnen plaatsvinden. Dat de aanbieders van de informatie als daders van het plegen van strafbare gedragingen mogen worden aangemerkt en strafrechtelijk vervolgd mogen worden, daaraan bestaat geen twijfel. In de virtuele wereld van Internet gelden dezelfde rechtsregels als in de 'echte' wereld. Daarover wordt elders in deze bundel geschreven. De vraag is hier of de positie van de provider strafrechtelijk relevant is. Hij doet toch niet meer dan het datatransport en het beschikbaar stellen van computerfaciliteiten? Verkeert hij als zodanig niet in een vergelijkbare positie als bij voorbeeld de telecommunicatieleverancier, de uitgever of de drukker, die ook geen boodschap aan de boodschap hebben?

Het antwoord op deze vraag is echter 'Ja', de positie van de provider is strafrechtelijk relevant⁷. Zo zien we ten eerste dat de formuleringen van de meeste strafbepalingen zich evenzogoed uitstrekken over de gedragingen van de provider. De formulering van het in voorraad hebben van kinderpornografie strekt zich evenzogoed uit over de computer van de provider waarop de afbeeldingen zich bevinden. Het is voorts de provider die door zijn samenstel van technische faciliteiten de afbeeldingen openbaar maakt, althans gelegenheid geeft tot openbaarmaking⁸. Uitzonderingen voor het aandeel van de provider in de verspreiding en/of openbaarmaking worden niet gegeven. Door de providers zijn hiertegen wel verschillende bezwaren aangevoerd. Zo is wel tegengeworpen dat het onmogelijk zou zijn alle dataverkeer te controleren op eventueel 'strafbaar materiaal'. Bovendien is het aan de rechter, en niet aan de provider,

om uit te maken of - bij voorbeeld - een afbeelding is aan te merken als kinderpornografie. Voorts zou het vooraf screenen van informatie-inhoud neerkomen op censuur, wat evenmin is toegestaan. En als dan al strafbaar materiaal zou worden aangetroffen, dan zou het niet gewist mogen worden omdat dat zaaksbeschadiging zou opleveren. Nu is voor deze 'excuses' wel iets te zeggen, maar echt overtuigen kunnen ze niet. Het is juist dat het onmogelijk is alle dataverkeer te controleren, hoewel het met behulp van search agents ook weer niet geheel onmogelijk is. Maar, zoals hierboven uiteengezet, als het materiaal encrypt is, dan kan het ook niet door providers gelezen worden. Maar moet dit dan betekenen dat providers in het geheel geen verantwoordelijkheid hoeven te dragen? Ook niet in het geval men concreet wetenschap heeft dat op een bepaalde site strafbaar materiaal aanwezig is, bij voorbeeld omdat daar door anderen op gewezen is? Ook de stelling dat het aan de rechter is om uit te maken of een bepaalde afbeelding onder een delictsomschrijving valt is in beginsel wel juist. Maar geldt die terughoudendheid dan ook in die gevallen waarin het onmiskenbaar duidelijk is dat het om - bij voorbeeld - een kinderpornografische afbeelding gaat? Dat de hier bedoelde afbeeldingen niet gewist zouden mogen worden door providers is natuurlijk niet houdbaar. Niemand kan immers worden verplicht mee te werken aan het plegen of in stand houden van een strafbaar feit.

De providers, verenigd in NLIP (Vereniging van Nederlandse Internet Providers), hebben in 1995 besloten tot de oprichting van verschillende meldpunten, teneinde door middel van deze vorm van zelfregulering strafrechtelijke aansprakelijkheid te voorkomen. Er is een meldpunt kinderporno, een meldpunt discriminatie en een meldpunt overig illegaal materiaal.

De analogieën met de telecommunicatieleverancier, uitgever en/of drukker hebben maar een beperkte geldigheid, zo zij op grond van het legaliteitsbeginsel uit het strafrecht al toelaatbaar zouden zijn. Maar de positie van de provider is puur feitelijk nu eenmaal niet dezelfde als die van de telecommunicatieleverancier. Anders dan bij de doorgifte van telefoongesprekken, worden bij internetcommunicatie de gegevens opgeslagen in de computer van de provider, en blijven daar beschikbaar totdat ze worden verwijderd. De wetgever heeft evenwel de onwenselijkheid van het ongeregeld zijn van de strafrechtelijke positie van providers onderkend, en in het voorontwerp van het Wetsvoorstel Computercriminaliteit II wordt dan ook voorgesteld artikel 53 Sr, dat de condities stelt voor strafrechtelijke immuniteit van drukkers en uitgevers te moderniseren⁹. In de Memorie van Toelichting op het voorontwerp blijkt onder verwijzing naar het antwoord¹⁰ van 19 augustus 1996 op kamervragen het standpunt van de minister 'dat de providers reeds naar huidig recht onder omstandigheden strafrechtelijk aansprakelijk zijn - te denken valt aan medeplichtigheid - voor de via hen verspreide strafbare informatie, mits zij op de

hoogte waren van de aard van de informatie, althans indien het aan hun ernstige nalatigheid te wijten was dat het betrokken materiaal op Internet voor het publiek beschikbaar was.' Een speciale bescherming voor providers zoals thans in de artikelen 53 en 54 Sr is voorzien voor uitgevers en drukkers wordt wenselijk geacht. In het herziene artikel 53 Sr wordt nu voorgesteld dat in het geval van verspreidingsdelicten tussenpersonen als zodanig niet vervolgd worden indien a. hij bij de openbaarmaking of verspreiding zijn identiteit heeft bekend gemaakt, 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. De voorwaarde uit het huidige artikel 53 Sr, dat de dader binnen Nederland is gevestigd, is gelet op het internationale karakter van Internet niet overgenomen. De voorwaarde dat providers in het geval van een gerechtelijk vooronderzoek verplicht worden de identiteit van de dader bekend te maken, staat overigens niet in de weg aan de dienstverlening van (sommige) providers internetgebruikers anoniem toegang tot Internet te verschaffen. Wel brengt art. 53 met zich mee dat de identiteit bij de providers zelf bekend moet zijn.

5. Medewerkingsverplichtingen van de provider

Zoals gezegd, is de provider als de spin in het web van de internetcommunicatie. Met de inwerkingtreding in 1993 van de Wet Computercriminaliteit (I) zijn specifieke opsporingsbevoegdheden opgenomen in het Wetboek van Strafvordering ter zake van onderzoek in computersystemen. De bevoegdheid uit art. 125i Sv om in het kader van een gerechtelijk vooronderzoek onderzoek te doen naar in computersystemen opgeslagen gegevens geldt natuurlijk evenzeer de computersystemen van providers. Gegevens, bij voorbeeld email-berichten, die zijn opgeslagen op de computers van providers kunnen aldus ter beschikking komen van justitie. Interessant in dit verband is de weigering in november 1997 van de provider XS4ALL gehoor te geven aan een vordering van Justitie, gebaseerd op 125i Sv, om het internetverkeer van een van haar gebruikers af te tappen. De reden voor de weigering was dat XS4ALL de mening was toegedaan dat 125i onvoldoende wettelijke grondslag bood voor het ten behoeve van Justitie vastleggen van *toekomstige* email van haar gebruiker. Daartoe zou eigenlijk een bepaling nodig zijn analoog aan die van 125g Sv, het aftappen van telefoongesprekken. De arrondissementsrechtbank te Amsterdam heeft op 21 mei 1999¹¹ uitspraak gedaan in de vervolgens door Justitie tegen XS4ALL ingestelde strafvervolgung en XS4ALL ontslagen van rechtsvervolgung. De rechtbank was van oordeel dat 125i Sv inderdaad geen juiste grondslag was voor het aftappen van toekomstige email. XS4ALL had dus gelijk in haar

weigering Justitie de verlangde gegevens te verstrekken. Wat dan wel opmerkelijk wordt, is het feit dat diverse andere providers steeds wel gehoor hebben gegeven aan Justitie, naar achteraf blijkt op een onbevoegd gegeven bevel. Of dit tot de consequentie zou moeten leiden dat in die gevallen sprake is van onrechtmatige bewijsgaring is blijkens de uitspraak van de Hoge Raad in het arrest van 9 maart 1999¹² in een hieraan verwante problematiek afhankelijk van de vraag of de gegevens als bewijs zijn gebruikt. In deze zaak speelde dat de officier van justitie een vordering heeft gedaan op grond van art. 125f Sv aan de provider Euronet. Op basis van de van Euronet verkregen persoonsgegevens kon de verdachte worden opgespoord. In het geding was onder meer de vraag of providers kunnen worden gerekend tot de beperkte groep van concessiehouders of machtiginghouders uit art. 125f. De A-G beantwoordt deze vraag ontkennend (al sluit hij niet uit dat Euronet nog andere diensten exploiteert waardoor zij tot de geadresseerden van de vordering van art. 125f Sv zou kunnen behoren) doch meent tevens dat een vordering op de voet van 125f Sv niet nodig was om op rechtmatige wijze aan de informatie te komen, omdat informatie als de tenaamstelling van een abonneenummer - waaronder ook de naam van de houder van een emailadres - niet beschermd wordt door de regeling van art. 125f Sv. De Hoge Raad oordeelde dat uit het proces-verbaal van de terechtzitting van het Hof slechts blijkt dat de verkregen inlichtingen de opsporingsambtenaren op het spoor van de verdachte hebben gezet, maar niet dat het gebruikte bewijsmateriaal uitsluitend is verkregen als gevolg van of met gebruikmaking van het gestelde onrechtmatig optreden.

De uitspraak in de zaak XS4ALL heeft inmiddels nog maar beperkte betekenis, tengevolge van aanpassingen in het Wetboek van Strafvordering¹³ en de inwerkingtreding van de Telecommunicatiewet¹⁴. De artikelen 125f tot en met 125h Sv (onderzoek van telecommunicatie) zijn vervallen. Daarvoor in de plaats is een nieuwe afdeling zeven gekomen, waarin de tapbevoegdheid van justitie is geregeld in de artikelen 126m en 126t (oud 125g). Artikel 13.1 van de Telecommunicatiewet stelt dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend aan gebruikers beschikbaar stellen indien deze aftapbaar zijn¹⁵. Artikel 13.2 verplicht aanbieders van telecommunicatienetwerken en aanbieders van telecommunicatiediensten 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, respectievelijk van door hen verzorgde telecommunicatie. Op grond van artikel 13.4 worden zij voorts verplicht aan de autoriteiten de informatie te verstrekken die noodzakelijk is om de bevoegdheden tot het aftappen of opnemen van telecommunicatie, dan wel tot het vorderen van gegevens ter zake van alle verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten,

plaatsvindt te kunnen uitoefenen. Deze verplichting omvat in ieder geval het telecommunicatienummer en de naw-gegevens.

Nu de tap- en opnamebevoegdheden adequaat geregeld schijnen te zijn, dient zich echter wederom het schrikbeeld van de encryptie aan. Want wat heeft Justitie nu aan een tapbevoegdheid indien deze er alleen maar toe leidt dat - voor Justitie - onleesbare berichten worden vastgelegd? Het voorontwerp Wetsvoorstel Computercriminaliteit II gaat dan ook een stap verder. Voorgesteld wordt de artikelen 126m en 126t uit te breiden met een vijfde lid waarin wordt bepaald dat tot degenen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de telecommunicatie het bevel kan 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. Het goede aan dit voorstel is dat de regeling aanmerkelijk minder verstrekkend is dan het encryptie-voorontwerp uit 1994. Verstrekkend zijn de gevolgen echter wel voor de telecommunicatieleveranciers en de dienstenaanbieders. Ingevolge artikel 13.6 Telecommunicatiewet komen de investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die door hen zijn of worden gemaakt teneinde de telecommunicatienetwerken en -diensten aftapbaar te maken en te houden te hunner laste. Zoals volgt uit paragraaf 3, valt het sterk te betwijfelen of deze investeringen wel verantwoord kunnen worden met een beroep op de bestrijding van de georganiseerde criminaliteit, gelet op de diversiteit van de encryptiemogelijkheden en de verwachting dat criminelen zich daaraan weinig gelegen zullen laten. Met dit soort bepalingen, die toch niet als voorbeeld kunnen dienen voor een rationele benadering van vraagstukken met betrekking tot informatietechnologie, wekt Justitie eerder de schijn op zich kennis te willen verwerven op kosten van het bedrijfsleven.

Ter afronding van deze paragraaf dient nog kort gewezen te worden op de ontwikkelingen rond het briefgeheim op Internet en de al dan niet beschermde status van email¹⁶. In het voorstel tot wijziging van de Grondwet¹⁷ was oorspronkelijk voorzien in een formulering van het brief-, telefoon- en telegraafgeheim die zich mede zou uitstrekken over emailberichten. In het voorontwerp Wetsvoorstel Computercriminaliteit II zou aan artikel 372 Sr een nieuw lid worden toegevoegd waarin de strafbaarheid zou worden uitgebreid naar de persoon werkzaam bij openbare telecommunicatienetwerken of -diensten, die opzettelijk en wederrechtelijk email (gesloten elektronisch bericht) opent, inziet of de inhoud ervan aan een ander bekend maakt. In artikel 125n wordt vervolgens voorgesteld dat de rechter-commissaris bevoegd is te bepalen dat van email-berichten kennis zal worden genomen, voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem zijn bestemd of tot het begaan van het strafbare feit hebben gediend, ofwel klaarblijkelijk met betrekking tot

die gegevens het strafbare feit is gepleegd. De verdere behandeling van deze voorstellen is evenwel afhankelijk gesteld van het advies van de bij Besluit van 23 februari 1999 ingestelde Commissie Grondrechten, welke commissie de taak heeft gekregen de regering met het oog op de ontwikkelingen op het terrein van de informatie- en communicatietechnologie te adviseren over de aanpassing van de grondrechten en de wenselijkheid van de vaststelling van nieuwe grondrechten¹⁸.

6. Privaatrechtelijke aspecten en de positie van de provider.

Ten aanzien van de civielrechtelijke aansprakelijkheid van internet-providers is een richtinggevende uitspraak bekend in de zaak van de Scientology Church uit 1996, in welke zaak de rechter zich onlangs ook in de bodemprocedure heeft uitgesproken¹⁹. Het betreft hier de situatie waarin naast de internetgebruiker die teksten op haar homepage had gepubliceerd waarmee zij beweerdelijk inbreuk zou hebben gemaakt op het auteursrecht van de Scientology Church, ook een 22-tal internet-providers waren gedagvaard. Omdat via de providers toegang tot de betreffende werken wordt verkregen, zouden ook de providers openbaarmaken. De President van de Haagse rechtbank oordeelde in 1996 dat providers 'niet meer doen dan gelegenheid geven tot openbaarmaking en dat zij in beginsel geen invloed kunnen uitoefenen op of zelfs maar kennis dragen van datgene wat diegenen 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 inbreukmakende - handelingen van gebruikers.' Providers maken als zodanig dus niet openbaar en zijn 'in beginsel' niet aansprakelijk voor inbreuken van gebruikers op auteursrechten van derden. De President vervolgt dan met een nadere precisering in welke situatie er wel aansprakelijkheid zou kunnen worden aangenomen en formuleert daarvoor twee cumulatieve vereisten, namelijk '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 provider bekend is, bijvoorbeeld doordat deze op een en ander is geattendeerd.' Een jaar eerder speelde overigens een verwante vraag voor de Arrondissementsrechtbank te Rotterdam²⁰. In deze zaak was onder meer de vraag of bulletinboard-houders, door De Mulder getypeerd als 'Internet-providers avant la lettre', door 'uploaden' en 'downloaden' van programma's en/of gegevens mogelijk te maken, ook zelf openbaarmaakten en/of verveelvoudigden. Bulletinboard-houder Lenior stelde dat de Bridgesoft toernooisoft-ware door een derde was 'ge-upload' en door negen anderen was 'gedownload', zodat hij een en ander niet zelf had verveelvoudigd. De President oordeelde daarop dat het downloaden door anderen kennelijk mogelijk was doordat Lenior een wijziging heeft aangebracht in de Title Allocation Table - hij had het in de lijst met beschikbare bestanden opgenomen - en dat Lenior door de waarschu-

wing dat het programma voorzien was van een kopieerbeveiliging verdacht had moeten zijn op de mogelijkheid van auteursrechtinbreuk. Lenior viel derhalve een verwijt te maken van de door hem gepleegde auteursrechtinbreuk. Wanneer we deze uitspraak vergelijken met de Scientology-zaak, valt op dat hier aan beide cumulatieve vereisten uit de Scientology-zaak is voldaan.

Op 9 juni 1999 heeft de Arrondissementsrechtbank uitspraak gedaan in de bodemprocedure van Scientology tegen de internetgebruiker en de providers en alle eisen afgewezen. De internetgebruiker, die na 23 februari 1996 de werken niet meer integraal op haar homepages had opgenomen maar slechts een relatief klein gedeelte, mocht zich beroepen op het citaatrecht van artikel 15a lid 1 Auteurswet 1912. De rechtbank gaat evenwel ook nog omstandig in op de vraag in hoeverre service providers zelf auteursrechtinbreuk plegen indien gebruikers van hun diensten inbreukmakende documenten op het Internet zetten. 'De rechtbank stelt voorop dat de activiteiten van de service providers waar het in deze zaak om gaat zijn beperkt tot het doorgeven van informatie van en/of aan haar gebruikers en de opslag van die informatie. De service providers selecteren de informatie niet en bewerken haar evenmin. Zij verschaffen slechts de technische faciliteiten teneinde openbaarmaking door anderen mogelijk te maken. Met haar president (in diens kort geding-vonnis van 12 maart 1996) is de rechtbank van oordeel dat de service providers onder deze omstandigheden niet zelf openbaar maken maar slechts gelegenheid geven tot openbaarmaking.' Ook het oordeel dat er situaties kunnen zijn waarin wel aansprakelijkheid van de service provider zou kunnen worden aangenomen, wordt door de rechtbank bevestigd: '... dat de service provider die ervan in kennis wordt gesteld dat een gebruiker van zijn diensten op diens homepage auteursrechtinbreuk pleegt of anderszins onrechtmatig handelt, terwijl aan de juistheid van die kennisgeving in redelijkheid niet valt te twijfelen, zelf onrechtmatig handelt indien hij aldan niet ingrijpt.'

Naast openbaarmaking is een tweede aspect van eventuele auteursrechtinbreuk, dat in deze uitspraak ook aan de orde komt, de vraag of de activiteiten van service providers wellicht een auteursrechtelijk relevante verveelvoudiging inhouden. Deze vraag ziet op het gegeven dat het inzien van bestanden op Internet in feite wordt mogelijk gemaakt doordat de bestanden steeds worden gekopieerd. Er wordt een verveelvoudiging van het werk opgeslagen op de betreffende homepage, welke opslagcapaciteit door de provider ter beschikking kan zijn gesteld, maar ook bij de opvraging en het 'transport' van het materiaal worden - tijdelijke - verveelvoudigingen geproduceerd. Over deze, aan de informatietechniek inherente verveelvoudigingen is al jaren veel te doen.

7. De elektronische kopie

Digitale opslag van informatie heeft de toegankelijkheid van die informatie ongekend doen toenemen. Digitale informatie kan zeer snel en bovendien perfect worden gekopieerd. Er is eigenlijk geen onderscheid meer tussen het 'origineel' en de gekopieerde exemplaren. Dit gegeven, gevoegd bij de huidige telecommunicatiemogelijkheden van Internet, maakt wereldwijde verspreiding van informatie uiterst eenvoudig. Dommering spreekt in dit verband over een 'elektronische vergiet'. Los van de aaneenschakeling van vastleggingen is ook de weergave van de informatie op het beeldscherm van de internetsurfer alleen maar mogelijk doordat het bestand in het werkgeheugen van diens computer wordt opgeslagen. Of, zoals Hugenholtz het formuleert: 'vrijwel iedere verzending, transport, ontvangst en gebruik van informatie in een digitaal netwerk gaat met enige vorm van tijdelijke opslag gepaard. Cruciale vraag: is deze tijdelijke opslag een auteursrechtelijk relevante verveelvoudiging?'²¹ Door de industrie zijn, in een poging de kwetsbaarheid voor auteursrechtinbreuken zoveel mogelijk in te dammen, tot heden succesvolle lobby's ingezet, teneinde deze tijdelijke kopieën onder de werking van het auteursrechtelijke reproductie-recht te brengen.

De Europese Commissie stelt in haar Groenboek over het auteursrecht en de naburige rechten in de informatiemaatschappij²² dat met betrekking tot de omschrijving van het begrip reproductie in een digitale omgeving een communautair antwoord noodzakelijk is. Dit antwoord zou gebaseerd moeten zijn op de oplossingen die in de richtlijn softwarebescherming zijn aangedragen²³. De Raad van Ministers van de Europese Unie heeft zich bij het opstellen van deze richtlijn laten leiden door een door de techniek bepaalde invulling van het verveelvoudigingsbegrip. Artikel 4 sub a van de richtlijn bepaalt dat onder de exclusieve rechten van de rechthebbende valt *'de permanente of tijdelijke reproductie voor een deel of het geheel van een computerprogramma, ongeacht op welke wijze en in welke vorm'*. De softwarerichtlijn is per 1 september 1994 in de Auteurswet 1912 geïmplementeerd²⁴. Artikel 45i bepaalt dat onder het verveelvoudigen mede wordt verstaan 'het laden, het in beeld brengen, de uitvoering, de transmissie of de opslag, voor zover voor deze handelingen het verveelvoudigen van het werk noodzakelijk is'. Dit betekent dat de toestemming van de auteursrechthebbende zich mede is gaan uitstrekken tot 'gebruik'²⁵. Het beginsel van het eigen vrije gebruik is verlaten. Evenals in de softwarerichtlijn heeft de Europese wetgever in de databankrichtlijn²⁶ bepaald dat tot de exploitatierechten eveneens behoort een exclusief recht van 'permanente of tijdelijke reproductie'. Hugenholtz meent dat het herleven van het verbodsrecht ten aanzien van de privé-kopie op gespannen voet staat met de communicatie- en ontvangstvrijheid die tot op heden kenmerkend is voor Internet²⁷. Visser merkt op dat ook de bescherming van de persoonlijke levenssfeer hier in het

geding is, aangezien een verbodsrecht dat zich uitstrekt tot de inhoud van de harde schijf van iedere burger moeilijk te rijmen valt met artikel 8 EVRM²⁸.

In het op 25 mei 1999 door de Commissie ingediende Gewijzigd voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij²⁹ lijkt de Commissie wat meer afstand te nemen van deze op de techniek gebaseerde opvatting ten aanzien van de tijdelijke kopie. Weliswaar wordt in artikel 2 van het voorstel inzake het reproductierecht nog steeds gesproken over 'de directe of indirecte, tijdelijke of duurzame, volledige of gedeeltelijke reproductie', in artikel 5 worden hiervan uitgezonderd 'tijdelijke reproductiehandelingen, zoals voorbijgaande en bijkomende reproductiehandelingen die een integrerend en onmisbaar onderdeel vormen van een technisch procédé met inbegrip van diegene die het doelmatig functioneren van transmissiesystemen bevorderen, dat wordt toegepast met als enig doel een gebruik van een werk of een andere zaak mogelijk te maken, en die geen zelfstandige economische betekenis bezitten. De Haagse rechtbank oordeelt in de Scientology-zaak dan ook, met verwijzing naar het gewijzigd voorstel, dat de activiteiten van de service providers ook niet een auteursrechtelijk relevante verveelvoudiging inhouden. 'Het gaat hier om door de technologie gedicteerde reproducties die ontstaan niet zozeer als gevolg van een handeling van de service provider als wel van de houder van een homepage of de consument die thuis informatie opvraagt.'

9. Hyperlinks, browsing en caching

Voor de Haagse Rechtbank was voor de vraag of de activiteiten van service providers wellicht een auteursrechtelijk relevante verveelvoudiging inhouden, niet van belang of de informatie toegankelijk is via een 'internet-adres' dan wel via een hyperlink (een vanuit een homepage 'aanklikbare' elektronische doorverwijzing). Volgens het persbericht dat XS4ALL - een van de gedaagden in de Scientology-zaak - op 9 juni heeft uitgegeven, zou dit betekenen dat providers die kennis dragen van eventuele hyperlinks naar materiaal dat auteursrechtinbreuk maakt, tegen deze hyperlinks moeten optreden. Deze interpretatie lijkt te ver te gaan. Eerder mag uit deze uitspraak worden afgeleid dat providers verplicht zijn op te treden tegen de aanbieder van de homepage waarop het auteursrechtinbreukmakende materiaal wordt gepubliceerd en waarnaar de hyperlink verwijst.

Nu uit de uitspraak van de rechtbank en het richtlijnvoorstel duidelijk is geworden dat browsen ('bladeren') op Internet niet als een auteursrechtelijk relevante handeling is aan te merken, resteert nog de vraag of datzelfde gezegd kan worden over caching. Caching is een technische voorziening die internet-

providers hanteren om veelvuldig opgevraagde pagina's gedurende enige tijd (enkele uren, of één of enkele dagen) op de eigen computer beschikbaar te houden. Het voordeel daarvan is de grote tijdwinst voor internetgebruikers bij het opvragen van de betreffende pagina's. De vraag hier is nu of caching mag worden begrepen onder de uitzondering van artikel 5 lid 1 van het richtlijnvoorstel, of caching een 'onmisbaar onderdeel' vormt van een technisch procédé en geen zelfstandige economische betekenis bezit. Voor het functioneren van Internet is caching natuurlijk niet onmisbaar. Internet zou wel veel trager worden. Aan caching kan bovendien economische betekenis niet worden ontzegd, omdat providers die veel pagina's cachen, of veel pagina's met betrekking tot bepaalde onderwerpen, daardoor voor sommige gebruikers aantrekkelijker worden. Ten opzichte van de informatieaanbieder evenwel kan niet worden volgehouden dat hij daar schade door zou lijden, immers hij is juist gebaat bij exposure van de door hem op het net geplaatste informatie. De beperking in het vierde lid van artikel 5, dat geen afbreuk mag worden gedaan aan de normale exploitatie van het werk, is hier dan ook niet aan de orde. Ten overvloede valt in de considerans in overweging 23 te lezen dat 'onder deze voorwaarden ook 'caching' en 'browsing' onder deze uitzondering (van artikel 5) vallen'. Helemaal zonder risico is de provider echter niet. Hij dient er wel voor te waken dat zijn cache-geheugen tijdig wordt verversd, om niet het risico te lopen verouderde informatie door te geven. In dat geval loopt hij het risico zowel door de informatieaanbieder als door de informatievrager aansprakelijk gesteld te worden (zie paragraaf 10 hierna).

Op 18 augustus 1998 heeft de Commissie Auteursrecht haar advies uitgebracht over auteursrecht, naburige rechten en nieuwe media. In de Brief van de minister van justitie en de staatssecretaris van onderwijs, cultuur en wetenschappen³⁰ wordt, uitgaande van het advies van de commissie, een aantal beleidsuitgangspunten geformuleerd die de basis kunnen vormen bij de standpuntbepaling bij toekomstige wet- en regelgeving, zowel nationaal, Europees als mondiaal. In uitgangspunt 3. meent de minister dat het aan de rechter is om de inhoud van het verveelvoudigings- en het openbaarmakingsrecht aan de hand van de in beginsel open en flexibele begrippen als verveelvoudiging en openbaarmaking op normatieve wijze nader in te vullen. Ten aanzien van de tijdelijke kopie wordt in uitgangspunt 4. opgemerkt dat een benadering waarin ook voor communicatie noodzakelijke puur technische kopieën onder het verveelvoudigingsrecht vallen onnodig en onwenselijk is. De benadering die is gekozen in het richtlijnvoorstel van de Europese Commissie (artikel 5), wordt overwogen. In uitgangspunt 10. valt voorts te lezen dat leveranciers van telecommunicatiediensten aanspraak hebben op een zekere vrijheid om materiaal over hun verbindingen te transporteren. Rechthebbenden hebben geen recht op een vergoeding als de activiteit slechts bestaat als doorgiftemedium en van enige inhoudelijke bemoeienis geen sprake is. De

aansprakelijkheid van de providers dient te worden geregeld in het horizontale kader van het richtlijnvoorstel juridische aspecten van de elektronische handel. Deze uitgangspunten verdienen instemming. Gedragingen op Internet laten zich heel wel beschrijven in termen van verveelvoudigen en openbaarmaken, zoals onder meer blijkt uit de uitspraak in de Scientology-zaak. Indien deze begrippen voorts niet louter technisch worden opgevat, maar worden afgezet tegen het criterium of zij auteursrechtelijk relevant zijn, blijkt de dienstverlening van providers moeiteloos te passen binnen het huidig auteursrechtelijk kader. Voor eventuele aanvullende vergoedingen voor de auteursrechthebbenden is voor wat betreft de enkele transportdienst en daaraan gerelateerde diensten geen plaats.

10. Elektronische handel en de aansprakelijkheid van providers

Een nadere afbakening van de aansprakelijkheid van providers wordt gegeven in het op 23 december 1998 door de Commissie ingediende Voorstel voor een richtlijn van het Europese Parlement en de Raad betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt³¹. In afdeling 4, aansprakelijkheid van tussenpersonen, bepaalt artikel 12 dat de aansprakelijkheid van de transmissie- dienstverlener zich, behalve in het kader van een vordering tot staking, niet tot de doorgegeven informatie afkomstig van de afnemer van de dienst uitstrekt, op voorwaarde dat hij a) niet degene is van wie de informatie stamt, b) de afnemer van de doorgegeven informatie niet heeft geselecteerd, en c) de doorgegeven informatie niet heeft geselecteerd en gewijzigd. Artikel 13 gaat specifiek in op caching, en daarin wordt bepaald dat de aansprakelijkheid van de dienstverlener zich niet mag uitstrekken tot de automatische, tussentijdse en tijdelijke opslag van de informatie, wanneer dit uitsluitend ten doel heeft de latere transmissie van de informatie op verzoek van andere afnemers van de dienst doeltreffender te maken, op voorwaarde dat a) de dienstverlener de informatie niet wijzigt, b) de dienstverlener de toegangsvoorwaarden voor de informatie naleeft, c) de dienstverlener de regels naleeft betreffende de bijwerking van de informatie, die in overeenstemming met de bedrijfstaknormen zijn aangegeven, d) de dienstverlener niet de aan de bedrijfstaknormen beantwoordende technologie voor het verkrijgen van gegevens over het gebruik van de informatie wijzigt, en e) de dienstverlener prompt handelt om de informatie te verwijderen of de toegang ertoe onmogelijk te maken zodra hij daadwerkelijk kennis heeft genomen van een van de volgende feiten: i) de informatie is van de plaats waar deze zich oorspronkelijk in het net bevond, verwijderd, ii) de toegang tot de informatie is onmogelijk gemaakt, iii) een bevoegde autoriteit heeft de verwijdering van de informatie gelast of de toegang daartoe verboden.

Ten aanzien van 'host'-diensten bepaalt artikel 14 dat de aansprakelijk van dienstverleners zich niet uitstrekt tot de op verzoek van een afnemer van de

dienst bij de dienstverlener opgeslagen informatie, op voorwaarde dat a) de dienstverlener niet daadwerkelijk kennis ervan heeft dat de activiteit onwettig is en, wanneer het een schadevergoedingsvordering betreft, geen kennis heeft van de feiten of omstandigheden waaruit het onwettige karakter van de activiteiten duidelijk blijkt, of b) de dienstverlener, zodra hij bovenbedoelde kennis bezit, prompt handelt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken. Artikel 15 tenslotte bepaalt dat op de dienstverleners geen algemene verplichting mag worden gelegd toezicht te houden op de informatie die zij doorgeven of opslaan, noch om actief naar feiten of omstandigheden die op onwettige activiteiten duiden, te gaan zoeken.

11. Slot

De juridische problemen met betrekking tot Internet worden veroorzaakt door de nieuwe functionaliteit telecommunicatie. De nieuwe functionaliteit komt beschikbaar hoewel de kosten een veelvoud bedragen van verwerken en bewaren, maar de kosten van alles nemen structureel af. Belangrijk bij de juridische problemen met name voor de uiteindelijke beperkingen van mogelijke juridische oplossingen zijn de mogelijkheden om met behulp van cryptografische technieken vrijwel perfecte vertrouwelijkheid, identificatie en authenticiteit te bereiken tussen twee partijen, maar de perfectie wordt snel minder als het aantal betrokken partijen stijgt.

De populariteit van Internet is pas van de laatste jaren. Er is nog niet veel ervaring mee opgedaan; ecommerce en informatiehandel over Internet staan nog in de kinderschoenen. Toch ligt er al een groot aantal wetgevende initiatieven die, vanwege het grensoverschrijdend karakter van Internet, met name binnen EU-verband zijn en worden ondernomen. Een zich verder ontwikkelend proces van internationale afstemming en harmonisatie is te verwachten. Internetcommunicatie is voor onder meer de economie van grote betekenis. Het is daarom van belang dat duidelijkheid wordt geschapen omtrent de aansprakelijkheid van providers voor hun aandeel in deze communicatie. Zonder te menen dat providers daarvan geheel vrij zouden moeten zijn, moet die aansprakelijkheid niet te ruim worden geformuleerd. Dat zou een onderschatting zijn van de door de technologie geboden mogelijkheden, zowel om rechtsinbreuken te maken, als om deze te voorkomen. De belangrijkste verantwoordelijkheid ligt derhalve bij de internetgebruikers. Het zou daarom wenselijk zijn dat de voorstellen enige afstand creëren van directe inmenging in de organisatie van het internetverkeer. Daarbij moet worden opgemerkt, dat in het algemeen enige terughoudendheid voor wettelijke bepalingen ingevolge het gebruik van informatietechnologie op zijn plaats is. De echte vraagstukken achter de juridische vraagstukken, die veroorzaakt worden door het gebruik van informatietechnologie, zijn immers met juridische bepalingen niet weg te nemen.

Noten:

- ¹ De algemene vergadering van de Nederlandse Juristen-Vereeniging in 1998 stond eveneens in het teken van Recht en Internet. De preadviezen van prof.dr. A.W. Koers, prof.mr. M.V. Polak, prof.mr. Y. Buruma en mr. P.B. Hugenholtz (W.E.J. Tjeenk Willink, Deventer, 1998) worden besproken in het Nederlands Juristenblad 1998 nr. 23. Een Internet special was reeds eerder verschenen in 1996, nr. 41.
- ² Zie voor een uitgebreid overzicht: A.-M. Kemna en A. Tuinder, *'Regulering van encryptie'*, ITeR 3, Samsom Bedrijfsinformatie, 1996.
- ³ Een multilaterale organisatie die de export van wapens wil beperken, waarbij 33 landen zijn aangesloten.
- ⁴ Rapport *'Informatietechniek en Strafrecht'*, Commissie Computercriminaliteit, Staatsuitgeverij 1987; Wet Computercriminaliteit, i.w.t 1 april 1993. Zie voor kritiek op de benaderingswijze van de commissie en de voorstellen bij voorbeeld het preadvies van de werkgroep van de Nederlandse Vereniging voor Informatica en Recht 1987.
- ⁵ Zie voor een uitvoerige bespreking van het belangenconflict tussen informatiebeveiliging en opsporing: B.J. Koops, *'The Crypto Controversy. A Key Conflict in the Information Society'*, (diss.), Kluwer 1998.
- ⁶ Zie bij voorbeeld R.V. De Mulder: *Wetgeving maakt technologie tot veelkoppige draak'*, Nederlands Juristenblad 1993/39, pp. 1429 en 1430.
- ⁷ Zie bij voorbeeld H.W.K. Kaspersen, *'Aansprakelijkheid van Internet-providers'*, Computerrecht 1996/1; Prof.mr. Th.A. de Roos en mr. L.W. Wissink, *'Uitingsdelicten op het Internet en strafrechtelijke repressie'*, Nederlands Juristenblad 1996/41.
- ⁸ President Arrondissementsrechtbank 's-Gravenhage, 12 maart 1996, (*Scientology*), Computerrecht 1996/2 pp. 73-77, met noot D.W.F. Verkade; Informatierecht/AMI 1996/5, pp. 96-97, bevestigd in de bodemprocedure, 9 juni 1999 (nog niet gepubliceerd). Zie verder paragraaf 6. Privaatrechtelijke aspecten en de positie van de provider.
- ⁹ Zie Th.A. de Roos, *'Het concept-wetsvoorstel computercriminaliteit II'*, Computerrecht 1998/2. Voor een uitvoerig overzicht van uitingsdelicten en aansprakelijkheid op Internet, zie: Th. de Roos, G. Schuijt en L. Wissink, *'Smaad, laster, discriminatie en porno op het Internet'*, ITeR 3, Samsom Bedrijfsinformatie, 1996.
- ¹⁰ Kamerstukken II 1995/96, Aanh. 1582.
- ¹¹ Ten tijde van het schrijven van deze bijdrage was het vonnis nog niet gepubliceerd.
- ¹² Hoge Raad 9 maart 1999, NJ 1999 nr. 346.
- ¹³ Wet van 27 mei 1999 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Staatsblad 1999, nr. 245.
- ¹⁴ Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), Staatsblad 1998, nr. 610.
- ¹⁵ Het Besluit aftappen openbare telecommunicatienetwerken en -diensten van 10 november 1998 (Staatsblad 1998, nr. 642) geeft uitvoering aan de artikelen 13.1 en 13.2 ter zake van de regels voor aanbieders inzake de technische aftapbaarheid. De Tweede Kamer heeft een motie aangenomen (kamerstukken II 1997/98, 25 533, nr. 64) om providers gedurende een overgangperiode ontheffing te verlenen van deze verplichting.
- ¹⁶ Zie over de vertrouwelijkheid van email: R. Kaspersen, A. Hofman en J. Verbeek, *'Vertrouwelijkheid van e-mail'*, ITeR 13, Samsom Bedrijfsinformatie, 1999.
- ¹⁷ Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepalingen inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim, TK '96'97, 25 443.
- ¹⁸ Besluit van 23 februari 1999, houdende instelling van de Commissie 'Grondrechten in het digitale tijdperk', Staatsblad 1999 nr. 101.
- ¹⁹ Zie noot 8.

20 Arrondissementsrechtbank Rotterdam, 24 augustus 1995, (*Bridgesoft/Lenior*), Computerrecht
1996/5, met noot R.V. De Mulder.

21 P.B. Hugenholtz, *'Het auteursrecht, het internet en de informatiesnelweg'*, NJB 1995/14, p.515:
Zie ook: D.J.G. Visser, *'Auteursrecht op toegang'*, 's-Gravenhage 1997, p.61-82.

22 Groenboek van de Europese Commissie, *'Het Auteursrecht en de Naburige rechten in de
23 Informatiemaatschappij'*, Brussel, 19 juli 1995, COM(95)382.

24 Richtlijn 91/250/EEG van de Raad van 14 mei 1991 betreffende de rechtsbescherming van
computerprogramma's, Pb EG 1991 L 122/42.

25 Wet van 19 juli 1994, Stb. 1994, 521.

De nodeloze ingewikkeldheid van deze constructie, waarin het laden van het programma eerst
onder de werking van het reproductierecht wordt gebracht, blijkt uit de daaruit volgende
noodzaak vervolgens een uitzondering te maken ten behoeve van de 'rechtmatige gebruiker'
van het programma.

26 Richtlijn 96/9/EG van het Europese Parlement en de Raad van 27 maart 1996 betreffende de
rechtsbescherming van databanken, Pb EG 1996 L 77/20.

27 P.B. Hugenholtz, *'De Databankrichtlijn eindelijk aanvaard een zeer kritisch commentaar'*,
Computerrecht 1996/4, p.131-138.

28 D.J.G. Visser, *'Copyright exemptions old and new: learning from old media experiences'*, in:
The Future of Copyright in a Digital Environment, p.49-50.

29 PB C 180 van 25.6.1999.

30 10 mei 1999, TK '98'99, 26 538 nr. 1

31 COM(1998) 586 def.