Kroniek van het ICT-recht. Megatrends in 2002 en 2003

Koops, E.J.; Stuurman, C.

Published in:
Nederlands Juristenblad

Publication date:
2004

B.J. Koops & C. Stuurman (2004), 'Kroniek van het ICT-recht. Megatrends in 2002 en 2003'
Verschenen in: Nederlands Juristenblad 2004, p. 539-547.

Kroniek van het ICT-recht

versie 6, bjk, 06/02/04

Bert-Jaap Koops is uhd recht & techniek bij het Centrum voor Recht, Bestuur en Informatisering van de Universiteit van Tilburg.
Kees Stuurman is hoogleraar normering van informatietechnologie bij het Centrum voor Recht, Bestuur en Informatisering van de Universiteit van Tilburg, en advocaat te Amsterdam.

Megatrends in 2002 en 2003

Deze kroniek van het ICT-recht beslaat de periode van 2002 en 2003. In een ICT-samenleving is dat een bijna onvoorstelbaar lange periode, waarin enorm veel is gebeurd op ICT-rechtgebied. Dat valt niet allemaal in één kroniek te behandelen.[1] Wij kiezen er daarom voor de afgelopen periode te bespreken aan de hand van de onderliggende tendensen die ons het meest zijn opgevallen bij het overzien van de afgelopen twee jaar: de megatrends in het ICT-recht.[2] Wij signaleren de volgende brede, onderling samenhangende tendensen:

1. *afsluiting*: steeds meer lijken gegevens of informatie achter slot en grendel te worden gezet, slechts af en toe tegengehouden door een omgekeerde beweging: het geven van toegang tot informatie of gegevens;
2. *veiligheid*: de behoefte aan meer veiligheid is een brede maatschappelijke tendens, die resulteerde in een stroom van ICT-gerelateerde maatregelen om de (subjectieve ervaring van) veiligheid te vergroten;
3. *stroomlijning*: veel reguleringsinitiatieven van de afgelopen tijd stonden in het teken van het versoepelen van informatie- en communicatiestromen, zoals het faciliteren van e-handel, e-overheid en e-geldverkeer; ook bleek de telecommunicatiewetgeving onvoldoende toegerust op de Internetomgeving, reden voor stroomlijning van de regelgeving voor telecommunicatie, media en informatietechnologie;
4. *handhaving*: steeds meer nadruk lijkt te worden gelegd op de handhaving van wet- en regelgeving, en juist in een ICT-omgeving vraagt handhaving vaak om zelfstandige aandacht met eigen oplossingen, zoals gedragscodes en alternatieve geschillenbeslechting.

1. Afsluiting

1.1 Auteursrecht en IE

De discussie over de relatie tussen bescherming van IE-rechten en toegang tot informatie is ook in deze kroniekperiode weer volop aan de orde geweest. Het spanningsveld tussen 'afsluiting' van gegevens en open toegang lijkt door diverse ontwikkelingen te zijn verscherpt.
De Europese Auteursrechtrichtlijn (2001/29/EG) doet ook in het implementatietraject het nodige stof opwaaien. Onderwerpen als tijdelijke reproductierechten (*caching*), driestappentoets en bescherming van technologische beveiligingsmaatregelen vormen dan ook zware kost. Volgens sommigen is zelfs sprake van een fundamentele koerswijziging in het nationale auteursrecht. Het wetsvoorstel ('Auteursrecht en naburige rechten in de informatiemaatschappij') lag in januari 2004 nog bij de Tweede Kamer, terwijl de implementatietermijn al in december 2002 is

[1] Zie voor overzichten de besprekingen over Informaticarecht van Corien Prins en over Telecommunicatierecht van Nico van Eijk in de kwartaalkaternen van Ars Aequi, de elektronische nieuwsbrief van Leo van der Wees bij het losdelige handboek Recht & Informatietechnologie (Sdu), de nieuwsberichten in *Privacy & Informatie*, *Mediaforum* en *Computerrecht*, en – recentelijk – de blawg van SOLV (<http://www.solv.nl> onder 'Nieuws'). (Een blawg is een juridische blog, een Internetdag- en knipselboek.) Zie ook de essays in ITeR-deel 67, Den Haag: Sdu 2003. Wij wijzen ook op de elders in dit nummer opgenomen kronieken inzake intellectueel eigendom, vermogensrecht en strafrecht, en de voorgaande kronieken op de uiteenlopende rechtsgebieden.
Vanwege de opgelegde ruimtebeperking duiden wij in deze kroniek kamerstukken slechts aan met kamerstuknummer en volgnummer; de traditionele juridische verwijzing met I, II en jaartallen is door de zoekmogelijkheden op www.overheid.nl/op/ immers overbodig geworden. Eveneens vanwege de ruimtebeperking hebben we de verwijzingen naar verschillende bronnen grotendeeels samengebracht per alinea.
[2] De indeling in megatrends is geïnspireerd door Marc Groenhuijsens kroniek van het strafrecht in *NJB* 1996, p. 1527-1537.

verstreken. De Nederlandse bijdrage aan de beoogde Europese harmonisatie van het auteursrecht laat dan ook nog even op zich wachten.[3]
In de softwarewereld waren software-octrooien en 'open source' de voornaamste thema's in de strijd tussen afsluiting en toegang. 'Open source' is computerprogrammatuur waarvan de broncode openbaar is en– op grond van een gratis licentie – kan worden bewerkt. Dit zou flexibelere, stabielere en veiligere softwarepakketten moeten opleveren. In de politiek kreeg deze ontwikkeling bijval in de vorm van de door de Tweede Kamer breed aanvaarde motie-Vendrik c.s., waarin wordt gesteld dat in 2006 alle software in de publieke sector aan open standaarden moet voldoen. In reactie op de motie ontwikkelde de overheid het Programma voor Open Standaarden en Open Source Software voor de Overheid (OSOSS). Ook in Europa staat het onderwerp volop in de belangstelling.[4]
Op datzelfde Europese niveau laaide de strijd tussen de voor- en tegenstanders van ruimere octrooieringsmogelijkheden sterk op. Op grond van het Europees Octrooiverdrag (EOV) is geen octrooiering van computerprogramma's *als zodanig* mogelijk, en in de jurisprudentie is deze uitzondering ook steeds verder beperkt. De Verenigde Staten kennen een dergelijke beperking echter niet, hetgeen mede een reden kan zijn via een nieuwe richtlijn de Europese software-industrie een duwtje in de rug te geven. Het voorstel kreeg een 'warm' onthaal; voor- en tegenstanders rollen – nog steeds – over elkaar heen. Het verlenen van software-octrooien staat echter haaks op de gedachten van de 'open source- wereld'; de reacties op het richtlijnvoorstel vanuit die kring zijn dan ook sterk negatief. Nadat een hele reeks amendementen is aangenomen, wacht men nu op een gemeenschappelijk standpunt van Raad en Parlement.[5]

Jurisprudentie leverde diverse nieuwe inzichten over de omvang van IE-bescherming van gegevensverzamelingen. De zaterdagadvertenties uit de krant van Wegener werden als een databank beschouwd; samenvattingen daarop mochten niet worden opgenomen in een vacaturesite. Ook kregen dagbladuitgevers het gelijk aan hun zijde in de strijd tegen knipseldiensten. Een beroep op de Databankenwet werd afgewezen (krant is in onvoldoende mate een naslagwerk); het auteursrecht bracht echter toch uitkomst. Ook de on-line verzameling van gegevens van de NVM betreffende woningen en makelaars is aan te merken als een databank, ook al is het maken daarvan niet het primaire doel van de NVM. De mogelijkheden om de toegang tot programmagegevens af te sluiten lijken voor de NOS langzaam maar zeker uitgeput; de strijd duurt echter nog voort. In de kroniekperiode werd de strijd vooral via de band van het mededingingsrecht gevoerd.[6]
Minder onderworpen aan 'afsluiting' dan de Staat meende, bleken domeinnamen met een publieke klank (prinsjesdag.nl. miljoenennota.nl, troonrede.nl). De regel 'wie het eerst komt, het eerst maalt' leek na een uitspraak van de Haagse president (Scarabeo/ Zumpolle) aan terrein te verliezen; in hoger beroep werd deze regel echter in ere hersteld.[7]

1.2 Privacy en verstrekking van gegevens

Op het gebied van privacy zien we min of meer twee tegengestelde bewegingen: enerzijds de grijparmen van het persoonsgegevensbeschermingsregime om zoveel mogelijk gegevens te

[3] Richtlijn 2001/ 29/ EG van 22 mei 2001, *PbEG* L 167/ 10; Reactie op het Wetsvoorstel 28 482 tot uitvoering van de Richtlijn Auteursrechten en naburige rechten in de informatiemaatschappij (2001/ 29/ EG), Rapport van de Studiecommissie Informatiemaatschappij van de Vereniging voor Auteursrecht, 10 oktober 2002, <http:/ / www.ivir.nl/ vva/ publicaties/ rapport_studiecommissie_VvA_IM(10.10.2002).doc>; wetsvoorstel: kamerstuk 28482, H. Cohen Jehoram, 'Implementatie van de Auteursrechtrichtlijn', *NJB* 2002, p. 67-76.
[4] Kamerstuk 28600 XIII, nr. 30; <http:/ / www.ososs.nl/ index.jsp>; <http:/ / europa.eu.int/ information_society/ activities/ opensource/ index_en.htm>.
[5] Voorstel voor Richtlijn van het Europese Parlement en de Raad betreffende de octrooieerbarheid van in computers geïmplementeerde uitvindingen, COM (2002) 92def, 20 februari 2002; status: zie <http:/ / wwwdb.europarl.eu.int/ oeil/ oeil.fr111_en >.
[6] Hof Leeuwarden 27 november 2002, LJN-nr. AF1109 (Wegener c.s./ Hunter Select); Rb. Amsterdam 4 september 2002, LJN-nr. AE7317 ('dagbladen'/ 'knipseldiensten'); HR 22 maart 2002, LJN-nr. AD9138 (NVM/ Telegraaf)); HR 6 juni 2003, LJN-nr: AF5100 (NOS/ Telegraaf) en CBb 9 april 2003, LJN-nr. AF7441 (Telegraaf/ NMa).
[7] Hof Amsterdam 20 februari 2003 (De Staat/ De Kreek II), DomJur 2003-170; Hof Den Haag 31 januari 2002 (Zumpolle/ Scarabeo), DomJur 2002-129, <http:/ / www.domjur.nl>.

beschermen, en anderzijds de toenemende mogelijkheden tot verstrekking en opvraging van gegevens en daarmee deze bescherming in te perken.
De beweging van afsluiting van gegevens blijkt uit de brede reikwijdte van de richtlijn en de Wet bescherming persoonsgegevens: bijna alle gegevens zijn persoonsgegevens, zoals vaste IP-adressen. Het College Bescherming Persoonsgegevens (CBP) houdt strak de hand aan de meldingsplicht (die nu overigens ook elektronisch mag plaatsvinden): in december 2003 werden de eerste boetes uitgedeeld.[8]
Het prangendst komt het spanningsveld tussen afsluiting en verstrekking echter naar voren in de doorgifte van persoonsgegevens naar landen buiten de EU en de EER. Deze doorgifte is in principe verboden indien het derde land niet een passend beschermingsniveau biedt voor persoonsgegevens. Aangezien nog slechts Argentinië, Canada, Guernsey, Hongarije en Zwitserland als 'veilige exportgebieden' zijn aangewezen, alsmede de Amerikaanse bedrijven die aan de 'Safe Harbor Principles' voldoen, zal de bescherming contractueel moeten worden geregeld alvorens een verwerker persoonsgegevens buiten de EU/ EER kan exporteren. De Europese Commissie lanceerde daartoe modelcontractbepalingen. Tegelijk werd een opvallende uitzondering gemaakt onder druk van de veiligheidstendens: in maart 2003 werden luchtvaartmaatschappijen gedwongen vluchtpassagiersgegevens door te geven aan de VS-overheid; sindsdien wordt naarstig gewerkt aan een Europese oplossing via een Commissiebesluit en afspraken over gegevensbescherming.[9]
De formele benadering van de richtlijn en de Wbp om export te regelen staat op gespannen voet met de realiteit van de Internetwereld: met wat muisklikken zijn persoonsgegevens overal te verspreiden, zonder dat de verzender zich hoeft te realiseren waar zij terechtkomen. Ook het Lindqvist-arrest (HvJEG) gaf aan dat de richtlijn niet Internetbestendig is: er is geen rekening gehouden met het plaatsen van persoonsgegevens op het Internet, zodat dit niet als export van persoonsgegevens geldt. Daardoor ontstaat een opmerkelijke techniekafhankelijkheid: per netpost verzenden is exporteren, op een webstek plaatsen niet, terwijl de reikwijdte van het laatste veel groter kan zijn. Bij de evaluatie van de richtlijn (die zich nu vooral richt op de verschillende implementaties) zou dit punt zeker meegenomen moeten worden.[10] De regelgeving is meer in het algemeen evenmin toegerust op de moderne ICT-omgeving: de bijzondere privacyrichtlijn werd aangepast, na veel gesteggel over spam en cookies, en er rezen vragen rond bijvoorbeeld de whois-databanken met persoonsgegevens van domeinnaamhouders. Gelukkig publiceerde de OESO een rapport met handvatten voor de online toepassing van de algemene privacybeginselen, alsmede een rapport over online handhaving.[11]
Een ander prominent domein van het spanningsveld tussen afscherming en openbaarmaking was het cameratoezicht. Heimelijk cameratoezicht op openbare plaatsen werd verboden, maar het openlijke cameratoezicht nam explosief toe – een duidelijk effect van de veiligheidstendens. Of het cameratoezicht daadwerkelijk helpt, is niet duidelijk. Gerelateerd hieraan is het monitoren van werknemers, een van de heetste hangijzers in de afgelopen periode die resulteerde in veel rechtspraak, een raamregeling van het CBP en gedragscodes; de Europese Commissie heeft aangekondigd met een aparte 'werkplekrichtlijn' te willen komen.[12]

---

[8] IP-adres: <http:/ / www.cbpweb.nl/ documenten/ uit_z2000-0340.htm> ; e-melding: Stb. 2002, 244; Stcrt. 22 juli 2002, 137.
[9] Derde landen: <http:/ / europe.eu.int/ comm/ internal_market/ privacy/ adequacy_en.htm# countries> , <http:/ / www.export.gov/ safeharbor/ > , HvJEG 20 mei 2003, C-465/ 00 (*Rechnungshof v Österreichischer Rundfunk and Others*); modelbepalingen: <http:/ / europe.eu.int/ comm/ internal_market/ privacy/ modelcontracts_en.htm> ; vgl. het aanvullend protocol bij Verdrag 108 van de Raad van Europa, Trb. 2003, 122, over grensoverschrijdend gegevensverkeer; Passagiersgegevens: COM(2003) 826 final, <http:/ / europe.eu.int/ comm/ internal_market/ privacy/ docs/ adequacy/ apis-communication/ apis_en.pdf> .
[10] HvJEG 6 november 2003, C101/ 01, Lindqvist/ Zweden; evaluatie: Kamerstuk 28600 VI, nr. 6, <http:/ / europa.eu.int/ comm/ internal_market/ privacy/ lawreport/ data-directive_en.htm> .
[11] Richtlijn privacy en e-communicatie: 2002/ 58/ EG, kamerstukken 28962; whois: <http:/ / europe.eu.int/ comm/ internal_market/ privacy/ docs/ wpdocs/ 2003/ wp76_en.pdf> ; OESO: *Privacy Online: Policy and Practical Guidance*, <http:/ / www.olis.oecd.org/ olis/ 2002doc.nsf/ LinkTo/ dsti-iccp-reg(2002)3-final> , uitgewerkt in *Privacy Online: OECD Guidance on Policy and Practice* van november 2003, <http:/ / www.oecd.org/ document/ 49/ 0,2340,en_2649_33703_19216241_1_1_1_1,00.html> ; *Report on Compliance with, and Enforcement of, Privacy Protection Online*, <http:/ / www.olis.oecd.org/ olis/ 2002doc.nsf/ LinkTo/ dsti-iccp-reg(2002)5-final> .
[12] Camera's: Stb. 2003, 98, resp. *Cameratoezicht in de openbare ruimte*, rapport CBP, november 2003, <http:/ / www.cbpweb.nl/ documenten/ rap_2003_cameratoezicht_in_de_openbare_ruimte.htm> en zie algemeen <http:/ / www.cbpweb.nl/ themadossiers/ th_cam_index.htm> ; monitoren werknemers: voor een overzicht van rechtspraak, zie

De vraag wanneer persoonsgegevens aan derden mogen worden verstrekt, kwam vaak aan de orde. Vooral in de justitiële sfeer was dit een belangrijke vraag, waarbij de veiligheidsdrang sterk de overhand had boven afschermingsbelangen. Dit bleek prominent uit het kabinetsstandpunt over strafvorderlijke gegevensvergaring (n.a.v. de Commissie-Mevis), uitmondend in een door de ministerraad goedgekeurd wetsvoorstel dat (volgens velen té) ruime mogelijkheden geeft om in het kader van opsporing gegevens bij burgers en bedrijven op te vragen. Het parlement had geen moeite met de daarop vooruitlopende wetsvoorstellen over financiële gegevens en telecom-verkeersgegevens; slechts de Eerste Kamer uitte enkele bedenkingen bij het laatste voorstel, dat justitie de mogelijkheid geeft om enorme aantallen verkeersgegevens en abonneegegevens op te vragen. Ook vrijwillig worden echter al NAW-gegevens verstrekt: saillant was de vrijwillige verstrekking van gegevens door een Amerikaanse *anonymizer* aan de Nederlandse politie om de toetjesterrorist op te sporen. Die zaak was ook interessant omdat het de eerste ons bekende praktijkzaak betreft van steganografie, de ultieme vorm van 'afsluiting' waarbij informatie wordt verborgen in bijvoorbeeld een digitaal plaatje.[13] Tot slot was over de gegevensuitwisseling tussen politie en inlichtingen- en veiligheidsdiensten veel te doen, waarbij 'wordt bezien of het juridisch en technisch mogelijk is om de informatieverstrekking langs geautomatiseerde weg te faciliteren'. Ook noopten vrijspraken van de Rechtbank Rotterdam in juni 2003 tot voorstellen AIVD-informatie in strafzaken als bewijs toe te laten; de minister moet nu wetgeving ontwikkelen over de toelaatbaarheid en wijze van gebruik. De verruiming van AIVD-bevoegdheden en het beperkte openbare toezicht daarop (zie 2.1) nopen volgens ons tot terughoudendheid in dezen.[14] De zaken rond verstrekking tussen burgers onderling neigden echter meer naar afscherming. Zo hoefde Teleatlas geen abonneegegevens te verstrekken van een abonnee die illegaal gekopieerde cd's aanbood, en gaf de Amerikaanse rechter uiteindelijk aan dat Verizon geen gegevens van Kazaa-abonnees hoeft te verstrekken aan de muziekorganisatie RIAA. Afsluiting is echter geen uitgemaakte zaak: de onmogelijkheid om tegen een anonieme lasteraar te procederen kan ook nopen tot verstrekking van NAW-gegevens door de aanbieder, aldus de Haarlems voorzieningenrechter.[15]

1.3 Overheidsinformatie en grondrechten

De publicatie van juridische overheidsinformatie via Internet is goed op dreef: de ontsluiting van volledige en actuele wetsteksten en de kamerstukken op overheid.nl en van steeds meer rechtspraak op rechtspraak.nl vormen een fantastische bron voor rechtswetenschap en -praktijk. Actieve openbaarmaking krijgt aandacht door het actieprogramma Overheidscommunicatie. Maar niet alle overheidsinformatie is gratis: de kaders voor verkopen van publieke informatie krijgen langzaam vorm via onder andere een richtlijn voor hergebruik van overheidsinformatie; ook al is daarbij 'commerciële exploitatie' uit de eerdere titel verdwenen, er mag wel een 'redelijk rendement op investeringen' worden gerekend bovenop de kostprijs. Ook andere belangen kunnen openbaarmaking van overheidsinformatie tegenhouden, zoals privacy; de Europese Ombudsman waarschuwde dat hierdoor de openbaarheid van overheidsinformatie in gedrang komt.[16]
En helaas bleef het oorverdovend stil rond het voorgestelde grondrecht op openbaarheid van overheidsinformatie – net zoals rond de andere grondrechten in het digitale tijdperk: na de

<http:/ / www.p-plus.nl/ beelden/ rechters.pdf>, P. De Hert, 'Internetrechten in het bedrijf', *Auteur & Media* 2001 (1), p. 1-16; CBP: <http:/ / www.cbpweb.nl/ downloads_overig/ Raamregeling.PDF>, <http:/ / www.cbpweb.nl/ documenten/ av_21_Goed_werken_in_netwerken.htm>; CNV: <http:/ / www.cnv.nl/ Nieuws/ internet.doc>.

[13]

[14] Gegevensvergaring: zie <http:/ / www.gegeven.nl> voor de relevante stukken en meningen over strafvorderlijke gegevensvergaring; financiële gegevens: kamerstukken 28353; verkeersgegevens: kamerstukken 28059, zie nr. 187a voor kritiek; toetjesterrorist: <http:/ / www.netkwesties.nl/ editie67/ artikel1.php>; uitwisseling politie-ivd, zie rapport Algemene Rekenkamer 10 april 2003 en kabinetsreactie: kamerstuk 28845, nrs. 1-2; AIVD-informatie in strafzaken: kamerstuk 28463, nr. 25, *Handelingen II* 2003, 34-2390.

[15] Rb. Utrecht 9 juli 2002, LJN-nr AE5537; U.S. Court of Appeals, D.C. Circuit, 19 december 2003, No. 03-7015 (*RIAA* vs. *Verizon*), <http:/ / pacer.cadc.uscourts.gov/ docs/ common/ opinions/ 200312/ 03-7015a.pdf>; Vzr.Rb. Haarlem 11 september 2003 (Pessers/ Lycos), *Computerrecht* 2003-6, p.363-367 m.nt. Ekker.

[16] Kamerstuk 26387, nr. 15, zie ook ITeR-deel 59; voorstel: COM (2002) 207 def; richtlijn 2003/ 98/ EG van 17 november 2003, *PbEG* L 345/ 90; <http:/ / www.euro-ombudsman.eu.int/ letters/ en/ 20020925-1.htm>. Zie ook COM(2004) 45def voor een evaluatie van de transparantieverordening 1049/ 2001.

indiening in augustus 2001 van vier wetsvoorstellen bij de Raad van State, werd niets meer vernomen van de digitale grondrechten. Als troost kwam de Raad van Europa met een *Declaration on freedom of communication on the Internet* en publiceerde het kabinet een notitie over pluriformiteit, kwaliteit en toegankelijkheid van inhoud op digitale netwerken.[17]

1.4 Spam

Vrij unaniem is de gedachte dat spam eerder lastpost dan reclamepost is en dat afsluiting daarvan juist wel moet worden nagestreefd. Hoe pak je dat echter aan? In de afgelopen twee jaar werden er verschillende strategieën ontwikkeld ('opt-in', 'opt-out', filteren, ingebouwde vertraging bij versturen), maar het probleem lijkt vooralsnog alleen maar groter te worden. XS4ALL probeerde de overlast door de rechter aan banden te laten leggen. Tot nu toe zonder blijvend succes, maar als de Hoge Raad de conclusie van advocaat-generaal Huydecoper volgt, gloort er hoop.[18]
In VS is met ingang van dit jaar de Can-Spam Act van kracht. Anders dan de naam wellicht doet vermoeden, betreft het geen uitnodiging om te spammen maar een poging tot inblikken ('can') daarvan. Spam mag wel worden verzonden, mits er een afmeldingsmogelijkheid wordt geboden ('opt-out'). In Europa wordt via een slingerpad van 'opt-out' (Richtlijn elektronische handel) naar 'soft opt-in' (Richtlijn e-privacy) toegewerkt; de Commissie zet daarnaast in op zelfregulering en bewustwording. Ook in Nederland leidde de spamregulering tot hevige debatten, onder meer over de sanctionering. Voor wat dit laatste betreft won Minister Donner het pleit; er komt alleen een bestuursrechtelijke boete op overtreding. Onder meer in China, een van de grootste spam-exporteurs, zullen ondernemers daar waarschijnlijk niet erg van onder de indruk raken. Een elektronische brievenbus blijft dan ook de komende jaren zeker nog een onrustig bezit. De mobiele telefoon(rekening) wordt hopelijk minder geplaagd, nu er een sms-gedragscode is.[19]

2. Veiligheid

2.1 Terrorismebestrijding

De afgelopen jaren stonden in het teken van post-11-september veiligheidsmaatregelen. Voor het ICT-recht was de belangrijkste gebeurtenis de inwerkingtreding van de Wet op de inlichtingen- en veiligheidsdiensten 2002, met ruime ICT-bevoegdheden als hacken, scannen en een met maar liefst twee jaar gevangenisstraf gesanctioneerde ontsleutelplicht. Over grootschalig afluisteren verscheen een notitie, maar de enkele jaren geleden in Europa aangezwengelde discussie lijkt inmiddels doodgebloed: het afluisternetwerk Echelon lijkt na 11 september 2001 definitief geaccepteerd.[20] Of en hoe de ruime mogelijkheden in de praktijk worden toegepast, zal wellicht bekend worden nu de Commissie van Toezicht sinds medio 2003 actief is, maar in de Wiv 2002 prevaleert de afsluiting van informatie boven de controle: het toezichtsjaarverslag is slechts gedeeltelijk openbaar, en het openbare jaarverslag van de ministers bevat geen zicht op in concreto aangewende middelen (art. 8 lid 3, 79 Wiv 2002).

2.2 Computercriminaliteit

De grote belangstelling voor het Cybercrime-Verdrag van de Raad van Europa, in november 2001 ondertekend door maar liefst 30 landen, had ongetwijfeld ook te maken met het wereldbeeld na 11 september 2001. Het verdrag is inmiddels door vier landen geratificeerd; nog één ratificatie, en dan treedt het in werking. Bij het verdrag verscheen een aanvullend protocol over racisme en xenofobie op netwerken, een onderwerp dat door het Amerikaanse Eerste

[17] <http:/ / www.coe.int/ T/ E/ Communication_and_Research/ Press/ News/ 2003/ 20030528_declaration.asp> of <http:/ / www.legi-internet.ro/ lib_com.htm>; kamerstuk 26643, nr. 37.
[18] Hof Amsterdam 18 juli 2002, LJN-nr. AE5514.; tekst conclusie< http:/ / www.xs4all.nl/ nieuws/ overzicht/ spamabfab.pdf>; ten tijde van het afsluiten van deze tekst werd verwacht dat de Hoge Raad uitspraak doet op 13 februari 2004.
[19] E-handel: richtlijn 2000/ 31/ EG; kamerstukken 28197; E-privacy: richtlijn 2002/ 58/ EG; kamerstukken 28962; handhaving: zie ook kamervragen 26 januari 2004, Aanhangsel nr. 693; Commissie: Communication COM (2004) 28final van 22 januari 2004; zie over opt-in ook E. Thole, *NJB* 2004, p. xxx; sms-gedragscode: <http:/ / www.opta.nl/ index.asp?url=/ nieuwsenpublicaties/ document.asp&id=1085>.
[20] Wiv 2002: Stb. 2002, 148, inwerkingtreding 29 mei 2002, Stb. 2002, 196; zie ook Stb. 2003, 22, 37 en 212; Echelon: kamerstuk 27591, nr. 4.

Formatted

Amendement niet in het verdrag zelf kon worden behandeld. Als uitvloeisel van het verdrag werd virtuele kinderporno in Nederland strafbaar gesteld, en *en passant* werd vanwege het verdrag ook de leeftijdsgrens van fysieke kinderporno opgetrokken naar 18 jaar. Nu vallen wellicht dus ook ranzige tv-programma's van 17-jarige strandgangers onder de strafbaarstelling. Verder zal de Nederlandse wet nog op enkele punten moeten worden aangepast; vooral de strafbaarstelling van misbruik van hulpmiddelen gaat ver en vraagt om bezinning.[21]
De implementatie zal worden gecombineerd met het wetsvoorstel Computercriminaliteit II. In alle Donneriaanse dadendrang is dat voorstel compleet verstoft: nog steeds wacht het kamercommissieverslag uit september 2000 (!) op antwoord. Gelukkig werd wel prioriteit gegeven aan de praktische kant: met het Stappenplan aangifte computercriminaliteit en de Handleiding Cyber Crime hebben burgers en vooral bedrijven handvatten gekregen om aangifte te doen van computercriminaliteit en om sporen veilig te stellen. Niet specifiek voor computercriminaliteit maar wel relevant in dit licht is ook het EU-instrument Cyber Tools On-Line for Evidence. Zelfs werd in november 2003 elektronische aangifte mogelijk gemaakt, vooralsnog alleen bij eenvoudige delicten; de e-aangifte moet echter merkwaardigerwijs plaatsvinden via het plaatselijke politiebureau en is nog in lang niet alle plaatsen mogelijk.[22]

Verder werd ook via de Europese Unie gewerkt aan aanscherping van strafbaarstellingen. Fraude met elektronische betaalmiddelen wordt harder aangepakt, onder andere via voorbereidingshandelingen, en hacken om economisch voordeel te behalen moet strafbaar worden gesteld, ook als daarbij geen beveiliging wordt doorbroken; volgens de wetgever is voor dat laatste (wellicht onterecht) wetsaanpassing niet nodig. Verstikkingsaanvallen (*denial-of-service attacks*) moeten strafbaar worden gesteld (ook volgens het Cybercrime-verdrag), en de EU blijft actief op het terrein van schadelijke en illegale inhoud: het Safer Internet Action Plan werd verlengd.[23]
De toepassing van bestaande strafbepalingen leverde interessante uitspraken op. Zo blijkt het verwijderen uit een mobiele telefoon van een sim-lock (dat het overstappen naar een andere telecom-aanbieder bemoeilijkt) niet strafbaar, maar het ombouwen van een Sony-spelcomputer wel (art. 32a Aw). Strafbare telecomfraudevoorbereidingshandelingen (art. 326c lid 2) bleken het uit winstbejag bewaren van apparatuur om telefoonkaarten op te waarderen en het publiceren van een (papieren!) artikel met een stappenplan voor telecomfraude – dat laatste gaat annotator Kaspersen te ver. Fraudebepalingen zijn moeiteloos toepasbaar op Internetverkeer: geruchtspreiding (ook vruchteloos) op een WWW-discussieforum is koersmanipulatie (art. 334 Sr), en Nigeriaanse e-bedelbrieven worden hard afgestraft als oplichting.[24]

2.3 Opsporing

Bij de ICT-opsporing stond vooral het tappen in de belangstelling. Het is kennelijk niet te achterhalen bij de overheid hoeveel dit essentiële middel wordt gebruikt: een Wob-verzoek tot openbaarmaking van tapcijfers werd afgewezen, en de minister achtte het niet zinvol dit bij te gaan houden. Dat zal in de toekomst wellicht veranderen nu gewerkt wordt aan een Landelijk Interceptie Orgaan (LIO) dat de tap moet gaan coördineren in centrale tapkamers. Het tappen

[21] Tekst, toelichting en ratificaties: <http:/ / conventions.coe.int/ Treaty/ EN/ WhatYouWant.asp?NT=185>; zie over het verdrag en de implementatie in Nederland het dossier in *Computerrecht* 2003/ 2. Protocol: Trb. 2003, 60; virtuelekinderpornowet: Stb. 2002, 388; misbruik van hulpmiddelen, zie Koops & Prins, 'De toenemende strafbaarstelling van technische hulpmiddelen: over intenties, bestemmingen en instrumentele wetgeving', in: Groenhuijsen & Simmelink (red.), *Glijdende Schalen*, Nijmegen: Wolf Legal Publishers, 2003, p. 341-386.
[22] CCII: Kamerstuk 26671, nr. 6; <http:/ / www.kwint.org/ result_files/ Stappenplan_Aangifte_Computercriminaliteit.pdf>; <http:/ / www.bof.nl/ docs/ HandleidingCyberCrime_ned.pdf>.; CTOSE: IP/ 03/ 1443, 24/ 10/ 2003, <http:/ / europa.eu.int/ rapid/ start/ cgi/ guesten.ksh?p_action.gettxt=gt&doc=IP/ 03/ 1443| 0| RAPID&lg=NL>; e-aangifte: <http:/ / www.politie.nl/ Overige/ Aangifte/ > en <http:/ / burger.overheid.nl/ nieuws/ ?id=569>.
[23] Betaalkaarten: besluit 28 mei 2001, PbEG L149; Kamerstuk 29025, nrs. 1-3; economischvoordeelhacken: kaderbesluit bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten, *PbEG* 2001, L 149, kamerstuk *II*, 29025, B; verstikkingsaanvallen: COM2002/ 173def, *PbEG* C203E/ 109, 27 augustus 2002; Safer Internet: Besluit 1151/ 2003/ EG van 16 juni 2003, <http:/ / europa.eu.int/ information_society/ programmes/ iap/ index_en.htm>, <http:/ / www.saferinternet.org/ >.
[24] Sim-lock: Rb. Maastricht 12 maart 2002, LJN-nr. AE0125; Sony-spelcomputers: Rb. Breda 24 april 2002, LJN-nr AE1864; telefoonkaarten: HR 15 april 2003, LJN-nr. AF3372; stappenplan: Rb. Haarlem (politierechter) 16 januari 2003, *Computerrecht* 2003/ 2 m.nt. Kaspersen; koermanipulatie: Rb. Amsterdam 3 juli 2003, LJN-nr. AH9509; e-Nigeria: Rb. Amsterdam 28 mei 2003, LJN-nummers AF9286, AF9292, AF9294-296.

van Internet kwam enigszins op gang nu de aftapbaarheidsplicht voor Internetaanbieders na jarenlange ontheffing en gedogen van kracht werd; hiertoe werd onder andere een Nationale Beheersorganisatie Internet Providers opgericht om een mobiel tapkastje bij (vooral kleinere) aanbieders te installeren. Het blijft echter de vraag of de aftapregeling Internetbestendig is; zo rijzen vragen over de afgrenzing van inhoud en verkeersgegevens en over het opvragen van locatiegegevens, en is het onduidelijk of ook locale WiFi-netten (draadloze communicatie) onder de tapplicht van de Telecomwet vallen.[25]
De tappraktijk bleek overigens verre van vlekkeloos: geheimhoudersgesprekken werden in strijd met de wet structureel vastgelegd, hetgeen leidde tot de nodige discussie en aanbevelingen. Ook gaf een (beperkt) onderzoek aan dat tapkamers kwetsbaar zijn bij gebrek aan (naleving van) goede interne procedures; de minister kondigde daarop maatregelen aan naleving van de Normstelling Inrichting Interceptiefaciliteiten te waarborgen. Ook werden beveiligingsverplichtingen gepubliceerd voor telecom-aanbieders om tapgegevens te beveiligen. Commotie veroorzaakte ook de Baybasin-zaak, waarin taps beweerdelijk waren gemanipuleerd; hof en Hoge Raad schoven de bezwaren van de verdediging als onrealistisch terzijde.[26]
De veiligheidsdrang kwam niet alleen tot uiting in de voorstellen voor gegevensvergaring (zie par. 1.2), maar ook in de discussie over een verplichte bewaarplicht voor verkeersgegevens. Een ontwerp-kaderbesluit lekte uit dat lidstaten zou verplichten om telecommunicatie-verkeersgegevens gedurende 1 tot 2 jaar te laten opslaan. In Nederland waren vooral tegengeluiden te horen, en gelukkig is het de laatste tijd wat stiller rond dit paardenmiddel. Ook lijkt de overheid in te zien dat maatregelen om cryptografie aan banden te leggen via Trusted Third Parties niet werken: de uitkomst van het project Rechtmatige Toegang was dat de overheid – thans – afziet van een regeling.[27]

2.4 Beveiliging

De discussie over veiligheid leek vaak meer in de richting te wijzen van verruiming van bevoegdheden en meer repressie dan in de richting van preventie. Ondanks de wat passieve houding van de overheid in de nota KWINT, is er toch wel iets gebeurd om de kwetsbaarheid van netwerken tegen te gaan. Zo verscheen een nota over bescherming van vitale infrastructuren en werd de actielijn van een Nationaal Continuïteitsplan Telecommunicatie (NACOTEL) ontwikkeld.[28] Belangrijker was de oprichting van een Computer Emergency Response Team voor de overheid, GOVCERT.nl, die een waarschuwingsdienst lanceerde om abonnees via netpost of sms in te lichten over actuele bedreigingen als virussen en de nieuwste zwakke plekken in Microsoftware. Ook op Europees niveau werd de oprichting voorgesteld van een agentschap voor informatieveiligheid, het European Network and Information Security Agency.[29]

[25] Cijfers: Rb. Amsterdam 19 februari 2003, AWB 01/ 1813 WOB; Aanhangsel handelingen 2002/ 03, nrs. 1035 en 1553 en 2003/ 04, nr. 219; Internet-tap: <http:/ / www.nbip.nl/ >; verkeersgegevens: L. Asscher & A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam: Otto Cramwinckel 2003; I.M. Koopmans & A.H.H. Smits, 'Mobiele telefonie en plaatsbepaling: het afluisteren voorbij?' *NJB* 2002, p. 1888-1895; WiFi: <http:/ / www.netkwesties.nl/ editie68/ artikel5.php>.
[26] Geheimhouders: zie bijvoorbeeld <http:/ / www.minbzk.nl/ contents/ pages/ 00020071/ brieftkkwetsbaarheidsanalysedef.pdf> en <http:/ / www.cbpweb.nl/ documenten/ div_hz_geintercepteerde%20gesprekken.htm>; kwetsbaarheid: <http:/ / www.minbzk.nl/ contents/ pages/ 00020071/ brieftkkwetsbaarheidsanalysedef.pdf>; Kamerstuk 29 200 VII, nr. 39; Stb. 2003, 472; tapmanipulatie: Hof Den Bosch 30 juli 2002, LJN-nr. AE5920; HR 21 oktober 2003, LJN-nr. AH9922.
[27] Bewaarplicht: *Draft Framework Decision on the retention of traffic data and on access tot this data in connection with criminal investigations and prosecutions*, <http:/ / www.statewatch.org/ news/ 2002/ aug/ 05datafd.htm>, A. Patijn, 'Verplichte opslag van verkeersgegevens?', *Computerrecht* 2003/ 2, p. 134-8; TTP's: kamerstuk 26581, nr. 2.
[28] KWINT: kamerstuk 26643, nr. 30; vitale infrastructuren: kamerstuk 26643 nr. 43; <http:/ / www.ez.nl/ beleid/ home_ond/ dgtp/ veiligheid/ nacotel.html>. Vgl. kamerstukken 28684, 'Naar een veiliger samenleving'. Zie ook de OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, <http:/ / www.oecd.org/ dataoecd/ 16/ 22/ 15582260.pdf>.
[29] Govcert: <http:/ / www.govcert.nl/ >; <http:/ / www.waarschuwingsdienst.nl/ >; ENISA: COM(2003) 63final.

3. Stroomlijning

3.1 Elektronische handel

Op tal van terreinen vormt formele regelgeving nog een belemmering voor het op ruimere schaal toepassen van elektronische handel. Het kan daarbij gaan om het ontbreken van rechtszekerheid, maar ook om dwingende vormvoorschriften die aan gebruik van zuiver elektronische communicatie in de weg staan. De weg voor elektronische communicatie dient derhalve (beter) te worden geplaveid. De stortvloed aan Europese initiatieven voor deze stroomlijning kan op nationaal niveau maar moeizaam worden verwerkt. Voor de praktijk ligt er de uitdaging om gehanteerde ICT-contracten ook Internetbestendig te maken.[30]

De 'Aanpassingswet richtlijn inzake elektronische handel' heeft inmiddels de Eerste Kamer bereikt. Het wetsontwerp bevat onder meer eisen voor aanbieders van 'diensten van de informatiemaatschappij' en regels inzake elektronische reclame-uitingen, aansprakelijkheid van aanbieders en elektronisch contracteren. De uiterste implementatiedatum, 17 januari 2002, is nu al ruim twee jaar overschreden. Niet veel beter verging het de Nederlandse wetgever met de implementatie van de Europese richtlijn inzake een gemeenschappelijk kader voor elektronische handtekeningen. Sinds 21 mei 2003, bijna twee jaar na de implementatietermijn, is de Wet elektronische handtekeningen van kracht. Of dit een nuttig bezit vormt wordt betwijfeld. De Minister heeft wel al aangegeven aan welke eisen naar zijn oordeel een 'elektronische akte' moet voldoen.[31] Een wettelijke regeling voor 'elektronisch papier' ontbreekt echter nog – als het erop aan komt blijft de digitale inkt voorlopig nog voor eigen risico.
De elektronische weg is ook na deze stroomlijning nog lang. Een aantal verdere stappen is in voorbereiding, onder meer voor financiële diensten (zie 3.3) en voor communicatie door en met de overheid (zie 3.2). Met deze initiatieven is het wetgevend karwei nog (lang) niet af. Onder meer voor wat betreft civielrechtelijke vormvoorschriften ligt er nog een uitdaging voor de wetgever.[32]

Zo langzaam maar zeker zien we ook in de rechtspraak met betrekking het Internet het hele scala aan menselijke zwakten langskomen. Naast seks (pornosurfen op het werk, zie 1.2) was er in deze kroniekperiode ook voor het gokken een prominente rol weggelegd. Stroomlijning op Europees niveau werd bevorderd door Gambelli, een handlanger van een in Italië opererende Engelse wedmakelaar. Hij waagde ook een gokje bij het Hof van Justitie en maakte naam. De door de Italiaanse wetgever opgelegde beperkingen (exclusieve positie voor de Staat) zijn strijdig met onder meer de vrijheid van dienstverlening (art. 49 EG-Verdrag). Volgens het Hof Arnhem (Ladbrokes/ Lotto) is de Wet op de kansspelen wel in overeenstemming met artikel 49 EG-Verdrag en is het derhalve niet toegestaan om zonder vergunning Nederlandse ingezetenen te laten deelnemen aan lotto's en gokken op sportwedstrijden via Internet. De Antillen vormen voor Internetcasino's geen vrijhaven.[33]

Conflicten op het terrein van de elektronische handel kennen in veel gevallen een ipr-aspect. In de eerder aangehaalde Ladbrokes-zaak had de Arnhemse voorzieningenrechter geen behoefte aan verdere stroomlijning van de regelgeving. Voor zowel het beantwoorden van de bevoegdheidsvraag als voor de vaststelling van het toepasselijk recht bleken de relevante regels (de nieuwe EEX-Verordening respectievelijk de Wet Conflictenrecht Onrechtmatige Daad)

[30] J.M.A. Berkvens & A.H.J. Kuus, 'FENIT-voorwaarden 6: the next generation', *Computerrecht* 2003/ 6, p. 346-349; C.E. Drion, C. Stuurman & W. Wefers Bettink (red.), *Internet en e-commerce*, Boom, 2003 (modelcontracten).
[31] E-handel: kamerstuk 28197; richtlijn 2000/ 31/ EG, PbEG L 178 van 17 juli 2000; zie voor de invloed op het contractenrecht : C.E. Drion en T.H.M. van Wechem, 'Kroniek van het vermogensrecht', *NJB* 2002, p. 437-451; e-handtekeningen: richtlijn 1999/ 93/ EG, *PbEG* L 13 van 19 januari 2000, kritisch: R.E. van Esch, 'De betrekkelijke waarde van de Wet elektronische handtekeningen voor de elektronische handel', *Computerrecht* 2003/ 6, p. 337-345; e-akte: kamerstuk 27743, nr. 35b.
[32] Zie essay R. van Esch in ITeR-deel 67 (Sdu 2003).
[33] HvJEG 6 november 2003, zaak C 243/ 01 (Gambelli/ Italië); Hof Arnhem 2 september 2003, LJN-nr. AJ9996 (Ladbrokes); Rb. Utrecht 27 februari 2003, LJN-nr. AF5121 (Antillen); zie ook ITeR-deel 53.

voldoende houvast te bieden. Op Europees niveau wordt nog beraadslaagd over aanpassing van het Verdrag van Rome. De gevolgen van de specifieke conflictenregels voor consumentencontracten bijvoorbeeld zijn in de Internet-omgeving op dit moment onvoldoende duidelijk.[34]

Internetaanbieders opereren in de voorhoede van de informatiemaatschappij. Die koppositie levert ook veel juridische zorgen op, claims vormen daarvan niet de minste. In hoger beroep verloor de Scientology-kerk opnieuw. Het Hof Den Haag stelde daarbij onder meer vast dat aanbieders slechts technische faciliteiten verschaffen om openbaarmaking door anderen mogelijk te maken; zij maken daardoor niet zelf werken openbaar. Interessant waren ook de afwegingen tussen auteursrecht en informatievrijheid; het algemeen belang bij informatievrijheid van artikel 10 lid 1 EVRM weegt in casu niet minder zwaar dan het belang van handhaving van het auteursrecht.[35] Scientology is inmiddels in cassatie gegaan.
Al ver voor de huidige kroniekperiode (1999) zette de Haagse rechtbank de toon: aanbieders handelen onrechtmatig als inbreukmakende informatie op hun systemen blijft staan op het moment dat zij op de hoogte raken van het onrechtmatige karakter van deze informatie en aan de juistheid van de desbetreffende kennisgeving in redelijkheid niet valt te twijfelen. In de Richtlijn elektronische handel wordt eenzelfde lijn gekozen. Wanneer de onrechtmatigheid onmiskenbaar is dient een provider na een melding te hebben ontvangen direct over te gaan tot het verwijderen van de informatie. Het beroep van XS4ALL tegen Deutsche Bahn op onder meer verplichtingen jegens haar abonnees uit hoofde van haar algemene voorwaarden en de Wet bescherming persoonsgegevens, mocht niet baten.[36]

3.2 Elektronische overheid

De elektronische overheid stond voor het grootste deel in het teken van het stroomlijnen van gegevensstromen, zowel binnen de overheid zelf als in de contacten met burgers en bedrijven. Een belangrijk deel vond plaats onder de paraplu van het in 2001 opgerichte ICTU, de stichting voor coördinatie van e-overheid. De eindrapportage van het Actieprogramma Elektronische Overheid liet zien dat weliswaar het nodige is bereikt, maar dat slechts een begin is gemaakt met daadwerkelijke integratie van ICT in de overheidcommunicatie- en informatiehuishouding. Met name de rijksoverheid loopt tegen barrières aan, niet alleen technische, maar vooral ook bestuurlijke, organisatorische en financiële. Dat blijkt ook uit de ontwikkeling PKIoverheid, een infrastructuur voor betrouwbare communicatie binnen de overheid, die veel trager liep dan gepland.[37] Het programma Stroomlijning Basisgegevens ('de overheid vraagt niet naar de bekende weg', maar gebruikt de gegevens die zij heeft) werd eveneens afgerond, merkwaardigerwijs voordat het goed en wel op gang kwam. Volgens de eindrapportage is de 'gecoördineerde impuls' geslaagd en is het nu verder aan de ministeries om authentieke registraties (AR) verder te ontwikkelen. De GBA is nog allerminst een AR, maar wel werd een stap gezet met de ontwikkeling van een Landelijk Raadpleegbare Deelverzameling (LRD), waarmee GBA-gegevens on-line kunnen worden opgevraagd. Ook de ontwikkeling van een beleidskader voor persoonsnummers kreeg vorm; het Burgerservicenummer (BSN) zal uitgroeien tot een super-sofinummer, mede ingegeven door 'de wens naar betere mogelijkheden voor gegevenskoppeling ten behoeve van de rechtshandhaving en opsporing'. De veiligheidsdrang om één gekoppelde identificatiestructuur op te richten kan naar wij vrezen echter ook averechts uitpakken vanwege de privacy- en beveiligingsrisico's die het oproept.[38]

---

[34] Verordening EG/ 44/ 2001 van 22 december 2000, *PbEG* L 12 van 16 januari 2001, in werking getreden op 1 maart 2002 (Brussel II); Stb. 2001, 190; Green paper on the conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernisation, COM (2002) 654final.
[35] Hof Den Haag, 4 september 2003, LJN-nummer AI5638.
[36] Voorzieningenrechter Amsterdam 25 april 2002, LJN-nr. AE1935 en Hof Amsterdam 7 november 2002, LJN-nr. AF0091.
[37] <http:/ / www.ictu.nl> ; eindrapportage: kamerstuk 26387, nr. 19; PKI: <http:/ / www.pkioverheid.nl>, <http:/ / www.elektronischehandtekening.overheid.nl> en kamerstuk 28600 VII, nr. 7. De PKI had in 2002 volledig ingevoerd moeten zijn (kamerstuk 26387, nr. 5) maar staat eind 2003 slechts in de steigers.
[38] Stroomlijning basisgegevens: kamerstuk 29200/ VII, nr. 2, p. 19; GBA: vgl. LJN-nr. AF7409: GBA-gegevens moeten ook worden verstrekt aan derden die geen beroepsgroepgedragscode kennen; identificatie: kamerstuk 28600/ VII, nr. 21; over de risico's, zie B.J.

Geslaagder is het initiatief van het platform burger@overheid, dat op 3 april 2002 werd gelanceerd. De webstek biedt informatie maar ook volop reactiemogelijkheden, en bijvoorbeeld een meldpunt voor klachten over trage netpostafhandeling of onvindbare overheidsinfo. Het platform is zelf ook actief om de afsluiting van overheidsinformatie, zoals het Srebrenica-rapport, tegen te gaan. Ook positief is het wetsvoorstel elektronisch bestuurlijk verkeer, dat eind 2003 bij de Eerste Kamer lag; dit maakt elektronisch verkeer mogelijk tussen burgers en bestuursorganen, mits de partij heeft aangegeven elektronisch te willen of kunnen communiceren en aan de voorwaarden van de nieuwe afdeling 2:3 Awb wordt voldaan. Opmerkelijk is dat het schriftelijkheidsvereiste in veel bestuurswetten volgens de wetgever mag worden uitgelegd als mede omvattend de elektronische vorm (indien dit een functioneel equivalent is), waardoor 'ex post de wil van al die historische wetgevers op dit punt nader wordt geconcretiseerd'.[39]
Overigens blijkt wel dat de e-overheid bij de stroomlijning meer aandacht mag besteden aan veiligheid: zo bevat 80% van de gemeentelijke websites veiligheidsrisico's, waardoor in sommige gevallen zelfs gevoelige informatie naar buiten kan komen; ook de plannen om in 2004 Nederlanders in het buitenland via Internet te laten stemmen lijken onvoldoende oog te hebben voor veiligheid.[40]

3.3 Geldzaken

Zoals altijd stond geld weer in het middelpunt van de belangstelling. Nu dat geld steeds vaker elektronisch vorm krijgt, is het zaak de geldverkeerregelingen te stroomlijnen. Op 1 juli 2002 trad de Wet elektronisch geld in werking, waardoor instellingen die e-geld uitgeven nu ook onder de Wet toezicht kredietwezen vallen. Voor financiële diensten is voorts regelgeving in de maak ter bescherming van consumenten bij financiële dienstverlening op afstand.[41]
De opkomst van de elektronische handel heeft belangrijke gevolgen voor de fiscale regelgeving. Kernbegrippen op dat terrein zijn in hoofdzaak nog gekoppeld aan de meer traditionele modellen voor zakendoen en dito aanknopingspunten voor fiscale heffing. Via de Europese BTW-richtlijn wordt getracht het concurrentienadeel weg te nemen dat voor EU-leveranciers (wel BTW-plichtig) bestond ten opzichte van hun concurrenten van buiten de Unie (niet BTW-plichtig). De wetgeving is inmiddels ook hier aangepast – en heeft als voordeel dat de fiscus extra inkomsten tegemoet kan zien.[42]
Ook stroomlijning van de eisen die aan facturen worden gesteld bleek noodzakelijk. Het wetsvoorstel ter implementatie van de Europese richtlijn facturering ligt bij de Eerste Kamer. In het voorstel wordt op bepaalde punten aangesloten bij de regelgeving inzake de digitale handtekening. Ook hier wordt wel de wetgeving gestroomlijnd maar is het proces op weg daarnaar toe dat nog niet; de implementatietermijn (1 januari 2004) is niet gehaald. Een off-line succes voor de fiscus was het oordeel van de Hoge Raad inzake telecommunicatiekabels. Kabelnetten zijn onroerend, en daarom is er overdrachtsbelasting verschuldigd bij verkoop. Hoewel onroerend, worden zij echter niet door natrekking eigendom van de eigenaar van de grond.[43]

3.4 Telecommunicatie en mededinging

Tarieven, toegang, prijsvechten, veilingen, reclameruzies, en een ingrijpende herziening van de regelgeving. Voor deze kroniekperiode bleken dit belangrijke steekwoorden voor de juridische ontwikkelingen op het terrein van de telecommunicatie. Meest fundamenteel is de komende herziening van het wettelijk kader op basis van de Europese regelgeving inzake elektronische

Koops, 'Een nieuwe GBA, digitale kluisjes en identificatiedrang', *NJB* 2001, p. 1555-1561, het redactioneel van J.E.J. Prins in *Computerrecht* 2003/ 1, p. 2-3, en vgl. <http:/ / www.consumer.gov/ idtheft/ >.
[39] <http:/ / www.burger.overheid.nl>; <http:/ / www.burger.overheid.nl/ persberichten/ ?id= 270>; e-bestuurlijk verkeer: kamerstuk 28483, nr. 199; kamerstukken I, 28483, nr. A, p. 4 en B, p. 2.
[40] <http:/ / www.gemeenteweb.nl/ show?id= 408260&frameid= 312868>; experimentwet e-kiezen: Stb. 2003, 569, en veiligheid daarvan: <http:/ / www.epn.net/ content/ berichten.asp?action= bericht&id= 491>.
[41] E-geld: Stb. 2002, 330; kritisch hierover: A.A.P. Schudelaro, *NJB* 2002, p. 1943-1945; financiële diensten: richtlijn 2002/ 65/ EG , *PbEG* L 271 van 9 oktober 2002.
[42] Richtlijn 2002/ 38/ EG, *PbEG* L 128; Wijziging Wet op de omzetbelasting 1968, Stb. 2003, 378.
[43] Richtlijn 2001/ 115/ EG , *PbEG* 2002, L 15; Kamerstukken 29036; HR 6 juni 2003, LJN-nrs. AD3578 en AD3591.

communicatienetwerken.[44] Een zestal Europese richtlijnen zal worden geïmplementeerd door aanpassing van onder meer de Telecommunicatiewet. Hierdoor zal een gemeenschappelijk uniform regelgevend kader ontstaan voor alle transmissienetwerken en diensten in de sectoren telecommunicatie, media en informatietechnologie. Het nieuwe, zeer brede, centrale begrip wordt 'elektronisch communicatienetwerk'. Het huidige onderscheid tussen omroepnetwerken, omroepzendernetwerken en (tele)commmunicatienetwerken komt te vervallen. De Mediawet en de Mededingingswet blijven relevant; de afstemming, ook bij de uitvoering, zal worden verbeterd. Hoewel ingrijpend, is door tijdgebrek geen sprake van een volledig nieuwe start. De gevolgde implementatiemethode ('vernieuwbouw') verdient geen schoonheidsprijs.[45]
Voor het algemene mededingingsrecht is nog van belang dat de op instigatie van het Ministerie van Economische Zaken gestelde vraag of de Mededingingswet voldoende ICT-proof is, 'grosso modo' positief werd beantwoord.[46]

4. Handhaving

4.1 Auteursrecht en IE

Handhaven kan ook door de inzet van techniek, zoals systemen voor 'Digital Rights Management' (DRM) waarmee elektronische 'content' op een beveiligde wijze ter beschikking wordt gesteld, met mogelijkheden voor monitoring en betaling. In het in de vorige kroniekperiode verschenen rapport 'Auteursrecht in de informatiemaatschappij' werden strategieën voor de inzet van DRM en de betekenis daarvan voor het wetgevingsbeleid ontvouwd. Maatschappelijke kritiek leidde vooralsnog niet tot aanpassing van de implementatieregeling voor DRM (zie 1.1).[47]
Op het terrein van de domeinnamen werd een arbitrageregeling van kracht (zie 4.4). Handhaving was voorts aan de orde bij de heffing op lege dragers: om de naleving effectiever te maken wordt een wetswijziging voorbereid waarin de aansprakelijkheid van de verkopers van drager wordt 'verlengd'. Vooral pregnant was de discussie rond *peer-to-peer*netwerken als Kazaa. Waar in eerste aanleg de rechter Kazaa verantwoordelijk achtte voor auteursrechtinbreuken binnen het netwerk, werd in hoger beroep en cassatie vastgesteld dat niet de programma-aanbieder maar de gebruikers de (eventuele) schuldigen zijn. Dat betekent dat de handhaving binnen *peer-to-peer*netwerken problematisch wordt: de rechthebbende moet nu de individuele gebruiker zien op te sporen (vgl. 1.2).[48]
Tot slot blijkt ook handhaving tegen de wil van de betrokkenen voor te komen. Buma/ Stemra eiste vergoeding van XS4ALL voor het op haar site zetten van de muziek die werd gespeeld tijdens het tiende verjaardagsfeest van de aanbieder – ook al zagen de betrokken muzikanten af van hun aanspraak op vergoeding. XS4ALL stapte daarop naar de NMa met een klacht over misbruik door Buma/ Stemra van haar monopolie-positie.[49] Het oordeel van de NMa wordt nog afgewacht.

4.2 Identificatie

Een belangrijk hulpmiddel in de handhaving van wet- en regelgeving is identificatie – niet voor niets dreef de veiligheidsdrang de wetgever tot het voorstel van een algemene identificatieplicht. De afgelopen tijd is er veel aandacht besteed aan het ontwikkelen van ICT-gerelateerde

[44] Kamerstuk 28851; zie ook <http:/ / www.ivir.nl/ dossier/ wijziging-Tw/ wijziging-Tw.html>.
[45] Zie voor een overzicht van de diverse aspecten van deze wetgevingsoperatie het Dossier Telecommunicatierecht, *Computerrecht* 2003/ 1.
[46] Zie <http:/ / www.ez.nl/ upload/ docs/ Kamerbrieven/ PDF-Documenten/ 02027286-bijlage8.pdf>.
[47] Rapport: <http:/ / www.justitie.nl/ images/ 11_7772.pdf>; kritiek: <http:/ / www.bof.nl/ nieuws/ 021108.html>; vgl. <http:/ / www.justitie.nl/ Images/ 11_7448.doc> en ITeR-deel 57.
[48] Dragers: kamerstukken 28486, kritisch hierover P. van Schelven in *Computerrecht* 2003/ 1, p. 61-66; Kazaa-Buma/ Stemra: Rb. Amsterdam 29 november 2001, LJN-nr. AD6395, *AMI* 2002/ 1, p. 21; Hof Amsterdam 28 maart 2002, LJN-nr. AE0805, *Mediaforum* 2002/ 5, p. 188, HR 19 december 2003, LJN-nr. AN7253, *AMI* 2004/ 1, p. 9; zie ook ITeR-deel 64; vgl. voor de handhaving ook kamerstuk 27088, nr. 32 over digitale tv.
[49] Zie <http:/ / www.xs4all.nl/ c-free/ download.html>.

identificatiemiddelen en de juridische context daarvan. Het Burgerservicenummer (zie par. 3.2), biometrie in het paspoort en de bestrijding van identiteitsfraude zijn primaire voorbeelden van overheidsactiviteiten op dit vlak. De vele activiteiten binnen de overheid zijn nogal versnipperd; het Rathenau Instituut vroeg om overzicht en bezinning op alle identificatieontwikkelingen. De overheid is echter zeker niet de enige speler: Microsoft ontwikkelde zijn .NET-Passport-systeem verder; privacy- en veiligheidsbezwaren noopten tot een schikking met de Amerikaanse toezichthouder FTC; vervolgens zegde het bedrijf substantiële aanpassing toe na 'overleg' met de Europese Artikel-29-werkgroep.[50]

4.3 Jurisdictie en territorialiteit

Waar het ICT-recht en de beoefenaars en analisten daarvan sinds de beginjaren van het Internet worstelden met handhavingsproblemen veroorzaakt door deterritorialisering en daarmee samenhangende jurisdictieproblemen, lijkt er langzaam een kentering te komen. In plaats van deterritorialisering wordt nu soms gesproken van herterritorialisering: in toenemende mate wordt rechtsmacht opgeëist zodra er een aanknopingspuntje bestaat. Een spraakmakend voorbeeld is de uitspraak van de Australische rechter in de zaak-Gutnick, waarin de Amerikaanse uitgever Dow Jones aansprakelijk werd gesteld voor smaad door publicatie op een Amerikaanse weblocatie die in Australië te zien was. Ook de uitspraken rond de toepasselijkheid van bestuurlijke wetgeving op buitenlandse aanbieders van online gokken passen in dit beeld (zie 3.1). De rechtshandhaving lijkt bovendien te profiteren van het opdelen van het Internet in territoriaal onderscheiden delen waarin een duidelijk – en veelal nationaal – wettelijk kader van toepassing is. Techniek speelt hierbij een belangrijke rol: '[technology] is reshaping the Internet to match more closely its real-space equivalent, complete with borders that mirror those found in a *Rand McNally Atlas*'.[51]

4.4 ADR/ODR

De tendens om te handhaven door zelfregulering, die in de vorige kroniek reeds aan bod kwam, zette zich door, bijvoorbeeld via velerlei gedragscodes en meldpunten. Overigens kunnen wij ons niet aan de indruk onttrekken dat de vaker gehoorde roep om zelfregulering, zoals de Balkenendse roep om eigen verantwoordelijkheid van burgers, voornamelijk uit doelmatigheidsoverwegingen geschiedt en allerminst de overheid weerhoudt van reguleringsactiviteiten wanneer dat om andere redenen goed uitkomt. Dat neemt niet weg dat met name op het gebied van alternatieve geschillenbeslechting serieuze stappen worden gezet, mede vanuit de overtuiging dat dit – en niet alleen vanwege doelmatigheid – beter is voor betrokkenen. Binnen ICT-recht is in dit verband de arbitrageregeling van belang die SIDN 29 januari 2003 instelde voor .nl-domeinnamen, ondergebracht bij het WIPO Arbitration and Mediation Centre. Op 17 oktober 2003 werd de eerste uitspraak gedaan – met opmerkelijk genoeg een Italiaanse eiser en verweerder. Verder werd ook online geschillenbeslechting, Online Dispute Resolution (ODR), nader ontwikkeld, bijvoorbeeld met de afronding van het ECP-project ODR.NL, het proefproject ECODIR voor ODR in e-handel, en ontstond zelfs een Nederlands commercieel initiatief.[52]

[50] Identificatieplicht: kamerstukken 29218; biometrie in paspoort: kamerstukken 28342; bestrijding identiteitsfraude: Kamerstuk 17050, nr. 234; C. Prins & M. de Vries, *ID or not to be?*, Rathenau Instituut 2003, <http:/ / www.rathenau.nl/ nl/ publicaties/ showpagetekst.asp?artid=280> en *NJB* 2004, p. 114-118; .NET: <http:/ / www.ftc.gov/ opa/ 2002/ 08/ microsoft.htm>, <http:/ / europa.eu.int/ comm/ internal_market/ privacy/ docs/ wpdocs/ 2003/ wp68_en.pdf>. Zie ook noot 38.

[51] Michael Geist, 'Cyberlaw 2.0', *Boston College Law Review* 44 (2003), p. 357.

[52] ADR: zie <http:/ / www.geschillenbeslechting.nl/ > en OECD, *Legal Provisions Related to Business-to-Consumer Alternative Dispute Resolution in Relation to Privacy and Consumer Protection*, <http:/ / www.olis.oecd.org/ olis/ 2002doc.nsf/ linkto/ dsti-iccp-reg-cp(2002)1-final>; domeinnamen: <http:/ / arbiter.wipo.int/ domains/ cctld/ nl/ index.html>, uitspraak: <http:/ / www.domjur.nl>, nr. 2003-181, WIPO2003NL1, ITeR-deel 58; vgl. *NJB* 2002, p. 1242; ODR: <http:/ / www.geschillenbeslechting.nl/ > onder 'ODR', <http:/ / www.ecodir.org/ >, <http:/ / www.emediation.nl/ index2.html>.

5. Literatuur

Elektronisch publiceren blijkt vooralsnog geen megatrend binnen ICT-recht; nog steeds verschijnt het leeuwendeel van bijvoorbeeld dissertaties in boekvorm. Zonder ook maar enigszins uitputtend te kunnen zijn, willen wij – ongetwijfelde gekleurd door persoonlijke achtergrond – uit de kroniekperiode uitlichten het boek met zeven essays dat de oogst van acht jaar ITeR afsloot, dissertaties op het gebied van digitale communicatiegrondrechten (Asscher), het recht op privacy (Blok), ipr & auteursrecht (van Eechoud), auteursrecht & contracten (Guibault), ipr & e-handel (Van der Hof), aansprakelijkheid & telecom (Huisjes), DRM (Koelman), e-geld & witwassen (Schudelaro), oraties over BTW & Internet (Kemmeren), normering van informatietechnologie (Stuurman), en een overzicht van ICT-regulering in acht landen.[53]

6. Inleiding

Aangezien wij begonnen zijn met een afsluiting, past het te eindigen met een inleiding. De megatrends van afsluiting, veiligheid, stroomlijning en handhaving geven alle blijk van een toenemende greep van (overheids)regulering op ICT. Het is de inleiding op een nieuw tijdperk: de afgelopen twee jaar kunnen worden gezien als de lancering van een nieuwe versie van het programma ICT-recht: Cyberlaw 2.0, zoals Michael Geist het uitdrukt.[54] De verwarringsfase van de bètaversies 0.x (1970-1995) en de achtervolgingsfase van versies 1.x (1995-2000) zijn achter de rug; in versie 2.0 (vanaf 2001) herterritorialiseert nu het (overheids)recht het Internet. Internationalisering doordringt op alle niveaus het ICT-recht, maar lijkt geen onoverkomelijk obstakel voor nationale ontwikkeling en toepassing van het recht, zelfs niet op het grensoverschrijdende Internet. Naar onze verwachting zal deze versie de komende jaren goed doorstaan en – met tussentijdse aanpassingen – steeds robuuster kunnen worden. Het zal nog vele jaren duren voor een nieuwe versie, 3.0, op de markt zal moeten komen om de volgende revolutie in het ICT-recht – zelfhandelende systemen – te lijf te gaan. Tot die tijd zullen we het moeten – en kunnen – doen met versie 2.0.

[53] *Zeven essays over informatietechnologie en recht*, Sdu 2003, ITeR-deel 67; Asscher, *Communicatiegrondrechten* (Cramwinckel), Blok, *Het recht op privacy* (Boom), van Eechoud, *Choice of Law in Copyright and Related Rights* (KLI), Guibault, *Copyright Limitations and Contracts* (KLI), Van der Hof, *Internationale on-line overeenkomsten* (Sdu), Huisjes, *Over dode lijnen en een heuvel recht* (Kluwer), Koelman, *Auteursrecht en technische voorzieningen* (Sdu), Schudelaro, *Electronic Payment Systems and Money Laundering* (Wolf Legal Publishers); Kemmeren, *E-business en vaste inrichtingen: paniek voetbal* (Kluwer), Stuurman, *Digitale ruimte, analoge regels?* (Boom); *ICT-regulering anno 2002*, <http:/ / rechten.uvt.nl/ crbi/ ICT-regulering2002.pdf>. Terzijde willen we nog wijzen op een proefschrift in het (stief?)zustervakgebied van de rechtsinformatie, C. Grütters, *Asieldynamiek. Een systeemdynamische analyse van de Nederlandse asielprocedure in de periode 1980 – 2002* (Wolf Legal Publishers).

[54] Michael Geist, 'Cyberlaw 2.0', *Boston College Law Review* 44 (2003), p. 323-58. Zie ook Joel R. Reidenberg, 'States and Internet Enforcement', *University of Ottawa Law & Technology Journal* 2004/ 1, SSRN-nr. 487965, en daar aangehaalde literatuur.

Formatted

Formatted