COMPACT

TIJDSCHRIFT EDP-AUDITING

RECHT EN EDP-AUDIT

1996/4

Compact ®
Jaargang 23, nummer 4
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers RE
Drs. R.G.A. Fijneman RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Prof.dr. J.C. Arnbak
J.H. Buisman RA
Mr. P. van Dijken
Prof.mr. H. Franken
Dr. K.IJ. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning, Samsom Bedrijfsinformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 746
Fax : 0172 – 466 569
Vormgeving
Bureau Karakter, Delft
Opmaak
Sander Pinkse Boekproduktie, Amsterdam
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom Bedrijfsinformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij het redactiesecretariaat. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
Drs. Th.P.M. Brinkman

NOTU VAK
Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

"The first thing we do, let's kill all the lawyers".
William Shakespeare, *Henry VI* (Part II).

Dit is het juridisch nummer van Compact, door juristen, voor EDP-auditors.
Wat vindt de EDP-auditor van het recht, en wat van degene die zich hier dagelijks mee bezighoudt, de jurist? Ziet de EDP-auditor hem of haar als 'part of the problem' of juist als 'part of the solution'? Negen van de tien keer zal de EDP-auditor de eerste mogelijkheid noemen. Ten onrechte.

In Nederland is er bijvoorbeeld een discussie over het al of niet reguleren van encryptie en hoe dat zal moeten gebeuren. Is dat dan een taak voor de overheid of moet cryptografie geheel vrij worden gelaten? In het eerste artikel wordt nagegaan wat de belangen en voor- en nadelen van regulering zijn.

Een ander juridisch aspect van de EDP-audit-werkzaamheden komt naar voren bij het verwerven van opdrachten in de overheidsbranche, waar aanbestedingsprocedures gelden. Niet alleen grote infrastructurele projecten, maar ook de uitvoering van een automatiseringsproject bij de overheid zal volgens vastgestelde selectie- en gunningscriteria aan een bepaalde dienstverlener worden toegewezen. Het tweede artikel geeft een helder inzicht in de regels en richtlijnen die daarvoor gelden.

Over infrastructuur gesproken: met het afbreken van de monopoliepositie van de PTT's en het liberaliseren van de telecommunicatie-infrastructuur komt de problematiek van interconnectie duidelijk naar voren. Er zijn steeds meer spelers die hun telecommunicatiediensten tegelijkertijd over dezelfde netwerken willen aanbieden. Het derde artikel bespreekt de implementatiemogelijkheden en de juridische aspecten daarvan.

Vervolgens zijn er drie artikelen die ingaan op de juridische haken en ogen van gegevensverzamelingen. Commercieel gezien zijn databanken namelijk steeds belangrijker geworden. Daarmee neemt ook het belang van een goede juridische verankering van het gebruik ervan toe. Databanken worden beschermd door auteursrecht en per 1 januari 1998 wordt de bescherming nog uitgebreid. Anderzijds kunnen informatiesystemen registraties bevatten die onder de reikwijdte van de Wet persoonsregistraties vallen. Onderzocht is hoe de houders van registraties omgaan met de Wet persoonsregistraties die een wet voor 'buitenstaanders en ingewijden' blijkt te zijn. Inmiddels is men bezig de Wet persoonsregistraties aan te passen aan de Europese Privacyrichtlijn. Deze richtlijn heeft mogelijkerwijs verder gaande consequenties. In het artikel wordt aangegeven in hoeverre de privacyrichtlijn verschilt van de huidige Wet persoonsregistraties, en welke – voor de EDP-auditor belangrijke – implementatie-aspecten daaraan zijn verbonden.

Een ander hot item in IT-land is het Internet. Bedrijven gebruiken Internet steeds meer als een medium om in te adverteren en creëren hun eigen web-sites. De rol van de Internet-provider daarbij komt in de laatste twee artikelen uitvoerig aan de orde. Het eerste geeft een overzicht van de juridische gevolgen indien daarbij inbreuk wordt gemaakt op bijvoorbeeld een auteursrecht of als er onjuiste informatie wordt verstrekt. In het EDP-Auditorium wordt ten slotte aan de hand van de Scientology-zaak de jurisprudentie op het gebied van Internet-aansprakelijkheid doorgelicht.

Aan al deze aspecten ziet u duidelijk: het recht, u kunt er niet om heen. En de jurist kan als 'part of the solution' de EDP-auditor prima van dienst zijn.

Mw. mr. E. Wiersema
Mr. P.P.J.L. Enneking

Regulering van encryptietechnieken in westerse landen: pro en contra

Mw. A.K.I. Tuinder en
mw. mr. A.M.Ch. Kemna MBA

Aan de hand van de stand van zaken op het gebied van de encryptiewetgeving in westerse landen worden de voor- en tegenargumenten van regulering behandeld. De afweging tussen vertrouwelijkheid voor de gebruikers en toegankelijkheid voor de overheden komt hierbij duidelijk naar voren.

INLEIDING

Het versleutelen van informatie is sinds mensenheugenis in gebruik. De gebruiksmogelijkheden van citroensap en kaarsvet zijn menigeen bekend. Zo is er bijvoorbeeld de in citroensap geschreven tekst uit de *Poetica* van Aristoteles, welke de monnik Venantius van Salvemec fataal werd in het boek *De naam van de roos* van Umberto Eco. Geheimteksten, waarbij de leesbare informatie wordt versleuteld tot gecodeerde woorden of letterreeksen, hebben ook al een zeer lange geschiedenis; een zeer eenvoudige vorm van encryptie was bijvoorbeeld al de Caesar-substitutie, waarbij iedere letter van het alfabet door een vaste andere letter wordt vervangen. Een bekend voorbeeld dat deze vorm van encryptie gebruikt is de ENIGMA uit de Tweede Wereldoorlog. In de Tweede Wereldoorlog konden de nazi's door middel van deze machine geheime teksten produceren. De ENIGMA werkte volgens het rotor-principe, waarbij iedere letter op arbitraire wijze door een andere werd vervangen. De ENIGMA versleutelde teksten op deze wijze twee maal vijf keer. Toch werd de code door Poolse cryptografen gebroken gedurende de oorlog. De ENIGMA is wellicht ook de eerste vorm waarbij een min of meer programmeerbare machine werd gebruikt voor versleuteling. Pas de toepassing van binaire computers luidde een nieuw tijdperk in voor cryptografiegebruik. Door de binaire versleuteling in plaats van de op letterrepresentaties gebaseerde versleuteling te gebruiken, werd encryptie steeds sterker en moeilijker kraakbaar. Diezelfde computers bieden paradoxaal genoeg echter ook steeds meer en krachtiger mogelijkheden om 'zware' encryptie te kraken, zeker indien rekencapaciteit gecombineerd wordt, bijvoorbeeld binnen het Internet.

Encryptie werd voorheen, althans op grote schaal, met name in militaire en overheidskringen gebruikt. In commerciële zin wordt encryptie sinds een jaar of twintig toegepast. Ondanks deze (althans in een digitale omgeving) betrekkelijk lange periode is de 'hype' rondom encryptiegebruik pas van zeer recente datum. De reden zal liggen in het feit dat elektronische commercie en elektronische communicatie de laatste jaren meer en meer ingeburgerd raken, terwijl de private sector zich daarbij meer en meer bewust wordt van de risico's voor vertrouwelijkheid en betrouwbaarheid van de berichtgeving en daarmee van de digitale samenleving. Tegelijkertijd ontstaat de angst in de publieke (justitiële) sector dat er in een digitale geëncrypteerde samenleving geen orde meer te handhaven is, laat staan virtueel geboefte op te sporen zal zijn. Ziedaar de bron voor een discussie tussen overheid en private sector omtrent de wenselijkheid van encryptieregulering versus de (eveneens legitieme) behoefte aan privacy en betrouwbaarheid.

De Nederlandse overheid heeft in 1994 als één van de eerste een voorzichtige poging ondernomen te komen tot een vorm van regulering. Zij heeft in dat kader onder meer een aantal onderzoeken laten uitvoeren naar de diverse aspecten die afgewogen dienen te worden bij regulering, zoals daar zijn: de bedrijfseffecten van wetgeving voor Nederland en

de juridische wenselijkheid en mogelijkheid tot regulering van gebruik te komen. Het voorontwerp van wet heeft nooit de tekentafel verlaten, waarschijnlijk niet in de laatste plaats vanwege de onrust die het teweeg bracht in 'cyberland'. De (ook internationale) discussies in diverse media en newsgroups waren helaas niet altijd even accuraat: men had kennelijk niet steeds de tekst gelezen, laat staan de ontwerp-Memorie van Toelichting. Ondanks dit feit geeft de heftigheid van de meningsuitingen van voor- en tegenstanders aan, dat het hier een precair onderwerp betreft: encryptieregulering doet mensen denken aan Orwelliaanse taferelen, terwijl het voor de overheid veelal als een laatste en onontbeerlijke strohalm wordt gezien om grip te houden op de digitale communicatie van de georganiseerde misdaad.

ACHTERGRONDEN

Reden genoeg om aan dit onderwerp aandacht te besteden in het Nederlandse Nationaal Onderzoeksprogramma IT en Recht (ITeR), een samenwerkingsverband tussen NWO en de ministeries van Economische Zaken, Binnenlandse Zaken, Justitie, Onderwijs, Cultuur en Wetenschappen en Verkeer en Waterstaat. Dit onderzoeksprogramma heeft tot doel de Nederlandse wetgeving voor te bereiden op de IT-toekomst en zo nodig oude wetgeving te herzien. In de periode van september 1995 tot januari 1996 is in het kader van dit ITeR-programma een onderzoek uitgevoerd door KPMG EDP Auditors, ondersteund door de Afdeling Recht & Informatica van de Rijksuniversiteit Leiden, naar de stand van zaken ten aanzien van (voornemens tot) encryptiewetgeving in westerse landen. Het doel van dit onderzoek was een inventarisatie te geven van de (voorstellen tot) regulering van encryptie in westerse landen, bijna alle behorend tot de OESO-staten, alsmede een overzicht te geven van de voors en tegens zoals verwoord in de relevante literatuur.

Er moet een balans komen tussen veiligheid, opsporingsmogelijkheden, privacy en het recht op informatiebeveiliging.

In de huidige ontwikkelingen op het gebied van de communicatie zijn twee trends te bespeuren. De eerste trend laat zien dat mensen steeds vaker via elektronische weg met elkaar gaan communiceren. De tweede is dat communicatie meer en meer plaatsvindt in een open in plaats van in een gesloten elektronische omgeving. Het verschil zit in het feit dat partijen elkaar in een gesloten omgeving kennen en vertrouwen. In een open omgeving kent men elkaar nog niet en is men nog niet zeker hoe een wederpartij zich zal gedragen. Het vertrouwen is er nog niet. Een voorbeeld van zo'n open systeem is het Internet. Hierin kan een ieder participeren zonder dat vooraf bekend behoeft te zijn wat zijn of haar identiteit is.
Een open omgeving brengt enige bezwaren met zich mee. De belangrijkste is wel, dat de beveiliging van netwerken, computers en communicatie tegen inbreuken door onbevoegden sterk onder druk komt te staan. Inbreuken van buitenaf, door hackers of bedrijfsspionnen, kunnen enorme schade aanrichten. Informatie kan worden gewijzigd, gewist of gekopieerd en verhandeld. Daarnaast is het volgens steeds meer partijen wenselijk dat de identiteit van de wederpartij en de integriteit van elektronische communicatie kunnen worden gewaarborgd in zo'n open omgeving.

Encryptie

Algemeen wordt aangenomen, dat encryptietechnieken voor deze problemen een oplossing kunnen bieden. Door middel van het op de juiste wijze versleutelen van berichten kan de exclusiviteit in hoge mate gewaarborgd worden, terwijl bepaalde vormen van encryptiemogelijkheden dienst kunnen doen als elektronische handtekening. Hiermee kunnen identiteit en integriteit (daaronder begrepen authenticiteit) worden gewaarborgd.

Deze mogelijkheden, toegepast door burgers en bedrijfsleven, stellen de overheid echter voor een probleem. In haar taak te zorgen voor de staatsveiligheid en het opsporen van criminele activiteiten wordt ze nu gestoord door versleutelingstoepassingen. Justitie ziet haar politietaak in de knel komen en de mogelijkheden tot effectieve opsporing drastisch verminderen. De regering zag een oplossing in een verbod van encryptietechnieken ten behoeve van vertrouwelijkheid, met daaraan gekoppeld een vergunningenstelsel met sleuteldeponering bij een derde onafhankelijke partij.
Dit voorstel heeft de kamer niet gehaald, maar is wel aanleiding geweest voor de zogenaamde crypto-discussie in Nederland. De vraag of het gebruik van encryptietechnieken al dan niet gereguleerd moet worden, blijkt in de politiek en het bedrijfsleven zeer gevoelig te liggen.

Argumenten van privacy, algemene veiligheid, het nut van digitale handtekeningen en essentialiteit van afluisterpraktijken worden door de verschillende partijen vaak gebezigd. Het is duidelijk dat er een balans moet worden gevonden tussen nationale veiligheid, opsporingsmogelijkheden, individuele privacy en het recht op informatiebeveiliging.

Onderzoeksopzet

Zoals eerder aangegeven was het doel van het in dit artikel beschreven onderzoek inzicht te geven in de vraag of er in westerse landen wetgeving bestaat (of voornemens daartoe bestaan) op het gebied van het gebruik, het voorhanden hebben, het verhandelen dan wel het ontwikkelen van cryptografiemethoden. Tevens is een inventarisatie gemaakt van voor- en nadelen van dergelijke wetgeving zoals beschreven in de westerse literatuur.

Gepoogd is deze problematiek vanuit verschillende gezichtspunten te benaderen: vanuit de veiligheid van de staat, vanuit een effectieve opsporing van criminele gedragingen, vanuit de bescherming van bedrijfs- en persoonsgegevens en vanuit het oogpunt van facilitering van een betrouwbare en integere commerciële en niet-commerciële elektronische communicatie.

RESULTATEN ONDERZOEK

Specifieke wet- en regelgeving op het gebied van cryptografie blijkt in veel westerse landen (nog) niet aanwezig te zijn. Inmiddels is in een aantal landen wel de vraag aan de orde gesteld hoe eventueel het encryptieprobleem (belangen van justitie versus burgers/bedrijfsleven) aangepakt dient te worden. Voorgestelde oplossingen variëren van in het geheel niets doen, het instellen van een verbod, licentiëren en sleuteldeponering tot het beperkt toelaten van zwakke encryptievormen. Bovendien vraagt men zich af of eventuele regulering op nationaal dan wel op Europees of mondiaal niveau aangepakt dient te worden.
Uit de eerder genoemde bedrijfseffectenrapportage van 1994 kwam al naar voren dat wettelijke regelingen op nationaal niveau tot grote bezwaren leiden zolang die regels niet tevens op mondiaal niveau gelden. Het verhuizen van bedrijven kan één van de gevolgen zijn van een ondoordachte stap in de regelgeving.

Frankrijk, het enige land met expliciete beperkende cryptografiewetgeving, laat zien dat bestaande regelgeving in de praktijk lastig uit te voeren is en bovendien tot grote vertragingen in de handel kan leiden. Het verkrijgen van de benodigde licentie voor gebruik, fabriceren, uitvoer etc. laat soms maanden tot een jaar op zich wachten. Het wetgevingsprobleem blijkt dus tevens een handhavingsprobleem in te houden.

Exportregulering

De beantwoording van de vraag of er specifieke regelingen op het gebied van gebruik van cryptografische technieken dienen te komen heeft nog een andere dimensie. Sinds lange tijd worden encryptiemethoden binnen het COCOM[1]-verdrag tot de categorie 'strategische wapens' gerekend. Daarmee vallen deze technieken onder de strenge exportbeperkingen die gelden binnen het verdragsgebied. Rond februari 1991 heeft de COCOM besloten de export van cryptografiesoftware die is bestemd voor het grote publiek, toe te laten. Encryptieproducten zijn namelijk als 'dual-use'-producten gekwalificeerd (ofwel geen wapentuig). Toch is in de meeste landen de regeling nog gebaseerd op het classificeren van cryptografie en cryptografische toepassingen als oorlogstuig/wapentuig. Het resultaat daarvan is dat dergelijke producten even strikt kunnen worden gecontroleerd als het 'echte wapentuig'. Defensie en staatsveiligheid zijn dan de beslissende belangen bij de besluitvorming omtrent het al dan niet toelaten van export (en soms ook het gebruik) van cryptografie in zowel de private als de publieke sector. Over het algemeen is de export van een Europees land naar een COCOM-land en/of andere West-Europese landen geen probleem, mits de eindbestemming eenduidig bekend is. Ondanks dat het COCOM-verdrag begin 1994 is afgelopen, volgen de meeste landen nog steeds zijn oude regels totdat het nieuwe verdrag tot stand is gekomen.

Nationale regelingen

Gebleken is dat er ook overigens recent niet veel verandering is te zien op het gebied van encryptiewetgeving in de diverse onderzochte landen.

Zoals hiervoor genoemd hanteert Frankrijk specifieke wetgeving die het gebruik van encryptie in verband met telecommunicatie direct reguleert. In het Franse bestel is verplichte sleuteldeponering voor zover bekend geen vereiste, doch bij het verzoeken om een vergunning of een toelating dient wel informatie aan een specifiek informatiebeveiligings- en toezichthoudend overheidsorgaan (de SCSSI[2]) te worden verschaft omtrent de mogelijkheden die er zijn voor justitie om de encryptie in voorkomende, toegestane gevallen op te heffen. Voorts houdt toelating/vergunning een verplichting in aangifte te doen van inbreuken op de encryptiefaciliteit en het SCSSI hierover informatie te verschaffen.

In Portugal is encryptie alleen geregeld in de vorm van specifieke wetgeving op het gebied van vertrouwelijke overheidsinformatie die verzonden wordt over telecommunicatielijnen. De wet geeft aan welke soorten van encryptie in bepaalde gevallen gebruikt kunnen worden.

In Noorwegen wordt de introductie van wetgeving overwogen, doch juist om het gebruik van encryptie voor specifieke toepassingen te faciliteren. Het betreft een voorstel van wet in verband met informatiebeveiliging en een wetsvoorstel voor regionale medische datacentres waarbij de gegevens onder een op cryptografische wijze berekend pseudoniem worden vastgelegd.

In Denemarken is eveneens op andere wijze aandacht besteed aan cryptografie, namelijk in het onderzoeken van de veiligheids- en professionaliteitseisen die te stellen zijn aan toekomstige key centres (en het opzetten van een overkoepelend, certificerend orgaan, het CCA) indien met name asymmetrische key-services-aanbieders de Deense markt gaan betreden. De regulering van encryptie in de zin van verplichte sleuteldeponering waardoor toegang mogelijk wordt tot de communicatie wordt in Denemarken expliciet afgewezen als een risico voor de privacy en het briefgeheim.

In Italië is het onderwerp uitsluitend geregeld in verband met de blijvende toegankelijkheid van administratieve gegevens voor de fiscus. Degene die zijn boekhouding en administratie of andere geautomatiseerde gegevens encrypt, dient informatie beschikbaar te hebben omtrent de cryptogra-

1. Coördinating Committee for Multilateral Export Controls, bestaande uit Japan, Australië en alle NAVO-leden exclusief IJsland. De Commissie werd in 1949 opgericht voor het toezicht op de export van apparatuur die zou kunnen worden gebruikt voor (communistische) strategische (militaire, terroristische) doeleinden.
2. Service Central de la Securité des Systèmes d'Information.

fische toepassing, bijbehorende uitleg en procedures. In wezen is dit een concretisering van de ook in Nederland geldende verplichting aan de fiscus gedurende de wettelijke bewaartermijn toegang en inzage te kunnen verstrekken in administratie en ondersteunende gegevens.

In de Verenigde Staten is encryptie nog steeds onderwerp van strenge exportregulering. Die regulering wordt nogal eens omzeild; bijvoorbeeld met de op RSA gebaseerde en aan het Amerikaanse MIT ontwikkelde PGP-encryptietoepassing die veel op het Internet wordt gebruikt: deze is internationaal inmiddels gewoon verkrijgbaar. Mocht men de Verenigde Staten binnen willen komen met PGP-gerelateerde toepassingen op de laptop, dan zou dit echter wel eens problemen kunnen opleveren.

Enige tijd geleden is er echter een initiatief op gang gekomen met betrekking tot de zogenaamde Clipper/Skipjack-encryptiechip. Deze chip, die in eerste instantie voor overheidsgebruik is ontwikkeld maar ook door de private sector gebruikt kan worden, gaat gepaard met het deponeren van sleutels bij twee bewarende instanties ('key escrowing'). Het initiatief is volgens de Amerikaanse regering niet gebaseerd op regulering van encryptiegebruik als zodanig, maar op het bieden van een vertrouwelijkheidstoepassing aan het publiek, een standaard, die tegelijkertijd justitie de mogelijkheid verschaft de encryptie op te heffen in toegestane gevallen. In september 1995 heeft de regering-Clinton in dat kader ook een nieuw beleid ten aanzien van cryptografie afgekondigd. Dit beleid houdt in dat de desbetreffende exportregelingen worden versoepeld, doch alleen ten aanzien van encryptiemiddelen waarvan de encryptiesleutels bekend zijn bij een goedgekeurde derde sleutelbeherende partij (een zogenaamde Trusted Third Party of TTP) en waarvan de hardware alleen berichten kan decrypten die afkomstig zijn van eenzelfde soort apparaat, waarvan de sleutels ook bij een TTP bekend zijn (zoals de genoemde Skipjack). De Skipjack wordt voor de particuliere sector op vrijwillige basis voor gebruik aangeboden. De vrees bestaat echter in de Verenigde Staten dat in plaats van gebruik op vrijwillige basis de gebruikers in de praktijk wel zullen worden gedwongen de chip te gebruiken willen ze kunnen communiceren met de overheid en anderen die gebruik maken van deze hardware (met de desbetreffende soort encryptiechip). De hardware waarvan de Skipjack onderdeel is behoort namelijk door dit nieuwe beleid geen andere geëncrypte berichten te accepteren en te versleutelen dan berichten die zijn versleuteld met een Skipjack. Het privacy-argument en de verminderde bruikbaarheid voor authenticatie zijn de belangrijkste redenen voor oppositie.
Telecommunicatiewetgeving verbiedt in de meeste gevallen niet het gebruik van encryptietechnieken voor telecommunicatie als zodanig. Met behulp van dergelijke wetgeving kan wel in veel gevallen indirect invloed op encryptiegebruik worden uitgeoefend door technische en administratieve eisen te stellen aan telecommunicatierandapparatuur die gekoppeld moet of gaat worden aan de publieke infrastructuur. Ook de Nederlandse wetgeving geeft deze mogelijkheid. Daarbij is de ratio van de wetgeving veelal echter niet gelegen in het faciliteren van opsporing binnen de telecommunicatie, maar veeleer in continuïteit en betrouwbaarheid van de telecommunicatie.

Het bereiken van een gezamenlijke regeling is nog toekomstmuziek.

Inmiddels zijn er in enkele landen (Duitsland, Japan, Nederland, Verenigde Staten) wel discussies ontstaan over de vraag hoe cryptografie gereguleerd moet worden, en inventariseert men (Finland, Duitsland, Nederland) de belangen die spelen rond deze problematiek. Naar welke kant de balans zal doorslaan is nog niet bekend, maar voor die landen die al wel ervaring hebben op dit gebied (Frankrijk, Verenigde Staten, Nederland) blijkt de handhaving en controle grote problemen op te leveren. Pasklare oplossingen zijn hier nog steeds niet voor gevonden. In de meeste landen vormt de materie aangaande cryptografiewetgeving nog steeds geen groot politiek probleem, en hebben andere zaken een hogere prioriteit.

Internationaal versus nationaal

Wat voor regelgeving er ook mag komen, het wordt steeds meer duidelijk dat de voorkeur uitgaat naar internationale initiatieven. De materie van telecommunicatie en encryptie heeft naar haar aard een sterk internationale dimensie waardoor ze uitstijgt boven het niveau van een nationale regelgeving. Mocht ieder land toch besluiten tot eigen wetgeving, dan zal dit kunnen uitlopen op een onhandelbare situatie. Wetgeving in een beperkt aantal landen en verschillende wetgeving per land zullen kunnen zorgen voor een verhuizing van een aantal bedrijven naar het meest gunstige klimaat. 'Land-shoppen' zou eveneens voor de thuisbasis van criminele organisaties kunnen gelden, hetgeen de handhaving van wetgeving wederom bemoeilijkt.

Mogelijk ook dat een aantal bedrijven encryptiebeperkingsregulering zal negeren. Dit komt omdat voor de meeste bedrijven exclusiviteit en authenticiteit belangrijke aspecten van handelscommunicatie zijn. Zonder deze mogelijkheden kan men niet handelen in een open systeem, waar iedereen elkaars communicatie kan volgen en eventueel vervalsen.

Geëncrypte communicatie tussen verschillende landen zal bij diversiteit in nationale wetgeving mogelijk moeten voldoen aan verschillende regels die elkaar kunnen tegenspreken. Deze regels moeten dan alsnog op elkaar worden afgestemd. Het zal praktischer zijn voor elk land dezelfde regels te hanteren zodat een standaard bereikt kan worden. Deze afstemming tot een Europese wet of regelgeving zal zeker de nodige moeite kosten, daar in vele landen deze materie ietwat gevoelig ligt, of zoals in Frankrijk als een strikt nationale aangele-

genheid wordt beschouwd. Hoewel er momenteel wel enige belangwekkende initiatieven in de sfeer van aanbevelingen worden ontplooid door de Raad van Europa en de Europese Commissie, is het bereiken van een gezamenlijke regeling nog toekomstmuziek.

Voor- en tegenstanders van regulering

Overheden en justitie die zich met de encryptieproblematiek bezighouden zijn over het algemeen sterke voorstanders van encryptieregulering. Zij beargumenteren deze positie door te wijzen op de taak van overheid en justitie om te zorgen voor de openbare orde, nationale veiligheid en bestrijding van de misdaad. De mogelijkheid tot aftappen van spraak- en datacommunicatie zou bij de opsporing een essentieel onderdeel vormen.

Tegen regulering zijn veelal het bedrijfsleven en particulieren. Men is bang dat regulering van cryptografie de privacy zal schaden. Bovendien zal het bedrijfsleven grote hinder ondervinden doordat bedrijven wellicht de beste mogelijkheden tot authenticatie en bewaking van exclusiviteit bij elektronische communicatie ontnomen worden dan wel dat zij hierin toch ernstig beperkt worden.

Van de mogelijkheden: vrijlaten, regulering en/of sleuteldeponering wordt het verbod op encryptie in de huidige discussie wel als het minst nuttige alternatief gezien. De mogelijkheden van digitale netwerken zullen mogelijk niet tot hun volle potentieel benut worden als er geen gelegenheid wordt geboden enige privacy, vertrouwelijkheid en authenticatie te kunnen waarborgen.
Het volkomen vrijlaten van cryptografie is het andere uiterste. Dit alternatief is zeer gunstig voor de privacy van burgers en bedrijfsleven. Men behoudt zo optimaal de mogelijkheid om bijvoorbeeld door middel van public key cryptografie de authenticatiemethode te bepalen en exclusiviteit te waarborgen. Bovendien biedt het gelegenheid aan het bedrijfsleven de encryptiemarkt (verder) te onderzoeken en te ontwikkelen. Op die manier ontstaan voor elke behoefte op maat gesneden encryptiemogelijkheden en vormen van beveiliging. Voor justitie is dit uit het oogpunt van controlemogelijkheden uiteraard een zeer moeilijke situatie.

Het handhaven en controleren van ontworpen regelgeving blijft echter eveneens een moeilijke zaak en ook het bestrijden van criminaliteit wordt er waarschijnlijk niet eenvoudiger door. Daar de hoeveelheid elektronisch informatieverkeer steeds omvangrijker wordt, zal binnen niet al te lange tijd het aantal berichten zo groot zijn dat een geëncrypt bericht nauwelijks meer te traceren valt. Criminele organisaties zullen bovendien manieren trachten te vinden om toch langs versleutelde weg hun informatie te versturen. De computerkracht benodigd voor het kraken van een sleutel is bovendien niet gering en het kraken zelf kost hoe dan ook veel tijd.

Van veel landen is over de keuze van een goed alternatief geen (actuele) literatuur bekend. Dit is vaak inherent aan het feit dat er geen wetgeving is en er soms ook geen specifiek nationaal gerichte discussie plaatsvindt. De meeste beschikbare literatuur handelt over de techniek van encryptie als zodanig (cryptografiemogelijkheden, symmetrische en asymmetrische encryptie), niet zozeer over regelgeving. Wel beschikbare literatuur handelt veelal over het Amerikaanse Clipperchip/Skipjack-voorstel en over de exportbeperkingen van de Verenigde Staten.

Ten aanzien van bestaande initiatieven op het gebied van encryptie en cryptografie kan concluderend worden gesteld dat deze geen eenduidige oplossingen bieden voor alle praktische vraagstukken die op dit onderwerp betrekking hebben. Deze vraagstukken doen zich voor op:
- *juridisch vlak:* de grens tussen het recht op privacy/geheimhouding versus gerechtvaardigde opsporingsbelangen, maar ook de juridische positie en bevoegdheden van key centres en de onderlinge verhouding tussen nationale wetgevingen;
- *technisch vlak:* de meeste huidige cryptografische toepassingen en berichtenstandaarden zijn niet ingericht op sleuteldeponering bij een derde of het meezenden van een escrow-veld in de berichtgeving, dan wel bieden operationele problemen, omdat sleutels in hoog tempo per sessie wisselen;
- *organisatorisch vlak:* de besturing en organisatie van key centres, van toezichthoudende organen of van internationale organen die zich bezighouden met security en cryptografie in telecommunicatie.

TRUSTED THIRD PARTIES

Een allesomvattend voorstel lijkt vooralsnog een onhaalbare kaart. Toch is het wellicht interessant omwille van de beheersbaarheid (private) initiatieven op het gebied van TTP's die worden ingezet ten behoeve van de betrouwbaarheid en vertrouwelijkheid van elektronische communicatie te steunen en te stimuleren. Met name indien deze private TTP's betreffen, zal de weerstand om tot sleutelbeheer en -depot over te gaan minder zijn dan indien sleutels op verplichte basis bij overheidsinstanties dienen te worden afgegeven.

De huidige initiatieven bieden geen eenduidige oplossingen.

Een TTP kan tal van functies vervullen in het berichtenverkeer: sleutelgeneratie, -beheer en -uitgifte, het vaststellen van het tijdstip van communicatie ('time-stamping' door middel van de eigen digitale handtekening van de TTP), bewijsvaststelling, etc. In de markt wordt momenteel veel gediscussieerd over de vraag aan welke TTP's behoefte bestaat en aan welke (betrouwbaarheids- en vertrouwelijkheids)eisen deze zelf dienen te voldoen

Mw. A.K.I. Tuinder
Studeert rechten aan de Rijksuniversiteit Leiden en was als stagiaire verbonden aan KPMG in het kader van het ITeR-onderzoek naar regulering van encryptie in westerse landen. Momenteel doet zij bij de Stichting Ediforum onderzoek naar juridische aspecten van TTP's en TTP-diensten.

Mw. mr. A.M.Ch. Kemna MBA
Is manager bij de sectie informaticarecht van KPMG EDP Auditors. Zij is tevens als onderzoeker verbonden aan de Afdeling Recht & Informatica van de Rijksuniversiteit Leiden, waar zij zich bezighoudt met bewijsaspecten in een digitale omgeving.

om het predikaat 'trusted' te kunnen dragen. Ook binnen KPMG wordt onderzoek gedaan naar mogelijkheden voor TTP-dienstaanbieders alsmede naar de mogelijkheden de kwaliteit van een bepaalde TTP-dienst te kunnen bepalen en auditen. De Koninklijke Notariële Broederschap discussieert dit najaar omtrent een pré-advies inzake de mogelijkheid voor notarissen om universele TTP-certificatiediensten aan te bieden. Daarnaast wordt bijvoorbeeld bij de Stichting Ediforum een onderzoek uitgevoerd naar de eisen die men in het algemeen dient te stellen aan TTP-diensten. Daarbij wordt tevens getracht de begripsvorming ten aanzien van TTP's te uniformeren.

Het is overigens niet onaannemelijk dat er in de toekomst voor verschillende marktsectoren verschillende TTP's zullen opereren met elk zo zijn eigen dienstenpakket.
Voor de justitie zou de mogelijkheid kunnen bestaan (in geval van gerechtvaardigde verdenking en na verkregen toestemming van – in Nederland – de Rechter Commissaris) in voorkomende gevallen voor de opsporing gebruik te maken van de informatie beschikbaar bij TTP's.

Uiteraard blijven ook hierbij de nodige vragen open staan. Hoe weet men bijvoorbeeld wat de waarde en kwaliteit is van buitenlandse TTP-diensten, nu er (nog) geen wettelijk kader is voor TTP's? En hoe zullen justitie en overheid bij internationale misdaad met informatievergaring dienen om te gaan? En bovendien: de benodigde informatie voor justitieel onderzoek zal (ook bij verplichte sleuteldeponering) in veel gevallen niet bij TTP's aanwezig zijn. Zo is het immers over het algemeen een kenmerk van georganiseerde misdaad dat zij zich niet al te veel stoort aan regelgeving ...

TOT SLOT

Het voortzetten van een brede maatschappelijke discussie op internationaal niveau lijkt nodig ten aanzien van het encryptiereguleringsprobleem, waarbij alle betrokken gerechtvaardigde belangen, van overheid en particuliere sector, duidelijk gecommuniceerd en besproken kunnen worden, niet in de laatste plaats via elektronische netwerken als het Internet.

Overheidsaanbestedingen in de IT-branche

Mr. M.J. van Bommel,
mw. R. van der Velden en
mw. mr. drs. A.W. Duthler

Ook projecten in de IT-branche vallen onder de Europese aanbestedingsrichtlijnen. Naast een uiteenzetting van de procedures komt de effectiviteit van de richtlijnen aan bod, alsmede de economische en sociale gevolgen ervan.

INLEIDING

Sinds 1 juli 1993 gelden er EU-richtlijnen voor het aanbesteden van leverings- en dienstleveringscontracten. Het doel van de richtlijnen is de markt voor overheidsopdrachten te liberaliseren. In de richtlijnen zijn procedures beschreven die ertoe moeten leiden dat nationale leveranciers of dienstverleners niet worden bevoordeeld boven leveranciers of dienstverleners uit andere landen. Door publicatie van alle overheidsopdrachten boven een bepaald drempelbedrag in het Supplement op het Publicatieblad van de EG, krijgt in beginsel iedere dienstverlener de kans op een opdracht in te schrijven. De aanbestedende diensten moeten ervoor zorgen dat tussen verschillende dienstverleners niet wordt gediscrimineerd. Dit kan worden bewerkstelligd door de opdracht te gunnen aan de inschrijver die het best voldoet aan de in de richtlijnen vastgelegde selectie- en gunningscriteria.

Een goed inzicht in de regelgeving omtrent Europese aanbestedingen is voor accountants en EDP-auditors van tweeledig belang. Enerzijds omdat het inschrijven op overheidsopdrachten actuele kennis vraagt over de te volgen procedures waarbij de kans op het verwerven van de opdracht toeneemt indien men inzicht heeft in de procedure en nauwkeurig weet wat de gunningscriteria zijn, zodat de offerte hierop kan aansluiten. Anderzijds dient bij de jaarrekeningcontrole van overheidslichamen getoetst te worden of de richtlijnen van toepassing zijn en zo ja, of de juiste procedure op de juiste wijze door het overheidslichaam is gevolgd.

Hierna wordt allereerst ingegaan op de belangrijkste elementen van een aanbestedingsprocedure. Daarbij wordt aandacht besteed aan vragen als: welke procedures zijn er; wat is een aanbestedende dienst; welke drempelbedragen gelden en hoe worden deze berekend? Daarna worden enkele specifieke aandachtspunten en vragen ten aanzien van aanbestedingen in de IT-branche uitgelicht en nader toegelicht. In de slotparagraaf worden de economische en sociale gevolgen van de richtlijnen behandeld. De doelstelling van de aanbestedingsrichtlijnen was de Europese overheidsmarkt te openen om bepaalde effecten te bereiken, zoals transparantie, eerlijke concurrentie, objectiviteit, kostenbesparingen en betere kwaliteit. De auteurs hebben in het kader van een studie van de Nederlandse Vereniging van Informatietechnologie en Recht (NVvIR) een onderzoek gedaan naar de mate waarin deze beoogde effecten ook daadwerkelijk worden bereikt ([Bank95]). In de genoemde paragraaf over de gevolgen van de richtlijnen wordt verslag van dit onderzoek gedaan.

DE AANBESTEDINGSPROCEDURES

Om inzicht te krijgen in de regelgeving omtrent Europese aanbestedingen is het noodzakelijk enkele belangrijke elementen van een aanbestedingsprocedure te kennen. Het is van belang om te weten welke richtlijnen van toepassing kunnen zijn op aanbesteding van IT-producten, welke aanbestedingsprocedures te onderscheiden zijn, wanneer sprake is van een aanbestedende dienst (wie is een aanbestedende dienst?) en welke drempelbedragen gelden. In de hiernavolgende subparagrafen gaan we op deze elementen in.

Doel van de aanbestedingsrichtlijnen

In geval van onduidelijkheden over bepaalde begrippen uit de richtlijnen, inconsistenties tussen (artikelen van) de richtlijnen onderling en/of het al dan niet toepassen van de richtlijnen of artikelen dient te worden uitgegaan van de doelstellingen van de richtlijnen. De belangrijkste doelstellingen van de aanbestedingsrichtlijnen zijn:
1. transparantie (doorzichtigheid);
2. non-discriminatie;
3. openstelling overheidsmarkt.

Ad 1.
Met transparantie wordt bedoeld dat de procedures helder en inzichtelijk moeten zijn. Om transparantie te garanderen, kennen de richtlijnen onder andere publicatieverplichtingen en procedurevoorschriften. Zo dient een aankondiging volgens een voorgeschreven model in het Publicatieblad van de EG te worden geplaatst als men voornemens is aan te besteden. Ook is men verplicht de selectie- en gunningscriteria vooraf kenbaar te maken en dient men het resultaat van de procedure, de gunning, te annonceren.

Overheden worden aangespoord zich zowel nationaal als internationaal open te stellen voor leveranciers.

Ad 2.
Non-discriminatie komt tot uitdrukking in de selectie- en gunningscriteria die objectief behoren te zijn. Hiermee wordt voorkomen dat nationale leveranciers bevoordeeld zouden kunnen worden omdat de criteria naar bepaalde leveranciers, dan wel hun producten of diensten zijn toegeschreven.

Ad 3.
De Commissie beoogt met de aanbestedingsprocedures overheden aan te sporen zich, zowel nationaal als internationaal, open te stellen voor leveranciers. Dit zou als gevolg moeten hebben dat de te leveren producten of af te nemen diensten van een betere kwaliteit en/of een lagere prijs zouden zijn. Bovendien krijgen hierdoor meer leveranciers de mogelijkheid om door te dringen tot de doorgaans nogal gesloten overheidsmarkt. Ook het Nederlandse bedrijfsleven zou meer kansen moeten krijgen om op nieuwe markten omzet te genereren of een vergrote omzet op bestaande markten te genereren ([Dank93]). Uiteindelijk zou dit zowel het bedrijfsleven als de burger ten goede komen.

Richtlijnen

De belangrijkste aanbestedingsrichtlijnen die directe werking hebben gekregen in de Nederlandse wetgeving zijn:
1. Richtlijn werken (bouwwerken) 93/37/EEG;
2. Richtlijn diensten 92/50/EEG;
3. Richtlijn levering (levering van producten) 93/36/EEG;
4. Richtlijn nutssectoren (water, energie, vervoer en telecommunicatie) 93/38/EEG.

Voor de IT-branche zijn met name de richtlijnen diensten en leveringen van belang. Afhankelijk van de aard van het project zal moeten worden bekeken welke richtlijn van toepassing is. Met name leverings- en dienstverleningsopdrachten willen nog wel eens door elkaar heen lopen. Er moet dan worden bezien welk deel van de opdracht het grootste aandeel heeft (in het projectbudget): leveringen of diensten.

Welke aanbestedingsprocedures kennen de richtlijnen?

Als men wordt geconfronteerd met een aan te besteden project zal de aanpak van het project afhankelijk zijn van het soort aanbestedingsprocedure. Er zijn vijf mogelijke procedures:
1. de openbare procedure;
2. de niet-openbare procedure;
3. onderhandelingsprocedure na voorafgaande publicatie;
4. onderhandelingsprocedure zonder voorafgaande publicatie (versnelde procedure);
5. prijsvragen-procedure.

Doorgaans worden de openbare en de niet-openbare procedures toegepast. Het kenmerkende verschil tussen de openbare en de niet-openbare procedures is dat er bij de niet-openbare procedure een voorselectie van potentiële leveranciers plaatsvindt. Daarmee kan worden voorkomen dat een zeer groot aantal potentiële leveranciers een aanvraag tot inschrijving indient. Hoewel de onderhandelingsprocedures bij de aanbestedende diensten het meest geliefd zijn, kunnen deze procedures slechts in uitzonderingssituaties gevolgd worden. Het gaat zelfs zo ver dat een wetsaanpassing die een aanbestedende dienst ertoe dwingt om op korte termijn nieuwe programmatuur te ontwikkelen, niet als uitzonderingssituatie aanvaard wordt door de Europese Commissie.

Drempelbedragen

Pas als de waarde (exclusief BTW) van een aan te besteden project uitstijgt boven het zogenaamde drempelbedrag dienen de richtlijnen te worden toegepast. Deze drempelbedragen, in ECU's uitge-

drukt, staan vermeld in de richtlijnen. Om de twee jaar wordt de tegenwaarde in nationale valuta berekend. De drempelbedragen per 1 januari 1996 zijn afgebeeld in tabel 1.

Om te beoordelen of een project boven het drempelbedrag uitkomt, zal gekeken worden naar de geraamde waarde van het aan te besteden project. In geval van een meerjarig contract wordt (dient) de waarde (te worden) berekend door de jaarlijkse vergoeding te vermenigvuldigen met de looptijd van het contract (uitgedrukt in het aantal maanden), tot een maximum van vier jaar.

Vaak is de geraamde waarde al door de aanbestede dienst bepaald, aangezien zij aan het begin van het begrotingsjaar een budget heeft ingediend. De keuze van de ramingsmethode mag niet bedoeld zijn om toepassing van de aanbestedingsrichtlijnen te ontlopen ([Klaa94]). Tevens mag een opdracht niet worden gesplitst met het doel te voorkomen dat de drempelbedragen worden overschreden.

Het begrip 'aanbestedende dienst'

Elke organisatie die kan worden gekwalificeerd als een aanbestedende dienst dient in principe de aanbestedingsrichtlijnen te volgen. De vraag is: wanneer is sprake van een aanbestedende dienst? In de richtlijnen wordt het begrip aanbestedende dienst omschreven als 'de Staat, de territoriale lichamen, publiekrechtelijke instellingen en verenigingen, gevormd door één of meer van deze lichamen of instellingen'.

Onder publiekrechtelijke instellingen wordt iedere instelling verstaan die:
- is opgericht met het specifieke doel te voorzien in behoeften van algemeen belang andere dan die van industriële of commerciële aard, en
- rechtspersoonlijkheid heeft, en
- waarvan ofwel de activiteiten in hoofdzaak door de Staat of de territoriale of andere publiekrechtelijke instellingen worden gefinancierd, ofwel het beheer is onderworpen aan toezicht door deze laatste, ofwel de leden van de directie, de raad van bestuur of de raad van toezicht voor meer dan de helft door de Staat, de territoriale lichamen of andere publiekrechtelijke instellingen zijn aangewezen.

De lijsten van de instellingen en van de categorieën van publiekrechtelijke instellingen die voldoen aan de genoemde criteria staan eventueel in een bijlage die is gevoegd bij de desbetreffende richtlijn. Deze lijsten zijn zo volledig mogelijk en kunnen worden herzien volgens de procedure van een eventueel in de richtlijn genoemd artikel.

In ieder geval behoren hiertoe de centrale overheid, provincies, gemeenten, waterschappen, zelfstandige bestuursorganen, de Nederlandse Spoorwegen, Luchthaven Schiphol en de Gemeentelijke Vervoer- en Havenbedrijven. In de bijlagen van de richtlijnen staat een opsomming van voorbeelden van aanbestedende diensten vermeld. Deze opsomming kan echter niet als eenduidig, noch als limitatief worden geïnterpreteerd. Vaak zijn andere instanties ook aan te merken als aanbestedende dienst door hun financiering of de wijze waarop het bestuur is samengesteld. Indien het niet duidelijk is of een organisatie als aanbestedende dienst kan worden gekwalificeerd, dient het begrip te worden uitgelegd in het licht van de aanbestedingsrichtlijnen ([Klaa94]).

	Leveringen en diensten	Werken
Centrale overheid	137.537 ECU = *f* 293.888	5.289.883 ECU = *f* 11.303.384
Mede-overheden	211.595 ECU = *f* 452.135	5.289.883 ECU = *f* 11.303.384
Nutssector	423.191 ECU = *f* 904.271	5.289.883 ECU = *f* 11.303.384
Telecommunicatie	600.000 ECU = *f* 1.282.076	5.000.000 ECU = *f* 10.683.965

Tabel 1. Drempelbedragen

Handhaving

Indien de aanbestedingsprocedures niet of niet juist worden toegepast, zijn er verschillende sanctiemogelijkheden. Eén van de mogelijkheden is dat de Europese Commissie een administratieve boete oplegt aan de Staat, die deze vervolgens mogelijk zal gaan doorberekenen aan de overtredende aanbestedende dienst zelf. Ook is het mogelijk dat een leverancier of adviseur een klacht indient bij de Europese Commissie. De Europese Commissie kan deze klacht eventueel voorleggen aan het Europese Hof van Justitie. De laatste zal echter alleen een oordeel geven over het al of niet juist toepassen van de aanbestedingsprocedure. Het zal geen boete of schadevergoeding opleggen. Daarnaast kan een niet toegelaten of afgewezen leverancier of adviseur een schadeverordering instellen bij de burgerlijke rechter.

SPECIFIEKE AANDACHTSPUNTEN BIJ AANBESTEDING IN DE IT-BRANCHE

De selectie van leveranciers en de gunning van overheidsopdrachten is gebonden aan kenbare, objectieve, non-discriminatoire criteria. Dit heeft doorgaans tot gevolg dat er niet meer onderhandeld kan worden met de potentieel gegadigden. Het bestek (met name de daarin geformuleerde technische specificaties) dient objectief maar eveneens exact weergegeven te worden. In het bijzonder in de IT-branche vormt dit een probleem omdat hier vaak zeer ingewikkelde projecten worden gepland. Deze projecten werden voorheen, voordat de aanbestedingsrichtlijnen golden, met een leverancier op grond van grove probleemstellingen en kostenramingen gedurende het project verder uitgewerkt. De aanbestedende diensten kunnen nu niet meer samen met een leverancier tot een uitwerking van het bestek komen. Belangrijke technische aspecten, die een toegevoegde waarde leveren aan het project, kunnen daardoor over het hoofd worden gezien. De aanbestedende dienst heeft

immers niet dezelfde deskundigheid als de leverancier. Ook kostenramingen kunnen ver van de realiteit komen te liggen. Binnen de huidige aanbestedingsrichtlijnen bestaat er nog nauwelijks ruimte om deze problemen op te vangen.

In het geval van een zeer ingewikkelde opdracht (bijvoorbeeld het renoveren van een informatiesysteem) zal de aanbestedende dienst zich genoodzaakt voelen deze in twee aanbestedingen te splitsen (waarbij de eerste aanbesteding het schrijven van de systeemdefinities omvat terwijl de tweede aanbesteding een invulling van de geleverde systeemdefinitie moet opleveren) dan wel de technici binnen de eigen organisatie op te zadelen met een (te) grote verantwoordelijkheid bij het invullen van de specificaties.

De technische specificaties dienen objectief maar exact te worden weergegeven.

Overheidsorganisaties gebruiken voor de invulling van de technische specificaties van (ingewikkelde) IT-opdrachten voornamelijk externe deskundigen. Dit wordt echter door recentelijk in werking getreden regelgeving ernstig bemoeilijkt. Per 1 januari 1996 namelijk zijn de aanbestedingsregels aangevuld met de bepaling dat overheidsorganisaties zich dienen te onthouden van het vragen dan wel aanvaarden van advies van partijen die een commercieel belang bij de opdracht zouden kunnen hebben (de zogenaamde Chinese Wall-bepaling). Dit betekent dat de leverancier die de overheidsorganisatie adviseert, niet meer op de opdracht zelf kan inschrijven. In tegenstelling tot de bouwbranche is binnen de IT-branche de adviserende deskundige welhaast onvermijdelijk tevens de potentieel gegadigde.

ECONOMISCHE EN SOCIALE GEVOLGEN VAN DE RICHTLIJNEN

Zoals gezegd wil de Europese Commissie met de aanbestedingsrichtlijnen bepaalde effecten bereiken, zoals transparantie, eerlijke concurrentie, objectiviteit, kostenbesparingen, betere kwaliteit. Ook in Nederland is er veel nadruk gelegd op de positieve kanten van de richtlijnen. Onderzoekers van de NVvIR zijn door middel van het enquêteren van leveranciers en overheden nagegaan of deze doelstellingen ook inderdaad worden gerealiseerd. De enquête had onder andere betrekking op de volgende vragen:

- Hebben de aanbestedingsrichtlijnen inderdaad een open markt in Europa bevorderd?
- Leveren de richtlijnen besparingen op voor de aanbestedende diensten?
- Welke extra kosten brengen de richtlijnen met zich mee, zowel voor de leveranciers als voor de aanbestedende diensten?
- Zien partijen nog mogelijkheden tot onderhandelen?

Om een zo volledig en representatief mogelijk beeld te kunnen schetsen van de huidige aanbestedingspraktijk zijn naar zowel aanbestedende diensten als leveranciers in totaal 400 enquêtes verstuurd. Hiervan zijn er 64 ingevuld geretourneerd. Hoewel de steekproef daarmee niet geheel representatief is, zijn de onderzoekers van mening dat de antwoorden voldoende indicatief zijn voor het beantwoorden van de hiervoor genoemde vragen. Om eventuele verschillen te kunnen constateren in de gevolgen van de richtlijnen voor IT-leveranciers en niet-IT-leveranciers en voor kleinere en grotere ondernemingen is een onderscheid gemaakt tussen:

- IT-midden- en kleinbedrijf;
- grote IT-leveranciers;
- niet-IT-midden- en kleinbedrijf;
- grote niet-IT-leveranciers.[1]

Resultaten ten aanzien van effecten voor leveranciers

Voor leveranciers blijken de effecten van de openstelling van de Europese markt beperkt te zijn gebleven.

Openstelling Europese markt
Zoals eerder genoemd wordt met de aanbestedingsrichtlijnen openstelling van de Europese markt beoogd. Uit de resultaten van de enquête blijkt dat het afzetgebied voor de meeste leveranciers beperkt blijft tot Nederland. Daarbij zijn geen significante verschillen geconstateerd tussen bedrijven die worden gerekend tot het midden- en kleinbedrijf en de grote leveranciers.

Voor de meeste leveranciers heeft het systeem van Europese aanbesteding meer kosten met zich meegebracht, waarbij vooral bedrijven uit het MKB-segment aangeven dat hun marges onder druk zijn komen te staan. Ook hebben de Europese aanbestedingsrichtlijnen geen extra opdrachten noch extra omzet voor hen opgeleverd.

Uit de enquête blijkt dat de meeste bedrijven sinds de invoering van de richtlijnen niet meer hebben meegedongen naar opdrachten in het buitenland dan voorheen.

Leveranciersstatus
Opvallend is dat weinig leveranciers uit het MKB hun positie als huisleverancier zijn kwijtgeraakt, in tegenstelling tot de grote IT-bedrijven en de overige bedrijven. Eén van de subdoelstellingen van de aanbestedingsrichtlijnen is het inschakelen van onderaannemers en toeleveranciers uit het MKB-segment. Uit de enquête blijkt dat deze doelstelling voor de IT-sector is bereikt nu tweederde van de MKB-bedrijven ingeschakeld wordt als onderaannemer of toeleverancier en de meeste leveranciers zelf ook onderaannemers of toeleveranciers inschakelen.

Procedure
De meeste leveranciers zijn tegenwoordig meer tijd

1 Er zijn meerdere manieren om aan te geven of bedrijven tot het MKB behoren. In deze enquête is uitgegaan van de personeelsomvang, waarbij de door het Instituut voor het midden- en kleinbedrijf doorgaans gehanteerde grens van 200 personen is aangehouden.

kwijt aan de opstelling van een offerte dan voor de invoering van de aanbestedingsrichtlijnen, hetgeen als nadelig wordt ervaren. De extra tijd is vooral nodig voor het beantwoorden van uitgebreidere vraagstellingen, het verstrekken van informatie, de complexiteit van de aanvraag, onervarenheid en voor interne coördinatie. Ook de duur van de gehele procedure (vanaf de publicatie tot en met het sluiten van de overeenkomst) wordt als langer ervaren dan voorheen. Daarnaast geldt voor veel leveranciers, met name grote IT-leveranciers, dat hun handelwijze ten aanzien van aanbestedende diensten is gewijzigd. Men stelt zich kritischer en formeler op tegenover de aanbestedende diensten. Tevens kan niet meer worden vertrouwd op de persoonlijke relaties.

Resultaten ten aanzien van effecten voor aanbestedende diensten

Voor de aanbestedende diensten zijn de effecten van de richtlijnen wel duidelijk merkbaar.

Openstelling Europese markt
Tweederde van de aanbestedende diensten ontvangt inschrijvingen uit het buitenland. Hieruit kan worden afgeleid dat de doelstelling van transparantie van de overheidsmarkt is bereikt. De resultaten van de enquête geven helaas geen inzicht in hoeverre overheidsopdrachten daadwerkelijk zijn gegund aan buitenlandse inschrijvers.

Ongeveer de helft van de aanbestedende diensten geeft aan dat Europese aanbestedingen meer kosten met zich mee hebben gebracht. Slechts een derde van de aanbestedende diensten geeft aan dat de aanbestedingsprocedures besparingen hebben opgeleverd. Het merendeel van de aanbestedende diensten geeft aan dat de voordelen van Europese aanbestedingen opwegen tegen de extra kosten. De voordelen liggen vooral op het gebied van prijsaanpassingen op de thuismarkt, het betere marktoverzicht, de grotere concurrentie, de kwaliteitsverbetering (ook van hun eigen inkoopproces) en ten slotte de controleerbaarheid van de interne medewerkers.

Leveranciersstatus
De meeste aanbestedende diensten kunnen steeds gebruik maken van hun vroegere huisleveranciers. Uit de enquête voor leveranciers blijkt dat het vooral de grote leveranciers zijn die hun positie als huisleverancier verliezen. Het niet meer gebruik kunnen maken van de opgebouwde deskundigheid wordt door een groot deel van de aanbestedende diensten als nadelig ervaren. De op termijn door concurrentie ontstane betere verhouding tussen prijs en kwaliteit weegt hier veelal tegenop.

Procedure
In tegenstelling tot de meeste leveranciers heeft maar liefst driekwart van de aanbestedende diensten geen problemen met de extra tijd die het naleven van de procedure vergt. De helft van de aanbestedende diensten vindt deze extra benodigde tijd nuttig besteed vanwege de voordelen of het beoogde nut van de richtlijnen.

Conclusie

Uit de enquête blijkt dat zowel het midden- en kleinbedrijf als de grote leveranciers door de richtlijnen hindernissen ondervinden bij hun toetreding tot de markt voor overheidsopdrachten. Die hindernissen bestaan vooral uit het opzetten van interne procedures, het veel uitvoeriger moeten offreren, de grote mate van ambtelijke betrokkenheid, de veel grotere concurrentie en vooral de extra kosten die zijn ontstaan door de arbeidsintensieve tijdrovende procedures. Hieruit kan de conclusie worden getrokken dat het betreden van de overheidsmarkt een gedegen voorbereiding vereist. Deze voorbereiding werd jaren geleden al voorzien door de Europese Commissie ([SEC92]).

Toekomst

De Europese Commissie ziet een vereenvoudiging van de procedures als een verandering die niet alleen ten goede zou komen aan alle ondernemingen, maar ook aan de aanbestedende diensten zelf. De lidstaten dienen er zelf vooral voor te zorgen dat de procedures voor kleine opdrachten, waarvoor het midden- en kleinbedrijf relatief meer belangstelling heeft, zo duidelijk en doorzichtig mogelijk zijn ([Com95]).

Een standaardregeling of een aanbestedingsreglement per branche kan ervoor zorgen dat er overleg plaatsvindt tussen de desbetreffende leveranciers en opdrachtgevers. Gezien het feit dat dit in de bouwwereld heeft geleid tot een grotere duidelijkheid van de procedures is navolging ook binnen de IT-branche gewenst ([Corv95]).

SAMENVATTING

In dit artikel is een overzicht gegeven van de belangrijkste aspecten van Europese aanbestedingsprocedures. Naast de doelstellingen van de aanbestedingsrichtlijnen werden onder andere de verschillende soorten procedures, de relevante begrippen en de drempelbedragen nader toegelicht. Bovendien werd ingegaan op de problematiek die specifiek voor de IT-branche geldt als gevolg van de verplichte toepassing van de Europese aanbestedingsregelgeving. Met name de zogenaamde Chinese Wall-bepaling zal in het bijzonder voor de IT-branche nog de nodige problemen met zich meebrengen. Als laatste zijn de resultaten van een enquête besproken, die is gehouden onder aanbestedende diensten en leveranciers. Met behulp

Het betreden van de overheidsmarkt vereist een gedegen voorbereiding.

Mr. M.J. van Bommel en mw. R. van der Velden Zijn werkzaam bij het advocatenkantoor Cordemeyer & Slager. Zij houden zich bezig met de verschillende aspecten van het informatica-, telecommunicatie- en aanbestedingsrecht.

Mw. mr. drs. A.W. Duthler Is adviseur informaticarecht bij KPMG EDP Auditors. In deze functie houdt zij zich bezig met juridische aspecten van EDP-auditing, in het bijzonder met Trusted Third Parties. Daarnaast is zij docent aan de postdoctorale EDP-auditing-opleiding van de Erasmus Universiteit Rotterdam en bereidt zij een proefschrift voor op het gebied van Trusted Third Parties.

van de enquête is onderzocht in hoeverre de doelstellingen van de Europese aanbestedingsregelgeving daadwerkelijk zijn gerealiseerd en is aangegeven hoe de wetgever in de toekomst een vereenvoudiging van de aanbestedingsprocedures zou kunnen bewerkstelligen.

LITERATUUR

[Bank95] E.A. Banki, M.J. van Bommel, A.W. Duthler en R. van der Velden, *Economische en sociale gevolgen van de richtlijnen*, in: S. Corvers, F. van der Klaauw-Koops en W. Wedekind (red.), *Overheidsaanbestedingen in de IT: van onderhandelingsmodel naar aanbestedingsmodel*, Preadviezen voor de najaarsvergadering van 9 november 1995 van de Nederlandse Vereniging voor Informatietechnologie en Recht, Samsom BedrijfsInformatie bv, 1995.

[Com95] Mededeling van de Europese Commissie aan de Raad betreffende de bevordering van de deelneming van midden- en kleinbedrijf aan de overheidsaanbestedingen in de Gemeenschap, COM(90) 166, 7 mei 1995.

[Corv95] S.F.M. Corvers, F.A.M. van der Klaauw-Koops en W. Wedekind, *IT en de Europese aanbestedingsrichtlijnen*, Computerrecht 1995/1.

[Dank93] P. Dankert, *De BV Nederland en de concurrentieverhoudingen op de interne markt*, TMC Asser Instituut, Den Haag 1993.

[Klaa94] F.A.M. van der Klaauw-Koops en S.F.M. Corvers, *Overheidsaanbestedingen en de informatietechnologie*, Tjeenk Willink, 1994.

[SEC92] Mededeling van de Europese Commissie aan de Raad betreffende de deelneming van het midden- en kleinbedrijf aan de overheidsopdrachten in de Gemeenschap, SEC (92)722, 1 juni 1992.

Interconnectie, technisch- en juridisch-relationele aspecten

Mr. drs. E.F. Clarkson

Netwerkinterconnecties nemen steeds ingewikkelder vormen aan. Mede in verband met mededingingsaspecten en regelgeving is het belangrijk de mogelijke interconnectierelaties te kunnen onderscheiden. Het rapport van de Europese Commissie inzake interconnectie biedt een overzicht van de regelgevingsaspecten.

INLEIDING

Interconnectie, in de zin van onderlinge koppeling van telecommunicatienetwerken van verschillende infrastructuurexploitanten, is een onderwerp dat de komende tijd de nodige bijzondere aandacht zal krijgen. Het betreft hier een problematiek waarvan de toenemende complexiteit – welhaast paradoxaal – verband houdt met de verder gaande liberalisering van de telecommunicatiemarkt. In dit artikel zal getracht worden een duidelijk beeld te schetsen van de interconnectieproblematiek, met een nadruk op de technische en juridische aspecten van interconnectierelaties tussen aanbieders van telecommunicatienetwerken en/of -diensten.

Koppeling van netwerken speelt natuurlijk al praktisch even lang als de telecommunicatie zelf. Sinds het vroege begin van telecommunicatie is het overheersende patroon van interconnectie geweest de koppeling van netwerken van exploitanten die opereerden in lokaal, regionaal of nationaal gescheiden markten. Het belangrijkste doel van interconnectie was om gebruikers in het ene gebied in staat te stellen gebruikers in andere gebieden te bereiken. Bezien we bijvoorbeeld de telefonie in Nederland, die zich – zoals in zovele andere landen – ontwikkeld heeft vanuit lokale netten, in eerste instantie aangelegd en geëxploiteerd door particuliere ondernemingen. Al spoedig na de ingebruikstelling van het eerste lokale net (Amsterdam 1881, Nederlandsche Bell Telephoon-Maatschappij) werden in 1888 de (NBTM-)netten van Amsterdam, Haarlem en Zaandam met elkaar verbonden[1]; enkele jaren later volgden – onder het alleenrecht van de overheid – de eerste internationale verbindingen (België 1895, Duitsland 1896). De (totstandkoming van) interlokale aansluiting leverde overigens de nodige problemen op. Deze problemen vloeiden ten dele voort uit het monopolistische gedrag van de NBTM, ten dele uit het bestaan van het grote aantal kleine telefoonbedrijfjes, ieder met een eigen, van de ander afwijkend technisch systeem ([Hoge93]). Via een geleidelijk proces van overneming van particuliere en gemeentelijke netten en aanleg van eigen rijksnetten, zijn echter zo rond de jaren twintig de lokale netten in handen van het rijk (lees: PTT) geraakt.[2] Met dit concentratieproces zijn vorenbedoelde problemen minder geworden, een situatie die tot slechts enkele jaren terug heeft voortbestaan.

NAAR EEN PLURALISTISCH NETWERKSYSTEEM

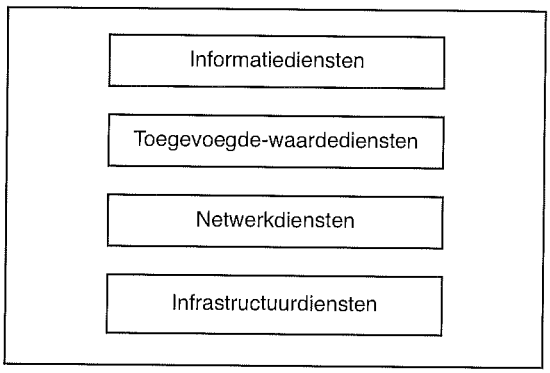
Met het afbreken van de monopolieposities van de PTT's is de interconnectieproblematiek evenwel – en in verhevigde mate en complexiteit – teruggekeerd. Het Europese liberaliseringsbeleid is immers (uiteindelijk) ook gericht op de telecommunicatie-infrastructuur. Binnen de Europese Unie wordt de reikwijdte van vrije mededinging op het gebied van data- en toegevoegde-waardediensten uitgebreid tot de 'core business' van telecommunicatie, namelijk (vaste) spraaktelefonie en infrastructuur. Het houdt in dat de – in de meeste lidstaten bestaande – exclusieve rechten van de PTT voor het aanbieden van telecommunicatiediensten, inclusief het aanbieden van spraaktelefonie en telecommunicatienetwerken, ingetrokken dienen te worden. Dus meerdere dienstenaanbieders, inclusief infrastructuuraanbieders, moeten tot de(zelfde) telecommunicatiemarkt toegelaten worden ([Rich96a]). Een nieuwe dimensie van interconnectie in de huidige tijd is de wens van exploitanten om hun netwerken te (kunnen en mogen) koppelen aan die van andere exploitanten in *dezelfde* regio of markt. Aangenomen wordt dat toetredingsdrempels lager en economische voordelen hoger zullen zijn indien interconnectie tussen concurrerende netwerken mogelijk is. Voor daadwerkelijke mededinging op de telecommunicatiemarkt wordt interconnectie als een noodzakelijke voorwaarde beschouwd ([Netw94], [Walk93]). In meerdere opzichten is sprake van de ontwikkeling van een pluralistisch netwerksysteem, waarvan de reguleringsproblematiek met name betrekking heeft op de verschillende aspecten van interconnectie ([Noam92]). De belangrijkste aspecten zullen in dit artikel nader aan bod komen. Dit zal gebeuren vooral vanuit het perspectief van het tot stand brengen van een competitieve omgeving.

INTERCONNECTIERELATIES

Interconnectie omvat niet enkel onderlinge koppeling van infrastructuren. In de Europese (voorstel-) *Richtlijn Interconnectie in Telecommunicatie* wordt onder interconnectie verstaan de fysieke en logische verbinding van de faciliteiten van organisaties die telecommunicatienetwerken en/of -diensten aanbieden, teneinde de gebruikers van de ene organisatie in staat te stellen te communiceren met gebruikers van een andere organisatie, of om toegang te krijgen tot diensten die door een andere organisatie aangeboden worden ([Rich95]). Hierin valt zonder moeite te lezen dat er een veelheid en veelvormigheid van interconnecties kunnen bestaan.

Het 'lagenmodel'

Om een inzicht te verkrijgen in deze complexiteit van interconnectierelaties kan gebruik worden gemaakt van het conceptuele 'lagenmodel' van de Mediaraad ([Medi93]). Het proces van (elektronische) informatievoorziening kan worden ingedeeld in een aantal lagen. Kenmerkend in deze *lagenstructuur* is de (functionele) scheiding tussen informatiediensten (die betrekking hebben op de inhoud van de informatie zelf) en de diensten die een keten vormen in het transport van informatie. Voorts is cruciaal het uiteenleggen van de transportketen in de volgende drie componenten: infrastructuur(diensten), netwerkdiensten en toegevoegde-waardediensten.
Infrastructuur(diensten) betreft het leveren van transmissiecapaciteit (bandbreedte). Netwerkdiensten verzorgen, met gebruikmaking van de geleverde transmissiecapaciteit, de routering van signalen. Toegevoegde-waardediensten vormen een toevoeging op de netwerkdiensten en leveren toegang tot informatie die door een individuele gebruiker geselecteerd kan worden. De 'informatielaag' ten slotte heeft, zoals gezegd, betrekking op de inhoud van de informatie zelf.
Deze lagenstructuur kan grafisch worden weergegeven als in figuur 1.



Figuur 1. Lagenstructuur in het proces van elektronische informatievoorziening.

De 'interconnectieruimte'

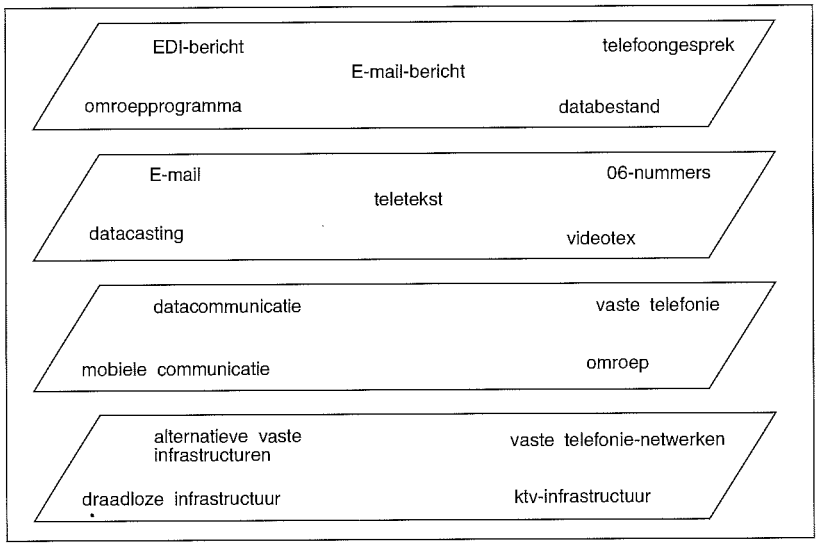
Binnen elke laag kan men zich vervolgens meerdere aanbieders en diensten voorstellen. Op infrastructuurniveau bevinden zich verschillende 'soorten' vaste en draadloze infrastructuren en verscheidene exploitanten daarvan. Bijvoorbeeld de vaste netwerken van de PTT, kabeltelevisie-infrastructuren, 'alternatieve' kabelnetwerken (zoals van de spoorwegen, energiebedrijven), radio- en satellietverbindingen. Binnen de laag van netwerkdiensten gaat het met name om vaste telefonie, datacommunicatie, mobiele communicatie en omroepdistributie. Bij toegevoegde-waardediensten kan men bijvoorbeeld denken aan E-mail, EDI, 06-nummers, teletekst, videotex en dergelijke, die door verschillende exploitanten aangeboden kunnen worden. Ten slotte bevat de informatielaag bijvoorbeeld databestanden, omroepprogramma's, E-mail- en EDI-berichten, reisinformatie, telefoongesprekken. Elke laag kan op deze wijze tot een vlak worden uitgebouwd, waardoor duidelijker de

1. Slechts één onderneming, de NBTM, kreeg het recht interlokale verbindingen te openen; vanaf 1897 echter werd de interlokale telefonie het exclusieve domein van de rijksoverheid ([Hoge93], [NEHA93]).
2. In 1927 waren slechts de gemeentenetten te Amsterdam, Rotterdam en Den Haag nog niet in handen van het rijk; dit proces werd in 1940 door de Duitse bezetter voltooid door de overdracht van vorengenoemde netten aan de PTT ([Hoge93]).

mogelijkheid van competitief aanbod van diensten kan worden getoond. Dit kan grafisch worden weergegeven als in figuur 2.
Figuur 2 geeft als het ware de 'interconnectieruimte' weer. Binnen elk vlak en tussen vlakken zijn velerlei verbindingen mogelijk, die exploitanten in staat stellen telecommunicatiediensten te leveren aan de (eind)gebruikers.

Daarbij moet worden bedacht dat door technologische ontwikkelingen, zoals digitalisering en toepassing van compressietechnieken, en opheffing van wettelijke belemmeringen diensten uit de bovenste lagen steeds minder gebonden zijn aan een bepaalde infrastructuur. Er vindt met andere woorden een steeds verder gaande technische en juridische ontkoppeling plaats van diensten en infrastructuur. Breedbandige videobeelden kunnen in principe ook over het (PTT-)telefonienetwerk getransporteerd worden, terwijl omgekeerd vaste telefonie in principe ook over de kabeltelevisie-infrastructuur gerouteerd kan worden. Door deze ontwikkelingen, die de omvang van de 'opvulling' door de (in het algemeen nog immer dominante) PTT van de interconnectieruimte onder druk zetten, worden nieuwe interconnectierelaties gecreëerd tussen de verschillende aanbieders van telecommunicatiediensten.

Voorts is van belang dat hedendaagse telecommunicatietechnologie wat betreft het hiërarchisch niveau van interconnectie vrijwel geen dwingende beperkingen oplegt aan aanbieders van telecommunicatiediensten. Bij interconnectie kan het in principe gaan om interconnectiediensten die op verschillende niveaus tussen verschillende typen netwerkarchitecturen en -technologieën afgewikkeld kunnen worden. De technologie maakt een breed scala van wegen mogelijk om telecommunicatiediensten aan te bieden en er zijn vele potentiële interconnectiepunten en interfaces tussen exploitanten. Economische factoren – zoals 'economies of scale and scope' en productdifferentiatie – veeleer dan strikt technische factoren bepalen waar operators en service-providers interconnectie zoeken. Dit laat een grote mate van vrijheid aan exploitanten ten aanzien van hun productie-organisatie om zich te kunnen presenteren als aanbieders van 'end-to-end'-diensten. Een exploitant kan twee of meer lagen binnen de eigen organisatie integreren (verticale integratie) of binnen een laag twee of meer hiërarchische niveaus van een bepaalde dienst integreren (horizontale integratie). Dit laatste kan bijvoorbeeld op infrastructuurniveau de integratie betreffen van het toegangsnet, het lokale, interlokale en internationale netwerk, dan wel van een deel van deze keten. Horizontale integratie vindt soms plaats dwars door verschillende typen netwerken. Het markantste voorbeeld van verticale en horizontale integratie is de PTT die bijvoorbeeld telefonie routeert (netwerkdienst) over haar eigen – van 'local loop' tot 'international gateway' uitgestrekt – telefoonnetwerk (infrastructuurdienst) en daarbij aan de telefonie gerelateerde toegevoegde-waardediensten en informatie aanbiedt. Specialisatievoordelen evenwel kunnen exploitanten ertoe brengen zich juist te richten op bepaalde (delen van) diensten, binnen één of meer lagen, en zodoende te desintegreren of te 'ontvlechten'. De 'omtrek' van vele



Figuur 2. Interconnectieruimte voor (competitief) aanbod van telecommunicatiediensten.

telecommunicatiebedrijven staat door diverse technologische en marktontwikkelingen en ontwikkelingen in de regelgeving voortdurend onder druk en is aan verandering onderhevig. Door dergelijke veranderingen kunnen volkomen nieuwe (interconnectie)paden door de interconnectieruimte heen ontstaan. Belangrijke implicaties van deze ontwikkelingen zijn dat 'key interfaces', die voorheen binnen een onderneming of netwerk (aan)gestuurd of beheerd werden, nu punten van technische en commerciële interconnectie kunnen zijn ([Netw94]).

TECHNISCHE ASPECTEN VAN INTERCONNECTIE

In de interconnectieruimte, zoals weergegeven in figuur 2, kunnen interconnectierelaties geclassificeerd worden naar:
- type spelers (telecom-operator, service-provider, eindgebruiker);
- type faciliteit (vast, mobiel, satelliet);
- type dienst (basisdienst, toegevoegde-waardedienst, intelligente netwerkfuncties);
- type gebruikers (gebruikers van private netwerken en van publieke netwerken).

Tussen en binnen deze classificaties bestaan vele mogelijke combinaties. Als de meest relevante actuele interconnectierelaties worden beschouwd ([Netw94], [Scha94]):
- tussen vaste netwerken onderling;
- tussen mobiele en vaste netwerken;
- tussen mobiele netwerken onderling;
- connecties met intelligente netwerkfuncties.

Bij 'vast-vast'-interconnectie kan worden gedacht aan koppeling van netwerken van nationale PTT's (via internationale 'gateways'), van PTT en een 'tweede' landelijke netwerkexploitant of van PTT en een (lokale of regionale) kabelexploitant. Interconnectie tussen mobiele en vaste netwerken kan betrekking hebben op een GSM-exploitant en PTT, en tussen mobiele netwerken onderling op de kop-

peling van twee GSM-netwerken. Interconnectie met intelligente netwerkfuncties vormt eigenlijk een toegevoegde dimensie aan de voorgaand genoemde interconnecties; steeds meer intelligentie wordt in het netwerk aangebracht.

De technische mogelijkheden voor interconnectie tussen twee netwerken worden bepaald door hun architectuur, dat wil zeggen de fysieke en logische inrichting van transportverbindingen, schakelingen en besturingsfaciliteiten. Interconnectie op zich kan worden totstandgebracht door interconnectietoegangspunten van netwerken door middel van een transmissiefaciliteit met elkaar te verbinden.

Er vindt een steeds verder gaande technische en juridische ontkoppeling plaats van diensten en infrastructuur.

Relevante technische (en operationele) aspecten van de interconnectie-interface betreffen:

– Niveau interconnectiepunt
Een (landelijk) vast-netwerkarchitectuur bijvoorbeeld, zoals van de PTT, kan interconnectietoegang verschaffen op verschillende niveaus in de netwerkhiërarchie: lokaal – regionaal – nationaal toegangspunt, primair gelokaliseerd in centrales. Ook andere punten (bijvoorbeeld vóór het lokale distributienetwerk) kunnen evenwel van belang worden, bijvoorbeeld als publieke telefonie lokaal aangeboden kan worden door niet-PTT's die zelf verschillende 'local-loop'-technologieën gebruiken, zoals kabeltelevisie of draadloze toegang.
In een GSM-architectuur wordt interconnectietoegang (externe interface tot vaste of andere mobiele netwerken) verschaft op het niveau van het (Gateway) Mobile Switching Centre.

– Uitvoering 'point of interconnect'
Naast aantal en (geografische en netwerktopologische) locatie van interconnectiepunten is er de kwestie van uitvoering. Hier speelt de keuze ten aanzien van een verbinding tussen een knooppunt van de ene partij en een centrale van de andere partij (die dan de interconnectiediensten verricht), en virtuele of fysieke collocatie. Collocatie betreft met name de mogelijkheid van plaatsing van (interconnectie-)apparatuur van de ene partij in de nabijheid van ('Point of Presence', virtuele collocatie) of in (fysieke collocatie) een schakelcentrale van de andere exploitant.

– Specificatie interfaces voor fysieke interconnectie
Voor typen vaste verbindingen waarmee koppelingen tussen diverse netwerken kunnen plaatsvinden, zijn interfaces gedefinieerd en zijn er internationale standaarden ontwikkeld (bijvoorbeeld CCITT-standaarden voor digitale interfaces).

– Specificatie van transmissie- en signaleringsdiensten (bijvoorbeeld ETSI-standaarden)
Essentiële 'intelligente netwerkdiensten' kunnen over afzonderlijke netwerken aangeboden worden, enkel indien de signaleringssystemen van elk netwerk aan elkaar gekoppeld zijn.

– Circuitcapaciteit, kwaliteit en beschikbaarheid van transmissiefaciliteit.

Andere relevante technische en operationele aspecten van interconnectie betreffen:

– Standaarden en interfaces met betrekking tot netwerk- en servicemanagement
Netwerk- en servicemanagement heeft betrekking op het genereren, bewerken, analyseren en evalueren van informatie om beheer van netwerken en diensten mogelijk te maken. Bij koppeling van infrastructuren is het noodzakelijk dat bepaalde beheersinformatie onderling wordt uitgewisseld tussen beide netwerken. In CCITT- en ISO-verband zijn en worden standaardiseringsactiviteiten op dit terrein uitgevoerd (bijvoorbeeld Telecommunications Management Network – TMN – standaarden).

– 'Measuring, charging and billing', voor toerekening van kosten en opbrengsten.

– Nummerbeheer
Dit betreft aspecten als nummerherkenning (voor routering naar het andere netwerk), nummertoegang, nummerbehoud ('portability') en nummerinformatie ('directory services').

– 'Essential requirements'
Beperkingen ten aanzien van open toegang kunnen gerechtvaardigd zijn in verband met essentiële eisen die in acht genomen dienen te worden, zoals behoud van netwerkintegriteit, veiligheid van het functioneren van het netwerk en, in gerechtvaardigde gevallen, interoperabiliteit van diensten en gegevensbescherming ([ONP90]). Deze eisen leggen stringente voorwaarden op aan interconnectieafspraken op technisch en administratief gebied, met name in geval van toegang tot intelligente netwerkfuncties.

INTERCONNECTIE IN DE CONTEXT VAN MEDEDINGING

Telecommunicatiebedrijven zullen zich in de regel aan de (potentiële) klanten willen presenteren als aanbieders van 'end-to-end'-diensten, op basis van het 'one stop shopping'-concept. Uit het voorgaande is duidelijk geworden dat vrijwel geen van deze aanbieders hiervoor zelf over alle benodigde telecommunicatiefaciliteiten beschikt. Doel van interconnectie is dan ook om diensten aan (eind)gebruikers te kunnen leveren via gebruikmaking van netwerken en diensten van anderen, zonder zelf in deze infrastructuren en diensten te hoeven investeren.

Interconnectie als markttransactie

Vanuit economisch perspectief kan interconnectie

beschouwd worden als een input die een producent, om zijn eigen product te kunnen realiseren, 'inkoopt' bij een ander. In algemene termen kan hier gesproken worden van een (markt)transactie, leidend tot een economische relatie. De juridische vormgeving van dergelijke transacties en relaties is in het algemeen het contract, zo ook bij interconnectie. De totstandkoming van interconnectie en de verdere modaliteiten daarvan, met andere woorden de invulling van interconnectierelaties, is op grond van het algemene beginsel van contractvrijheid in principe aan partijen zelf overgelaten. Partijen zullen bij zo'n interconnectie-overeenkomst, naast het formuleren van algemene contractuele rechten en verplichtingen, afspraken maken omtrent bovengenoemde technische en operationele aspecten (betreffende bijvoorbeeld interconnectiepunten, netwerk- en servicemanagement, nummerbeheer, 'essential requirements') en uiteraard omtrent de financiële aspecten (tariefstelsel, methodieken voor kosten- en opbrengstverdeling, voorwaarden voor verrekening). In geval van gelijk(waardig)e posities van partijen hoeft een dergelijke 'zelfregulering' niet echt tot problemen te leiden.

Asymmetrische (markt)relaties

In de huidige situatie, en de eerstkomende jaren, zal er evenwel in de meerderheid van de gevallen van (de wens tot) interconnectie niet sprake zijn van symmetrische maar van *asymmetrische* relaties. Dit heeft met name te maken met de marktstructuur van de telecommunicatiesector, gekenmerkt door een nog steeds monopolistische of in ieder geval dominante positie van 'de PTT'. Voor interconnectie zal een exploitant praktisch altijd aangewezen zijn op (de telecommunicatie-infrastructuur en -diensten van) de PTT. Door de ongelijkheid tussen partijen is sprake van asymmetrische betrekkingen. In deze gevallen dient gewaarborgd te worden dat toetredende concurrenten toegang verkrijgen tot 'bottlenecks' (en dat PTT's de nodige technische veranderingen aanbrengen), vereist om gelijke toegang mogelijk te maken teneinde eerlijke mededinging te bereiken.

'Bottlenecks'

Interconnectie is veelal een 'bottleneck input' in die zin dat de vrager een faciliteit die essentieel is voor het voortbrengen van zijn eigen 'product', vanwege technische, economische of wettelijke belemmeringen niet zelf kan produceren, terwijl vrager en leverancier op dezelfde markt concurreren; toegangsweigering, zonder geldige bedrijfsreden, zal ernstige schade voor de mededinging betekenen.

Gesteld kan worden dat een dominante PTT in het algemeen verschillende bottlenecks controleert ([Netw94]):
- toegang tot eindgebruikers (het verkeersvolume van een toetreder is veelal te gering om eigen 'local loops' aan te leggen);
- lokale schakeling (de kosten, bijvoorbeeld voor kabeltelevisie-exploitanten, om zelf in lokale schakeling te voorzien zijn veelal excessief hoger dan interconnectie met het PTT-netwerk);
- nummering (nummerbehoud);
- toegang tot interlokaal netwerk (in de opbouwfase van een nieuwkomer);
- intelligente netwerkdiensten;
- industriële eigendomsrechten met betrekking tot interfaces.

Bij interconnectie spelen niet alleen technische aspecten, maar speelt ook en veeleer een strategische problematiek van marktafscherming en marktontwikkeling. Gezien bovengenoemde bottlenecks kan een PTT concurrentie in diverse sectoren of segmenten van de telecommunicatiemarkt in principe zeer effectief belemmeren, bijvoorbeeld door interconnectie te weigeren of aantal, niveau of uitvoering van 'points of interconnect' te beperken, door excessief hoge prijzen te vragen of door een discriminatoire behandeling (ten aanzien van technische kwaliteit of andere voorwaarden van interconnectie) van interconnectievragers. In het algemeen zullen er voor de PTT geen positieve prikkels zijn om interconnectie aan te bieden aan andere exploitanten, wier diensten substitutief of competitief zijn met die van de PTT.
Dergelijke mededingingsbelemmeringen staan natuurlijk haaks op het, hierboven in de Inleiding geschetste, liberaliseringsstreven. Het is derhalve niet verwonderlijk dat zowel op nationaal als, primair, op Europees niveau, de interconnectieproblematiek de zorg heeft van de beleids- en regelgevende instanties.

REGELGEVINGSKADER VOOR INTERCONNECTIE

Gegeven de realiteit van imperfecties in de markt voor interconnectiediensten wordt een interventie van de regelgever ten aanzien van ten minste een aantal interconnectiekwesties noodzakelijk geacht. In de afgelopen jaren zijn op Europees niveau telecommunicatieregelingen totstandgekomen, met name in de vorm van Richtlijnen, die – direct of indirect – van belang zijn voor interconnectie.

ONP-Richtlijnen

Basisbeginselen voor een communautair interconnectiebeleid zijn in eerste instantie ontwikkeld binnen het raamwerk van Open Network Provision (ONP). ONP is bedoeld om het aanbieden van diensten te faciliteren, gebruik makend van publieke telecommunicatienetwerken en/of -diensten. In overeenstemming hiermee is ONP erop gericht eerlijke concurrentie mogelijk te maken, met name tussen verticaal geïntegreerde PTT's en dienstenaanbieders die van 'de PTT' afhankelijk zijn om hun diensten te kunnen aanbieden. Een tweede belangrijke doelstelling van ONP is het aanbieden van pan-Europese telecommunicatiediensten te faciliteren.

De *ONP-(kader)Richtlijn 90/387* ([ONP90]) heeft

betrekking op de harmonisatie van de voorwaarden voor een efficiënte en open toegang tot en gebruik van openbare telecommunicatienetwerken en -diensten. Hierbij moet bedacht worden dat ten tijde van het tot stand brengen van deze Richtlijn nog werd uitgegaan van (het handhaven van) exclusieve rechten van 'de nationale PTT's' ten aanzien van infrastructuur en bepaalde basisdiensten, waaronder in ieder geval de (vaste) spraaktelefonie.
De ONP-voorwaarden bevatten *geharmoniseerde voorwaarden* met betrekking tot technische interfaces, leverings- en gebruiksvoorwaarden, en tariefbeginselen.
Basisbeginselen waaraan deze ONP-voorwaarden moeten voldoen, zijn objectiviteit, non-discriminatie, transparantie en proportionaliteit.
Voorts is in de Richtlijn bepaald dat ONP-voorwaarden de toegang tot openbare telecommunicatienetwerken of -diensten niet mogen beperken, behalve om redenen gegrond op *essentiële eisen*: operationele veiligheid van netwerken, behoud van netwerkintegriteit, interoperabiliteit van diensten, en bescherming van gegevens.

Interconnectie is in principe een zaak voor onderhandelingen tussen partijen zelf.

Ook een tweetal specifieke ONP-Richtlijnen kent enkele bepalingen betreffende interconnectie. De *ONP-Richtlijn Huurlijnen 92/44*[3] bevat regels voor interconnectie van huurlijnen onderling of met openbare netwerken. De *ONP-Richtlijn Spraaktelefonie 95/62* ([ONP95]) bevat eveneens regels voor interconnectie, onder meer het recht op interconnectie voor publieke mobiele telefonie en vaste publieke telefoonnetwerken van exploitanten van andere lidstaten, en (commerciële) onderhandelingen over interconnectiecontracten door partijen zelf.

'Diensten'-Richtlijn

Enkele interconnectiebepalingen zijn ten slotte ook te vinden in de (reeds enkele malen gewijzigde) *'Diensten'-Richtlijn 90/388* ([Rich96a], [Rich96b]), de liberaliseringsrichtlijn gericht op vrije mededinging op de markten voor telecommunicatiediensten. De bedoelde bepalingen betreffen het opheffen van (wettelijke) beperkingen inzake interconnectie tussen kabeltelevisienetten onderling en met publieke netwerken, respectievelijk tussen mobiele telecommunicatiesystemen onderling en met publieke netwerken. Voorts wordt bepaald dat interconnectie in principe een zaak is voor onderhandelingen tussen partijen zelf. Gegeven de onevenwichtigheid in onderhandelingspositie evenwel moeten, voor een periode van zeker vijf jaar, waarborgen geschapen worden. Gezien hun dominante positie dienen de huidige telecom-operators interconnectie met hun spraaktelefoniedienst en hun geschakelde netwerken toe te staan op objectieve, non-discriminatoire, proportionele en transparante voorwaarden.

Bovenbedoelde bepalingen, en met name de fundamentele ONP-beginselen, bieden wel een goede basis voor een interconnectiebeleid, maar zijn voor een consistent en alomvattend communautair interconnectiebeleid te ruim geformuleerd en dekken niet alle relevante interconnectievraagstukken. Dit is de reden waarom recentelijk een afzonderlijke en specifieke Interconnectie-Richtlijn is ontworpen.

(Voorstel-)Richtlijn Interconnectie

De bedoelde Richtlijn betreft de (voorstel-)*Richtlijn Interconnectie in Telecommunicatie – Waarborging van Universele Dienstverlening en Interoperabiliteit middels toepassing van de beginselen van ONP* ([Rich95]). Deze Richtlijn legt geharmoniseerde voorwaarden voor open en efficiënte interconnectie met *publieke* telecommunicatienetwerken en -diensten vast. Deze voorwaarden dienen op nationaal niveau geïmplementeerd te worden.

De belangrijkste kenmerken van de Richtlijn zijn:
- toepassing van de *ONP-beginselen* van objectiviteit, non-discriminatie, transparantie en proportionaliteit;
- prioriteit voor *(commerciële) interconnectie-onderhandelingen* door partijen, waarbij evenwel bepaalde *(rand)voorwaarden* tevoren zijn vastgelegd door nationale telecom-regelgevers;
- duidelijke *rol en verantwoordelijkheden voor nationale regelgevers*, in overeenstemming met het beginsel van subsidiariteit, mede omvattend effectieve mechanismen voor geschillenbeslechting;
- onderkenning dat er *verschillende typen spelers* op de telecommunicatiemarkt zijn, waarbij het vast te stellen evenwicht tussen rechten en plichten van partijen kan verschillen naar type marktspeler.

Categorieën marktspelers
Wat betreft de verschillende typen marktspelers nemen aanbieders van *publieke*[4] *telecommunicatienetwerken of -diensten die significante marktmacht* hebben een bijzondere plaats in. Marktmacht kan in het algemeen gedefinieerd worden in (een combinatie van) bepaalde factoren, zoals marktaandeel, grootte, mate van verticale integratie, in staat zijn onafhankelijk van concurrenten te handelen, beschikking over schaarse middelen, bepaalde voorrechten in verhouding tot andere marktdeelnemers, etc. In de Overwegingen bij de Richtlijn wordt gesteld dat in het kader van deze Richtlijn een onderneming met een marktaandeel van meer dan 25% van een bepaalde telecommunicatiemarkt in het geografisch gebied in een lidstaat waarbinnen zij gemachtigd is te opereren *vermoed* wordt significante marktmacht te bezitten; de nationale regelgever kan evenwel bepalen dat dit niet zo is, maar kan anderzijds ook bepalen dat een onderneming met minder dan 25% marktaandeel toch significante marktmacht bezit.

3. Recentelijk is een voorstel ingediend tot wijziging van de ONP-(kader)Richtlijn 90/387 en de ONP-Richtlijn Huurlijnen 92/44, met het oog op de aanpassing aan een door concurrentie gekenmerkte context in de telecommunicatie (Pb. 1996 C 62/3); zie over dit voorstel [Duiv96].
4. Onder publiek telecommunicatienetwerk wordt verstaan een telecommunicatienetwerk gebruikt onder meer voor het aanbieden van publieke telecommunicatiediensten, dat wil zeggen diensten beschikbaar voor het publiek (art. 2).

Verplichtingen / Aanbieders	interconnectie	tarieven	kosten-toerekening	gescheiden boekhouding	openbaarmaking gegevens
A. telecomnetwerken en -diensten	vrijwilligheid	algemene ONP-beginselen		(zie hoofdtekst)	jaarrekening
B. 'bottleneck' draag-faciliteiten tot aan gebruikers	onderling recht op en plicht tot interconnectie	algemene ONP-beginselen			
C1. vaste telefoonnet-werken of -diensten, of huurlijnen	onderling recht op en plicht tot interconnectie	algemene ONP-beginselen			kostencalculatie universele dienstverplichting
C2. C1 met significante marktmacht	elk redelijk verzoek voor interconnectie (incl. 'special network-access')	kostengeoriënteerd en voldoende opgesplitst	voorschriften (goed te keuren) toe-rekeningsmethodiek		interconnectie-contracten; methodiek kosten-toerekening; lijst van interconnectie-diensten en tarieven
D1. mobiele telefoon-netwerken of -diensten	onderling recht op en plicht tot interconnectie	algemene ONP-beginselen			
D2. D1 met significante marktmacht	elk redelijk verzoek voor interconnectie (incl. 'special network-access')	algemene ONP-beginselen			interconnectie-contracten
E. C2 + D2: aanbieders met significante markt-macht	zie bij C2 en D2	zie bij C2 en D2	zie bij C2 en D2		zie bij C2 en D2

Figuur 3. Categorieën marktspelers en hun belangrijkste verplichtingen.

Uit de Richtlijnbepalingen (en de daarbij behorende eerste twee Bijlagen) kunnen de volgende (hoofd)categorieën marktspelers onderscheiden worden:

A aanbieders van publieke telecommunicatienetwerken en -diensten *in het algemeen*;
B aanbieders van geschakelde en niet-geschakelde *draagfaciliteiten tot aan gebruikers, van welke faciliteiten andere telecommunicatiediensten afhankelijk zijn* (dit betreft bijvoorbeeld exploitanten van vaste en/of mobiele publiekgeschakelde telecommunicatie-netwerken en/of -diensten, en die daarbij de controle hebben over de toegangsmiddelen tot één of meer netwerkaansluitpunten, geïdentificeerd door één of meer unieke nummers in het nationale nummerplan);
C1 aanbieders van *vaste* publieke *telefoon*netwerken of -diensten, of van *huurlijnen* op commerciële basis;
C2 categorie C1, met significante marktmacht;
D1 aanbieders van publieke *mobiele telefoon*netwerken of -diensten;
D2 categorie D1, met significante marktmacht;
E categorie C2 en D2, dus aanbieders van bedoelde netwerken of diensten, met *significante marktmacht*.

Deze categorieën aanbieders, en de daarbij behorende (hoofd)verplichtingen in het kader van interconnectie, kunnen schematisch worden aangegeven als vermeld in figuur 3.
Gesteld kan worden dat, gaande van (A) tot (E), in het algemeen sprake is van toenemende specifieke verplichtingen met betrekking tot allerlei aspecten van interconnectie. Dit kan bijvoorbeeld betreffen de verplichting om interconnectie toe te staan, te hanteren interconnectietarieven en kostentoerekeningssystemen, openbaarmaking van gegevens, etc.

Lidstaten dienen in ieder geval alle belemmeringen op te heffen ten aanzien van de mogelijkheid voor partijen – in dezelfde lidstaat of in verschillende lidstaten – om onderling interconnectie overeen te komen. Daarbij dienen de lidstaten de adequate en efficiënte interconnectie met betrekking tot publieke netwerken en -diensten van categorie (C) – vaste spraaktelefonie en huurlijnen – te waarborgen, in de mate als noodzakelijk is om universele voorziening van deze diensten voor alle gebruikers binnen de Europese Unie te verzekeren.

Recht en plicht tot interconnectie
Wie hebben, en in welke mate, recht op en/of verplichting tot interconnectie?
Aanbieders uit de (B)-categorie hebben in beginsel recht op en – indien verzocht – de verplichting tot (onderhandelingen over) *onderlinge* interconnectie. Aanbieders uit de (E)-categorie hebben een verder gaande verplichting: zij dienen te voldoen aan *elk* redelijk verzoek om interconnectie, inclusief verzoeken van dienstenaanbieders voor 'special network access'.

'Leverings'voorwaarden
Van cruciaal belang zijn uiteraard de voorwaarden en kwaliteit, en de prijzen of tarieven van de te verlenen interconnectiediensten. De aanbieders uit de (E)-categorie in het bijzonder dienen de beginselen van non-discriminatie en transparantie in acht te nemen. Dit houdt onder meer in dat zij interconnectiefaciliteiten en -informatie aan anderen ter beschikking moeten stellen onder dezelfde voorwaarden en van dezelfde kwaliteit als die voor hun eigen diensten (of die van dochterondernemingen of partners), en dat interconnectiecontracten – met uitzondering van gevoelige commercieel-strategische informatie – ter openbare inzage worden gelegd. Voorts dienen deze aanbieders – met uit-

zondering van de mobiele exploitanten – zich te houden aan (gedetailleerde) bepalingen betreffende de prijzen/tarieven van interconnectie. Deze dienen kostengeoriënteerd en voldoende opgesplitst ('unbundled') te zijn, en ondersteund te worden door een transparante kostentoerekeningsmethodiek. Onder bepaalde voorwaarden en met inachtneming van bepaalde (gedetailleerde) voorschriften mogen als kostenbestanddeel de (netto)kosten van (de last van) universele dienstverplichtingen opgenomen worden. Met betrekking tot een en ander gelden ook hier bepaalde openbaarmakingsverplichtingen.

Gescheiden boekhouding
Organisaties die publieke telecommunicatienetwerken en/of -diensten aanbieden en exclusieve of bijzondere rechten voor het aanbieden van diensten in andere sectoren hebben, dienen voor de verschillende activiteiten een gescheiden boekhouding te voeren. Hierbij kan gedacht worden aan bijvoorbeeld energiebedrijven of spoorwegen. Dit voorschrift is met name bedoeld om oneerlijke kruissubsidiëring te voorkomen. De verplichting geldt ook voor (verticaal geïntegreerde) organisaties die – volgens aanmerking door de nationale regelgever – significante marktmacht hebben en aan eindgebruikers publieke telecommunicatienetwerken en/of -diensten aanbieden, én interconnectiediensten aan andere organisaties aanbieden. Voor genoemde organisaties geldt de plicht tot gescheiden boekhouding overigens niet indien hun 'telecom-omzet' minder is dan 50 mln. ECU.

Contractsonderhandelingen door partijen
Zoals gezegd wordt prioriteit gegeven aan de 'zelfwerkzaamheid' van partijen. Partijen zelf dienen in onderhandelingen (trachten) te komen tot een interconnectiecontract, uiteraard met inachtneming van – onder meer – de hierboven geschetste voorschriften die als het ware een 'onderhandelingsraamwerk' vormen ([Stra95]). Dit raamwerk bestaat uit een lijst van voorwaarden/onderwerpen – opgenomen in een Bijlage bij de Richtlijn – die uit drie onderdelen is opgebouwd: (1) voorwaarden die *vooraf* door de nationale regelgever vastgesteld moeten zijn; (2) onderwerpen die in interconnectiecontracten geregeld *moeten* zijn; (3) onderwerpen die in interconnectiecontracten geregeld *kunnen* worden.

Opmerkelijk hierbij zijn enkele bepalingen van de Richtlijn over de bevoegdheden en verantwoordelijkheden van de 'national regulatory authorities' in dezen. Het desbetreffende overheidsorgaan mag onder andere, indien gerechtvaardigd bijvoorbeeld om effectieve concurrentie en/of interoperabiliteit van diensten voor gebruikers te waarborgen, interveniëren in onderhandelingen of veranderingen eisen in reeds tot stand gekomen interconnectiecontracten, of zelfs interconnectie opleggen. Voorts dient door de regelgever te worden voorzien in een procedure voor geschillenbeslechting, voor het geval partijen niet tot overeenstemming kunnen komen. Daarbij kan een (wettelijk geregelde) tijdlimiet aan partijen worden gesteld om tot afronding van hun onderhandelingen te komen. Andere verantwoordelijkheden van de nationale regelgever liggen op het gebied van 'essential requirements', collocatie, nummerbeheer, technische standaarden, publicatie van gegevens, beslechting van grensoverschrijdende (interconnectie)geschillen en het verstrekken van inlichtingen aan de Europese Commissie.

SLOT

In het voorgaande is een beeld geschetst van (aspecten van) de interconnectieproblematiek in een toenemend competitief wordende telecommunicatie-omgeving. Aangegeven is dat door technologische en marktontwikkelingen, alsmede door ontwikkelingen in telecommunicatiebeleid en -regelgeving er een breed scala van interconnectierelaties kan bestaan en ook zal ontstaan. Met betrekking tot de daadwerkelijke totstandbrenging van interconnectie wordt prioriteit gegeven aan (commerciële) contractonderhandelingen door partijen zelf. Voor deze onderhandelingen – en voor enkele andere relevante interconnectie-onderwerpen – zijn specifieke regels aangegeven in de Europese (voorstel-)*Richtlijn Interconnectie*. Daarbij worden met name voorschriften opgelegd aan aanbieders van publieke telecommunicatienetwerken en/of -diensten die significante marktmacht hebben; voorts worden vrij vergaande bevoegdheden tot interventie toegekend aan de nationale regelgevende of toezichthoudende instanties. Van cruciaal belang voor de betrokkenen, zowel de contracterende partijen als de eindgebruikers, zal zeker zijn wanneer en op welke wijze bedoelde instantie zal interveniëren. Op basis van welke criteria of methodologie bijvoorbeeld zal en kan in de praktijk beoordeeld worden dat 'kostengeoriënteerde interconnectieprijzen' overeengekomen zijn, of moeten worden? De 'vertaling' en nadere uitwerking van de Richtlijnbepalingen in de nationale telecommunicatiewetgeving zal nog de nodige hoofdbrekens kosten. Een nadere bespreking van deze problematiek zal, gezien het huidige tijds- en ruimtebestek, op een volgende gelegenheid moeten wachten.

LITERATUUR

[Duiv96] G.P. van Duijvenvoorde, *Een nieuw kader voor ONP*, Nederlands tijdschrift voor Europees recht, 1996/5.

[Groe94] *Groenboek inzake de liberalisering van telecommunicatie-infrastructuur en kabeltelevisienetwerken, Deel I*, COM(94)440 def. 25 oktober 1994 en *Deel II*, COM(94)682 def. 25 januari 1995.

[Hoge93] G. Hogesteeger, *Van lopende bode tot telematica*, Groningen 1989.

[Medi93] Mediaraad, *Advies van de Mediaraad inzake herstructurering beleid informatievoorziening, Deel I: het Informatietransport*, juni 1993.

[NEHA93] NEHA, *Openbare nuts- en communicatiebedrijven. Een geschiedenis en bronnenoverzicht*, Amsterdam 1993.

[Netw94] *Network Interconnection in the Domain of ONP*, studie voor DG XIII van de Europese Commissie, Eindrapport november 1994.

[Noam92] E. Noam, *Telecommunications in Europe*, Oxford University Press 1992.

[ONP90] *ONP-(kader)Richtlijn 90/387 betreffende het totstandbrengen van de interne markt voor telecommunicatiediensten d.m.v. tenuitvoerlegging van Open Network Provision*, 28 juni 1990, Pb. L 192/01.

[ONP92] *ONP-Richtlijn Huurlijnen 92/44*, 5 juni 1992, Pb. L 165/27.

[ONP95] *ONP-Richtlijn Spraaktelefonie 95/62*, 13 december 1995, Pb. L 321 van 30-12-1995.

[Rich95] *Voorstel aan het Europese Parlement en de Raad voor een Richtlijn betreffende Interconnectie in Telecommunicatie*, 19 juli 1995, COM(95)379.

[Rich96a] *Richtlijn 90/388 (de 'Diensten'Richtlijn)*, laatstelijk gewijzigd door *Richtlijn 96/19* 13 maart 1996, *betreffende de implementatie van volledige mededinging in telecommunicatiemarkten*.

[Rich96b] *Richtlijn 95/51 (Kabeltelevisienetten) en Richtlijn 96/2 (Mobiele communicatiediensten)*.

[Scha94] H. Schaffers, *Interconnectie en concurrentie in de telecommunicatie*, TNO-rapport STB/94/005, februari 1994.

[Stra95] A. van Straalen en P. de Roover, *Interconnectie: onderhandelen of reguleren?*, Informatie & Informatiebeleid, 1995/2.

[Walk93] D. Walker en J. Solomon, *The interconnection imperative*, Telecommunications Policy, may/june 1993.

Mr. drs. E.F. Clarkson
Is werkzaam als universitair docent bij de sectie Recht en Techniek aan de faculteit Technologie Management van de Technische Universiteit Eindhoven.

Bescherming van databases

Mr. A.P. Meijboom

Het commercieel kunnen gebruiken van databases maakt de auteursrechtelijke bescherming ervan nodig. Naast de Auteurswet zal binnen afzienbare tijd ook de Europese databaserichtlijn van toepassing zijn. Er is een aantal rechthebbenden aan te wijzen.

INLEIDING

Door de snelle ontwikkelingen in de informatica en telematica zijn databanken voor een steeds groter publiek toegankelijk en bovendien eenvoudiger actueel te houden. Vanuit commercieel oogpunt zijn databanken dan ook steeds belangrijker geworden. Traditioneel bestonden databases uit gegevensverzamelingen op papier, bijvoorbeeld als lijsten met gegevens (zoals het telefoonboek of het spoorboekje), en gaandeweg werden gegevensverzamelingen op een gestructureerde wijze in de computer opgeslagen. Aangezien voor een commerciële toepassing van databases grote opslagcapaciteit én – meer in het bijzonder – snelle toegang tot de gegevens vereist zijn, is eerst in de jaren tachtig voor een grotere groep personen toegang tot databases gerealiseerd. De eerste toepassing was via *online*-benadering van een centraal opgesteld bestand, later hebben commerciële uitgevers databanken op gegevensdragers (CD-ROM's) uitgebracht. Veel *multimedia* CD-ROM's zijn in feite niets anders dan elektronische databases en *Internet* zelf kan ook als een verzameling van allerlei verschillende databases worden gekenschetst.

Voor de vraag naar juridische bescherming van databases is het vanzelfsprekend relevant om te bepalen waarover we spreken. Een database kan worden gedefinieerd als een op enige wijze geordende verzameling van gegevens die op een of andere wijze kan worden gemanipuleerd (bewerkt, aangevuld, geraadpleegd, etc.) – al dan niet elektronisch. Er zijn verschillende aspecten aan databases te onderscheiden, die voor het beschermingsvraagstuk relevant zijn.

De essentie van een database is dat zij bepaalde gegevens bevat die op een bepaalde wijze zijn geordend. De gegevens die een database bevat kunnen 'naakte feiten' (bijvoorbeeld de namen en adressen van alle abonnees op een bepaald tijdschrift – dit zijn zogenaamde 'NAW-gegevens') en samengestelde gegevens zijn. De laatste kunnen ook weer zeer divers zijn: jurisprudentie, elektronische berichten, teksten van artikelen, foto's, etc. Deze *inhoud* van databases wordt in beginsel *niet* als voorwerp van databasebescherming gezien. De vraag of bijvoorbeeld de foto's op een foto-CD-ROM door intellectueel eigendomsrecht zijn beschermd, dient zelfstandig beantwoord te worden. In het algemeen zal de inhoud van een database door auteursrecht zijn beschermd. Wél interessant in het kader van het onderwerp van databasebescherming is de vraag of het compileren van gegevens en werken is toegestaan en, zo dit geschiedt, tot een nieuw, beschermbaar werk leidt.

Een tussenopmerking verdient dat de *impact* van exploitatie van elektronische databases ten opzichte van papieren databases veel groter kan zijn, waardoor de economische positie van de rechthebbenden op de inhoud van databases kan worden benadeeld. De rechter zal mogelijk de uitzonderingen op de verbodsrechten van de auteur in dit licht waarderen. Aanwijzing daarvoor is bijvoorbeeld de procedure over de LiteROM – een CD-ROM met daarop onder meer boekrecensies – waarvan de

samensteller betoogde dat dit zou zijn toegestaan omdat het een 'digitale (literaire) knipselkrant' zou zijn, die zonder toestemming van de makers mag worden vervaardigd (Rb. Den Haag 3 mei 1995, *Computerrecht* 1995, blz. 175). De rechtbank oordeelt echter, nadat zij heeft overwogen dat de LiteROM via allerlei ingangen kan worden benaderd: *'Gelet op de wijze waarop raadpleging kan geschieden en de volledigheid van de opgeslagen gegevens, is hier veeleer sprake van een* databank *(dan van een knipselkrant)'*.

Steeds meer databases staan in de computer en zijn dientengevolge elektronische databases. Om dergelijke databases te benaderen is het nodig een *zoekprogramma* (i.e. een computerprogramma) te gebruiken. Dit computerprogramma wordt veelal tezamen met de gegevensverzameling aangeboden en de twee zijn meestal op een voor de gebruiker onherkenbare manier geïntegreerd. Desondanks dient de computerprogrammatuur die een database *bestuurt* als een van de database separaat object van bescherming te worden aangemerkt. Er bestaat afzonderlijke auteursrechtelijke softwarebescherming, die is geïnitieerd door de Europese Gemeenschap ([Rl 91/250], artt. 45h t/m 45n Auteurswet 1912 (*Aw*)[1]), terwijl in sommige gevallen ook nog de mogelijkheid van octrooirechtelijke bescherming bestaat ([Meij92]).

EUROPESE DATABASERICHTLIJN

Sinds het begin van de jaren negentig houdt de Europese Commissie zich bezig met het vraagstuk van databasebescherming omdat zij meende dat de uiteenlopende bescherming van databases een negatieve invloed op de interne markt heeft, in het bijzonder omdat deze vrij verkeer van goederen en diensten via online-databases zou belemmeren.

Tijdens een hoorzitting die de Commissie in april 1990 over het onderwerp organiseerde bleek dat belanghebbenden van mening waren dat er behoefte was aan harmoniserende maatregelen ter bescherming van databases én dat iedereen van mening was dat databases door auteursrecht beschermd (dienen te) zijn. Dit leidde ertoe dat reeds in 1991 een ontwerp-richtlijn werd gepubliceerd, die, met de nodige aanpassingen, in 1992 in een definitief formeel voorstel voor een richtlijn is omgezet.

Het voorstel van de Commissie zou alleen aan elektronische databases bescherming bieden en wel op twee wijzen. Allereerst bepaalde het voorstel dat op grond van nationale wetgeving van lidstaten databases auteursrechtelijk dienen te zijn én dat er een nieuw, *sui generis*, recht in het leven geroepen dient te worden dat de maker van een database bescherming biedt tegen het geheel of gedeeltelijk voor commerciële doeleinden opvragen en hergebruiken van de inhoud van zijn database.

Vanzelfsprekend is veel commentaar gekomen op het voorstel en, nadat het Economisch en Sociaal Comité en het Europees Parlement zich over het voorstel hebben uitgelaten en het laatste een aantal amendementen heeft voorgesteld, heeft de Commissie in 1993 een gewijzigd voorstel openbaar gemaakt dat door de Raad op 10 juli 1995 als gemeenschappelijk standpunt is vastgesteld. Op 11 maart 1996 is het gemeenschappelijk standpunt omgezet in een definitieve richtlijn, die door de lidstaten uiterlijk op 1 januari 1998 in nationale wetgeving moet zijn geïmplementeerd ([Rl 96/6]). In de komende jaren zal Nederland derhalve de Auteurswet 1912 (en wellicht tevens de Wet op de naburige rechten) aanpassen om onderdak te bieden aan databasebescherming.

Databanken kunnen door de keuze of de rangschikking van de stof een eigen intellectuele schepping van de maker vormen.

Het begrip 'database'

Onder het regime van de richtlijn zal een 'database' niet alleen een elektronische database zijn, maar ook de meer traditionele, handmatige database. De door de richtlijn gebezigde definitie luidt *'een verzameling van werken, gegevens of andere zelfstandige elementen, systematisch of methodisch geordend, en afzonderlijk, met elektronische middelen of anderszins toegankelijk'*. Een database is derhalve een compilatiewerk dat onafhankelijk van de drager (papier, diskette, CD-ROM, CD-i, hard disk, etc.) bestaat en op allerlei manieren (met de hand, met een CD-speler, via een computernetwerk, etc.) kan worden benaderd en geraadpleegd.

> Overweging 17 bij de richtlijn legt nadruk op de systematische of methodische ordening van de zelfstandige elementen van een database en de afzonderlijke toegankelijkheid daarvan. Dit betekent volgens deze overweging *'dat de vastlegging van een audiovisueel, cinematografisch, literair of muzikaal werk als zodanig niet binnen het toepassingsgebied van deze richtlijn valt'*. Ik betwijfel dat in geval van bijvoorbeeld doorsnee muziek-CD's met daarop een verzameling van nummers, verhalen- en gedichtenbundels, etc.

Van belang is zich te realiseren dat de richtlijn alleen maar van toepassing is op de keuze of de rangschikking van het in een database vervatte materiaal en *niet* op de inhoud zelf. Met andere woorden, databasebescherming is bescherming van de structuur, de opzet, maar kan tevens de thesaurus en het indexeringssysteem omvatten indien deze van de database onderdeel uitmaken.

1. Dat dit onderscheid niet altijd even goed begrepen wordt, blijkt bijvoorbeeld uit Pres. Rb. Breda 12 oktober 1994, Computerrecht 1995, blz. 120, m.nt. Stuik. De CD-foongids van PTT Telecom, met daarop alle telefoonboeken, kan volgens de president niet (langer) als onpersoonlijk geschrift (infra) worden beschermd omdat het bestand computerprogrammatuur zou zijn, waarvoor de regeling niet langer geldt.

AUTEURSRECHTELIJKE BESCHERMING

Databases worden, zoals al eerder gezegd, in beginsel beschermd door het auteursrecht. Daarvoor is natuurlijk wél vereist dat ze oorspronkelijk zijn, dat wil zeggen een eigen, oorspronkelijk karakter hebben en het persoonlijk stempel van de maker dragen. Dit laatste criterium in deze bewoordingen vindt zijn oorsprong in misschien wel de bekendste procedure die in Nederland over databasebescherming is gevoerd, de *Van Dale/Romme* zaak (Hoge Raad 4 januari 1991, *Computerrecht* 1991, blz. 84, met noot Hugenholtz). In deze procedure stond de vraag centraal of de verzameling van Nederlandse woorden ten behoeve van de 'Dikke Van Dale' oorspronkelijk is. De Hoge Raad heeft het arrest van het Hof Amsterdam vernietigd omdat het onvoldoende heeft onderzocht of de *'verzameling het resultaat (is) van een selectie die een persoonlijke visie van de maker tot uitdrukking brengt'*, waarbij overwogen wordt dat het een verzameling van woorden die deel uitmaken van de Nederlandse taal betreft die in beginsel niet meer is dan *'een hoeveelheid feitelijke gegevens die als zodanig voor auteursrechtelijke bescherming niet in aanmerking komt'*. Enkele schrijvers hebben betoogd dat de Hoge Raad met zijn arrest een criterium voor oorspronkelijkheid heeft willen maken dat strenger is dan tot dan toe gebruikelijk.

Uitputting heeft enkel betrekking op de verkoop van exemplaren.

Het oorspronkelijkheidscriterium dat de richtlijn gebruikt is verwant aan het *Van Dale/Romme* criterium en is in de considerans te vinden. Daar wordt gesteld dat de *structuur* van een database auteursrechtelijk is beschermd indien zij *'door de keuze of rangschikking van haar inhoud een eigen intellectuele schepping van de auteur vormt'*. Kwantitatieve en esthetische criteria mogen hierbij geen rol spelen.

Een database die bestaat uit 'geschriften' – waarbij de heersende leer is dat het in beginsel irrelevant is of de geschriften op papier staan of op, bijvoorbeeld, een magnetische drager – kan, indien zij niet oorspronkelijk is, toch beschermd worden door het auteursrecht tegen directe ontlening op grond van het leerstuk van de 'onpersoonlijke geschriftenbescherming'[2] ([Verk92]). Hiervoor is wél vereist dat de onpersoonlijke database openbaar is gemaakt of daarvoor is bestemd. Het interne (elektronische) adressenbestand van een tijdschrift dat door een werknemer wordt meegenomen om voor zijn eigen, nieuwe tijdschrift te gebruiken is derhalve niet beschermd.[3]

Het laatste woord over de vraag of de onpersoonlijke geschriftenbescherming voor databases blijft gelden is overigens nog niet gezegd. De richtlijn bepaalt uitdrukkelijk dat zij van toepassing is op *'databanken die door de keuze of de rangschikking van de stof een eigen intellectuele schepping van de maker vormen'*. Via een *a contrario* redenering zullen niet-oorspronkelijke databases dan buiten de boot vallen. Ik wijs in dit verband naar de uitkomst van de verhitte discussie over de vraag of niet-oorspronkelijke computerprogramma's op grond van de softwarerichtlijn uit 1991 bescherming verdienden. Art. 10 lid 1, laatste zin bepaalt uitdrukkelijk dat dit *niet* het geval is. Voor databases behoeft dit overigens niet bezwaarlijk te zijn omdat de richtlijn immers uitdrukkelijk voorziet in een bescherming tegen opvraging en hergebruik van delen van een database, ongeacht of zij oorspronkelijk is.

De rechthebbende

De *auteurs*rechthebbende[4] op een database wordt gedefinieerd door het normale auteursrecht (artt. 1-9 Aw). Dit is derhalve in beginsel de natuurlijke persoon, c.q. de werkgever van de maker in dienstverband, c.q. de openbaarmakende rechtspersoon. De Auteurswet duidt de rechthebbende als 'maker' aan, bij welk begrip ik mij vanzelfsprekend aansluit.

Exclusieve rechten

Het auteursrecht verschaft de maker het recht om derden gedurende de normale auteursrechtelijke duur van ten minste zeventig jaar te verbieden bepaalde handelingen te verrichten. Deze handelingen – openbaarmaken en verveelvoudigen van het werk – betreffen de exclusieve rechten van de maker. De exclusieve rechten van de maker op grond van de richtlijn zijn de gehele of gedeeltelijke reproductie van de database 'met ieder middel en in iedere vorm', vertaling, bewerking, schikking en iedere andere verandering. Dit sluit aan bij het begrip 'verveelvoudigen' van art. 13 Aw. Verder komt volgens de richtlijn aan de maker het uitsluitend recht toe om de database of kopieën daarvan openbaar te verspreiden, en heeft hij het recht van 'elke mededeling (hiermee wordt waarschijnlijk bedoeld het verschaffen van inzicht in de inhoud en structuur van de database aan derden, *AM*), voorstelling of demonstratie voor het publiek'. Dit ligt besloten in het begrip 'openbaarmaken' van art. 12 Aw. Ten slotte heeft de maker ook nog het recht om de resultaten van vertaling, bewerking, schikking en mogelijke andere veranderingen van de database verder te reproduceren, verspreiden of hiervan mededeling, voorstelling of demonstratie voor het publiek te verzorgen. Alhoewel de richtlijn hierover niet expliciet is, gelden mijns inziens de in de vorige zin genoemde exclusieve rechten onverminderd de rechten van derden die de bewerking hebben verricht (voorzover een dergelijke bewerking overigens oorspronkelijk is).

Uitputting

Vermeldenswaard is verder nog dat de richtlijn een zogenoemde *communautaire uitputtingsregeling* kent, evenals bijvoorbeeld de softwarerichtlijn en de eerste merkenrichtlijn. Dit wil zeggen dat de maker over een exemplaar van de database die met

2. Een voorbeeld uit de (papieren) database-jurisprudentie waarin inbreuk op grond van de onpersoonlijke geschriftenbescherming is aangenomen: Rb. Haarlem 17 mei 1989, Computerrecht 1990, blz. 132. Uit Pres. Rb. Breda 12 oktober 1994 (supra, noot 1) kan a contrario worden afgeleid dat elektronische geschriften ook onder de regeling vallen.

3. Pres. Rb. Haarlem 5 december 1989, Computerrecht 1990, blz. 133.

4. Ter onderscheiding van de rechthebbende op de sui generis bescherming (infra).

zijn toestemming (bijvoorbeeld door de maker zelf of door zijn distribiteur) *in de Europese Economische Ruimte* in het verkeer is gebracht – de richtlijn spreekt overigens van eerste verkoop – de zeggenschap ter zake van verdere verspreiding van het bewuste exemplaar verliest ([Czar92], [Groe95]). De maker kan derhalve wél de doorverkoop van kopieën van de database die *buiten* de EER in het verkeer zijn gebracht verbieden. Hierbij passen twee opmerkingen.

Allereerst heeft uitputting alleen maar betrekking op de *verkoop* van exemplaren en derhalve niet op andere vormen van openbaarmaking en/of verveelvoudiging. Uitputting is derhalve niet van belang voor online-databases omdat deze gekopieerd moeten worden in geval van downloaden. Voorts is verdedigbaar dat de richtlijn, doordat zij het begrip 'uitputting' aan het begrip 'verkoop' verbindt, uitdrukkelijk bedoelt deze vorm van distributie af te zonderen van andere vormen van distributie, zoals verhuur of licentiëring, waarvoor de uitputtingsregeling dan niet geldt. Dit analoog aan de redenering voor [Rl 91/250]; zie [Czar92].
Ten tweede is op te merken dat de richtlijn ten tijde van het schrijven van deze bijdrage (juni 1996) voorlopig nog niet in Nederlandse wetgeving is omgezet. Vaste rechtspraak van het Hof van Justitie EG schrijft weliswaar richtlijnconforme interpretatie voor, maar bij gebrek aan (auteurs)wettelijke bepalingen ter zake van uitputting mag hiervan niet te veel worden verwacht. Communautaire uitputting van databases zal waarschijnlijk pas werken vanaf de inwerkingtreding van de Nederlandse implementatiewetgeving (1998 of later).[5]

Rechten van de 'rechtmatig gebruiker'

Evenals de softwarerichtlijn dit doet verschaft de richtlijn aan *rechtmatige gebruikers* van databases bepaalde rechten die een uitzondering op de exclusieve rechten van de maker vormen. Het gaat om gebruikers die door de maker zijn gelicentieerd of die op rechtmatige wijze een kopie van de database hebben verworven.
Een rechtmatige gebruiker is bevoegd alle handelingen te verrichten die noodzakelijk zijn om toegang te krijgen tot en normaal gebruik te maken van de inhoud van de database. De lidstaten wordt nog de keuze gelaten om in de implementatiewetgeving verder gaande beperkingen op de exclusieve databankrechten te geven, voor reproductie ten behoeve van privé-gebruik (de richtlijn zegt: 'reproductie voor particuliere doeleinden') van een *niet-elektronische* database, ter illustratie van niet-commercieel onderwijs of wetenschappelijk onderzoek, en voor gebruik voor openbare veiligheid of het goede verloop van een gerechtelijke procedure.

SUI GENERIS BESCHERMING VAN DATABASES

De richtlijn creëert een nieuw recht voor de 'fabrikant' van een database om opvraging[6] en hergebruik[7] van 'het geheel of een in kwalitatief of kwantitatief opzicht substantieel deel' van de inhoud van de database tegen te gaan, ongeacht of de database een oorspronkelijk, auteursrechtelijk beschermd werk is. In tegenstelling tot de hiervoor besproken auteursrechtelijke bescherming van databases gaat het derhalve om de bescherming van de *inhoud* van de database (teksten, foto's, etc.) en niet zozeer om de structuur daarvan.
De regeling beoogt de investeringen in de database te beschermen zodat zij alleen bescherming biedt indien de verkrijging, de controle of de presentatie van de database getuigt van een in kwalitatief of kwantitatief opzicht aanzienlijke investering.

Sui generis bescherming komt toe aan de fabrikant van de database.

Fabrikant

Sui generis bescherming komt toe aan de fabrikant van de database. Wie dit is maakt de richtlijn zelf niet duidelijk en ook andere taalversies van de richtlijn bieden geen duidelijkheid.[8] In de considerans wordt echter opgemerkt dat *'de fabrikant van een databank degene is die het initiatief neemt tot en het risico draagt van de investeringen; dat dit met name de toeleverancier uitsluit van de definitie van fabrikant'*. Waarschijnlijk wordt bedoeld dat de fabrikant degene is die kan worden vergeleken met de fonogrammenproducent uit de Wet op de naburige rechten ([Verk93]) of de filmproducent van art. 45a Aw.
Aangezien het niet denkbeeldig is dat de fabrikant een andere persoon is dan de maker van de database, respectievelijk de rechthebbende op de inhoud daarvan – op grond van auteursrecht en/of naburige rechten – kan een interessant probleem ontstaan in geval van onrechtmatige opvraging van de database. De fabrikant dient te bewijzen dat de inspanningen om de database te maken substantieel zijn geweest, de maker van de database dat de structuur en keuzen oorspronkelijk zijn en de maker van de inhoud van de database dat het gaat om oorspronkelijke werken.

Beschermingsduur

De richtlijn beschermt de fabrikant vijftien jaar nadat de 'fabricage van de databank' is voltooid, dan wel nadat de databank binnen vijftien jaar na 'fabricage' voor het eerst ter beschikking van het publiek werd gesteld na voltooiing (derhalve is door cumulatie een beschermingstermijn van maximaal dertig jaar mogelijk). Indien een database in kwalitatief of kwantitatief opzicht aanzienlijk verandert, gaat deze termijn opnieuw lopen. Onduidelijk is of deze vernieuwing geleidelijk mag verlopen (denk aan dynamische, regelmatig vernieuwde databases), en zo ja, wanneer de nieuwe termijn van vijftien jaar in een dergelijk geval gaat lopen.

5. Ik verwijs naar Pres. Rb. Den Haag 7 juli 1995, Computerrecht 1995, blz. 281 (Novell/America Direct), in welke uitspraak de president communautaire uitputting aannam voor programmatuur op grond van de geïmplementeerde softwarerichtlijn, maar uitdrukkelijk de Benelux Merkenwet niet merkenrichtlijnconform wilde interpreteren.
6. Gedefinieerd als 'het permanent of tijdelijk overbrengen van de inhoud van een databank of een substantieel deel ervan op een andere drager, ongeacht op welke wijze of in welke vorm.'
7. Gedefinieerd als 'elke vorm van het aan het publiek ter beschikking stellen van de inhoud van een databank of een substantieel deel ervan, door verspreiding van kopieën, verhuur, on line transmissie of in andere vorm.'
8. De Engelse versie spreekt van de 'maker of the database'. De maker in auteursrechtelijke zin wordt daar de 'author' genoemd.

Mr. A.P. Meijboom
Is partner van Kennedy Van der Laan advocaten te Amsterdam, en gespecialiseerd in informatica- en intellectueel eigendomsrecht. Van 1985 tot 1992 was hij wetenschappelijk onderzoeker bij het Instituut voor Informatica en Recht van de Vrije Universiteit Amsterdam en sinds 1990 is hij advocaat. Hij publiceert en spreekt regelmatig over het informaticarecht in binnen- en buitenland. Mr. Meijboom is redacteur informaticarecht van de tijdschriften Ars Aequi (Katern) en Bedrijfsjuridische Berichten, en editor rechtspraak van het tijdschrift Computerrecht. Hij is mede-oprichter en bestuurslid van de specialistenvereniging voor in het IT-recht gespecialiseerde advocaten, VIRA, alsmede lid van vele nationale en internationale organisaties.

Reciprociteit

Op grond van internationale verdragen geldt het beginsel van nationale behandeling voor makers van (auteursrechtelijk beschermde) databases uit niet-EU-lidstaten. Dit geldt niet voor het sui generis recht, zodat de richtlijn, zoals inmiddels gebruikelijk is, bepaalt dat alleen fabrikanten die, kort gezegd, gevestigd zijn in de EU beschermd zijn. Het beginsel van reciprociteit vindt dan alleen maar toepassing op basis van (nu nog niet bestaande) bi- of multilaterale verdragen.

In dit verband verwijs ik naar de Agreement on Trade Related Intellectual Property Rights ('TRIPs') – dat in het kader van de laatste GATT-ronde tot stand is gekomen en een bepaald minimumniveau van bescherming van intellectuele eigendom voorschrijft – dat reciprociteit voorschrijft en bepaalt dat gegevensverzamelingen dienen te worden beschermd. Dit heeft echter alleen betrekking op de in de Berner Conventie neergelegde regeling ter zake van auteursrechtelijke bescherming van makers van dergelijke verzamelingen en *niet* op sui generis bescherming van fabrikanten.

CONCLUSIE

Reeds nu bestaat een flink aantal Nederlandse rechterlijke uitspraken op grond waarvan de structuur – los van de inhoud – van een database auteursrechtelijk wordt beschermd. Van bijzonder belang is in dit verband het hierboven aangehaalde arrest inzake *Van Dale/Romme*.
De databaserichtlijn, die op 1 januari 1998 in onze nationale wetgeving moet zijn opgenomen, vereist náást auteursrechtelijke bescherming tevens *sui generis* bescherming van de kwantitatieve of kwalitatieve inspanningen van de fabrikant van de database. Dit is nog geen onderdeel van positief Nederlands recht en het is maar de vraag of een rechter een dergelijk recht zal willen aanvaarden voor de inwerkingtreding van de Nederlandse 'databasewet'.
Desalniettemin is het Nederlandse intellectueel eigendomsrecht in het verleden genoeg flexibel gebleken om 'Fremdkörper' zoals bijvoorbeeld software op een redelijk bevredigende manier bescherming te bieden. In de korte tijd die ons nog scheidt van een echte 'databasewet' naar Europees model mag dit ook verwacht worden voor (auteursrechtelijke bescherming van) databases.

LITERATUUR

[Czar92] B. Czarnota en R. Hart, *Legal Protection of Computer Programs in Europe – A Guide to the EC Directive*, blz. 59-60.

[Groe95] Groenboek van de Commissie betreffende *'Copyright and Related Rights in the Information Society'*, COM(95) 382 final, blz. 44 e.v.

[Meij92] A.P. Meijboom, *Octrooieerbaarheid van software-gerelateerde uitvindingen*, in: Franken, Kaspersen en De Wild (red.), *Recht en Computers*, 2e druk, blz. 98 e.v.

[Rl 91/250] Richtlijn 91/250/EG van de Raad van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's, *Publikatieblad EG* Nr. L 122/42 e.v.

[Rl 96/6] Richtlijn 96/6/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken, *Publikatieblad van de EG* Nr. L 77/20 e.v.

[Verk92] D.W.F. Verkade en J.H. Spoor, *Auteursrecht*, 2e druk, blz. 72 e.v.

[Verk93] D.W.F. Verkade en D. Visser, *Parlementaire geschiedenis WNR.*

De Wet persoons-registraties: wet voor buitenstaanders en ingewijden

Mw. prof. mr. J.E.J. Prins

De Wet persoonsregistraties blijkt in de praktijk nogal eens vergeten te worden door zowel de geregistreerden als de houders van registraties. Weliswaar meldt men zich keurig aan, maar met de verdere naleving is het minder goed gesteld. De resultaten van een onderzoek dienaangaande maken dit duidelijk.

INLEIDING

Aan het slot van het boek *In het licht van de Wet persoonsregistraties: zon, maan of ster* wordt vastgesteld dat de Wet persoonsregistraties (WPR) is te typeren als een wet voor buitenstaanders en ingewijden. In de zeven jaar van haar bestaan is de WPR vrijwel ontsnapt aan de aandacht van degenen voor wie zij bedoeld was: de geregistreerden. Buitenstaanders blijken ook zij te zijn die in de dagelijkse praktijk uitvoering moeten geven aan een ingewikkeld, moeilijk toegankelijk en slechts in geringe mate bruikbaar regelsysteem. Zo blijft de WPR een wet voor ingewijden.

Het voornoemde boek concludeert eveneens dat onze informatiesamenleving snel in een samenleving-op-maat verandert. Een samenleving die is gestoeld op een nauwe betrokkenheid van het individu bij productie- en dienstverlenende processen. Bovendien blijkt dit vaak een betrokkenheid te zijn die er in toenemende mate is zonder dat men zich daarvan bewust is. Denk bijvoorbeeld aan de via spaarsystemen eenvoudig aan te leggen digitale dossiers met het koopgedrag van consumenten. De bescherming van de persoonlijke levenssfeer zal in de verschuiving naar een samenleving-op-maat mee moeten gaan. Juist om deze reden zal de wetgeving inzake de bescherming van persoonsgegevens een systeem van normen moeten zijn, waarin, ook als het om de bescherming van de persoonlijke levenssfeer gaat, de 'buitenstaander' een 'ingewijde' wordt.

Dit artikel bevat een bespreking van de achtergronden en de belangrijkste uitkomsten van voornoemd boek, omdat daarin de resultaten zijn neergelegd van een studie naar mogelijke aanknopingspunten voor de 'mentaliteitsverandering' rondom de bescherming van persoonsgegevens. Nadat allereerst kort aandacht is besteed aan de achtergronden en doelstellingen van het onderzoek, worden aan de hand van de onderzoeksvragen die in het boek zijn behandeld de belangrijkste uitkomsten weergegeven.

ACHTERGRONDEN

In het najaar van 1994 verzocht het Ministerie van Justitie een onderzoeksteam van het Centrum voor Recht en Informatisering van het Schoordijk Instituut van de Katholieke Universiteit Brabant een onderzoek te verrichten naar de dagelijkse omgang met de WPR. Voor het ministerie speelden verschillende overwegingen een rol bij het besluit deze zogenaamde sociaal-wetenschappelijke evaluatie van de WPR uit te laten voeren.[1] Een eerste overweging was gelegen in de wens inzicht te krijgen in de *feitelijke* naleving van de WPR. Ten tweede kon een dergelijke evaluatie een rol spelen bij het aanbrengen van verbeteringen in bestaande wetgeving en het definiëren van criteria voor de nieuwe wetgeving. Zoals wellicht bekend, is nieuwe wetgeving noodzakelijk geworden doordat in 1995 op Europees niveau een richtlijn bescherming persoonsgegevens is aangenomen die uiterlijk in het najaar van 1998 in onze nationale wetgeving moet zijn geïmplementeerd. Ten slotte kwam het Ministerie van Justitie met de evaluatie tegemoet aan de indertijd, bij de behandeling van de WPR, door het parlement geuite wens daartoe. Het onderzoek is door het Centrum voor Recht en Informatisering in samenwerking met het IVA[2] uitgevoerd.

DOELSTELLING VAN HET ONDERZOEK

De belangrijkste doelstelling van het onderzoek was het in kaart brengen van de bijdrage die de WPR levert aan de bescherming van persoonsgegevens. Hierbij is niet de weg van een analyse van de diverse juridische haken en ogen bewandeld, maar bekeken welke factoren de naleving van de WPR in de praktijk belemmeren of bevorderen. Met andere woorden, het onderzoek concentreerde zich op het niveau van de 'werkvloer' binnen organisaties van houders en/of bewerkers. Daarbij is overigens niet uitsluitend een inventarisatie en analyse van bestaande knelpunten uitgevoerd, maar is eveneens gekeken naar problemen rondom de toekomstige wetgeving op het terrein van bescherming van persoonsgegevens. Ook ontwikkelingen op het gebied van de informatie- en communicatietechnologie, economie en bedrijf, politiek-bestuurlijke ontwikkelingen, en maatschappelijke ontwikkelingen zijn meegenomen.

Voor het verkrijgen van het inzicht in de omgang met de WPR op de werkvloer is een survey uitgezet onder 476 bij de Registratiekamer bekende houders en zijn casestudies uitgevoerd bij zes organisaties (twee in de private sector, twee in de semi-publieke sector, twee in de publieke sector), te weten: een bank, een postorderbedrijf, een ziekenhuis, een instelling voor HBO, een gemeentelijke sociale dienst en een eenheid Particulieren van de Belastingdienst.
Ook is getracht de geregistreerde in beeld te krijgen. Dit is gedaan via een survey onder 553 personen die bij één van de zes casestudie-organisaties waren geregistreerd. Aan hen zijn vragen gesteld die in z'n algemeenheid op de privacy betrekking hadden en die specifiek zagen op hun positie als geregistreerde bij één der organisaties (geregistreerd als patiënt, scholier, bankcliënt, etc.). Aldus is geprobeerd inzicht te krijgen in het oordeel van geregistreerden inzake diverse door de WPR beoogde aspecten van de bescherming van persoonsgegevens.[3]

ZES ONDERZOEKSVRAGEN

Aan de hand van de zes onderzoeksvragen worden de resultaten van het onderzoek nu stap voor stap behandeld.

Naleving van de WPR

De eerste onderzoeksvraag luidde kortweg: 'Hoe staat het met de naleving van de WPR?'
Het onderzoeksteam stelde vast dat het met de naleving van de wet als regelsysteem niet best is gesteld. Bij het overgrote deel van de houders geven de bepalingen van de WPR nauwelijks richting aan de dagelijkse praktijk. Naleving – zo laat het onderzoek zien – houdt veelal op op het moment dat de enveloppe naar de Registratiekamer op de bus is gedaan. In het algemeen wordt er wat betreft de formele procedures (de aanmelding van de registratie, het voorlichten van betrokkenen, etc.) weinig onderhoud aan persoonsregistraties gepleegd. Wel kon hierbij gelukkig worden vastgesteld, dat houders van zogenaamde gevoelige registraties zorgvuldiger met de gegevens omgaan dan houders die geen gevoelige registraties bijhouden.
Het onderzoeksteam stelde verder vast dat de zorgvuldige omgang met persoonsgegevens in de dagelijkse praktijk vooral afhankelijk is van andere factoren dan de normen en richtlijnen van het WPR-regime. Hierbij kan met name worden gedacht aan het eigenbelang van de organisaties, het persoonlijk commitment en de professionele normen van de medewerkers. In organisaties met een sterk professionele cultuur (zoals een ziekenhuis of de belastingdienst) wordt de naleving van de regels vooral bepaald door andere normen dan die neergelegd in de WPR.
Tevens bleek uit het onderzoek dat van een actieve benadering van de geregistreerde slechts zelden sprake is. Opvallend in dit licht is dat wanneer houders zich actief naar geregistreerden opstellen dit een grotere actieve betrokkenheid van geregistreerden oproept. Bovendien stelde het onderzoeksteam vast dat van de in de WPR onderscheiden maatschappelijke sectoren, de overheid zich meer bekommert om de naleving van de WPR dan het bedrijfsleven en de semi-overheid.

Een en ander leidt tot de conclusie dat één van de belangrijkste doelen van de wet, het nastreven van transparantie waardoor de geregistreerde inzicht heeft in wat er met zijn persoonsgegevens gebeurt, in onvoldoende mate wordt gehaald. Hierbij moet worden opgemerkt dat in het algemeen de con-

1. Een juridische evaluatie werd tegelijkertijd uitgevoerd, zie [Over95].
2. Instituut voor sociaal-wetenschappelijk beleidsonderzoek en advies van de Katholieke Universiteit Brabant.
3. Hiernaast zijn nog andere onderzoeksactiviteiten verricht, te weten: gesprekken met velddeskundigen/sleutelfiguren, een literatuurstudie, een expert-meeting waarin ontwikkelingen op het gebied van de informatie- en communicatietechnologie, economie en bedrijf, politiek-bestuurlijke ontwikkelingen en maatschappelijke ontwikkelingen aan de orde kwamen, panels van deskundigen en betrokkenen waarin de eerste resultaten van het onderzoek zijn besproken.

clusie niet kan worden getrokken dat er in Nederlandse organisaties onzorgvuldig met persoonsgegevens wordt omgegaan. De analyse van de dagelijkse praktijk binnen administratieve organisaties geeft echter aan dat er reden is om alert te blijven.

Het oordeel van de houders

De tweede onderzoeksvraag was als volgt geformuleerd: 'Hoe oordelen de houders van persoonsregistraties over de WPR?'
Wat blijkt is dat houders positief staan tegenover regelgeving op het terrein van de bescherming van persoonsgegevens. Zij ervaren dit ook als nuttig. Echter, komt het op de concrete regels van de WPR aan, dan stellen houders dat de wet te ingewikkeld is en ervaren ze deze regels als weinig praktisch. De moeilijk toegankelijke uitvoeringsregelgeving draagt hier zeker aan bij. Deze factoren bemoeilijken acceptatie en naleving van de WPR met name bij organisaties die niet de mogelijkheid hebben zelf met de wet aan de slag te gaan. Hier moet worden gedacht aan kleine zelfstandigen en kleine bedrijven.
Houders staan verder kritisch tegenover het functioneren van de Registratiekamer. Dit beeld vloeit in belangrijke mate voort uit de als omslachtig en weinig zinvol ervaren aanmeldingsprocedures en uit het eenzijdig juridisch-theoretisch perspectief dat door de Registratiekamer wordt gehanteerd. Een aansluiting bij de praktijk wordt gemist.

Voor naleving relevante omstandigheden

De derde onderzoeksvraag luidde: 'Welke omstandigheden beïnvloeden de naleving van de WPR op de werkvloer?'
Het blijkt dat de factoren die naleving van een wet als de WPR bevorderen vooral aan te treffen zijn in grote organisaties die een zekere ervaring hebben met het implementeren van omvangrijke complexen van interne of externe regelgeving. In organisaties waarin hiermee minder of geen ervaring bestaat en waarin onvoldoende capaciteit aanwezig is om deze ervaring op te doen, verloopt de naleving van de WPR minder soepel. Op grond van een analyse van de dagelijkse uitvoeringspraktijk in de zes bestudeerde organisaties kan echter worden gesteld dat de vertaalslag van WPR naar de dagelijkse uitvoeringspraktijk, zelfs in organisaties die de nodige voorzieningen hebben getroffen om de regels van de WPR uit te voeren, te wensen overlaat; het blijkt dat de wet zich moeilijk in heldere instructies laat vertalen.

Bij organisaties waar de dagelijkse uitvoeringspraktijk wel voldoet, blijkt dat de factoren die daaraan hebben bijgedragen slechts zeer indirect met de regels van de WPR te maken hebben. Voorbeelden van dergelijke factoren zijn de cultuur of het belang van een organisatie c.q. bedrijf en de reeds bestaande normen die afkomstig zijn uit andere bronnen, zoals het medisch beroepsgeheim. Veel van die factoren en omstandigheden vloeien voort uit karakteristieken van de taken en werkprocessen binnen zo'n organisatie.
Een belangrijke conclusie van het onderzoek is dat in veel situaties de doorwerking van de WPR in de dagelijkse praktijk in belangrijke mate afhankelijk is van goed management, van een adequate organisatie, van een adequate informatievoorziening, van de opleiding van de medewerkers, van de mate waarin gewenst gedrag door een technische infrastructuur wordt bevorderd of zelfs afgedwongen, van een systematische en herhaalde controle van de organisatieleiding, en van druk van de omgeving. Daarom kan worden gesteld dat zelfregulering alleen niet voldoende is; ook het *zelf handhaven* en *zelf evalueren* van die regels verdient de nodige aandacht. De WPR kent echter een ingewikkeld administratief regime, dat in veel gevallen het tot stand komen van een geschikt klimaat voor naleving van de wet in de weg staat. De papieren leiden de aandacht af van de manieren. De mogelijkheid de wet te vertalen in heldere instructies is niet altijd even groot, waarbij de controle van de ingewikkelde regels ook zelf al snel gecompliceerd is.

Geregistreerden maken nauwelijks gebruik van de door de wet aangereikte instrumenten.

Mening van geregistreerden

De vierde onderzoeksvraag luidde: 'Wat is de mening van de geregistreerde over de WPR?'
Het onderzoek wijst op dit punt uit dat de geregistreerde in zeer belangrijke mate hecht aan de rechten die hem in staat stellen zicht te houden op het gebruik dat de houder en mogelijke anderen van zijn persoonsgegevens maken. Toch blijkt ook dat de geregistreerde nauwelijks gebruik maakt van de instrumenten die hem daartoe in de wet worden aangereikt. Wat dit betreft blijkt het grote aantal inzageverzoeken bij het Bureau Krediet Registratie in Tiel een uitzondering. Het probleem ligt hem bij de meerderheid van de organisaties in het feit dat geregistreerden nauwelijks bekend zijn met de procedures die, indien nodig, moeten worden bewandeld om inzage te krijgen.
Wat uit het onderzoek eveneens naar voren komt, is dat de WPR niet alleen niet leeft bij de geregistreerden, maar dat ook de geregistreerde niet echt leeft bij de houders. Alhoewel houders – zoals reeds aangegeven – in algemene zin wel de noodzaak van het zorgvuldig omgaan met gegevens accepteren, is er slechts in zeer bescheiden mate sprake van een actief betrekken van de geregistreerden bij de gegevensverwerking en -verstrekking. Dit wordt door veel houders blijkbaar niet als belangrijk ervaren. Opvallend is – zoals eveneens eerder opgemerkt – dat werd geconstateerd dat er bij 'actieve' houders relatief vaker sprake is van 'actieve' geregistreerden.
Eén van de conclusies van het onderzoek is daarom dat het stimuleren van alerte en actieve geregistreerden waarschijnlijk één van de meest effectieve en doelmatige instrumenten is voor de handhaving van de regels rondom de omgang met persoonsgegevens. In dit verband is in de ogen van het onderzoeksteam een belangrijke rol weggelegd voor zowel de Registratiekamer alsook consumenten-, patiënten-, studenten- en vakorganisaties. De

wetgever doet er verstandig aan de positie van de geregistreerde serieus te nemen en hem vooral niet langer als slachtoffer te zien, maar als medespeler en medebepaler van beleid.

Nieuwe ontwikkelingen

De vijfde onderzoeksvraag betrof de vraag: 'Met welke ontwikkelingen moet rekening worden gehouden bij het formuleren van nieuwe regels?'
In de komende jaren zullen ontwikkelingen op het gebied van technologie, economie en bedrijf alsmede maatschappij, politiek en bestuur ertoe leiden dat het huidige instrumentarium van de WPR steeds minder zal aansluiten bij de praktijk. Het registreren van registraties en het uitoefenen van toezicht daarop is bij lange na niet toereikend als strategie voor de bescherming van persoonsgegevens. Het onderzoeksteam stelt in zijn onderzoek vast dat in relatieve en absolute zin het *belang* van het *zorgvuldig* omgaan met persoonsgegevens alleen maar groter wordt.

Stilstaand bij de technologische ontwikkelingen is daar het feit dat processen van gegevensverzameling, -opslag, -bewerking en -uitwisseling enorm in omvang en betekenis toenemen. Het toenemende gebruik van persoonsgegevens vraagt daarbij om een heroriëntatie van de regels. Zo is duidelijk dat het huidige in de WPR gehanteerde onderscheid in maatschappelijke sectoren (publieke, semi-publieke en private sector) niet langer voldoet. In het licht van de ontwikkeling naar een samenleving-op-maat, waarin het effect van technologische ontwikkelingen en de praktijk rondom gegevensverwerking in iedere sector verschillend zal zijn, zal ook het precieze regime voor de bescherming van persoonsgegevens per maatschappelijke sector sterk verschillen; studenten zijn immers geen patiënten en consumenten hebben andere belangen dan werknemers.
Technologische ontwikkelingen vormen echter niet alleen een bedreiging voor de persoonlijke levenssfeer. In het onderzoek werd vastgesteld dat technologische innovaties ook belangrijke kansen bieden voor meer effectieve waarborgen in een praktijk van het omgaan met persoonsgegevens. Geavanceerde vormen van invoercontrole, integrity-checking, auditability en toegangscontrole bieden steeds betere mogelijkheden om het aantal bestaande knelpunten rondom de naleving van de WPR te verminderen. Door middel van dergelijke technologische ontwikkelingen kunnen de verzameling, de verspreiding, de opslag en de bewerking van persoonsgegevens duidelijker in beeld worden gebracht en beheerst. Hiermee kunnen transparantie van en controle over het gebruik van persoonsgegevens gediend zijn.

Een politiek-bestuurlijke ontwikkeling die van belang is voor de bescherming van persoonsgegevens is de aandacht voor een integratie van gegevensbestanden of 'persoonsregistraties', maar ook de grenzen van bestaande organisaties. Immers, er zullen steeds vaker samenwerkingsverbanden en netwerkstructuren ontstaan, op tijdelijke, permanente of semi-permanente basis. Het identificeren van 'houders' van persoonsregistraties zal daardoor steeds problematischer worden. Andere politiek-bestuurlijke ontwikkelingen die voor nieuwe problemen rondom de naleving van de regels inzake de bescherming van persoonsgegevens zorgen, betreffen: het accent dat steeds vaker wordt gelegd op de bestrijding van misbruik en oneigenlijk gebruik van maatschappelijke voorzieningen, de integratie van dienstverlening door overheidsinstanties (de één-loket-gedachte) en de toenemende verzelfstandiging of privatisering van overheidsinstellingen.

Tot slot wordt gewezen op de economische ontwikkelingen. De economische waardestromen in onze maatschappij hangen in toenemende mate samen met informatieverwerking. Ook economisch gedrag wordt steeds meer geïnformatiseerd, zoals het elektronisch betalen via de 'chipknip'. Het consumentengedrag en, meer in het bijzonder, het bestedingsgedrag van consumenten kan via digitale dossiers helder in beeld worden gebracht. Met deze kennis kunnen het cliëntbeheer en de dienstverlening worden geoptimaliseerd, bijvoorbeeld tot op zeer persoonlijke maat toegesneden marketingprogramma's. Een en ander betekent overigens wel dat de bescherming van persoonsgegevens niet slechts van betekenis is voor de geregistreerde consument. Ze is ook van belang voor het bedrijfsleven zelf: bedrijven lopen immers grote risico's ten aanzien van de essentiële relaties met hun cliënten en consumenten wanneer zij het niet al te nauw zouden nemen met de zorg voor de bescherming van hun persoonsgegevens. In het onderzoek werd daarom vastgesteld dat de bescherming van persoonsgegevens ook kan worden beschouwd als een kwaliteitskenmerk van de producten en diensten van het bedrijfsleven.

Aanbevelingen

Welke lessen kunnen uit de voorgaande conclusies worden getrokken? Uit deze vraag vloeide de zesde en tevens laatste onderzoeksvraag voort: 'Welke punten moeten op de agenda van de wetgever worden gezet?'
Op basis van de uitkomsten van het onderzoek zijn acht uitgangspunten geformuleerd. Deze dienen naar de mening van het onderzoeksteam een rol te spelen in de voorbereiding van de nieuwe Wet bescherming persoonsgegevens, die – zoals hiervoor werd aangegeven – noodzakelijk is in het licht van de in 1995 afgekondigde Europese Richtlijn. Het betreft de volgende uitgangspunten:

- Allereerst: er bestaat volgens het onderzoeksteam slechts behoefte aan een zeer bondige en algemene wet die, als een ster aan de hemel, beknopt maar helder aangeeft welke hoofddoelstellingen en waarborgen op het gebied van de bescherming van persoonsgegevens in de verschillende specifieke domeinwetgeving (zoals bijvoorbeeld voor politie of gezondheidszorg) of arrangementen van zelfregulering moeten worden gerealiseerd.
- Ten tweede dient de privacyregulering zoveel mogelijk aan te sluiten bij de potentiële risico's van gegevensverwekkende en gegevensverwerkende processen, in plaats van bij maatschappelijke sectoren zoals dat onder het huidige regime gebeurt.

– Bij het ontwikkelen van nieuwe regelgeving dienen zowel technologie-onafhankelijke als (flexibele) contextgebonden normering en beleidsinstrumentatie de uitgangspunten te zijn.
– Ten vierde kan met het oog op zelfregulering een meer omvattende invulling van de eigen verantwoordelijkheid van de houders en bewerkers (en de organisaties waarbinnen zij samenwerken, zoals overkoepelende of bedrijfsorganisaties) zowel de effectiviteit als de doelmatigheid van de relevante normen versterken.
– Als vijfde dient bij de keuze van de sturingsinstrumenten telkens te worden geprobeerd deze te baseren op een grondige analyse van de factoren die in een bepaalde context de doorwerking en effectiviteit van een beleidsprogramma bevorderen en/of belemmeren.
– Zoals opgemerkt, kan de positie van de geregistreerde worden versterkt door deze (zo nodig via overkoepelende organisaties van geregistreerden) meer mogelijkheden voor betrokkenheid en medezeggenschap te verlenen.
– Vervolgens liggen er naar de mening van het onderzoeksteam meer kansen op acceptatie van de rol van de Registratiekamer wanneer door de kamer actief aansluiting wordt gezocht bij de praktijk, en niet zozeer bij de juridische theorie van de bescherming van persoonsgegevens.
– Tot slot dient de wetgever bij de ontwikkeling van beleid tevens oog te hebben voor het feit dat regulering van bepaalde handelingen ook kan worden geëffectueerd door gebruik te maken van de technologie.

AFSLUITING

De titel van het boek *In het licht van de Wet persoonsregistraties: zon, maan of ster?* is niet zomaar uit de lucht komen vallen. Kijkend naar het karakter van de WPR kan namelijk metaforisch de vraag worden gesteld: Is de WPR een zon of een maan?
Op het eerste gezicht heeft de WPR het karakter van een zon. Als een zon straalt de wet en draagt ze in belangrijke mate bij aan de naleving van de bepalingen inzake de omgang met persoonsgegevens. Het hier besproken onderzoek maakt echter duidelijk dat de WPR en de daaronder ressorterende uitvoeringsbepalingen – ondanks de mogelijkheden voor zelfregulering – het karakter hebben van een 'ancien regime'. In de praktijk worden de regels van de WPR als zeer ingewikkeld, gedetailleerd en star ervaren. De consequentie hiervan is dat de bepalingen van de WPR bij het overgrote deel van de houders nauwelijks richting aan de dagelijkse praktijk geven. Alhoewel de wet ruimte laat voor zelfregulering, blijkt deze in de praktijk zowel procedureel als inhoudelijk sterk geconditioneerd.
Aldus, kijkend naar de praktijk, blijkt de WPR daarom niet het karakter van een zon te hebben. Vanuit het perspectief van de werkvloer – de dagelijkse omgang met de regels die in dit onderzoek in zes organisaties is bestudeerd – is de WPR veeleer een maan. Niet zozeer de bepalingen van de wet, maar het geheel van alledaagse praktijken en handelingen dat uit kracht van andere bronnen en overwegingen wordt nagestreefd, realiseert de bescherming van persoonsgegevens. Het handelen in de dagelijkse praktijk blijkt vooral afhankelijk van andere factoren dan de normen en richtlijnen van de WPR. In het onderzoek worden in dit verband als voorbeelden genoemd het eigenbelang van de organisaties, het persoonlijk commitment en de professionele normen van de medewerkers.

Toch: noch het beeld van de zon, noch het beeld van de maan doet recht aan datgene waar een wettelijk regime inzake de bescherming van persoonsgegevens voor zou moeten staan. In het onderzoek wordt geconcludeerd dat de rol van een dergelijk regime eigenlijk die van een ster zou moeten zijn. De conclusies uit het onderzoek leiden dan ook tot de stelling dat de nieuwe Wet bescherming persoonsgegevens een zeer bondige en algemene wet moet blijven. Beknopt maar helder dient te worden aangegeven welke hoofddoelstellingen en waarborgen op het gebied van de bescherming van persoonsgegevens in de verschillende wetgeving voor specifieke sectoren moeten worden gerealiseerd. De onderzoekers verwachten met het oog op zelfregulering dat een meer omvattende invulling van de eigen verantwoordelijkheid van de houders en bewerkers alsmede de overkoepelende of bedrijfsorganisaties zowel de effectiviteit als de doelmatigheid van de relevante normen zal versterken. Terug naar de metafoor van het onderzoek: de Wet bescherming persoonsgegevens zal noch als zon, noch als maan moeten fungeren. Ze zal een heldere ster moeten zijn die richting wijst aan degenen die in uiteenlopende uitvoeringscontexten en praktijksituaties de wettelijke materiële normen tot gelding moeten brengen.

Op dit moment is de voorbereiding van de nieuwe Wet bescherming persoonsgegevens in volle gang. De verwachting is dat aan de Tweede Kamer in het eerste halfjaar van 1997 een tekst zal worden voorgelegd. Uit het concept dat op dit moment circuleert, blijkt al wel dat de bovenstaande aanbevelingen in lang niet alle opzichten in de wet gestalte zullen krijgen. In feite zal de nieuwe wet – zoals het er op dit moment uitziet – wat betreft opzet en systematiek niet veel veranderen ten opzichte van de huidige regeling. Een zeer bondige en algemene wet die, als een ster aan de hemel, beknopt maar helder aangeeft welke hoofddoelstellingen en waarborgen op het gebied van de bescherming van persoonsgegevens moeten worden gerealiseerd, zal het daarom wel niet worden. Een gemiste kans.

LITERATUUR

[Over95] M. Overkleeft-Verburg, *De wet persoonsregistraties. Norm, toepassing en evaluatie*, Zwolle 1995.

[Prin95] J.E.J. Prins e.a., *In het licht van de Wet persoonsregistraties: zon, maan of ster?*, Samsom, Alphen aan den Rijn 1995.

Mw. prof. mr. J.E.J. Prins Is hoogleraar Recht en Informatisering aan de Faculteit der Rechtsgeleerdheid van de Katholieke Universiteit Brabant, alsmede verbonden aan de Afdeling Recht en Informatica van de Rijksuniversiteit Leiden. Zij doceerde tevens als invited visiting professor aan Hastings School of Law (University of California, San Francisco). In 1994 heeft zij in opdracht van DG XV van de Europese Commissie onderzoek verricht naar de juridische en financiële implicaties van de ontwerp Privacy-richtlijn voor de Nederlandse situatie. In 1995 vond, in opdracht van het Ministerie van Justitie, onder haar supervisie de sociaal-wetenschappelijke evaluatie van de WPR plaats.

De Europese privacyrichtlijn

Prof. mr. J.M.A. Berkvens

De belangrijkste elementen uit de Europese privacyrichtlijn worden besproken met het oog op de integratie in de Wet bescherming persoonsgegevens die de Wet persoonsregistraties zal gaan vervangen. Ook de gevolgen daarvan voor het privacyrecht worden behandeld.

INLEIDING

In dit artikel wordt aan de hand van een vergelijking tussen de Europese privacyrichtlijn en de Wet persoonsregistraties (WPR) getracht een overzicht te geven van de belangrijkste veranderingen die binnenkort te verwachten zijn in ons privacyrecht. Het artikel beperkt zich tot de hoofdlijnen. Gezien de interpretatieruimte binnen de richtlijn is enig voorbehoud op zijn plaats.
Ongeveer vijf jaar nadat de tekst van een voorstel voor een Europese privacyrichtlijn werd gepubliceerd ligt er een definitieve privacyrichtlijn. Via Europees Parlement, Europese Commissie en de Raad van Ministers kwam de Richtlijn formeel tot stand op 24 oktober 1995 door de gezamenlijke ondertekening door de voorzitters van het Europees Parlement en de Raad. De implementatietermijn loopt af op 25 oktober 1998. Inmiddels wordt binnen het Ministerie van Justitie een wettelijke regeling voorbereid, de Wet bescherming persoonsgegevens (WBP), die de huidige Wet persoonsregistraties (WPR) moet gaan vervangen.
Ook wordt bezien welke andere wetten in het licht van de richtlijn moeten worden aangepast. In de andere lidstaten van de Europese Unie vinden thans vergelijkbare exercities plaats. Weliswaar kan de EU de nationale wetgevers niet dwingen om op bijvoorbeeld fiscaal of strafrechtelijk terrein bevoegdheden van functionarissen te wijzigen. Wel kan het wenselijk zijn om in de fiscale en de strafrechtelijke sfeer de gehanteerde definities en procedures te synchroniseren.

Het belangrijkste verschil van de richtlijn met de WPR vormt haar aangrijpingspunt. De WPR grijpt aan op persoonsgegevens die voorkomen in persoonsregistraties. De richtlijn grijpt daarentegen aan op iedere verwerking van afzonderlijke persoonsgegevens. Slechts voor niet-geautomatiseerde verwerkingen geldt nog de voorwaarde dat de persoonsgegevens deel moeten uitmaken van een persoonsregistratie. Daarnaast zijn er enkele andere nieuwe elementen. Op de eerste plaats omvat de richtlijn een regeling voor het gebruik van persoonlijkheidsprofielen. Op de tweede plaats wordt de mogelijkheid geïntroduceerd om binnen een onderneming of binnen een groep van ondernemingen een bestandstoezichthouder aan te stellen met als voordeel dat in een dergelijk geval de verplichting om verwerkingen bij de Registratiekamer aan te melden wordt beperkt. Voorts wordt een onderscheid ingevoerd tussen verwerkingen binnen de EU en daarbuiten. De geregistreerde wordt een recht van verzet toegekend in geval van op zich rechtmatige verwerkingen die evenwel bijzonder bezwarend voor betrokkene kunnen zijn. De richtlijn kent geen apart regime voor informatiebureaus zoals dat van art. 13 WPR. De regeling voor adresbestanden is gewijzigd en wordt toegespitst op uitsluitend direct marketing-activiteiten. Het onderscheid tussen de regimes voor interne en externe verstrekking van persoonsgegevens vervaagt. Er wordt geen expliciet onderscheid meer gemaakt tussen verwerkingen door overheid en particuliere sector (zij het dat diverse verwerkingen door de overheid op grond van verdragsrecht of specifieke nationale wetten een status aparte zul-

len krijgen). De risico-aansprakelijkheid van de houder voor de gevolgen van niet naleven van de WPR komt te vervallen zodat de houder bij afwezigheid van schuld niet meer per definitie voor eventuele schade opdraait.

Tijdens de behandeling van de richtlijn in Brussel heeft de Tweede Kamer nadrukkelijk gevolgd wat de mogelijke consequenties van die richtlijn zouden kunnen zijn. De Minister van Justitie heeft beloofd om bij de implementatie van de richtlijn een soepele benadering aan te houden en daarbij uitdrukkelijk rekening te houden met de belangen van gegevensverwerkende instellingen. Tijdens de behandeling van de richtlijn in Brussel zijn op verzoek van de Nederlandse delegatie diverse voorstellen gehonoreerd om de richtlijn werkbaar te houden.

DEFINITIES EN REIKWIJDTE

De in de richtlijn gehanteerde basisbegrippen komen in belangrijke mate overeen met die van de WPR. In aanvulling op het begrippenapparaat van de WPR is voorzien in afzonderlijke omschrijvingen voor de begrippen 'derde', 'ontvanger' en 'toestemming'. Deze laatste definitie vervangt het artikel 12 WPR waarin de vormvereisten voor toestemming zijn omschreven.

Het begrip 'persoonsgegeven' gaat uit van een tweetal premissen: het gegeven moet op een *persoon* betrekking hebben, zodat pure objectgegevens, die slechts zijdelings ook op een persoon betrekking kunnen hebben, als regel geen persoonsgegeven kunnen zijn; het gegeven moet bovendien herleidbaar zijn op een *bepaalde* persoon. Nieuw ten opzichte van de WPR is de uitdrukkelijke uitbreiding van het begrip 'persoonsgegeven' met geautomatiseerde vastleggingen van beelden en geluiden (vgl. considerans 14 t/m 17 en art. 33 Richtlijn).

Het begrip 'verwerking van persoonsgegevens' omvat alle mogelijke handelingen die met een persoonsgegeven kunnen worden verricht. Anders dan onder de WPR valt dus ook het vergaren van persoonsgegevens onder de definitie. De richtlijn doet ook een indirecte uitspraak over de juridische status van telecommunicatie (vergelijk considerans 47). In deze considerans wordt de opdrachtgever van een voor transport aangeboden bericht als houder aangemerkt. Er wordt evenwel geen uitspraak gedaan of de transporteur vervolgens als bewerker moet worden aangemerkt. De enkelvoudige transmissie van persoonsgegevens kan echter toch buiten de scope van de richtlijn vallen. Het begrip 'verwerking van persoonsgegevens' verwijst namelijk ter zake doorzending immers naar 'verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen', zodat het optreden als transporteur van informatie ten behoeve van een derde geen zelfstandige 'verwerking' door de transporteur vormt. Enkelvoudige transmissie met behulp van binnen de EU opgestelde middelen wordt in art. 4.1(c) van de richtlijn expliciet buiten de toepassingssfeer van de richtlijn gehouden indien sprake is van transmissie in het kader van uitwisseling van gegevens van een houder buiten de EU.

Nieuw is de uitdrukkelijke uitbreiding met geautomatiseerde vastleggingen van beeld en geluid.

Het begrip 'voor de verwerking verantwoordelijke' vervangt de thans gangbare term 'houder'. Centraal onderdeel van de definitie vormt het zeggenschapsvereiste ten aanzien van verwerkingen, zodat evenals onder de WPR voor de wetgever ruimte blijft bestaan binnen concernstructuren de holding als 'verantwoordelijke' aan te merken. Zou de wetgever geen gebruik maken van deze mogelijkheid dan zou dat grote gevolgen kunnen hebben voor de omvang van de rectificatie- en de protocolplicht met betrekking tot intern concernverkeer.

De term 'verwerker' vervangt de thans gangbare term 'bewerker'. Een belangrijk verschil met de WPR is dat het vereiste is komen te vervallen dat de 'verwerker' zijn activiteiten met behulp van informatietechnologie verricht. Dit brengt ons wel bij de vraag of activiteiten van externe consultants voortaan als activiteiten van een 'verwerker' moeten worden aangemerkt.

Het begrip 'bestand' omvat dezelfde elementen als onder de WPR het geval was. Derhalve vallen slechts goed gestructureerde gegevensverzamelingen die op systematische raadpleging zijn ingericht onder de richtlijn. De jurisprudentie op dit punt is overigens nog niet goed uitgekristalliseerd.

Reikwijdte

De richtlijn geldt ten aanzien van alle geautomatiseerde verwerkingen (inclusief het opgeslagen zijn) en ten aanzien van de verwerking van gegevens in bestanden. Daarbij wordt een bij elkaar horende groep van verwerkingsactiviteiten als één geheel aangemerkt. Dat heeft als voordeel dat bij het bestaan van aanmeldingsverplichtingen slechts één aanmelding hoeft plaats te vinden. Een nadeel zou kunnen zijn dat de archivering van tekstverwerkingsdocumenten als een geheel van verwerkingen wordt bezien met de vervaardiging van een dergelijk document. Dat zou betekenen dat ook documenten die in een buiten de richtlijn vallende dossierverzameling zijn opgeslagen onder de richtlijn blijven vallen.

Evenals onder de WPR het geval is, vallen verwerkingen voor persoonlijk en huiselijk gebruik buiten de toepassing van de regels. Schriftelijke publicaties worden echter niet meer uitgezonderd zodat het telefoonboek binnenkort ook onder de WBP zal gaan vallen. Een uitzondering vormen publicaties

voorzover daar onder art. 9 van de richtlijn in verband met de persvrijheid aparte regels voor worden opgesteld door de wetgever.
Evenals de WPR bevat de richtlijn geen aparte regels voor hulpbestanden zoals backups. De tekst van de richtlijn lijkt zich er echter niet tegen te verzetten dat conform de huidige praktijk van de WPR dergelijke hulpbestanden een status aparte wordt gegeven van hulpmiddel bij het voeren van de hoofdprocessen.

Territoriaal bereik

Een ander reikwijdte-aspect vormt het territoriale bereik van nationale privacyregels. Uit de overwegingen die bij art. 4 van de richtlijn horen (met name overweging 18), blijkt dat het de bedoeling is dat gegevensverwerkingen onder verantwoordelijkheid van een binnen de EU gevestigde verantwoordelijke gaan vallen onder de regels van de wetgeving van de lidstaat waar de verantwoordelijke is gevestigd. Dat betekent bijvoorbeeld dat een geregistreerde die in Nederland opkomt tegen activiteiten van een in Duitsland gevestigde verantwoordelijke te maken krijgt met een Nederlandse rechter die het Duitse privacyrecht toepast. Indien de verantwoordelijke echter buiten de EU is gevestigd, dient hij een vertegenwoordiger binnen de EU aan te wijzen.

Een geregistreerde kan te maken krijgen met een Nederlandse rechter die het Duitse privacyrecht toepast.

De artt. 25 en 26 van de richtlijn bevatten specifieke regels voor de export van persoonsgegevens naar landen buiten de EU. Indien deze landen onvoldoende bescherming van de te verwerken gegevens bieden kan de export worden verboden. Art. 26 bevat een opsomming van mogelijkheden om een verbod te voorkomen. Een mogelijkheid vormt een contractuele privacyregeling tussen exporteur en ontvanger.

NORMERING

De vraag of gegevens mogen worden verwerkt, moet langs een tweetal checklists worden gehaald. De eerste lijst (art. 6 Richtlijn) komt overeen met de artt. 4 t/m 6 en 11 WPR (en met de beginselen van het Verdrag van Straatsburg). Er moet derhalve sprake zijn van een redelijk doel, de gegevens moeten rechtmatig zijn verkregen, juist en volledig en voor het doel relevant zijn en het gebruik dient verenigbaar te zijn met het doel waarvoor de gegevens zijn verkregen. De tweede lijst (art. 7 Richtlijn) geeft een aantal aanvullende voorwaarden die er steeds weer op neerkomen dat moet worden nagegaan of de verwerking 'noodzakelijk' is voor een bepaald doel (vgl. art. 18 WPR voor overheidsregistraties). Indien een verwerking niet voldoet dient toestemming te worden verkregen van de betrokkene (art. 7(a)) of dient een beroep te worden gedaan op het algemene uitzonderingsartikel 7(f). Op grond van dat artikel is een verwerking (binnen de randvoorwaarden van art. 6 Richtlijn) toegestaan *'indien de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derden aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van artikel 1, lid 1, van deze richtlijn, niet prevaleren'*. Op grond van deze bepaling vervaagt dus ook het materiële onderscheid tussen interne en externe verstrekkingen van persoonsgegevens.
Een zeer specifieke normering is terug te vinden in art. 15 Richtlijn. Hierin wordt bepaald dat het niet is toegestaan beslissingen te nemen omtrent personen indien sprake is van geautomatiseerde besluitvormingsprocessen op basis van *persoonlijkheids*profielen. Deze bepaling vormt één van de hoekstenen van de huidige Franse privacywetgeving. Niet ieder profiel vormt echter een persoonlijkheidsprofiel. Zo kunnen in het kader van fraudepreventie *gebruiks*profielen van houders van betaalkaarten worden opgesteld die het mogelijk maken om, volledig langs geautomatiseerde weg, creditcard-transacties of geldopnames te weigeren indien sprake is van een significante afwijking van het normale gebruik. We zullen moeten afwachten hoe in de praktijk het verschil tussen beide soorten van profielen zal uitpakken.

Gevoelige gegevens

In art. 8 Richtlijn is een uitvoerige regeling voor zogenaamde gevoelige gegevens opgenomen. Anders dan in de WPR en het besluit gevoelige gegevens het geval is geldt de regeling niet alleen voor de vastlegging van de gegevens maar ook voor alle overige verwerkingen ervan. Er wordt een onderscheid gemaakt tussen het regime voor strafrechtelijke gegevens (art. 8 lid 5 Richtlijn) en dat voor de overige soorten gevoelige gegevens. Het regime voor de strafrechtelijke gegevens is zwaarder dan dat voor de overige gegevens. Bij de overige gegevens worden voor diverse soorten nog uitzonderingsregels gegeven. De richtlijn biedt de lidstaten een bepaalde bandbreedte voor het uitwerken van de richtlijn. De Europese Commissie wenst op de hoogte te worden gehouden van de wijze waarop de richtlijn wordt uitgewerkt.

Rechten geregistreerde

In de WPR heeft de geregistreerde een recht op kennisgeving van opname, inzage, correctie, protocol en rectificatie. Deze rechten komen hem ook toe onder de richtlijn. Evenals art. 30 WPR voorziet de richtlijn in een aantal weigeringsgronden. Naast onze 'klassieke' rechten is er nog een aantal andere rechten opgenomen. Eén daarvan is het recht om geïnformeerd te worden omtrent de logica die achter bepaalde verwerkingsprocessen schuil gaat. Een ander is het recht op informatie op het moment

dat gegevens worden vergaard bij de betrokkene zelf. Ten aanzien van marktbewerkingsactiviteiten is voorzien in een aantal specifieke informatieplichten. Alhoewel de richtlijn geen expliciete protocolplicht bevat is er wel degelijk sprake van een impliciete protocolplicht gezien de (in de tijd niet beperkte!) verplichting om derden aan wie foutieve gegevens werden verstrekt daaromtrent te informeren. Ten slotte voorziet de richtlijn in een recht van verzet voor de betrokkene. Dat houdt in dat deze een verwerking kan stopzetten indien sprake is *'van zwaarwegende en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie'*. Dat betekent dat ook verwerkingen die op zich genomen voldoen aan de eisen van de artt. 6 en 7 (en 8) van de richtlijn kunnen worden gestopt.

BUREAUCRATIE

De bureaucratische aspecten van de privacyrichtlijn richten zich met name op de toezichthoudende autoriteit en de aanmeldingsverplichtingen.

Toezichthoudende autoriteit

In Nederland is thans de Registratiekamer belast met het toezicht op de werking van de WPR. Ze heeft een gevarieerd takenpakket waarbij sprake is van een diversiteit aan petten. De Registratiekamer heeft een adviestaak als het gaat om voorgenomen wet- en regelgeving. Ook kan de rechtbank haar advies inwinnen bij bepaalde privacygeschillen. Daarnaast kan de Registratiekamer desgevraagd bemiddelen in geschillen tussen houders en geregistreerden. De Registratiekamer is belast met het behandelen van gedragscodes en het al dan niet verlenen van haar goedkeuring aan dergelijke gedragscodes. Ze heeft het recht om op eigen initiatief of in het verlengde van een klacht een onderzoek ter plaatse in te stellen. De mogelijkheid van controle op het handelen van de Registratiekamer is mede afhankelijk van de pet die zij op een bepaald moment draagt. De Wet Nationale Ombudsman is niet van toepassing. In plaats daarvan is er een klachtprocedure via de Hoge Raad. In een aantal gevallen kan de procedure van de Algemene Wet Bestuursrecht worden gevolgd. Van enkele beslissingen bepaalt de WPR uitdrukkelijk dat geen beroep mogelijk is.

In de richtlijn worden de bevoegdheden van de Registratiekamer sterk uitgebreid. Belangrijke bevoegdheden zijn de mogelijkheid om gegevensverwerkingen stop te kunnen zetten, het zelfstandig initiëren van gerechtelijke procedures en het verlenen van ontheffingen ter zake voorgenomen verwerkingen. De mogelijkheden voor de Registratiekamer om via een onderhandelingspositie haar wensen af te dwingen worden uitgebreid. In diverse gevallen krijgt de Registratiekamer meer dan thans het geval is de ruimte om op de stoel van de ondernemer te gaan zitten. Zo kan zij bijvoorbeeld de administratieve procedures van informatiebureaus sterk naar haar hand zetten.

Aanmeldingsverplichtingen

Onder de WPR kennen we een stelsel van aanmeldingsverplichtingen ter zake van persoonsregistraties. Het stelsel voorziet in de verplichting om een beschrijving van persoonsregistraties op te stellen, het bestaan ervan aan de Registratiekamer en aan het relevante publiek kenbaar te maken en om de beschrijving te onderhouden en wijzigingen door te voeren en eveneens bekend te maken. Van de aanmeldingsplicht kan vrijstelling worden verkregen indien wordt voldaan aan de randvoorwaarden van het Besluit genormeerde vrijstelling. De richtlijn voorziet in een vergelijkbaar stelsel. Nieuw is dat de aan de Registratiekamer toe te zenden aanmeldingsformulieren aldaar ter inzage liggen (behoudens beschrijvingen van beveiligingsmaatregelen).

Eveneens nieuw is de mogelijkheid van art. 18 lid 2 van de richtlijn om per bedrijf, concern of branche ontheffing te krijgen van de verplichting tot centrale aanmelding indien er in bedrijf, concern of branche een 'compliance-officer' wordt aangesteld. Dat is naar Duits model een interne 'registratiekamer' die bijhoudt welke gegevensverwerkingen er binnen haar organisatie plaatsvinden, die daar beschrijvingen van onderhoudt en die intern toeziet op de naleving van de krachtens de richtlijn gegeven voorschriften. De 'compliance-officer' is binnen de grenzen van de wet bevoegd om, toegesneden op de eisen van bedrijf of branche, zelf zijn administratie in te richten. Hij heeft een onafhankelijke positie en geniet derhalve waarschijnlijk ontslagbescherming. De richtlijn laat het aan de nationale wetgevers over om zelf een nadere uitwerking te kiezen. Daarbij kan zelfs gedacht worden aan varianten waarbij de taken van de compliance-officer op contractbasis worden uitbesteed aan externe organisaties. In alle gevallen waarin de compliance-officer niet in dienst is van de onder zijn bevoegdheden vallende rechtspersoon zijn nadere contractuele afspraken nodig.

De compliance-officer vormt een interne 'registratiekamer' naar Duits model.

Overgangsregeling

De richtlijn bevat een overgangsregeling die de lidstaten de ruimte biedt om op een aantal terreinen de toepassing van de richtlijn uit te stellen. Deze ruimte is echter geconditioneerd. In overweging 70 van de richtlijn wordt bepaald dat in die situaties waarin voor de toekomst een gekwalificeerde toestemming zou zijn vereist, er een eerbiedigende werking is ten aanzien van in het verleden afgegeven impliciete toestemmingen. Daardoor wordt bijvoorbeeld voorkomen dat oude contracten opnieuw moeten worden aangeboden aan klanten.

Prof. mr. J.M.A. Berkvens Is bijzonder hoogleraar Recht en Informatica aan de KUN. Hij is tevens werkzaam als bedrijfsjurist bij het Directoraat Juridische en Fiscale Zaken van Rabobank Nederland.

CONCLUSIE

Er ging een lange weg vooraf aan de totstandkoming van de Europese Privacyrichtlijn. De bepalingen van de richtlijn vormen vaak compromissen tussen uiteenlopende belangen. De tekst die thans voorligt munt, mede door vertaalperikelen, niet uit door helderheid van formulering. Daarnaast biedt de richtlijn zelf veel ruimte aan de nationale wetgever om keuzen te maken. Zoals in de inleiding al is aangegeven, streeft de wetgever naar een implementatie die zo dicht mogelijk blijft bij de huidige WPR. Er valt echter niet aan te ontkomen dat een groot aantal Brusselse trouvailles wordt toegevoegd aan het huidige stelsel van de WPR. Het zal een zeer lastige opgave worden om een en ander op begrijpelijke en uitvoerbare wijze in wetgeving te verwoorden. De richtlijn gaat naar het zich laat aanzien gevolgen hebben voor ieder detail in de samenleving. Op het oog geeft dat 'meer privacy'. Het zou echter wel eens zo kunnen zijn dat de kwantiteit ten koste gaat van de kwaliteit. Organisaties binnen overheid en bedrijfsleven kunnen weer vooraf beginnen met het analyseren van hun gegevensverwerkingsprocessen. Veel van wat er in het verleden is geïnvesteerd, is niet meer bruikbaar en dient te worden afgeschreven. Voorts breekt een periode van onzekerheid aan ten aanzien van de toelaatbaarheid van allerlei ingeburgerde bedrijfsprocessen.

De aansprakelijkheid van de Internet-aanbieder

Mr. S.C. Huisjes

De aansprakelijkheidspositie van een Internet-aanbieder is afhankelijk van zijn dienstverleningspakket. Bij gebrek aan specifieke regelgeving zal aan de hand van de verschillende bronnen van aansprakelijkheid in het algemeen moeten worden bepaald hoe ver zijn aansprakelijkheid reikt.

INLEIDING

Wie *Internet* zegt kan veel dingen bedoelen. Hij kan duiden op één van de diensten die via het wereldwijde netwerk-van-netwerken wordt aangeboden. Hij kan echter ook de bedoeling hebben te verwijzen naar het geheel van informatie- en communicatiediensten dat met behulp van 'het' Internet aangeboden wordt. Misschien heeft hij slechts de fysieke infrastructuur, het netwerk-van-netwerken, op het oog die de basis vormt voor de informatie-uitwisseling over het 'web'. In de meeste gevallen wordt met de aanduiding Internet echter de *World Wide Web-* (*WWW*) en/of de *E-mail*-dienst bedoeld. Het WWW en E-mail vormen samen de spil van het Internet. Het World Wide Web is het meest multifunctionele en meest gebruikte onderdeel van het veelkleurige geheel van Internet-diensten. Zonder moeite kan er via het WWW, wereldwijd, informatie openbaar worden gemaakt en worden ingewonnen. Nationale grenzen of aard van de (digitale) informatie – tekst, geluid of beeld – vormen geen obstakels meer bij de informatie-uitwisseling via het Internet.

Het antwoord op de vraag wat er wel en wat niet geoorloofd was in 'cyberspace' was lange tijd slechts afhankelijk van de stand der techniek en de zogenaamde Netiquette: de ongeschreven omgangsregels op het Internet. Toch is het niet zo dat het bestaande recht niet van toepassing is op het Internet. De grote vraag is echter op welke manier het bestaande, veelal op de traditionele vormen van informatie-uitwisseling geënte, recht toegepast moet worden in een juridisch terra incognita als het Internet. Deze vraag wordt met name door de tomeloze groei van het aantal gebruikers van het Internet en de intrede van handel en commercie, steeds belangrijker.

Na een korte introductie van het WWW, de E-maildienst en Usenet volgt in dit artikel een bespreking van de verschillende posities die een Internet-aanbieder met betrekking tot deze op het Internet dominerende communicatievormen kan innemen. Daarna zal aan de hand van voorbeelden uit de praktijk en de relevante Nederlandse wetsbepalingen, worden ingegaan op de belangrijkste aansprakelijkheidsvraagstukken die zich tot nu toe met betrekking tot het Internet hebben aangediend. Vooral de kwestie van de juridische aansprakelijkheid van de Internet-aanbieder komt in de casuïstiek, en daarom ook in het hierna volgende, sterk naar voren.

E-MAIL, WWW EN USENET

Het WWW en de E-mail-dienst zijn de belangrijkste onderdelen van het Internet. Het veelgebruikte E-mail is, afgezien van de gebruikte technieken, in juridische zin goed vergelijkbaar met de reguliere communicatievormen telefonie en post. In de regel gaat het om de vertrouwelijke uitwisseling van informatie tussen twee partijen, elk met een persoonlijk E-mail-adres.
Daar waar het bij E-mail vaak gaat om een tweezijdige conversatie kunnen op het WWW alle mogelijke vormen van informatie-overdracht worden teruggevonden: open en besloten informatie-uitwisseling en eenzijdige en interactieve communicatie. Bovendien kan de informatie die met behulp van het WWW wordt uitgewisseld, bestaan uit zowel tekst en geluid als bewegend of stilstaand beeld. De informatie wordt aangeboden op zogenaamde web-pagina's. Dit zijn met de traditionele papieren bladzijde vergelijkbare werken die op het beeldscherm van de eigen computer verschijnen door, met behulp van een zogenaamde web-browser, contact te leggen met een *web-server*: een andere op het Internet aangesloten computer welke dienst doet als informatiedrager. Groot verschil met op papier gedrukte tekst en beeld is dat de op het WWW beschikbare informatie wordt gekenmerkt door het gebruik van *hypertext* en *clickable images*. Hierdoor is het mogelijk zogenaamde *hyperlinks* op web-pagina's aan te brengen. Hyperlinks zijn verwijzingen naar andere web-pagina's, of delen daarvan, of op dezelfde server beschikbare plaatjes, teksten of geluidsfragmenten. De Usenet-dienst omvat vele duizenden verschillende discussiegroepen over de meest uiteenlopende onderwerpen. De dienst kan worden vergeleken met een elektronische en zeer uitgebreide versie van de ingezonden brievenpagina van een krant. Iedere Internetgebruiker kan met een digitale bijdrage zijn inbreng leveren aan het 'groepsgesprek'.

In beginsel bepaalt de klant de inhoud van zijn web-pagina en speelt de Internet-aanbieder hierbij een passieve rol.

DE VERSCHILLENDE HOEDANIGHEDEN VAN DE INTERNET-AANBIEDER

Naast de basisdienst die bestaat uit de toegangsverschaffing tot het Internet, waarbij de rol van de Internet-provider passief is, kan de klant van een Internet-aanbieder vaak ook zijn eigen web-pagina('s), ook wel *homepages* genoemd, op het computersysteem (web-server) van de Internet-aanbieder neerzetten en deze ter raadpleging beschikbaar stellen aan de Internet-gemeenschap. De klant krijgt hiertoe een hoeveelheid geheugenruimte tot zijn beschikking. Door in te loggen op het systeem van zijn Internet-aanbieder kan de klant naar eigen goeddunken en op elk gewenst tijdstip de inhoud van zijn web-pagina (her)bepalen. In de praktijk speelt de Internet-aanbieder ook bij de technische ondersteuning van web-pagina's in beginsel een passieve rol. Wel zal hij op gezette tijden controleren of de door hem ondersteunde particuliere web-pagina's niet voor commerciële doeleinden worden gebruikt. Daarvoor geldt een hoger abonnementstarief. Het behoort tot zijn theoretische mogelijkheden om met een technische ingreep een web-pagina uit zijn systeem te verwijderen of de toegang tot een pagina te blokkeren. Datzelfde kan hij doen als het gaat om de toegang tot een nieuwsgroep binnen Usenet. In de meeste gevallen stelt de Internet-aanbieder met behulp van zijn eigen web-pagina's ook zelf informatie op het Internet beschikbaar.

In de literatuur over de juridische aspecten van Internet tekent zich de gewoonte af om de Internet-aanbieder in zijn basisactiviteit van toegangsverschaffer als *access-provider* aan te duiden, bij beschikbaarstelling van zijn WWW-server en eventuele andere openbare diensten zoals Usenet als *service-provider*, en als verzamelaar, samensteller of redacteur van informatie als *information-provider*.
In het hierna volgende zullen de verschillende voor het Internet relevante Nederlandse wettelijke bronnen van aansprakelijkheid worden behandeld. Het antwoord op de vraag of een Internet-aanbieder handelt in de hoedanigheid van *access-*, *service-* of *information-provider* is, zo zal blijken, van invloed op zijn juridische aansprakelijkheid.

Discriminatie en racisme

Het Nederlandse recht bevat tal van strafbepalingen die betrekking hebben op zogenaamde uitingsdelicten ([Roos96]). Een belangrijke groep hiervan bevindt zich op het terrein van de discriminerende uitingen (artt. 137c – 137g Sr). Art. 137e Sr stelt het openbaar maken van een uitlating die voor een groep mensen op grond van hun ras, godsdienst, levensovertuiging of seksuele gerichtheid beledigend is, strafbaar. De uitdrukking 'openbaar maken' moet ruim worden uitgelegd. Het openlijk aanbieden van informatie, zelfs al is het in een besloten kring van gelijk gestemden, is voldoende om te voldoen aan dit element van de delictsomschrijving. In de beslotenheid van een point-to-point-conversatie per elektronische post zal nimmer voldaan worden aan het openbaarmakingsvereiste.[1] Dat iemand die racistische uitlatingen doet op zijn vrij toegankelijke WWW-homepage of binnen een openbare elektronische discussie over de grenzen van het wettelijk toelaatbare gaat staat daarentegen buiten twijfel.

In de zomer van 1995 kwam met betrekking tot een openbare discussie waarin racistische uitingen voorkwamen en welke ondersteund werd door het computersysteem van service-provider de Digitale Stad in Amsterdam de vraag naar voren of ook de service-provider, welke verder geen inhoudelijke invloed op de discussies binnen zijn systeem heeft en wil hebben, aansprakelijk gehouden kan worden voor de strafbare uitlatingen. Hoewel het

1. De E-mail-dienst kan niet alleen voor de vertrouwelijke vorm van 'point-to-point-conversatie' worden gebruikt, maar ook voor het opzetten van en deelnemen aan discussielijsten. Na inschrijving kan vrijelijk aan de discussie worden deelgenomen. Het leveren van een bijdrage aan een dergelijke discussielijst moet wél als een openbaarmaking worden gezien.

Amerikaanse rechtssysteem vanzelfsprekend niet het Nederlandse is, suggereren twee Amerikaanse gerechtelijke uitspraken toch dat het antwoord op deze vraag negatief moet zijn ([Kroe96]). In de zaak Cubby versus Compuserve, welke speelde in 1991, werd de online-dienstverlener Compuserve niet aansprakelijk gehouden voor onrechtmatige uitingen gedaan in een elektronisch discussieforum binnen zijn eigen systeem. De rechter kon het met Compuserve eens zijn waar deze aanvoerde slechts aansprakelijk te kunnen worden gesteld als hij van de onrechtmatige uiting geweten had of redelijkerwijs had kunnen weten. De rechter constateerde dat Compuserve geen redactioneel toezicht uitoefende en daardoor vergelijkbaar was met de eigenaar van een openbare bibliotheek, boekhandel of een kiosk.
In een juridisch geschil tussen Stratton Oakmont en de Amerikaanse online-onderneming Prodigy sloeg de wijzer van de weegschaal naar de andere kant door. Doorslaggevend hierbij was dat Prodigy zich geprofileerd had als een online-dienst welke zich actief inzette om bepaalde normen en waarden binnen de beschikbaar gestelde informatie hoog te houden. Hij maakte hiertoe gebruik van interne richtlijnen, gesprekleiders en software welke informatie kan controleren op ongewenst woordgebruik. Prodigy werd door de rechter vergeleken met een uitgever en aansprakelijk gehouden voor de schade welke de beledigde partij had geleden door de smadelijke uitlatingen binnen de discussiegroep. Een beroep van Prodigy op de vergaande gevolgen die een aansprakelijkheidsstelling zou hebben voor de vrijheid van meningsuiting werd door de rechter afgewimpeld: Prodigy wilde zelf de vrijheid van meningsuiting binnen zijn gespreksfora inbinden door het stellen van normen en waarden, maar als het aankwam op het dragen van de (juridische) gevolgen als hij deze pretenties niet waar kon maken gaf hij, onterecht, niet thuis.

Het voorgaande toont het belang aan om stil te staan bij het verschil tussen online-dienstverleners en Internet-aanbieders. Hoewel de meeste online-dienstverleners vandaag de dag ook toegang tot het Internet bieden zijn zij hun ondernemingsactiviteiten begonnen als, om een Internet-term te gebruiken, information-provider ([Kuip95]). Omdat de redactionele betrokkenheid van een online-dienstverlener over het algemeen vele malen groter is dan die van een Internet-access- en service-provider, moet worden aangenomen dat zijn aansprakelijkheid, tenminste voorzover het zijn eigen informatiediensten betreft, navenant groter is.

Kinderpornografie

Het per 1 februari 1996 aangescherpte art. 240b Sr stelt het in voorraad hebben, verspreiden, openlijk tentoonstellen, vervaardigen en in-, uit- of doorvoeren van kinderpornografie, onder alle omstandigheden, strafbaar. De reikwijdte van deze wetsbepaling is zeer ruim. Voor iemand die het nodig vindt om kinderpornografie beschikbaar te stellen op Internet zal het, eenmaal geïdentificeerd, opgespoord en gedagvaard, moeilijk zijn zichzelf te behoeden voor een veroordeling. Degene die de pornografie beschikbaar stelt zal daarom veel moeite doen om zijn identiteit te verhullen. De grote aanbieder van Internet- en online-diensten Compuserve heeft in december 1995 op last van de Duitse justitie een deel van de Usenet-discussiegroepen die via zijn systeem beschikbaar waren, ontoegankelijk gemaakt omdat deze erotisch of pornografisch getint waren. Het is in deze zaak nooit tot een gerechtelijke vervolging gekomen. Een veroordeling van een Internet-aanbieder vanwege een vergelijkbaar voorval is echter, gezien de ruime formulering van de strafbepaling en de sterke maatschappelijke veroordeling van kinderpornografie, zeker niet ondenkbaar. Als hij al niet direct als (mede)dader aansprakelijk kan worden gesteld op grond van de strenge antikinderpornowetgeving, zou hij allicht op grond van medeplichtigheid strafbaar kunnen worden geacht.

De Internet-aanbieder als mededader of medeplichtige: het getrapte aansprakelijkheidssysteem

Om de Internet-provider in strafrechtelijke zin als mededader of medeplichtige te kunnen beschouwen, is, uitzonderingen als die van kinderporno wellicht daargelaten, ten minste nodig dat hij zich bewust is van de strafbaarheid van de met behulp van zijn informatiesysteem openbaar gemaakte informatie en dat hem enigermate van verwijt te maken is ([Hart96]). Dit kan bijvoorbeeld het geval zijn als hij nalaat een technische ingreep te doen die de onrechtmatige informatie onbereikbaar maakt. In zijn hoedanigheid van access-provider, die zijn klanten toegang verschaft tot de overvloed aan informatie op het omvangrijke en inhoudelijk constant veranderende Internet, is de strafrechtelijke aansprakelijkheid van de Internet-aanbieder daarom weinig aannemelijk. Voor zijn activiteiten als service-provider ligt dit wellicht anders. Maar ook hier moet worden aangenomen dat de Internet-aanbieder slechts strafrechtelijk aansprakelijk dient te worden gehouden indien hij op de hoogte is, of dit redelijkerwijs had moeten zijn, van de onrechtmatigheid van de door één van zijn klanten via zijn informatiesysteem op een web-pagina openbaar gemaakte informatie. Als dit niet het geval zou zijn, en de hierdoor risico-aansprakelijke service-provider actief censuur zou moeten toepassen om vervolging te voorkomen, zou de grondwettelijk vastgelegde vrijheid van meningsuiting danig in de verdrukking komen.

Wat betreft de aansprakelijkheid van de Internet-aanbieder bij inbreuk op auteursrechten, is de tendens niet eenduidig.

Rekening houdend met een soortgelijk gevaar, maar dan met betrekking tot de positie van uitgevers en drukkers, heeft de wetgever in de artt. 53 en 54 Sr een zogenaamde getrapte aansprakelijkheidsregeling opgenomen ([Hins95]). Simpel gesteld komt deze erop neer dat in eerste instantie

slechts de schrijver aansprakelijk is. Voorwaarde hiervoor is wel dat de naam van de schrijver bekend is of, op eerste verzoek van het openbaar ministerie, door de uitgever of drukker bekend wordt gemaakt. De bepalingen van artt. 53 en 54 Sr zijn blijkens de parlementaire geschiedenis slechts van toepassing op de uitgever en drukker voorzover deze de schrijver slechts materiële medewerking verlenen bij het (doen) drukken van een geschrift en daarbij geen bemoeienis hebben met de inhoud. Het ligt voor de hand om de service-provider zonder inhoudelijke inbreng als een digitale uitgever te benaderen en hem, in rechtspraak of wetgeving, naar analogie, het strafrechtelijke privilege van artt. 53 en 54 Sr toe te kennen ([Roos96]). In deze opzet behoeft de service-provider weliswaar geen controle uit te voeren op de met behulp van zijn systeem openbaar gemaakte informatie, maar handelt hij wel wijs als hij een betrouwbare registratie voert van de identiteit van de door hem ten dienst gestane klanten. Het behoeft geen uitleg dat de Internet-aanbieder als samensteller van zijn eigen web-pagina's, als information-provider, aansprakelijk is voor de onrechtmatigheid van zijn openbaarmakingen. Zijn juridische positie is daarin goed vergelijkbaar met die van de uitgever van een tijdschrift.

De juridische positie van de Internet-aanbieder blijft betrekkelijk onzeker.

Auteursrechtelijk onrechtmatig handelen

De maker van 'werk van letterkunde, wetenschap of kunst' heeft in principe het alleenrecht op het openbaar maken en verveelvoudigen van zijn geesteskind. De auteurswetgeving bevat bepalingen die degene die iemands auteursrecht schendt, strafbaar stelt en bovendien privaatrechtelijk aansprakelijk maakt. Een auteursrecht rust bijvoorbeeld op teksten, muziek(fragmenten), software en beeldmateriaal. Door het grote gemak waarmee met behulp van de moderne informatietechnologie informatie kan worden gedigitaliseerd, openbaar gemaakt en gereproduceerd en het massale gebruik dat de Internet-gebruikers van deze mogelijkheid maakten, is de geldigheid van de auteursrechtelijke bescherming op het Internet lange tijd onmerkbaar geweest.

Het auteursrechtelijk tij lijkt echter gekeerd te zijn ([Huge95]). De eerste tekenen hiervan zijn te vinden in de Verenigde Staten. Daar werd in 1993 de beheerder van een elektronisch prikbord (Bulletin Board Service, BBS) veroordeeld omdat één van zijn klanten vele tientallen (auteursrechtelijk beschermde) foto's uit het blad Playboy op het elektronische prikbord had gehangen. Ondanks het verweer van de BBS-beheerder dat dit alles buiten zijn medeweten om was gebeurd, werd hij, vanwege de inbreuk op Playboys exclusieve rechten op openbaarmaking en verveelvoudiging, aansprakelijk geacht. In Nederland heeft de Buma/Stemra, het orgaan belast met het innen van vergoedingen voor reproductie van muziek, een actief inningsbeleid ingezet ten aanzien van de terbeschikkingstelling van muziekfragmenten op het WWW.
Maar van eenduidigheid in de rechtspraak, waar het de aansprakelijkheid van de Internet-aanbieder voor auteursrechtschendingen betreft, is vooralsnog geen sprake. De Scientology-kerk probeert met een beroep op het auteursrecht, zowel in de Verenigde Staten als in Nederland, met gerechtelijke stappen de ongeautoriseerde openbaarmaking van haar religieuze documenten tegen te gaan. De gevolgen van de aansprakelijkstelling van de Internet-aanbieder gingen de rechter die in november 1995 uitspraak deed in de zaak Scientology versus Netcom te ver ([Netc95]). Net als de Haagse rechtbankpresident die in maart 1996 uitspraak deed in een soortgelijk conflict – hierover later meer – vonniste hij dat de Internet-aanbieder niet als openbaarmaker van de beschermde werken aansprakelijk kon worden gehouden.

Een ander interessant auteursrechtelijk geschil ontstond tussen PTT Telecom en een Internet-service-provider te Haarlem.[2] Onder de naam Web-tel bood het bedrijfje toegang tot een geavanceerd elektronisch telefoonboek, beschikbaar gesteld op de web-server van de onderneming. PTT Telecom voerde aan dat het onderliggende databestand onrechtmatig overgenomen was van een eerder door haar op commerciële basis en onder auteursrechtelijke bescherming op de markt gebrachte CD-ROM. Afgezien van de vraag of dit laatste het geval was, moet worden geconstateerd dat het Haarlemse bedrijf in deze zaak optrad als information-provider en daarmee in beginsel verantwoordelijk was voor de veronderstelde onrechtmatige openbaarmaking van de informatie; niet een betalende klant maar een binnen de verantwoordelijkheidssfeer van de Internet-aanbieder vallende werknemer had de informatie via het WWW beschikbaar gemaakt.
Actueel is het standpunt van de Nederlandse Vereniging van Producenten en Importeurs van beeld- en geluidsdragers (NVPI), de belangenvertegenwoordiger van de Nederlandse platenimporteurs, die de Nederlandse Internet-aanbieders wil verplichten de Amerikaanse WWW-adressen waar tegen lage prijzen CD's kunnen worden besteld, onbereikbaar te maken. Aangezien de Internet-aanbieder in dit geval slechts als access-provider optreedt, valt als het aankomt op een juridische procedure de juistheid van een positieve respons van de rechter op de eis van de NVPI te betwijfelen.

In antwoord op de vraag naar de auteursrechtelijke aansprakelijkheid van de Internet-aanbieder voor de onrechtmatige doorgifte van informatie wordt vaak gewezen op de zogenaamde kabelarresten ([Kabe81], [Kabe83]). Het ging in deze gerechtelijke uitspraken om de auteursrechtelijke verantwoordelijkheid van een kabeltelevisie-exploitant voor de passieve doorgifte van programma's. In één van de gevallen waren de programma's afkomstig van een kabelpiraat die in de nachtelijke uren met een eigen zender wist in te breken in het kabeltelevisienet. De Hoge Raad velde het oordeel dat de kabel-

2. In bedoeld kort geding is op 10 juli door de president van de rechtbank te Haarlem uitspraak gedaan ten gunste van PTT Telecom. De inleidende dagvaarding en het vonnis zijn beschikbaar gesteld op het WWW: Http://194.178.232.2/web-tel/nieuws/.

televisie-exploitant aansprakelijk was. Dat alle initiatief tot de onrechtmatige uitzendingen bij de kabelpiraat gelegen had, deerde de Hoge Raad niet. De exploitant had nagelaten de nodige technische maatregelen te nemen om inbraak op het netwerk onmogelijk te maken en moest daarom als openbaarmaker worden bestempeld in de zin van de Auteurswet. De Haagse rechtbank is, zo blijkt uit haar vonnis in de Scientology-zaak, overigens allesbehalve overtuigd van de geldigheid van een juridische analogie tussen Internet-aanbieders en kabelexploitanten. Er valt dan ook heel wat af te dingen op de eventuele parallel ([Hove95]).

Privaatrechtelijke aansprakelijkheid

De privaatrechtelijke onrechtmatigheid van iemands handelen ligt, daar waar het om onrechtmatige uitingen gaat, voor een deel in het verlengde van de strafrechtelijke laakbaarheid. De privaatrechtelijke onrechtmatigheid is echter door de open formulering van het onrechtmatigheidscriterium van art. 6:162 Burgerlijk Wetboek een minder duidelijk afgebakend geheel dan zijn strafrechtelijk equivalent. Het even genoemde wetsartikel verplicht degene die jegens iemand anders een onrechtmatige daad pleegt diens schade te vergoeden. Een onrechtmatige daad, in privaatrechtelijke zin, wordt omschreven als 'een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt'. Bij het maken van inbreuk op een recht moet, in de context van het Internet, in de eerste plaats worden gedacht aan de schending van iemands auteursrecht. De onrechtmatigheid van iemands handelen die haar oorzaak vindt in de strijdigheid met een wettelijke plicht mag worden gezocht in de sfeer van de strafrechtelijk verboden handelingen en de privaatrechtelijke wetsbepalingen van dwingende aard. De in de omschrijving van de onrechtmatige daad in het Burgerlijk Wetboek opzettelijk open gehouden norm van de maatschappelijke betamelijkheid is met betrekking tot het Internet door de rechtspraak nog niet ingekaderd. Wel kan worden gezegd dat het antwoord op de vraag of een Internet-aanbieder maatschappelijk onzorgvuldig gehandeld heeft, en daardoor aansprakelijk is geworden voor de daaruit voortvloeiende schade, samenhangt met criteria als de (on)mogelijkheid van voorzorgsmaatregelen, de voorzienbaarheid van de schade en, niet in de laatste plaats, het kennis hebben van de Internet-aanbieder van de schadeveroorzakende toestand ([Kasp96]).

In de uitspraak in kort geding van de president van de Rechtbank te Den Haag in de Scientology-zaak wordt de lijdelijkheid van de Internet-aanbieder als service-provider met stelligheid onderstreept ([Comp96], [Medi96]). In de opvatting van de Haagse Rechtbank kan de Internet-aanbieder in beginsel geen invloed uitoefenen op of zelfs maar kennis dragen van datgene wat diegenen die via hem toegang tot Internet hebben gekregen daarop uitdragen. Hij doet, in de visie van de Haagse president, niet meer dan gelegenheid geven tot openbaarmaking en hij maakt dus niet zelf openbaar. Hoewel deze stellige uitspraken de voor het gerecht gedaagde Internet-aanbieders tevreden gestemd zullen hebben, valt te betreuren dat in het vonnis geen duidelijk onderscheid wordt gemaakt tussen de verschillende taken en diensten van de Internet-aanbieder. Iemands aansprakelijkheid voor de onrechtmatigheid van informatie zou immers moeten samenhangen met de aard en mate van diens betrokkenheid bij die informatie. De eerder aangegeven driedeling in het dienstenpakket van de Internet-aanbieder geeft een goed handvat bij het bepalen van deze betrokkenheid.

Bij ontstentenis van uitspraken van een gezaghebbend college als de Hoge Raad en specifieke regelgeving blijft de juridische positie van de Internet-aanbieder betrekkelijk onzeker. Om deze onzekerheid kleiner te maken zouden de gezamenlijke Internet-aanbieders, verenigd in de Nederlandse Vereniging van Internet-Providers, kunnen overwegen een gezamenlijke gedragscode op te stellen. Dit zou henzelf, maar ook de rechter of de arbiter, bij toekomstige geschillen kunnen ondersteunen bij het bepalen van de eisen die aan hen kunnen worden gesteld.

Overigens moet nog worden opgemerkt dat de Internet-aanbieder vanzelfsprekend aansprakelijk is voor de tekortkomingen in de nakoming van zijn contractuele verplichtingen. Als hij in zijn dienstverlenende activiteiten niet voldoet aan de verplichtingen die hij krachtens zijn overeenkomsten en algemene voorwaarden op zich genomen heeft is hij, behoudens overmacht, aan te spreken door de hierdoor schade lijdende wederpartij.

HANDHAVING EN JURISDICTIE

Of het nu om inbreuken op het auteursrecht, racistische uitlatingen, het openbaar maken van kinderporno of andere onrechtmatige daden gaat, de digitalisering en digitale transmissie van informatie doet in beginsel niets af aan de theoretische geldigheid van de reeds bestaande (rechts)normen en waarden. Dat op het Internet tot voor kort zeer weinigen zich iets van de verschillende nationale rechtsstelsels hebben aangetrokken, heeft verschillende oorzaken. In de eerste plaats kan worden gewezen op niet-commerciële vrijdenkersmentaliteit die, zeker in de beginjaren, onder de gebruikers van het Internet de boventoon voerde. Met behulp van sociale controle en de zogenaamde Netiquette konden, zo was de gangbare gedachte, alle interne problemen op het Internet het hoofd worden geboden. In de tweede plaats maken de virtuele grenzeloosheid van het Internet en het daarmee samenhangende gemak waarmee informatie op globale schaal verspreid en verplaatst kan worden het moeilijk om het recht in de praktijk op het Internet toe te passen.
Het is een niet te onderschatten probleem om in een conflictueuze situatie op het Internet te bepalen welk nationaal rechtsstelsel van toepassing is en welk land vervolgingsbevoegdheid en rechterlijke competentie toekomt. Daar waar het het strafrecht betreft hangt de beantwoording van deze vragen

ten nauwste samen met de vaststelling van de *locus delicti* ([Net96]). Twee van de benaderingswijzen om de locus delicti te bepalen kunnen worden omschreven als 'de leer van het instrument'[3] en de 'leer van het constitutieve gevolg'[4].
Uitgaande van de geldigheid binnen het Internet van deze, naast elkaar gebruikte, opvattingen over de vestiging van rechtsmacht kan de mondiale toepasselijkheid van het recht van elk op Internet aangesloten land worden beargumenteerd. Een rechter in bijvoorbeeld de Verenigde Staten zou zijn rechtsmacht kunnen onderbouwen in een zaak waarin het gaat om, naar het Amerikaanse recht, onrechtmatige informatie die beschikbaar wordt gesteld op een web-server in Zweden, dit ondanks het feit dat de Zweedse information- en service-provider zich keurig houden aan de Zweedse wet.
Een dergelijk scenario zou verre van denkbeeldig geweest zijn indien de strenge Amerikaanse Communications Decency Act niet kort na invoering wegens strijdigheid met de vrijheid van meningsuiting ongrondwettig zou zijn verklaard ([Huis96]). Het onverkort hanteren van de oude opvattingen over de vestiging van nationale rechtsmacht zou binnen het Internet tot vergaande en ongewenste conflicten kunnen leiden. Als het gaat om de vrijheid van meningsuiting bestaan er nu eenmaal hemelsbrede verschillen van inzicht tussen de diverse nationale overheden.

SLOTOPMERKINGEN

De verschillende juridische geschillen die de laatste tijd in binnen- en buitenland zijn ontstaan, en soms ook aan een rechterlijke instantie zijn voorgelegd, lijken erop te duiden dat het reguliere recht langzaam maar zeker zijn intrede doet op het Internet. Bij gebrek aan speciale wetgeving moet het algemene recht worden gebruikt om de juridische aansprakelijkheid van de Internet-aanbieder te bepalen. Het bepalen van de contractuele aansprakelijkheid van de Internet-aanbieder zal in de regel weinig problemen opleveren; de Internet-aanbieder is aansprakelijk voorzover hij tekort komt in de nakoming van zijn contractuele toezeggingen. Om alle onduidelijkheid te voorkomen doet de Internet-aanbieder er goed aan heldere contractvoorwaarden op te stellen.
De strafrechtelijke aansprakelijkheid van de Internet-aanbieder en zijn aansprakelijkheid uit onrechtmatige daad werpen meer vraagtekens op. Juridisch relevante concepten als 'openbaar maken' en 'hetgeen in het maatschappelijk verkeer betaamt' moeten worden vertaald naar de nieuwe en unieke omgeving van het Internet. Met een simpele analogie met de reeds langer bestaande media is niet te volstaan. Wel zijn er enkele handvatten aan te wijzen die een rol kunnen spelen bij het bepalen van de aansprakelijkheidspositie van de Internet-aanbieder. Allereerst moet rekening worden gehouden met de aard van de communicatiedienst die gebruikt wordt voor de onrechtmatige uiting. Terwijl belangrijke Internet-diensten als het WWW en Usenet openbaar van karakter zijn (*point-to-multipoint*-communicatie), is de E-mail-dienst in de eerste plaats bedoeld voor niet-openbare informatie-uitwisseling (*point-to-point*-communicatie). Met het grondwettelijk vastgelegde telefoon- en postgeheim in het achterhoofd zal een Internet-aanbieder zich niet verantwoordelijk hoeven te voelen voor onrechtmatige informatie-uitwisseling per E-mail met behulp van zijn computersysteem. Of dit ook bij de openbare communicatiediensten op het Internet het geval is hangt af van de mate van betrokkenheid van de Internet-aanbieder en daarmee van de aard van de diensten die de Internet-aanbieder levert.
In het dienstenpakket van een Internet-aanbieder kan een driedeling worden gemaakt welke haar weerslag zou moeten hebben op de beantwoording van eventuele aansprakelijkheidsvragen. Als access-provider levert de Internet-aanbieder aan zijn klant slechts de toegang tot het Internet. De aansprakelijkheid van de access-provider voorzover het de onrechtmatige verspreiding van informatie met behulp van zijn systeem betreft is miniem. Dit kan anders zijn als de Internet-aanbieder extra diensten levert die het de klant mogelijk maken om bijvoorbeeld met behulp van een eigen WWW-pagina zelf informatie openbaar te maken. In deze hoedanigheid wordt de Internet-aanbieder service-provider genoemd. Of de service-provider daadwerkelijk aansprakelijk is voor de onrechtmatige openbaarmakingen van zijn klanten hangt samen met de vraag of hij zich bewust is van de onrechtmatige situatie, of dat redelijkerwijs had moeten zijn, maar desondanks afziet van het nemen van maatregelen. Voorzover een Internet-aanbieder optreedt als information-provider, d.w.z. op eigen initiatief informatie openbaar maakt, bijvoorbeeld door middel van een bij hem in dienst zijnde redactie die de eigen web-pagina's van de Internet-aanbieder vult, kan hij in beginsel voor de onrechtmatigheid van de openbaarmaking van deze informatie aansprakelijk worden gehouden.

3. In het kort komt de leer van het instrument erop neer dat de locus delicti zich daar bevindt waar het gebruikte instrument (Internet) zijn uitwerking heeft.
4. De leer van het constitutieve gevolg: daar waar de voor de delictsomschrijving cruciale gevolgen plaatshebben, bevindt zich de locus delicti.

LITERATUUR

[Comp96] Computerrecht 1996 nr. 2.

[Hart96] A.E. Hartveld en J.L. van der Neut, *Internet-providers in de strafrechtelijke gevarenzone*, Delict en Delinquent 26, 1996, afl. 5.

[Hins95] A.W. Hins, J.M. de Meij, *Goede raad uit 1883 voor Internet*, Informatie en Informatiebeleid, winter 1995, nr. 4.

[Hove95] R. van den Hoven van Genderen, J. Nouwt, J.E.J. Prins, *Recht op de elektronische snelweg?!*, Samsom BedrijfsInformatie, Alphen aan den Rijn 1995.

[Huge95] P.B. Hugenholtz, *Het auteursrecht, het Internet en de informatiesnelweg*, NJB, 1995 nr. 14.

[Huis96] S.C. Huisjes, *Decency on the Web?*, IT&Recht, 1996 nr. 3.

[Kabe81] HR 30 oktober 1981 (CAI Amstelveen), NJ 1982, 435.

[Kabe83] HR 14 januari 1983 (KTA/Columbia), NJ 1984, 696.

[Kasp96] H.W.K. Kaspersen, *Aansprakelijkheid van Internet-providers*, Computerrecht, 1996 nr. 1.

[Kroe96] Q. R. Kroes, *Internet, Aansprakelijkheid in het Amerikaanse recht*, Computerrecht, 1996 nr. 1.

[Kuip95] H.H. Kuipers, *Internet versus de commerciële online-diensten?*, Informatie en Informatiebeleid, winter 1995 nr. 4.

[Medi96] Uitspraak van de President van de Haagse rechtbank in de zaak Scientology vs. XS4ALL e.a. en Karin Spaink, vonnis in kort geding van 12 maart 1996, gepubliceerd in Media*forum* april 1996 nr. 4.

[Net96] C.B. van der Net, *Locus Delicti op het Internet*, Computerrecht, 1996 nr. 2.

[Netc95] Religious Technology Center (Scientology) vs. Netcom online communication services, U.S. District Court, Northern District of California, d.d. 21-11-1995.

[Roos96] Th. de Roos, G. Schuijt, L. Wissink, *Smaad, laster, discriminatie en porno op het Internet*, ITeR-reeks, Samsom BedrijfsInformatie, Alphen aan den Rijn 1996.

Mr. S.C. Huisjes Studeerde rechten aan de Universiteit van Amsterdam. Hij is sinds 1994 als onderzoeker verbonden aan de Afdeling Recht en Informatica van de Rijksuniversiteit Leiden. Zijn aandachtsgebied beslaat het Nederlands en Europees Telecommunicatierecht en de juridische aspecten van Internet. Hij is, naast het door hem uitgevoerde onderzoek, betrokken bij het universitair onderwijs en vaste auteur van het tijdschrift Informatie Technologie & Recht (IT&R).

EDP AUDITORIUM

DE BOODSCHAPPER HEEFT GEEN BOODSCHAP AAN DE BOODSCHAP

Bespreking uitspraak Church of Scientology versus K. Spaink c.s.

Mr. P.P.J.L. Enneking

Op het Internet heeft de provider geen boodschap aan de boodschap, of toch wel ...?

INLEIDING

Op 12 maart 1996 diende een kort geding voor de president van de Rechtbank Den Haag inzake een geschil over inbreuk op auteursrechten via het Internet. Maken een access-provider en een gebruiker van het Internet inbreuk op auteursrechten door documenten via een zogeheten homepage ter beschikking te stellen aan andere gebruikers van het Internet?

De president oordeelde – kort weergegeven – dat een access-provider in beginsel geen inbreuk maakt, omdat deze niet meer doet dan gelegenheid geven tot openbaarmaking en in beginsel geen invloed kan uitoefenen op of kennis kan dragen van hetgeen via de homepage openbaar wordt gemaakt of wordt verveelvoudigd. Dat kwam overeen met de visie van de gedagvaarde access-providers, zij hadden zogezegd als boodschappers geen boodschap aan de boodschap.
Dit gold echter niet voor de gebruiker (mevrouw K. Spaink) die de documenten in haar homepage had opgenomen. In het onderhavige geval bleek echter dat zij de documenten inmiddels had vervangen door samenvattingen en citaten, waardoor een uitzondering op de Auteurswet van toepassing was.
Met deze uitspraak, waartegen overigens hoger beroep is ingesteld, moet ook in Nederland worden bevestigd dat het gebruik van Internet in Nederland niet alleen wordt beheerst door (ongeschreven) fatsoensregels van de zogeheten Netiquette, maar dat ook het Nederlandse (auteurs)recht integraal van toepassing is.

Het moge duidelijk zijn dat dit voor de rechtshandhaving, zeker ten aanzien van rechten van intellectuele eigendom, grote problemen met zich mee zal brengen. Wanneer de uitspraak van de president nog verder in ogenschouw wordt genomen, zullen zich overigens ook voor de access-providers de nodige problemen kunnen voordoen, nu de president heeft aangegeven dat deze wel degelijk aansprakelijk gehouden zouden kunnen worden indien zij bekend zijn met het feit dat inbreuk makende handelingen via hun systemen plaatsvinden, doordat zij bijvoorbeeld daarop worden geattendeerd.
Dan zullen access-providers dus wel zeker een boodschap aan de boodschap moeten hebben.
Het laatste woord is er nog niet over gezegd.

DE CASUS

Mevrouw K. Spaink maakte via een access-provider gebruik van het Internet. In een door haar opgezette homepage stelde zij andere gebruikers van het Internet in staat kennis te nemen van bepaalde (elektronisch weergegeven) documenten. Deze documenten betroffen onder meer enkele vertrouwelijke en niet-vertrouwelijke werken over de leer en de activiteiten van de Church of Scientology, van de hand van de in 1986 overleden oprichter L. Ron Hubbard.
De documenten (althans de inhoud daarvan) waren vermoedelijk afkomstig uit een bijlage van het zogeheten 'Fishman Affidavit'. Dit was een partijverklaring, opgesteld in het kader van een andere in de Verenigde Staten gevoerde gerechtelijke procedure tussen Church of Scientology International en de heer Steven Fishman. In de bewuste bijlage waren zonder toestemming van de auteursrechthebbende een kopie van het niet-vertrouwelijke werk 'Ability' en het ongepubliceerde vertrouwelijke werk 'Operating Thetan I t/m IV' opgenomen.
De auteursrechten (dan wel daarvan afgeleide licentierechten) op de via de homepage aangeboden werken komen toe aan de Church of Spiritual Technology, het Religious Technology Centre en New Era Publications International ApS (verder gezamenlijk te noemen 'Church of Scientology').
De Church of Scientology was van mening dat het beschikbaar stellen van deze werken via het Internet een inbreuk op haar auteursrechten betreft omdat sprake is van openbaarmaking[1] zodra gebruikers van het Internet in de gelegenheid worden gesteld kennis te nemen van de inhoud van deze werken. Zij was van mening dat in dit verband iedere in Nederland opererende access-provider via welke de documenten beschikbaar konden worden gesteld, alsmede de betreffende gebruiker mevrouw Spaink als inbreukmakers moeten worden beschouwd.

De Church of Scientology heeft in totaal 22 in Nederland opererende access-providers en mevrouw K. Spaink, in kort geding gedagvaard en – beknopt weergegeven – het volgende gevorderd:

- De access-providers en mevrouw Spaink moeten iedere inbreuk op auteursrechten welke aan de Church of Scientology toekomen staken en gestaakt houden.
- De access-providers moeten, zodra deze gewe-

zen worden op de aanwezigheid van inbreuk makende documenten die door gebruikers via hun computersysteem of door hun beheerste computersystemen beschikbaar zijn gesteld voor andere Internet-gebruikers, onmiddellijk verwijderen.

– De access-providers moeten dan voorts de desbetreffende gebruiker de toegang tot hun computersystemen weigeren.

– De access-providers moeten in dat geval tevens de Church of Scientology informeren welke gebruikers de inbreuk makende documenten via hun computersysteem hebben verveelvoudigd of openbaar gemaakt.

De Church of Scientology is van mening dat de access-providers geen lijdelijke rol spelen bij de informatieverschaffing via het Internet, doch de bewuste documenten openbaar maken dan wel deze openbaarmaking bevorderen door de documenten via hun computersystemen ter beschikking te stellen aan derden. In ieder geval zijn de access-providers reeds lange tijd op de hoogte van de inbreuk en werken zij daar willens en wetens aan mee, aldus de Church of Scientology.

Kort weergegeven verdedigen de access-providers en mevrouw Spaink zich met de volgende stellingen:

– Access-providers houden zich uitsluitend bezig met de infrastructuur voor de communicatie tussen gebruikers en niet met de inhoud van de informatie die de gebruikers ter beschikking stellen voor andere gebruikers. De rol van de access-providers is vergelijkbaar met die van PTT Telecom en zij hebben zogezegd 'geen boodschap aan de boodschap'.

– De access-providers spelen een passieve rol en maken geen verveelvoudigingen en zij maken evenmin openbaar. De kopie wordt niet door de access-provider, maar door de eindgebruiker ter beschikking gesteld.

– De access-providers hebben ook geen onrechtmatige daad gepleegd[2] door willens en wetens profijt te trekken van auteursrechtinbreuk. Zij hebben geen invloed op de inhoud van de boodschappen die via een homepage openbaar worden gemaakt. Zij zijn niet in staat de inhoud te controleren. Een dergelijke censuur zou ook in strijd zijn met het grondrecht van vrije meningsuiting op grond van art. 10 EVRM (Europees Verdrag van de Rechten van de Mens).

– De inbreukmakende werken zijn inmiddels door mevrouw Spaink van de homepage verwijderd en vervangen door een geparafraseerde versie. Daar waar stukken tekst letterlijk zijn overgenomen betreft het een citaat, hetgeen op grond van art. 15A Auteurswet is toegestaan omdat aan alle voorwaarden voor een citaat is voldaan.[3]

– Tot slot beroept mevrouw Spaink zich op de bescherming van art. 10 EVRM, het recht op de vrije meningsuiting.

HET OORDEEL

De president stelt vast dat de Church of Scientology de auteursrechten bezit op de bewuste werken en dat mevrouw Spaink een aantal passages uit deze werken op haar homepage had opgenomen. Dat na de wijziging van de homepage nog steeds inbreuk plaatsvindt is volgens de president niet aannemelijk geworden omdat art. 15A Auteurswet (citaatrecht) van toepassing is. Dat geldt ook voor de vertrouwelijke niet-openbare gedeelten (voorwaarde voor toepasselijkheid van art. 15A is namelijk onder meer dat geciteerd wordt uit rechtmatig openbaar gemaakte werken). Deze vertrouwelijke werken hebben namelijk in het kader van een gerechtelijke procedure in de Verenigde Staten vrijelijk voor iedereen ter inzage gelegen, zodat deze werken rechtmatig openbaar zijn gemaakt. De vorderingen gericht op mevrouw Spaink worden daarom door de president afgewezen.
Ten aanzien van de access-providers oordeelt de president dat deze niet meer doen dan gelegenheid geven tot openbaarmaking en dat zij in beginsel geen invloed kunnen uitoefenen op of zelfs maar kennis kunnen dragen van hetgeen via hun systemen door gebruikers beschikbaar wordt gesteld. In beginsel zijn de access-providers daarom niet aansprakelijk voor onrechtmatige handelingen van gebruikers.
De president voegt echter nog een belangrijke nuancering toe: 'Een aansprakelijkheid zou aangenomen kunnen worden 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. In een dergelijke situatie zou wellicht van de access-provider verlangd kunnen worden dat hij tegen de betrokken gebruiker optreedt.'

PUNTEN VAN AANDACHT

Uit de casus komen twee aandachtspunten naar voren: de vrijheid van meningsuiting en het intellectuele eigendomsrecht.

Vrijheid van meningsuiting en het Internet

Het in onze grondwet en art. 10 EVRM neergelegde grondrecht van vrijheid van meningsuiting[4] kan haaks komen te staan op de handhaving van auteursrechten en andere rechten van intellectuele eigendom, zo blijkt uit de casus. Access-providers mogen geen censuur toepassen op hetgeen door de bij hen aangesloten gebruikers via het Internet wordt openbaar gemaakt. Dat lijkt volstrekt terecht.
De vrijheid van meningsuiting mag echter niet zo ver gaan dat inbreuk op rechten van anderen wordt gemaakt. Dit blijkt ook uit de tekst van art. 10 lid 2 EVRM. De vrijheid van meningsuiting wordt derhalve begrensd door specifieke individuele rech-

ten, waaronder ook het auteursrecht.[5] Het beroep op art. 10 EVRM door mevrouw Spaink zou in beginsel dan ook moeten worden afgewezen. De president is echter aan dit beroep niet toegekomen omdat hij heeft vastgesteld dat in deze casus überhaupt geen sprake was van inbreuk op auteursrecht. Mevrouw Spaink kon zich op een uitzonderingsregel (het citaatrecht) beroepen. Wellicht komt de EVRM-discussie nog aan de orde in een eventuele bodemprocedure of in het hoger beroep.

Intellectuele eigendomsrechten en het Internet

Met de uitspraak wordt wederom bevestigd dat ook op het Internet het auteursrecht van toepassing is.[6] Dat dit voor de auteursrechthebbende enorme problemen voor de handhaving van zijn rechten met zich mee zal brengen is eveneens duidelijk, maar dat mag geen reden zijn om aan deze rechten voorbij te gaan.
Het is juist van eminent belang dat intellectuele eigendomsrechten zoals het auteursrecht, maar ook het octrooirecht, het merkenrecht en bijvoorbeeld het kwekersrecht in onze informatiemaatschappij een adequate en effectieve bescherming genieten. De intellectuele eigendomsrechten zijn immers één van de economische motoren van onze huidige maatschappij. Het wettelijke recht om uitvindingen en auteursrechtelijk beschermde werken exclusief, dus met uitsluiting van ieder ander te mogen exploiteren, is namelijk de belangrijkste prikkel om een nieuwe, inventieve of creatieve schepping te creëren en – belangrijker nog – daarin te durven investeren.[7]
Anders gezegd, de ontwikkelingen in techniek, cultuur en maatschappij zouden sterk stagneren indien de met deze ontwikkeling gemoeide investeringen niet kunnen worden terugverdiend. Dit geldt voor allerhande technologische zaken, maar evengoed voor artistieke en creatieve zaken.
Met de opkomst van het gebruik van het Internet zijn de mogelijkheden tot relatief eenvoudige openbaarmaking en verveelvoudiging enorm vergroot, waardoor de bezitter van rechten van intellectuele eigendom op dit punt voor complexe problemen is komen te staan. Deze handhavingsproblemen behoeven absoluut een oplossing. De vraag is welke.
Dat een oplossing ook vanuit het gezichtspunt van de access-providers nodig zal zijn blijkt uit de overweging van de president: '... en waarin redelijkerwijs mag worden aangenomen dat zulks ook bij de access-provider bekend is, ...'. Op dat moment kan deze zich niet meer 'verschuilen' achter de stelling dat hij niet weet en ook niet kan weten wat via zijn systemen het net wordt ingezonden en moet hij adequate maatregelen nemen om aansprakelijkheid te voorkomen. Dit zou kunnen betekenen dat de desbetreffende gebruiker of groep gebruikers moet worden afgesloten. De zich in Duitsland afgespeeld hebbende Compuserve-zaak demonstreert dat deze zeer ongewenste maatregelen zeker niet irreëel zijn.[8]
Overigens moet men zich afvragen of een access-provider überhaupt de mogelijkheid heeft zich te 'verschuilen' achter de stelling dat hij geen boodschap aan de boodschap heeft. Op grond van uitspraken van de Hoge Raad[9] is de exploitant van de kabeltelevisie als aansprakelijke openbaarmaker aangemerkt. Het betrof hier onder meer het clandestien instralen van films door kabelpiraten op de apparatuur van de kabelexploitant nadat de reguliere programma's waren beëindigd. 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. Deze uitspraak leidde er vervolgens toe dat de kabelexploitanten na het einde van de reguliere programma's de apparatuur afsluiten. De uitspraak heeft overigens tot de nodige kritiek geleid in juridisch Nederland.

Problemen rond de handhaving van intellectuele eigendomsrechten behoeven absoluut een oplossing.

Het zoeken is dus naar een oplossing die recht doet aan de belangen van de auteursrechthebbenden, de aanbieders van informatiediensten en aan de vrijheid van meningsuiting van de gebruikers van informatiediensten.

Access-providers zouden wellicht enigszins invloed kunnen uitoefenen op hetgeen via hun systemen in het Internet wordt gepompt zonder onevenredig afbreuk te doen aan het grondrecht van art. 10 EVRM. Als gezegd, een complete en actieve censuur is onwenselijk en overigens ook onmogelijk, maar in de abonnementsvoorwaarden voor de aangesloten gebruikers zou prima kunnen worden opgenomen dat de gebruiker zich verplicht zich te onthouden van inbreuk op rechten van intellectuele eigendom van derden. Een dergelijke bepaling zou zelfs in het verlengde passen van de veelal in de algemene voorwaarden opgenomen vrijwaringsclausules tegen claims voor inbreuk op intellectuele eigendomsrechten. Dit brengt dan met zich mee dat het voor de access-provider relatief eenvoudig is de desbetreffende gebruiker verdere toegang tot de aangeboden faciliteiten te ontzeggen zodra wordt geconstateerd (en de access-provider daarop wordt geattendeerd) dat inbreuk wordt gepleegd.

Auteursrechthebbenden zouden er voorts meer toe kunnen overgaan hun werken met technische of softwarematige hulpmiddelen te beschermen dan wel een verschijningsvorm te kiezen die moeilijk te verveelvoudigen of openbaar te maken is. Dit doet echter vaak geen recht aan de gewenste toegankelijkheid van het materiaal voor het publiek waarvoor het is vervaardigd en vaak zijn aan dit soort maatregelen hoge kosten verbonden waardoor ze hun doel voorbij schieten. Het inbrengen van virusachtige maatregelen die opspelen bij ongeautoriseerde verveelvoudiging of openbaarmaking moet in de meeste gevallen worden afgeraden omdat het risico van aansprakelijkheid te groot is. Bovendien is ook deze maatregel veelal 'klantonvriendelijk' en schiet dan ook zijn doel voorbij.
Wellicht zijn in de techniek toch nog wel creatieve

oplossingen te bedenken waardoor het handhavingsbelang van de auteursrechthebbende voldoende wordt gewaarborgd. De tijd zal het moeten leren.

Overigens zouden ook aan de kant van de regelgeving de benodigde maatregelen kunnen worden genomen. Wellicht moet het auteursrecht wel op de helling zoals prof. Dommering aangeeft in zijn artikel 'Het auteursrecht spoelt weg door het electronisch vergiet'.[10] Probleem blijft echter de handhaving van rechten. Ook op dit vlak zal de tijd het moeten leren.

NOTEN

1. In de Auteurswet 1912 staan de elementen 'verveelvoudiging' en 'openbaarmaking' centraal. Op grond van art. 1 van de Auteurswet heeft de maker van een werk het exclusieve recht op verveelvoudiging en openbaarmaking van dat werk, behoudens een aantal uitzonderingen en beperkingen.

2. Door onrechtmatig handelen ontstaat in het algemeen een civielrechtelijke aansprakelijkheid tot het vergoeden van de schade die door de ander wordt geleden. Als onrechtmatige daad wordt aangemerkt een inbreuk op een recht (bijvoorbeeld auteursrecht) en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond (art. 6:162 Burgerlijk Wetboek).

3. Op grond van art. 15A Auteurswet mag worden geciteerd zonder toestemming van de auteursrechthebbende indien: a) het geciteerde werk rechtmatig openbaar is gemaakt, b) het citeren geschiedt in overeenstemming met hetgeen in het maatschappelijk verkeer geoorloofd is en aantal en omvang van de geciteerde gedeelten door het te bereiken doel zijn gerechtvaardigd, c) de persoonlijkheidsrechten van de auteur in acht worden genomen en d) de bron en de maker op duidelijke wijze worden vermeld.

4. De tekst van art. 10 luidt als volgt: '1. Een ieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. Dit artikel belet Staten niet radio-, omroep-, bioscoop- of televisieondernemingen te onderwerpen aan een systeem van vergunningen. 2. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen.'

5. Een algemeen auteursrechtelijk verbod met betrekking tot de ontvangst en het gebruik van niet-geheime informatie staat met de vrijheid van meningsuiting op gespannen voet en zou met toepassing van art. 10 EVRM kunnen worden overruled door de rechter, aldus mr. P.B. Hugenholtz in NJB, 7 april 1995, afl. 14, blz. 516.

6. Dit is overigens ook af te leiden uit de Wet softwarebescherming (art. 45 g t/m n Auteurswet) welke is ingevoerd op basis van de Richtlijn softwarebescherming d.d. 14 mei 1991. Deze wet ziet weliswaar op bescherming van computerprogrammatuur (en is ten aanzien van software ook voor het Internet in Nederland rechtstreeks van toepassing), doch zou naar analogie ook voor (digitaal opgeslagen) geschriften kunnen worden toegepast.

7. In het rapport van de Commissie Bangemann (Europe's way to the information society – an action plan, Brussel, 19 juli 1994, Com (94) 347 final) wordt mede vanuit dit gezichtspunt hoge prioriteit toegekend aan adequate bescherming van intellectuele eigendom.
Ook in een in juli 1994 uitgebracht Amerikaans rapport van de Information Infrastructure Task Force van het Witte Huis is aangegeven dat praktisch ieder informatietransport op het Internet als een auteursrechtelijk relevante reproductie is aan te merken.

8. Het betrof hier echter geen auteursrechtelijke kwestie maar een strafrechtelijke. De Duitse justitie moest in deze zaak optreden tegen de verspreiding van kinderporno via het Internet en dreigde met beslaglegging. Compuserve besloot ter voorkoming daarvan bepaalde delen van het Internet in Duitsland af te sluiten in afwachting van een technische oplossing.

9. Hoge Raad 30 oktober 1981, vindplaats NJ 1982, 435 (CAI Amstelveen) en Hoge Raad 14 januari 1983, vindplaats NJ 1984, 696 (KTA/Columbia).

10. Computerrecht 1994/3, blz. 109 e.v.

Mr. P.P.J.L. Enneking
Is reeds geruime tijd werkzaam op het gebied van het bedrijfs- en informaticarecht, en sinds 1995 als Adviseur Informaticarecht verbonden aan KPMG EDP Auditors. Daarnaast heeft hij deelgenomen aan diverse werkgroepen op het gebied van informatica en recht en heeft hij een aantal publicaties op dit gebied vervaardigd.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact
Een compilatie van artikelen over informatica en recht die in eerdere Compacts zijn verschenen, is, aangevuld met actuele bijdragen over dit onderwerp, opgenomen in *Twintig over Informatietechnologie en recht*. Twintig auteurs behandelen een breed spectrum van aspecten van de raakvlakken van informatietechnologie en recht op voor EDP-auditor, manager, adviseur, jurist en accountant toegankelijke wijze.
Het boek is verkrijgbaar via de boekhandel onder ISBN 90 14 04634 0.

4 20e jaargang 93/4 winter 1993

Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving
Drs. R.G.A. Fijneman RE RA

Aandacht voor interne controle tijdens systeemontwikkeling
Drs. J.J. van Beek RE RA

Audit automation
Drs. L.H. Dam RA en drs. P. Veltman RE RA

Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?
J.C. Boer RE RA

Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking
Mw.mr.drs. A.W. Duthler

Automatiseringsrisico's, verzekeringen en de rol van de accountant
Drs. G.J.W.C. Vankan

Geautomatiseerde betalingen
Drs. R. Oudega en drs. P. Veltman RE RA

1 21e jaargang 94/1 lente 1994

De invloed van informatietechnologie op de beheersing van organisaties
Prof. A.W. Neisingh RE RA

Rekencentra: normen voor menskracht
Prof.dr.ir. R. Paans RE

Accountant en de kosten- en batenbeheersing van informatietechnologie
Prof. H.B. Moonen RE RA

Informatiebeveiliging: de tijd is rijp
Drs. H.G.Th. van Gils RE RA

Het beoordelen van het testen van systemen
P. van Berge

2 21e jaargang 94/2 zomer 1994

Audit van een SNA-netwerk
M.M. Buijs RI en E.J.M. Ridderbeekx RE RI

Beveiliging van analoge kieslijnen
Drs.ing. D. Brouwer RE

Beveiliging van UNIX
Mw.drs. M.C. van Lith RE

Typologie van workflow-managementsystemen
Drs. D.J.P. Witte

3 21e jaargang 94/3 herfst 1994

Inleiding tot op TCP/IP gebaseerde netwerken
Ir. P. Kornelisse

Internet? Maar dan wel met een firewall!
H. van Hulst

Netwerkverbindingen in een OpenVMS-omgeving
Ir. J.H. Lie-Tjauw

Enige juridische wegwijzers voor de elektronische snelweg
Mw.mr. G.P. van Duijvenvoorde

Betrouwbaarheid en beveiliging van een CICS-omgeving
Ing. G.H.M. Meijer RE en mw. J.A.M. Holla

4 21e jaargang 94/4 winter 1994

Geautomatiseerde gegevensbewerking en jaarrekeningcontrole
R.A. Jonker RA

De invloed van informatietechnologie op de interne-controleprincipes
J.C. Boer RE RA

Audit van een logistiek systeem
Drs. J.A.C. van Geel, ing. A.P.J. Mouwen en drs. E.P.R. van Vroenhoven RE RA

Informatiebeveiliging van theorie naar praktijk
Drs. P. Veltman RE RA

Informatie(beveiligings)beleid in concernverband
Prof. A.W. Neisingh RE RA

1 22e jaargang 95/1 lente 1995

Internetworking; beheerproblematiek en security-risico's
H. Roos RA en ir. M.T.H. Heesbeen

Geïntegreerd netwerkbeheer
Ing. W.A.A. Zoon

Client/server geconcretiseerd
J.C. van Praat RE RA

Radio-LAN's in de praktijk
Ir. B.J. Busropan, ir. G.J. de Groot, ir. W. Hollemans, ir. E.C. den Toom en ir. A. Verschoor

3DAS-kenmerk, een uniek middel voor identificatie en authenticatie
Ir. W.H.M. Sipman RI

2 22e jaargang 95/2 zomer 1995

Het beheer van PC-netwerken
Drs.ing. R.F. Koorn CISA

Multimedia nader bekeken
Drs. A.M. Buren

Introductie van een bancair systeem in een wide area netwerkomgeving
W.N.P. Zethof RE RA

GEBIT. Gestructureerd Evalueren van de Baten van IT-investeringen
Mw. M.S. Hablous

3 22e jaargang 95/3 herfst 1995

Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering
Mw. W.A. de Munck RA

Plaats en taken van de EDP-auditfunctie bij de KLM
J.G. de Vries RE RA

Wet op het consumentenkrediet: systeemgericht onderzoek vereist
R. van den Hoorn RA

Third party review en -mededeling bij uitbesteding van IT-services
Drs. P. Veltman RE RA

Maatwerk past informatiebeveiliging
Drs. E. Roos Lindgreen en mw.drs. C. Schönfeld RI

Stroomlijnen en herontwerpen in een onderhoudsbedrijf: gelijktijdig en/of volgtijdig?
Drs. O.C. van Leeuwen RA en drs. M.C. van Veen RC

Het ontwikkelen van methoden en technieken van EDP-auditing
Drs. R.G.A. Fijneman RE RA

4 22e jaargang 95/4 winter 1995

Informatieplanning en standaardpakketten
Drs. J. de Boer en ir. J.A.M. Donkers RE

Certificatie van een standaardpakket voor financiële administraties
Drs. H.G.Th. van Gils RE RA

AO en standaardpakketten: integratie verhoogt de kans op een succesvolle selectie en implementatie
Drs. J.J. van Beek RE RA, drs. W. Boogaard RA CPIM en drs. J.J.B. van den Oever

Waardebepaling van software
Ir. J.A.M. Donkers RE en drs. G.J.J. Timmer

Business Process Controlling
Drs. J.J. van Beek RE RA en W. Teeuwissen RA

1 23e jaargang 96/1

Normbesef
L. Annokkée RE en B. Sebregts RE

ISO 9000 en EDP-auditing
Mr. W.R. Nanninga RE en ltkol J.M.W. van de Garde RE

ITIL als inrichtings- en beoordelingsinstrument
Drs. F.J. Hut

De Code voor Informatiebeveiliging
Dr.ir. P.L. Overbeek

De Code voor Informatiebeveiliging als norm voor de EDP-auditor
W.S.C. Krol RE en drs. M.M. Smits

2 23 jaargang 96/2

Besluitvorming over IT-investeringen: gebruik de juiste criteria
Ing. E.M.H. Coorens BE MBA, drs. P.J.C. van Bladel en dr. M. Boogaard

Benchmarking, een hulpmiddel voor de EDP-auditor?
Ir. J.A.M. Donkers RE en mw. ir. E.R. van Sommeren

AS/400-networking
Mw. drs. A.L. Hristova RE

1 23e jaargang 96/3

Systeemsoftware onder controle
Drs. R.H.H.M. Bronzwaer

Fiscale bewaarplicht van gegevens
T.H.C. van de Molengraft RA

System Review Services
Mw. drs. M.J.A. Koedijk RA en mw. W.A. de Munck RA

De EDP-auditor: vertrouwensman, agent of ...?
Drs. H.E. Sijbring RE RA

KPMG EDP Auditors
Samsom BedrijfsInformatie