Kroniek Technologie en recht

Remy Chavannes en Niels van der Laan[1]

'Technologierecht' is geen afgebakend rechtsgebied, 'technologie en recht' is vooral een tijdelijke wachtkamer voor ontwikkelingen die nog niet door hun eigen rechtsgebied zijn opgehaald. De technologische vooruitgang bezorgde de uitvoerende, wetgevende en rechtsprekende machten wel veel moeilijke vragen en de respons was wisselend en aarzelend. Er dient zich een generatie *digital natives* aan, van burgers die met internet zijn opgegroeid en zich afvragen waarom die digibete stenentijdperkjuristen zoveel dode bomen nodig hebben om met hopeloze analogieën vragen te lijf te gaan die zij op basis van eigen kennis en intuïtie al kunnen beantwoorden. De komende verslagperioden zullen zij hun stempel zetten op de complexe afwegingen van botsende (grond)rechten die in de digitale informatiesamenleving onvermijdelijk zijn.

Elk tijdperk worstelt met de maatschappelijke en dus ook juridische consequenties van nieuwe technologie. De fotografische revolutie van de negentiende eeuw riep de vraag op hoe het nieuwe medium zich verhield tot kunst en auteursrecht.[2] Meer in zijn algemeenheid bezorgde de industriële revolutie de juridische klasse – traditioneel niet de meest technisch aangelegde – een waslijst aan 'nieuwe' problemen, van de bescherming van technische innovatie en de regulering van anonieme massatransacties tot het recht om met rust gelaten te worden en de strijd tegen exploitatie van minderjarigen. Of de eenentwintigste eeuw zich in dat opzicht wezenlijk onderscheidt van de negentiende (of de vijftiende) eeuw kan in het midden blijven: feit is dat technologische ontwikkelingen, vooral maar niet alleen in de manier waarop wij informatie creëren, gebruiken en communiceren, elkaar op dit moment zeer snel opvolgen en dat ook juristen het er soms behoorlijk lastig mee hebben.

Met deze kroniek willen de auteurs geen steun geven aan de gedachte dat er zoiets bestaat als 'technologierecht' of 'internetrecht' als zelfstandige rechtswetenschappelijke discipline. De praktijk van het 'technologierecht' is in onze beleving vaak niet meer dan het toepassen van bestaande regels op nieuwe producten en diensten;[3] de in deze kroniek beschreven ontwikkelingen laten zich voor een groot deel kwalificeren als in wezen commune kwesties met toevallig technische casuïstiek. Op termijn zullen zij naar onze verwachting, net zoals het Elektriciteitsarrest[4] en het Draadomroeparrest,[5] worden beschouwd als gewone zij het mogelijk historisch interessante zaken binnen hun respectievelijke rechtsgebieden.[6]

Die omstandigheid betekent ook dat er een grote overlap bestaat tussen ontwikkelingen op het gebied van 'recht en technologie' en ontwikkelingen die al voorwerp zijn van andere kronieken in het NJB, zoals digitaal berichtenverkeer in het bestuursrecht;[7] online terhandstelling van algemene voorwaarden in het vermogensrecht;[8] en de internettende rechter in het burgerlijk procesrecht.[9] In sommige rechtsgebieden wordt de wetenschappelijke en politieke discussie sterk beïnvloed zo niet gedomineerd door technische ontwikkelingen, zoals internetpiraterij en digitale mediaconsumptie in het auteursrecht en digitale verwerking van persoonsgegevens in het privacyrecht. In dergelijke overlapsituaties hebben wij grotendeels voorrang verleend aan de vakkronieken (in dit geval intellectuele eigendom[10] respectievelijk grondrechten[11]), indachtig ons uitgangspunt dat 'technologie en recht' vooral een tijdelijke wachtkamer is voor ontwikkelingen die nog niet door hun eigen rechtsgebied zijn opgehaald.

Gelukkig valt er ook met dit terughoudende selectiecriterium genoeg te melden over de kroniekperiode 2010-2012, al is het maar omdat er voldoende ontwikkelingen zijn die vanuit de klassieke rechtsgebieden misschien niet vermeldenswaard zijn maar wel een boeiend licht werpen op de receptie van technologische innovatie in het gewone recht. Bovendien verdienen sommige ontwikkelingen die in andere kronieken zijn gesignaleerd, in de context van 'technologie en recht' meer of andere aandacht. Zoals kan worden verwacht bij een onderwerp als het onderhavige biedt het internet een breed scala aan overzichten van 'internetrecht', aan de volledigheid waarvan deze papieren kroniek niet kan tippen.[12] Tijdschriften zoals *Computerrecht*, *Mediaforum* en het *Tijdschrift voor internetrecht* publiceren regelmatig thematische kronieken en zijn ook voor het overige veelal te beschouwen als doorlopende kronieken van technologie en recht.

1. Juridische status van hyperlinks

Hyperlinks behoren tot de meest basale kenmerken van het internet: een volgens een bepaalde standaard gecodeerde verwijzing naar informatie elders op het internet, die in bijvoorbeeld een browser of mailbericht kan worden aangeklikt om zonder verder tik- of klikwerk direct naar de desbe-

treffende bron te worden geleid. Dat zo'n hyperlink in principe niet meer is dan een elektronische voetnoot, waarvan het plaatsen nog niet leidt tot verantwoordelijkheid voor de inhoud of het openbaar maken van de informatie waarnaar wordt gelinkt, is een oeroud uitgangspunt van 'internetrecht'[13] dat ook in de verslagperiode diverse malen werd bevestigd.[14] Een poging van de RVD om dat anders te laten zijn voor hyperlinks naar privéfoto's van leden van het Koninklijk Huis vond weinig weerklank.[15] Een campagne van Buma Stemra om een vergoeding te eisen voor het aanbrengen van 'embedded' hyperlinks naar muziek(video's) werd door Visser op juridisch-pragmatische gronden bestreden;[16] kort geding procedures van Buma zijn tot op heden gestrand wegens gebrek aan spoedeisend belang[17] c.q. doorverwezen naar de bodemrechter.[18]

Vlak voor het ter perse gaan van de kroniek wees de rechtbank Amsterdam echter vonnis in een zaak over een blootreportage uit Playboy, die voortijdig was uitgelekt en waarover het weblog Geenstijl.nl een met hyperlink verrijkt artikel publiceerde.[19] Volgens de rechtbank is het plaatsen van een hyperlink, die verwijst naar de locatie op het internet waar een bepaald werk voor publiek toegankelijk is gemaakt, in beginsel geen zelfstandige openbaarmaking, omdat de feitelijke terbeschikkingstelling aan het publiek plaatsvindt op de website waar de hyperlink naar verwijst. Dat was in dit geval volgens de rechtbank echter anders, omdat de fotoreportage alleen beschikbaar was op één obscure plaats op internet en het door Geenstijl.nl plaatsen van de hyperlink moest worden beschouwd als de interventie waardoor een nieuw publiek ervan kennis kon nemen. De komende verslagperiode zal leren of het in deze context hanteren van de aan recente Europese rechtspraak arrest ontleende criteria van interventie, nieuw publiek en winstoogmerk[20] leidt tot een significante uitbreiding van het openbaarmakingsbegrip op internet.

Los van de auteursrechtelijke status van hyperlinken geldt dat het aanbrengen van een hyperlink onrechtmatig kan zijn. Afhankelijk van onder meer de context, doelstelling en wijze en van hyperlinken, kan dat wel degelijk het geval zijn, bijvoorbeeld wanneer sprake is van structureel, stelselmatig en om financieel gewin creëren van een verzameling hyperlinks naar illegale informatie (zie hierover meer in het volgende hoofdstuk). De Raad voor de Journalistiek, die begin 2011 haar statuten heeft aangepast om te verduidelijken dat zij ook oordeelt over journalistieke publicaties op internet, heeft in haar Leidraad een vergelijkbare regel opgenomen over de journalistiek-ethische aanvaardbaarheid van hyperlinken: 'De redactie die door middel van een duidelijk aangegeven hyperlink verwijst naar informatie van derden, is niet zonder meer verantwoordelijk voor de inhoud van de onderliggende informa-

Auteurs

1. Mr. R.D. Chavannes en mr. N. van der Laan zijn advocaat te Amsterdam bij respectievelijk Brinkhof en De Roos & Pen.
De auteurs danken Dorien Verhulst en Tineke van de Bunt (Brinkhof) respectievelijk Nieke Verschaeren en Fanny de Graaf (De Roos & Pen) voor hun hulp bij de totstandkoming van deze kroniek.

Noten

2. Zie daarover bijvoorbeeld R. Verhoogt, *Art in Reproduction. Nineteenth-Century Prints after Lawrence Alma-Tadema, Jozef Israëls and Ary Scheffer*, Amsterdam: AUP 2007; R.D. Chavannes, 'De kunst van het onzichtbaar blijven: het auteursrecht van de reproductiefotograaf', in: Van Eijk & Hugenholtz (red), *Dommering-bundel: Opstellen over informatierecht aangeboden aan prof. mr. E.J. Dommering*, Amsterdam: Otto Cramwinckel 2008.

3. Bij wijze van voorbeeld: A.P. Engelfriet, '3D printen: revolutie of de nieuwe Napster?', *Tijdschrift voor internetrecht* 2011/5, p. 141; J.J. Toet, 'Juridische implicaties bij de invoering van IPv6', *Tijdschrift voor internetrecht* 2010/2, p. 43.

4. Hoge Raad 23 mei 1921, *NJ* 1921/564.

5. Hoge Raad 27 juni 1958, *NJ* 1958/405.

6. Over de 'informatierechtelijke' benadering, waarbij de focus niet ligt op techniek maar op informatie als rechtsgoed, ongeacht de informatietechnologie, en dus op de eigendoms-, vrijheid- en ordeningsvragen van de al dan niet digitale informatiemaatschappij, zie: E.J. Dommering, 'Nieuwe visies op intellectuele vrijheid, producten van de geest en privacy: Het Instituut voor Informatierecht', in: M. Polak, J. Sevink & S. Noorda (red.), *Over de volle breedte: Amsterdams universitair onderzoek na 1970*, Amsterdam: Vossiuspers UvA 2007, p. 173-197. Voor erkenning van internetrecht als afzonderlijk, functioneel rechtsgebied pleit daarentegen A.R. Lodder, 'Recht rond cyberwar, het internet van dingen en andere internet (on)gemakken: de tien geboden van het internetrecht', oratie VU 30 maart 2012, p. 7-11.

7. E.J. Daalder en A.C. Rop, 'Kroniek van het algemene bestuursrecht', *NJB* 2011/1752, onder verwijzing naar de VAR-preadviezen over het thema 'De digitale overheid'.

8. R.-J. Tjittes en E. van Wechem, 'Kroniek van het vermogensrecht', *NJB* 2011/781, onder verwijzing naar HR 11 februari 2011, *LJN* BO7108.

9. M. Ynzonides en M. de Boer, 'Kroniek van het burgerlijk procesrecht', *NJB* 2011/1753, onder verwijzing naar HR 15 april 2011, *NJ* 2011/180. Zie verder: N. van der Laan, 'Bewijs rond krijgen met feiten van algemene bekendheid', *Advocatenblad* 2010/p. 184; L.A.R. Siemerink, 'Rechter gewaarschuwd voor googelen', *NJB* 2010/2145; Y.E. Schuurmans, K. Pill en M.M. Groothuis, 'De rechter op internet', *Computerrecht* 2012/118; HR 9 september 2011, *RvdW* 2011/1083; HR 13 september 2011, *LJN* BR1654; Hof Arnhem 17 april 2012, *LJN* BW3101.

10. Laatstelijk: D.J.G. Visser, 'Kroniek van de intellectuele eigendom', *NJB* 2012/884, onder verwijzing naar o.a. auteursrechthandhaving op internet, de aansprakelijkheid van online veilingplatforms, Google Adwords en het auteursrechtelijke openbaarmakingsbegrip bij satellietuitzendingen.

11. Laatstelijk: J.H. Gerards, 'Kroniek van de grondrechten', *NJB* 2011/1756, onder verwijzing naar o.a. vingerafdrukken in het paspoort, het elektronisch patiëntendossier en digitale schandpalen.

12. Zie onder meer de jaarlijkse overzichten internetrecht van Ius Mentis (laatstelijk http://blog.iusmentis.com/kroniek-internetrecht-2011/) en advocatenkantoor SOLV (laatstelijk http://www.solv.nl/weblog/jaaroverzicht-internetrecht-2011/18640) en de doorlopende verzameling van de Universiteit Utrecht (http://internetrechtspraak.wikispaces.com)

13. Zie bijv. D.J.G. Visser, *Auteursrecht op toegang. De exploitatierechten van de auteur in het tijdperk van digitale informatie en netwerkcommunicatie* (diss. Leiden), 's-Gravenhage: VUGA 1997, p. 178; Commissie Auteursrecht, 'Advies over auteursrecht, naburige rechten en de nieuwe media', 1998, p. 38; R.D. Chavannes, 'Hype of echt link: de hyperlinkaansprakelijkheid van informatieaanbieders, internetaanbieders en zoekmachines', *JAVI* februari 2003/1, p. 2; Spoor/Visser/Verkade, *Auteursrecht* (2005), par. 4.13, p. 174.

14. Hof Den Bosch 12 januari 2010, *IEPT* 20100112 (*C More/MyP2P*); Hof Amsterdam 16 maart 2010, *LJN* BL7920 (*Brein/X; Shareconnector*) Hof 's-Gravenhage 15 november 2010, *NJ* 2011/565 (*FTD/Eyeworks*); Rb. Den Haag 1 november 2011, *LJN* BU3223 (*RealNetworks*). Zie ook Supreme Court of Canada 19 oktober 2011, *Crookes vs. Newton*, 2011 SCC 47, [2011] 3 S.C.R. 269; Bundesgerichtshof, I. Zivilsenat 29 april 2010, Az. I ZR 39/08.

15. 'Linken naar privéfoto's koninklijk huis mag niet', IE-Forum 7 oktober 2011, IEF 10306.

16. D.J.G. Visser, 'Het 'embedden' van een You Tube-filmpje op een Hyves-pagina'.

17. Rb. 's-Gravenhage (vzr.) 8 juli 2011, *LJN* BR1058 (*Buma Stemra/Nederland FM*).

18. Rb. Amsterdam (vzr.) 26 juli 2011, IEPT20110726 (*Buma/Target Media*).

19. Rb. Amsterdam 12 september 2012, *LJN* BX7043 (*Sanoma/GS Media*). Co-auteur Chavannes treedt in deze zaak op voor GS Media.

20. Zie paragraaf 4.2 hierna, alsmede M. de Cock Buning en R. Kindt, 'Het Europese Hof doet nieuwe 'mededelingen aan het publiek', *IER* 2012/33.

tie. Wel dient zij steeds een afweging te maken of het belang dat met het plaatsen van een hyperlink in de publicatie is gediend, zwaarder weegt dan de belangen die hierdoor mogelijk worden geschaad.'[21]

2. Internettussenpersonen

Er is in de verslagperiode veel geprocedeerd over de aansprakelijkheid en verplichtingen van tussenpersonen op internet.[22] Onderscheid kan worden gemaakt tussen (a) de aansprakelijkheid van de tussenpersoon voor eigen rechtsinbreuken;[23] (b) afgeleide aansprakelijkheid vanwege het om eigen gewin structureel faciliteren van inbreukmakend of anderszins onrechtmatig gedrag van klanten;[24] en (c) informatie- en preventieverplichtingen zoals het verstrekken van naam-, adres- en woonplaats (NAW-)gegevens,[25] verkeersgegevens[26] of betalingsgegevens[27] van klanten of het blokkeren van toegang tot bepaalde informatie of functionaliteiten.[28]

De aansprakelijkheids- en medewerkingspositie is bovendien afhankelijk van de aard van de tussenpersoon: een verlener van internettoegang is minder snel aansprakelijk en heeft minder vergaande verplichtingen dan een verlener van hostingdiensten, zo blijkt ook uit art. 6:196c lid 1 respectievelijk lid 4 BW. De inhoudelijke bemoeienis van een tussenpersoon gaat soms zover dat deze in het geheel geen beroep op de hostingexceptie toekomt maar rechtstreeks aansprakelijk is. In de zaak-*Kim Holland Productions/123video.nl* verwierp de rechtbank het beroep van een video-uploadsite op de hostingexceptie van art. 6:196c lid 4 BW, onder verwijzing naar de extra diensten die de exploitant verleende om door derden geuploade filmpjes beter vindbaar te maken.[29] In zijn arresten inzake Google France had het Hof van Justitie inderdaad overwogen dat de hosting-exceptie alleen van toepassing is wanner de activiteit van de aanbieder een louter technisch, automatisch en passief karakter heeft, hetgeen inhoudt dat deze aanbieder noch kennis noch controle heeft over de informatie die wordt doorgegeven of opgeslagen, waarmee *en passant* overweging 42 bij de E-commerce richtlijn, die ziet op internettoegangsdiensten, werd uitgebreid naar aanbieders van hostingdiensten.[30] In een volgend arrest expliciteerde het Hof van Justitie dat hulp bieden aan klanten bij het optimaliseren van een advertentie of verkoopprommotie voldoende is om een beroep op de hostingexceptie te blokkeren.[31]

Ondertussen hamert het EU Hof van Justitie er steeds nadrukkelijker op dat bij de online handhaving van IE-rechten sprake is van een door de nationale rechter in concrete gevallen te beslechten conflict tussen verschillende fundamentele rechten van rechthebbenden, tussenpersonen en consumenten, waaronder het intellectuele eigendomsrecht, vrijheid van onderneming, privacy en vrijheid van meningsuiting. Het is dus niet vanzelfsprekend dat tussenpersonen bij een (dreigende) inbreuk op IE-rechten een verplichting hebben om preventieve maatregelen te treffen of informatie te verstrekken.[32] Het EHRM op zijn beurt stelt steeds strengere eisen aan de kwaliteit (voorzienbaarheid, waarborgen tegen misbruik en willekeur) van beperkingen van privacy en uitingsvrijheid,[33] die de wetgever op dit terrein tot verduidelijkende actie manen.

Kortgedingrechters lijken doorgaans weinig sympathie te hebben voor abstracte grondrechtenargumenten als verweer tegen praktische behulpzaamheidsvorderingen. Dat blijkt uit de hierboven aangehaalde uitspraken over verstrekking van klantgegevens en blokkering van toegang tot onrechtmatige content, maar wellicht nog het meest pregnant uit de curieuze casus van de zaak-*Zwartepoorte/Schoonderwoerd*. Als in de zoekmachine van Google werd gezocht op de woorden 'Zwartepoorte' en 'failliet', verscheen als eerste zoekresultaat een link naar de door Schoonderwoerd beheerde website klup.nl, met daarbij onder andere het citaat: '**Zwartepoorte** Specialiteit: BMW ... Dit bedrijf is **failliet** verklaard, het is overgenomen door het motorhuis.' Deze tekst kwam niet in deze vorm op klup.nl voor, maar was een ongelukkige samenvoeging door de zoekmachine van twee korte fragmenten die op andere delen van de pagina voorkwamen. De inhoud van de website klup.nl was op geen enkele manier onrechtmatig jegens Zwartepoorte, maar toch werd Schoonderwoerd in twee instanties veroordeeld om 'de inrichting van de website klup.nl zodanig aan te passen en aangepast te houden, dat niet langer via deze website, door middels van de website van Google, een zoekresultaat wordt weergegeven waarin de onjuiste indruk wordt gewekt dat Zwartepoorte failliet is.'[34] Daarbij lijkt doorslaggevend te zijn geweest dat Schoonderwoerd met een kleine ingreep op zijn site de voor Zwartepoorte schadelijke weergave in Google kon laten verdwijnen. Schoonderwoerds beroep op vrijheid van meningsuiting werd afgedaan met de overweging dat in de gegeven omstandigheden het belang van Zwartepoorte zwaarder weegt. Het 'internetrecht' bestaat langzamerhand uit een aaneenschakeling van dergelijke, overwegend praktische kort geding uitspraken, die in de context van de specifieke casus zijn te begrijpen maar vervolgens als 'jurisprudentie' een eigen leven gaan leiden.[35]

Dat tussenpersonen ook strafrechtelijke risico's lopen bleek in december 2011 toen het Meldpunt Discriminatie Internet (MDI) aangifte deed tegen Google (*YouTube/Blogger*) wegens discriminatie.[36] Google zou ondanks diverse verzoeken van het MDI discriminerende content niet hebben verwijderd. De vraag is echter of Google vervolgd kan worden.[37] Anders dan de civiele bescherming is de strafrechtelijke bescherming tegen aansprakelijkheid voor tussenpersonen absoluut. Blijkens art. 54a Sr (een Nederlandse implementatie van de e-commercerichtlijn) kan een tussenpersoon namelijk pas vervolgd worden eerst nadat een vordering van de rechter-commissaris wordt genegeerd.[38] Er is weliswaar een voorontwerp van wet geconsulteerd waarin de bevoegdheid tot het geven van een verwijderingsbevel van de rechter-commissaris naar de

Het EU Hof van Justitie hamert er steeds nadrukkelijker op dat bij de online handhaving van IE-rechten sprake is van een door de nationale rechter in concrete gevallen te beslechten conflict

Het 'internetrecht' bestaat uit een aaneenschakeling van dergelijke, overwegend praktische kort geding uitspraken, die in de context van de specifieke casus zijn te begrijpen maar vervolgens als 'jurisprudentie' een eigen leven gaan leiden

officier van justitie werd overgedragen in een nieuw art. 125p Sv, maar daarvan is na maar liefst 609 veelal zeer kritische reacties niet meer vernomen.[39]

3. Technologie en media

3.1 Regulering van digitale media

Vlak voor het begin van deze kroniekperiode, op 19 december 2009, trad de gewijzigde Mediawet 2008 in werking ter implementatie van de Richtlijn Audiovisuele Mediadiensten.[40] De meest ingrijpende wijziging die de implementatie met zich meebracht was dat voortaan ook audiovisuele mediadiensten op aanvraag, waarbij de kijker bepaalt wat hij ziet en wanneer, (ook wel 'non-lineaire mediadiensten of 'on-demand' diensten genoemd) gereguleerd worden en onder toezicht van het Commissariaat voor de Media vallen.

Vanaf het begin van het implementatieproces werd voorspeld dat discussie zou ontstaan over de vraag welke interactieve diensten onder dit nieuwe toezicht zouden moeten vallen.[41] Het Commissariaat heeft op dit punt meer duidelijkheid gebracht door op 22 november 2011 beleidsregels vast te stellen met daarin criteria voor het begrip 'mediadienst op aanvraag'.[42] Sprake moet zijn van een massamediale economische dienst; waarvan het aanbieden van video's aan de hand van een catalogus het hoofddoel is; en waarover een aanbieder redactionele verantwoordelijkheid uitoefent. In de toelichting op de Beleidsregels is verduidelijkt dat redactionele verantwoordelijkheid beslissende zeggenschap vereist over de selectie en organisatie van het aanbod. Als bij de selectie en organisatie verschillende partijen betrokken zijn, wordt de partij die zeggenschap heeft over de *selectie* geacht redactio-

21. Zie http://www.rvdj.nl/leidraad. De regel is gedestilleerd uit een aantal uitspraken op klachten van Manon Thomas, zie o.a. *RvdJ* 12 maart 2008, *RvdJ* 2008/6 (*Manon Thomas/Telegraaf.nl*).
22. Zie naast de jaarlijkse IE-kronieken van Visser onder meer: P. van Eecke, 'Online service providers and liability: a plea for a more balanced approach', *CMLR* 48: 1455-1502, 2011; M. de Cock Buning en A. Ringnalda, 'Maatregelen tegen auteursrechtinbreuk door P2P-filesharing: wat leert het Umfeld ons?', AMI 2010/nr. 1, p. 1; B. van der Sloot, 'Three Strikes You're Out. De bescherming van auteursrecht op internet', *AMI* 2011/nr. 3, p. 84; M.H.M. Schellekens, 'Internet-filteren: komt van het een het ander?', *Mediaforum* 2011/10, p. 286; B. van der Sloot, 'De verantwoordelijkheid voorbij: de ISP als verlengstuk van de overheid', *Mediaforum* 2010/5, p. 157; B. van der Sloot, 'De verantwoordelijkheid voorbij: de ISP op de stoel van de rechter', *Tijdschrift voor internetrecht* 2011/5, p. 136.
23. Bijv. Rb. Amsterdam 28 september 2011, B9 10203 (*Brein/News-Service*).
24. Bijv. Rb. Haarlem 9 februari 2011, *LJN* BP3757 (*FTD/Brein*); Rb. Amsterdam 28 september 2011, B9 10203 (*Brein/News-Service*).
25. Bijv. Hof Amsterdam 10 oktober 2010, *LJN* BP7309 (*Ziggo/123Video*); HvJ EU 19 april 2012, zaak C-461/10 (*Bonnier Audio/Perfect Communication*).
26. Rb. Amsterdam (vzr.) 9 oktober 2008, *LJN* BF7448 (*Iceshop/Google*); Rb. Alkmaar (vzr.) 4 november 2010, *LJN* BO2916, *Mediaforum* 2011/2, m.nt. Q.R. Kroes (*X/Y*).
27. Rb. Den Haag (vzr.) 6 december 2011, IEPT20111206 (*Brein/Techno Design*).
28. Rb. Den Haag 11 januari 2012, *LJN* BV0549 (*Brein/Ziggo en XS4ALL*); Rb. Den Haag (vzr.) 10 mei 2012, *LJN* BW5387 (*Brein/providers*); Rb. Den Haag (vzr.) 10 mei 2012, *LJN* BW5407 (*Brein/Piratenpartij*). Co-auteur Chavannes treedt op voor twee van de betrokken internetaanbieders.
29. Rb. Amsterdam 24 november 2010, *LJN* BP6880 (*Kim Holland Productions/123video.nl*).
30. HvJ EU 23 maart 2010, zaken C-236/08-C-238/08 (*Google France en Google*).
31. HvJ EU 12 juli 2011, zaak C-324/01 (*LÓréal/eBay*). Voor een recente toepassing op een Nederlandse veilingsite, zie Hof Leeuwarden 22 mei 2012, *LJN* BW6296 (*Stokke/Marktplaats*).
32. HvJ EU 24 november 2011, zaak C-70/10 (*Sabam/Scarlet*); HvJ EU 16 februari 2012, zaak C-360/10 (*Sabam/Netlog*); HvJ EU 19 april 2012, zaak C-461/10 (Bonnier Audio/Perfect Communication). Zie hierover o.a.: E.J. Dommering, 'De zaak Scarlet/Sabam: naar een horizontale integratie van het auteursrecht', *AMI* 2012/2, p. 49; S.H. Kingma, 'De botsing tussen IE- en privacyrechten. Het einde van het Lycos/Pessers tijdperk', *Privacy & Informatie* 2012/nr. 4, p. 170; B.D.P. van der Eijk, 'Bewaar- en weggooi-verplichtingen in de strijd tegen copyrightinbreuk', *Tijdschrift voor internetrecht* 2012/3, p. 83.
33. EHRM 29 maart 2011, *Mediaforum* 2011-11/12, nr. 30 m.nt D. Haije (*RTBF/België*).
34. Hof Amsterdam 26 juli 2011, *LJN* BR3418, IEF10021 (*Zwartepoorte/Schoonderwoerd*).
35. Zie over een eerder voorbeeld van dit verschijnsel: R.D. Chavannes, 'Brein/KPN: Het gevaar van een bagatel?', *Mediaforum* 2007/6. Ook het eerder aangehaalde arrest-*Lycos/Pessers*, waarin de Hoge Raad twee keer overweegt dat het Hof zijn oordeel heeft 'toegesneden op het onderhavige geval' (verstrekking van NAW-gegevens door de hosting provider van een niet onrechtmatig bevonden website) maar dat sindsdien dient als basis voor gegevensverstrekkingsbevelen van diverse aard, kan tot deze categorie worden gerekend.
36. http://www.nu.nl/internet/2691483/aangifte-google-discriminatie.html.
37. Co-auteur Van der Laan treedt in deze zaak op voor Google.
38. Zie bijvoorbeeld: Rb. Assen, *LJN* BD 8452 en Hof Leeuwarden, *LJN* BI1645.
39. Zie onder meer de reacties van Bits of Freedom, Stichting Brein, Leaseweb (bij monde van mr. F.F. Blokhuis), XS4ALL en Ziggo, gepubliceerd op http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit/reacties. Zie ook: J.J. Oerlemans, 'Het wetsvoorstel versterking bestrijding computercriminaliteit', *Tijdschrift voor internetrecht* 2010/5, p. 148; A.W. Hins, 'Computercriminaliteit en historisch besef', *Mediaforum* 2010/10, p. 309.
40. Wet van 10 december 2009 ter wijziging van de Mediawet 2008 en de Tabakswet ter implementatie van de richtlijn Audiovisuele mediadiensten, *Stb.* 2009, 552 en 553; Richtlijn 2007/65/EG van het Europees Parlement en de Raad van de Europese Gemeenschappen van 11 december 2007 tot wijziging van richtlijn 1989/552/EEG betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake de uitoefening van televisieomroepacitiviteiten, *Pb EG* L322.
41. Zie uitgebreider: J. Verweij, 'YouTube en de Richtlijn Audiovisuele Mediadiensten', *Mediaforum* 2011/4, p. 105; R.D. Chavannes, 'Wetsvoorstel Audiovisuele Mediadiensten: een eigenzinnige implementatie van een gebrekkige richtlijn', *Mediaforum* 2009/5, p. 197.
42. Beleidsregels classificatie commerciële mediadiensten op aanvraag (2011), *Stcrt.* 2011, nr. 18039.

nele verantwoordelijkheid te hebben. Video hosting sites, zoals YouTube, zijn volgens de toelichting in beginsel geen mediadienst op aanvraag vanwege het ontbreken van redactionele verantwoordelijkheid. Dat kan volgens de toelichting echter anders worden op het moment dat platformaanbieders overeenkomsten aangaan over de levering van specifieke content. Daarnaast kan een derde partij die via een video hosting site een eigen kanaal aanbiedt kwalificeren als aanbieder van een mediadienst.

Niet alleen het vaststellen van de grens tussen, enerzijds, mediadiensten op aanvraag die onder de Mediawet vallen en, anderzijds, niet-gereguleerde (audiovisuele) diensten is van belang. Op grond van de Mediawet 2008 geldt voor traditionele omroepdiensten een uitgebreider en strenger regulatoir regime dan voor mediadiensten op aanvraag, zodat ook het vaststellen van de grens daartussen van belang is. Het elementaire verschil is volgens het Commissariaat de keuzevrijheid van de gebruiker bij het bekijken van de uitzending. In de toelichting op de recent in werking getreden Beleidsregels reclame en Beleidsregels sponsoring voor commerciële media-instellingen wordt dat geïllustreerd aan de hand van een sportuitzending via internet.[43] Als het sportevenement live kan worden bekeken is sprake van een lineaire omroepdienst; als de gebruiker het evenement op een later moment op een moment naar keuze kan bekijken is sprake van een mediadienst op aanvraag.[44] Dat lijkt te betekenen dat voor een eenmalige *live stream* van een sportevenement toestemming voor het aanbieden van een omroepdienst moet worden verkregen, tenzij de aanbieder onder verwijzing naar het ontbreken van (zeggenschap over) een chronologisch schema onder toepasselijkheid van de Mediawet uit weet te komen.

Het Hof van Justitie harmoniseert in rap tempo het Europese openbaarmakingsbegrip

De zes landelijke commerciële radiovergunningen werden met zes jaar verlengd.[45] Voorwaarde voor verlenging van de vergunningen is dat aanbieders investeren in de ontwikkeling van digitale radio. De verlengde analoge vergunningen zijn daarom gebundeld met digitale radiovergunningen. Vergunninghouders zijn verplicht om twee digitale kanalen uit te zenden, waarvan één een simulcast van het analoge kanaal moet zijn. Eén kavel (A7) bleef na het faillissement van Arrow onverdeeld en kon in 2011 dankbaar worden ingezet om tijdelijk de radio-ontvangst in Noord-Nederland te verbeteren na het instorten van de zendmast in Smilde.[46]

3.2 Digitale mediadistributie en auteursrecht

Voor de omroeppraktijk is de auteursrechtelijke kwalificatie van nieuwe distributietechnieken van groot belang. Het Hof van Justitie harmoniseert in rap tempo het Europese openbaarmakingsbegrip: het vertonen van beelden van voetbalwedstrijden in een café is een openbaarmaking, net als het beschikbaar stellen van een cd-speler en cd's aan hotelgasten. Het laten horen van muziek in de wachtkamer van de tandarts echter niet.[47] Het parallel importeren van smartcards uit andere Europese landen om via abonneetelevisie voetbal te kijken is wél toegestaan. Een verbod daarop is namelijk in strijd met het vrije verkeer van diensten in Europa.[48]

In lijn met de Europese uitspraken oordeelde het Hof Den Haag dat de wijze waarop programma's tegenwoordig via de kabel worden doorgegeven vanuit auteursrechtelijk perspectief geen primaire of secundaire openbaarmaking (of (her)uitzending) vormt.[49] Opmerkelijk was het oordeel van de voorzieningenrechter van de rechtbank Amsterdam over de digitale, niet-geëncrypteerde doorgifte van Nederland 1, 2 en 3 door Digitenne, op verzoek van de Nederlandse Publieke Omroep na afschakeling van het analoge ethersignaal.[50] Hoewel de NPO al voor de doorgifte had afgerekend, werd de interventie van Digitenne beschouwd als een zelfstandige, secundaire openbaarmaking, omdat Digitenne de kanalen op haar website als onderdeel van haar pakket zou aanprijzen.

3.3 Het ijzeren geheugen van het internet

Het EHRM laat een ruime beoordelingsmarge voor de lidstaten voor wat het ziet als een secundaire taak voor de pers: het beschikbaar houden van het historische overzicht van artikelen op internet.[51] De bewaking van de integriteit en publieke toegankelijkheid van actuele krantenarchieven wordt in beginsel onder de bescherming van de vrijheid van meningsuiting gebracht, ook als die krantenarchieven online zijn te raadplegen. Die bescherming lijkt dus ook door te trekken naar de gedigitaliseerde historische kranten, waaronder de kranten uit de periode 1940-1945, die de Koninklijke Bibliotheek medio 2010 op haar 'website historische kranten' plaatste.[52]

Tegenover het beginsel dat de integriteit van archieven moet worden beschermd, staat het beginsel dat iemands reputatie niet tot in de lengte van jaren op internet door een valse beschuldiging of jeugdzondes wordt achtervolgd.[53] In 2009 verbood de rechter GeenStijl om het 'Majesteitfilmpje' te tonen, waarin een studente dronken lallend in beeld was ('Jullie moeten mij majesteit noemen, ik ben de praeses').[54] Het privacybelang van de studente prevaleerde boven het nieuwsbelang van GeenStijl. Het filmpje werd door GeenStijl verwijderd, maar bleef elders vindbaar op het internet en daarvoor bleef de studente dwangsommen claimen. In een executiegeschil oordeelde de rechter dat GeenStijl in theorie aansprakelijk kan zijn voor kopieën elders.[55] Daarvoor moeten de beelden nog wel vindbaar zijn voor de gemiddelde internetter. Dat was niet het geval: alleen door het intypen van de directe URL waren de beelden nog op te roepen. GeenStijl had gedaan wat 'redelijkerwijs van haar verwacht konden worden'.

Een oud-student van de Rijksuniversiteit Groningen verzocht zonder succes verwijdering van zijn persoonsgegevens uit een artikel van het Universiteitsblad dat was opgenomen in een online archief. In een ongelukkig interview werd hij opgevoerd als 'elfdejaarsstudent', wat hem nu hinderde in zijn professionele leven. De Afdeling

bestuursrechtspraak van de Raad van State kwalificeerde de opname in het online archief als een journalistieke (verdere) verwerking van persoonsgegevens, in de zin van art. 3 lid 1 van de Wet bescherming persoonsgegevens (Wbp) dat de eisen en waarborgen van de Wbp grotendeels buiten spel zet. In een belangenafweging op grond van art. 8 EVRM liet de Afdeling het belang van een betrouwbaar en representatief archief prevaleren boven het belang van de voormalig student.[56] Ook een verzoek van een woningbezitter tot verwijdering van een vermelding van de prijsgeschiedenis van zijn te koop staande woning op de website miljoenhuizen.nl faalde; huizenprijzen waren volgens de rechter geen persoonsgegevens.[57] Een ex-werkneemster van de TU Eindhoven verzocht zonder succes verwijdering van een artikel uit het online archief van het *Eindhovens Dagblad*. Daarin werd vermeld werd dat zij wegens een 'gevoelige personele kwestie' op non-actief was gesteld, wat het vinden van een nieuwe baan bemoeilijkte. De voorzieningenrechter achtte deze schade onvoldoende om verwijdering van de website te bevelen, dat zou erin kunnen resulteren dat de krant haar archief steeds zou moeten aanpassen als iemand schade zou ondervinden van een publicatie. Onduidelijkheid blijft bestaan over de vraag of de krant gehouden kan zijn tot een aanvulling of rectificatie bij het artikel: dat was niet verzocht.[58]

3.4 Wikileaks

Julian Assange werd in Nederland vooral bekend door publicatie van de video 'Collateral Murder', waarop te zien is hoe vanuit een Amerikaanse helikopter welbewust op ongewapende Irakese burgers wordt geschoten. Later dat jaar volgde de publicatie van honderdduizenden documenten over de oorlogen in Irak en Afghanistan. In november 2010 begon Wikileaks met het publiceren van meer dan 250 000 gelekte berichten van Amerikaanse ambassades en consulaten. Een deel van het diplomatiek verkeer van de Verenigde Staten lag op straat en de Verenigde Staten oefenden grote politieke druk uit om Wikileaks te stoppen.

In het geval van cablegate lijkt Wikileaks noch op de journalistieke uitingsvrijheid van art. 10 EVRM, noch op de uitsluiting van aansprakelijkheid voor internettussenpersonen aanspraak te kunnen maken. Voor het eerste is zij te passief: vrijwel al het verkregen berichtenverkeer werd gepubliceerd, nauwelijks voorzien van een toetsing, selectie of een redactioneel kader. Voor bescherming als internettussenpersoon lijkt Wikileaks te actief; zij biedt niet alleen een platform voor anderen, maar neemt het voortouw bij publicatie van de documenten.[59] Buruma wees erop dat elke vorm van repressie problematisch is. Acties om de Wikileaks uit de lucht te halen, of de beslissingen van onder andere Visa en Mastercard om financiele transacties te staken leidden tot tegenacties in de vorm van mirror sites en DDoS-aanvallen tegen de bedrijven. Hij wierp de vraag op of je de heraut van een nieuwe tijd moet willen onderdrukken.[60] Wikileaks gaf in ieder geval een impuls aan het publieke debat over de verhouding tussen geheimhouding door de overheid en informatievrijheid. Van Dalen wees erop dat de beveiliging van informatie steeds belangrijker wordt, die beveiliging is bijzonder complex; als iets eenmaal op internet staat kan publicatie niet meer worden tegengehouden. Dat betekent niet dat de overheid al haar informatie beter zou moet beveiligen. De overheid zou enerzijds terughoudend moeten zijn met de opslag van gegevens over burgers, maar anderzijds minder eigen gegevens als vertrouwelijk moeten classificeren en terechte geheimen beter moeten beveiligen.[61]

De overheid zou minder eigen gegevens als vertrouwelijk moeten classificeren en terechte geheimen beter moeten beveiligen

43. Beleidsregels reclame commerciële mediainstellingen (2012), *Stcrt.* 2012, nr. 15338; Beleidsregels sponsoring commerciele mediainstellingen (2012), *Stcrt.* 2012, nr. 15341.
44. Beleidsregels reclame commerciële mediainstellingen (2012), p. 7.
45. Zie: http://www.rijksoverheid.nl/onderwerpen/frequentiebeleid/vastgesteld-beleid/commerciele-radio.
46. Antwoord vragen Schaart en van Miltenburg over de slechte ontvangst van Radio 1, Radio 2, Radio 3, Radio 4, Omroep Drenthe en Q-Music in Noord-Nederland, 21 november 2011, Kamervragen (Aanhangsel) 2011-2012, 2011Z20605.
47. Zie verder D.J.G. Visser, 'Kroniek van de intellectuele eigendom', *NJB* 2012/884 onder verwijzing naar HvJ EU 24 november 2011, C-283/10, *IEF* 10550, B9 10453 (*Circul Globus Bucureti*); HvJ EU 4 oktober 2011, C-403/08 en C-429/08, *IEF* 10278, *B9* 10218 (*Premier League*); HvJ EU 13 oktober 2011, C-431/09 en C-432/09, *IEF* 10332, *B9* 10272 (*Airfield vs. Canal Digital*); HvJ EU 15 maart 2012, C-162/10, *IEF* 11046, *B9* 10942 (*Phonographic Performance vs. Ierland*); HvJ EU 15 maart 2012, C-135/10, *IEF* 11045, *B9* 10941 (*SCF vs. Marco Del Corso*). Zie hierover o.a. M. de Cock Buning en R. Kindt, 'Het Europese Hof doet nieuwe 'mededelingen aan het publiek'', *IER* 2012/33.
48. Zie ook: P.P.J. van Ginneken en R.D. Chavannes, 'De wet van Murphy: het Premier League-arrest en de toekomstige exploitatie van uitzendrechten', *Mediaforum* 2011-11/12, p. 329.
49. Hof Den Haag 10 april 2012, *LJN* BW1078 (NORMA/NL Kabel c.s.), bevestigt Rb. Den Haag 28 januari 2009, *AMI* 2009/p. 163-169 m.nt. K.J. Koelman. Zie ook HR 19 juni 2009, *LJN* BH7602, *AMI* 2010/1, p. 12 m.nt. P.B. Hugenholtz (*BUMA/Chellomedia*); ook besproken in D.J.G. Visser, 'Kroniek van de Intellectuele Eigendom', *NJB* 2010/15, p. 986.
50. Rb. Amsterdam (vzr.) 25 november 2010, *Mediaforum* 2011/2, p. 55. 56 m.nt. D.J.G. Visser (*Cedar c.s./Digitenne*).
51. EHRM 10 maart 2009 (*Times Newspapers/United Kingdom*), *NJ* 2010/109 m.nt. EJD; *Mediaforum* 2009/4, nr. 11, p. 167-169 m.nt. J.V.J. van Hoboken.
52. E.J. Dommering, 'Prima, al die 'foute' kranten op internet: Met deze zoekinstrumenten kan een ontginning van bronnen plaatsvinden die hiervoor ongekend was', *NRC Handelsblad*, Opinie, 25 augustus 2012.
53. A.W. Hins, 'Het ijzeren geheugen van het internet', *Ars Aequi* 2008, juli/augustus, p. 558-564.
54. Rb. Amsterdam (vzr.) 11 september 2009, *LJN* BK1859, *Computerrecht* 2010/nr. 38, p. 72.
55. Rb. Amsterdam 10 februari 2011, *LJN* BP3926.
56. ABRvS 8 september 2010, *Mediaforum* 2010, 11/12, p. 376-378 m.nt. T. Schiphof (*A/CvB Rijksuniversiteit Groningen*).
57. Rb. Rotterdam 5 januari 2010, *Mediaforum* 2010/3, p. 102-104, m.nt. Q. R. Kroes (*B/Schoonderwoerd*).
58. Rb. Amsterdam (vzr.) 19 februari 2010, *Mediaforum* 2010/4, p. 133-136 m.nt. J.P. van den Brink (*X/Eindhovens Dagblad*).
59. B. van der Sloot, 'Wikileaks: te actief voor een webhoster, te passief voor een journalistiek medium', *NJB* 2011/624.
60. Y. Buruma, 'Wikileaks: wat leert het ons echt?', *NJB* 2011/26.
61. O. van Daalen, 'De wereld na Wikileaks' Cablegate', *Mediaforum* 2011/1, p. 1.

4. Technologie en grondrechten

4.1 Privacy

Het Hof 's-Hertogenbosch oordeelde in een civiele zaak tegen Kleintje Muurkrant over de (gevolgen van) toepasselijkheid van de Wet bescherming persoonsgegevens (Wbp) op journalistieke publicaties op internet.[62] Het hof stelde vast dat de Wbp van toepassing was en door Kleintje Muurkant was geschonden, maar ging niet verder dan dit gegeven mee te wegen in de voor onrechtmatige openbaarmakingen 'gebruikelijke belangenafweging' zoals die bekend is uit het *Gemeenteraadslid*-arrest.[63] Annotator Kroes was terecht kritisch over de aangelegde rechtsnorm: kan er, gezien het specifieke regime in de Wbp voor verwerking van persoonsgegevens voor journalistieke doeleinden, na constatering van schending daarvan nog ruimte zijn voor een nadere belangenafweging?

Er was in de verslagperiode veel discussie over het door instanties geautomatiseerd delen van gegevens in het kader van veiligheid en opsporing. Hoe ver dit kan gaan blijkt de proefballon van de Gemeente Amsterdam om bodyscanners op straat in te gaan zetten, als aanvulling op preventief fouilleren.[64] De minister van Binnenlandse Zaken vertelde op het *Journaal* dat zij 'behoorde tot de school van veiligheid vóór privacy', maar het is de vraag of een dergelijke keuze in zijn algemeenheid kan en moet worden gemaakt.[65] Latere kabinetsnotities over privacybeleid[66] en het WRR-rapport over de iOverheid[67] bieden meer nuance. De rechterlijke macht lijkt evenzeer terughoudend als het gaat om het automatisme dat gegevens altijd moeten en kunnen worden gedeeld.[68]

Veel discussie was er over het gebruik van ANPR-gegevens (automatische kentekenregistratie).[69] Ondanks diverse toezeggingen, en in strijd met de Wet bescherming persoonsgegevens, bleken namelijk de zogeheten 'no-hits' (langdurig) te zijn bewaard. Het OM vorderde vervolgens deze gegevens op grond van art. 126nd Sv. Onrechtmatig, zo oordeelde het hof (en in cassatie werd daarover niet geklaagd). Tot bewijsuitsluiting van deze gegevens behoeft het volgens de Hoge Raad echter niet (zonder meer) te leiden. Een privacyschending leidt niet (automatisch) tot schending van het recht op een eerlijk proces.[70]

In de literatuur werd betwijfeld of IP-adressen zijn aan te merken als persoonsgegevens.[71] Het College bescherming persoonsgegevens (CBp) legde aan Google een last onder dwangsom op in verband met de verwerking, ten behoeve van Google's geolocatiediensten, van MAC-adressen en namen van wifi-routers in combinatie met locatiegegevens.[72] De NS moest een dwangsom betalen voor het onzorgvuldig verwerken van reisgegevens van studenten[73] en bracht na een kritisch rapport van bevindingen haar verwerking van OV-chipkaartgegevens voor marketingdoeleinden in overeenstemming met de Wbp.[74] Eerder deed het CBp een onthullend onderzoek naar gegevensuitwisseling tussen opsporingsdiensten en telecommunicatieaanbieders.[75] In de verslagperiode publiceerde de Artikel 29 Werkgroep van Europese privacytoezichthouders diverse andere opinies over het raakvlak tussen techniek en privacy, waaronder over behavioural targeting, gezichtsherkenning, slimme energiemeters, geolocatiediensten op smartphones en cloud computing.[76]

Ondertussen is het wachten op de vaststelling van een nieuwe EU-Verordening ter vervanging van de Privacyrichtlijn 95/46/EG; het Commissievoorstel voorziet onder meer in een verzwaring van de toestemmingsdrempel, een meldplicht voor datalekken, veel hogere boetes en een 'recht om vergeten te worden' van vooralsnog onduidelijke reikwijdte.[77]

4.2 Vrijheid van meningsuiting

De vrijheid van meningsuiting geeft geen recht op toegang tot elk medium. De NOS was volgens de Rechtbank Amsterdam vanwege haar journalistieke vrijheid niet verplicht de Partij voor de Dieren toe te laten tot een verkiezingsdebat.[78] Elsevier maakte volgens de Commissie Gelijke Behandeling geen verboden onderscheid op grond van politieke gezindheid door een man geen toegang meer te geven tot het forum op haar website: haar redactionele vrijheid ging voor.[79]

Joris van Hoboken promoveerde op een proefschrift over de betekenis van de vrijheid van meningsuiting voor de regulering van zoekmachines,[80] dat onder meer ook veel nuttige dingen zegt over de positie van persorganen, internetaanbieders en bibliotheken.

5. Telecommunicatie

Eind 2009 werd een nieuw Europees regelgevingspakket voor de elektronische communicatiesector van kracht. Het pakket bestaat uit twee richtlijnen en een verordening. De Richtlijn Betere Regelgeving 2009/140/EG wijzigt de Kaderrichtlijn, de Toegangsrichtlijn en de Machtigingsrichtlijn. De Richtlijn Burgerrechten 2009/136/EG wijzigt de Universele Dienstrichtlijn en de e-Privacyrichtlijn. De BEREC-Verordening 1211/2009 strekt tot oprichting van een orgaan van Europese regelgevende instanties, een *Body of European Regulators for Electronic Communications (BEREC)*. Inmiddels is het regelgevingspakket door een wijziging van de Telecommunicatiewet geïmplementeerd en in werking getreden.[81] Tijdens het implementatieproces werden twee opvallende amendementen over netneutraliteit en cookies aangenomen, die op 1 januari 2013 in werking zullen treden.

Als gevolg van het amendement-Verhoeven is Nederland de eerste lidstaat waar netneutraliteit wettelijk voorgeschreven is.[82] Het amendement beoogt de keuzevrijheid van eindgebruikers te beschermen en verbiedt aanbieders van openbare elektronische communicatienetwerken die internetdiensten aanbieden om de doorgifte van bepaalde

Het CBp deed een onthullend onderzoek naar gegevensuitwisseling tussen opsporingsdiensten en telecommunicatieaanbieders

Nederland is de eerste lidstaat waar netneutraliteit wettelijk voorgeschreven is

diensten te blokkeren of te belemmeren; bijvoorbeeld het populaire WhatsApp voor instant messaging, of YouTube voor video's. Er zijn slechts vier, limitatief opgesomde, uitzonderingen.[83] Diensten op IP-basis over het eigen netwerk, zoals IPTV, zijn uitgezonderd van de bepaling: aanbieders mogen bandbreedte reserveren voor het eigen IPTV-aanbod. Het momentum achter een netneutraliteitregeling nam sterk toe door de aankondiging van KPN dat zij *deep packet inspection* (DPI) zou toepassen om bepaalde diensten te blokkeren, of in de toekomst slechts tegen betaling aan te bieden. Dat leidde tot Kamervragen en onderzoek door OPTA.[84]

Het amendement-Van Bemmel-Van Dam voorziet in een strikt opt-in regime voor cookies: als cookies worden gebruikt voor het verzamelen van persoonsgegevens is de Wet bescherming persoonsgegevens van toepassing, waaronder het strikte toestemmingsvereiste.[85] De nieuwe bepaling bevat daarnaast bepaalde vermoedens dat persoonsgegevens worden verwerkt, bijvoorbeeld als een tracking cookie wordt geplaatst of uitgelezen om informatie over het internetgebruiker van een eindgebruiker te verzamelen, combineren of analyseren. Ook langs deze weg is het toestemmingsvereiste van de Wbp van toepassing, wat verder gaat dan de (op zichzelf al strikte) cookiebepaling in de e-Privacyrichtlijn. De cookie-bepaling heeft tot de nodige opschudding bij marktpartijen geleid, die zich beklagen dat de bepaling in de praktijk onwerkbaar is.[86] OPTA heeft handhaving van de cookie-verplichting niettemin tot prioriteit voor 2012 bestempeld,[87] al voldoen nog maar weinig websites aan de wettelijke vereisten.[88]

Onderdeel van het pakket was ook de nieuwe Aanbeveling relevante markten van de Europese Commissie, die al in 2007 in werking was getreden. Een belangrijk verschil met de vorige aanbeveling uit 2003 is dat de Commissie de meeste retailmarkten heeft geschrapt, vanwege toenemende concurrentie. OPTA heeft in 2008 al de eerste marktanalysebesluiten op basis van de Aanbeveling genomen, waarvan inmiddels een groot aantal is vernietigd door het College Beroep voor het bedrijfsleven (CBb).[89] Vernietiging geschiedde relatief vaak op fundamentele gronden: maar liefst zes besluiten werden vernietigd wegens gebreken in de marktafbakening. In het geval van de omroeptransmissie heeft OPTA geen herstelpoging meer ondernomen, zij is inmiddels tot het oordeel gekomen dat regulering van deze markt niet meer noodzakelijk is, met name omdat volgens de toezichthouder de overgang naar digitale televisie de machtspositie van de traditionele kabelexploitanten binnen afzienbare tijd zal eroderen.[90] De politiek was daar niet van overtuigd: tijdens het hiervoor beschreven implementatieproces werd het amendement-Van Dam aangenomen, op basis waarvan het analoge standaardpakket beschikbaar moet worden gesteld voor wederverkoop door alternatieve aanbieders.[91]

62. Hof Den Bosch 1 februari 2011, *LJN* BP3921, *Mediaforum* 2011/4, nr. 10, m.nt. Q.R. Kroes (*SDI De Stelling/X*).
63. HR 24 juni 1983, *NJ* 1984/801 m.nt. M. Scheltema.
64. http://www.nu.nl/binnenland/2845674/amsterdam-overweegt-bodyscanners-straat-.html.
65. R.D. Chavannes, 'Het valse veiligheidsdilemma', *Mediaforum* 2010/1, p. 1.
66. *Kamerstukken II* 2010/11, 32 761, nr. 1.
67. *Kamerstukken II* 2011/12, 26 643, nr. 211.
68. Rb. Utrecht 26 augustus 2011, *LJN* BR5923; Hof Amsterdam 18 oktober 2010, *LJN* BO6031.
69. Zie o.a. H.M. Griffioen, 'Automatische nummerherkenning: all systems are go?', *NJB* 2011/459.
70. HR 20 september 2011, *LJN* BR0554 en HR 3 juli 2012, *LJN* BV1800.
71. G.-J. Zwenne, 'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren', *Tijdschrift voor internetrecht* 2011/1, p. 4; G.-J. Zwenne, 'Regulering van IP-adressen (en andere mogelijke identifiers)', *Tijdschrift voor internetrecht* 2011/2, p. 40.
72. CBp 23 maart 2011, kenmerk z2010-01467, http://www.cbpweb.nl/pages/pb_20110419_google.aspx. Co-auteur Chavannes trad in deze zaak op voor Google.
73. CBp, persbericht 13 juni 2012 met verwijzing naar invorderingsbeslissing en eerdere dossierstukken: http://www.cbpweb.nl/Pages/pb_20120613_cbp-dwang-som-ns-studenten-ov-chip.aspx.
74. CBp, persbericht 28 augustus 2012 met verwijzing naar rapport van bevindingen: http://www.cbpweb.nl/Pages/pb_20120828-ov-chipkaart-ns-reisgegevens-marketing.aspx.
75. CBp, persbericht 28 april 2011 met verwijzing naar rapporten van bevindingen inzake het CIOT, politiekorps Haaglanden en de Dienst Nationale Recherche: http://www.cbpweb.nl/Pages/pb_20110428_ciot.aspx.
76. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. Zie ook: L. Viergever, 'Privacy in de clouds', *Tijdschrift voor internetrecht* 2010/3, p. 78.
77. Zie verder het themanummer van *Privacy & Informatie* 2012/3.
78. Rb. Amsterdam (vzr.) 28 februari 2011, *LJN* BP6121.
79. CGB 28 april 2011, http://www.cgb.nl/oordelen/oordeel/221894/volledig. Zie ook de verschillende commentaren op het *NJB*-discussieblog: njblog.nl/2011/05/19/mag-elsevier-reacties-verwijderen-van-web-bezoekers-vanwege-hun-politieke-kleur/.
80. J.V.J. van Hoboken, *Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines*, diss. UvA 2011
81. *Stb.* 2012, 235.
82. *Kamerstukken* 2010/11, 32 549, nr. 17 (amendement Verhoeven).
83. Zie uitgebreider: themanummer netneutraliteit, *Mediaforum* 2012/7-8.
84. Zie: J.M. Titulaer-Meddens, 'Deep Packet Inspection: vloek of zegen?', P&I 2012/1, p. 5 onder verwijzing naar o.a. bijlage bij *Kamerstukken II* 2010/11, 32 549, nr. 44 en nr. 45.
85. *Kamerstukken* 2010/11, 32 549, nr. 39 (gewijzigd amendement Van Bemmel/Van Dam).
86. Zie over de regulering van cookies o.a.: F.J. Zuiderveen-Borgesius, 'Verslag VMC Studiemiddag op 25 juni 2010 over behavioral targeting', *Mediaforum* 2010/10, p. 323-326; M. Bolhuis, 'Regulering van cookies – papier of praktijk?', *Mediaforum* 2011/3, p. 66-75; D. Verhulst, 'Verslag VMC Studiemiddag op 25 november 2011 over de nieuwe cookie-regulering', *Mediaforum* 2012/2, p. 45-47; F.J. Zuiderveen-Borgesius, 'De nieuwe cookieregels: alwetende bedrijven en onwetende internetgebruikers?', *P&I* 2011/1, p. 2-11; B. van der Sloot, 'Het plaatsen van cookies ten behoeve van behavioral targeting vanuit privacyperspectief', *P&I* 2011/2, p. 62-70; K. Crijns en B.W. Schermer, 'Nederlandse cookiewetgeving: wat is de stand van zaken?', *Tijdschrift voor internetrecht* 2012/1, p. 42.
87. OPTA's Focus 2012: internetvrijheid, ongevraagde telemarketing en de zakelijke telecommarkt, zie: http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3566.
88. Verslag rondetafelbijeenkomst over cookiebepaling (i.s.m. DDMA en IAB), 2 augustus 2012, zie: http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3635.
89. Q. Kroes, P. Glazener, 'De rechterlijke toetsing van OPTA's marktanalyses: de tweede ronde', Mediaforum 2012/6, p. 193-204.
90. *Id./* p. 195.
91. *Kamerstukken II* 2010/11, 32 549, nr. 28, *Handelingen II* 2010/11, 95, p. 18.

Op het gebied van handhaving en consumentenbescherming gaven de telemarketingregels uit 2009, waaronder het Bel-me-niet-register, aanleiding tot uiteenlopende, vaak lastig te beantwoorden vragen. Enkele daarvan zijn inmiddels van een antwoord voorzien in sanctiebesluiten van OPTA.[92] Het CBb liet OPTA's besluit om niet handhavend op te treden naar aanleiding van ongevraagde e-mailberichten van de VVD in het kader van de verkiezingen van Provinciale Staten van Overijssel in stand.[93] Ondanks de beginselplicht tot handhaving konden het incidentele karakter en de geringe omvang en ernst van de overtreding het niet-optreden rechtvaardigen. Ook misbruik van sms-diensten bleef in de belangstelling staan.[94] Na aanhoudende kritiek scherpte de Stichting SMS-Gedragscode in maart 2010 haar regels verder aan en in mei 2011 werd een aangescherpte reclamecode SMS-dienstverlening (SMS Reclamecode) van kracht.[95] Volgens de minister gingen de wijzigingen echter niet ver genoeg.[96] In de gewijzigde Regeling Universele Dienstverlening en Eindgebruikersbelangen (RUDE) zijn regels opgenomen met betrekking tot het afsluiten van mobiele telefoons als consumenten het deel van hun factuur dat betrekking heeft op premium sms-dienstverlening niet betalen.[97] Per 1 januari 2012 zijn aanbieders op grond van het RUDE daarnaast verplicht om een 'total opt-out' abonnement aan te bieden, waarin premium SMS-diensten (zonder tussenkomst van klanten) standaard zijn geblokkeerd.[98]

Ten slotte is van belang dat OPTA, de NMa en de Consumentautoriteit per 1 januari 2013 zullen fuseren tot één toezichthouder, de Autoriteit Consument en Markt (ACM).[99]

6. IT-recht en elektronische handel

6.1 Consumentenbescherming

Ter verbetering van de bescherming van de rechten van consumenten vooral ook op internet, zijn in de verslagperiode diverse maatregelen getroffen op zowel Europees als nationaal niveau. De Europese wetgever heeft met de Richtlijn consumentenrechten 2011/83/EU een belangrijke stap gemaakt in de verdere harmonisatie van het consumentencontractenrecht. De richtlijn ziet met name op overeenkomsten op afstand en colportage en beoogt zoveel mogelijk maximumharmonisatie te bereiken.

Met betrekking tot koop op afstand heeft het Hof van Justitie uitgemaakt dat informatie over het herroepingsrecht niet door de verkoper mag worden gegeven door middel van het aanbieden van een hyperlink naar deze informatie, aangezien er dan geen sprake is van 'verstrekken' van informatie.[100] Hoewel dit arrest zag op de uitleg van richtlijn 97/7, die is vervangen door de Richtlijn consumentenrechten, zal hetzelfde vermoedelijk gelden voor de nieuwe richtlijn: art. 6 lid 1 sub h spreekt nog altijd van 'verstrekken' van informatie over het herroepingsrecht. Voor een uitgebreide analyse verwijzen wij naar eerdere artikelen in onder andere dit tijdschrift.[101]

6.2 Koop en software

Het Hof van Justitie wees een principieel arrest over de beschermbaarheid van programmeertalen, bestandsformaten en software-interfaces.[102] Kort daarna heeft het Hof in het baanbrekende *UsedSoft*-arrest[103] duidelijkheid gegeven over toepassing van de uitputtingsregeling in de Softwarerichtlijn.[104] Het Hof stelt voorop dat op grond van art. 4 lid 2 van de richtlijn de eerste verkoop in de EU van een kopie van standaardsoftware door (of met toestemming van) de rechthebbende kan leiden tot verval van het distributierecht voor die kopie. Het downloaden door de klant van een kopie van de standaardsoftware en het sluiten van de licentieovereenkomst tussen de leverancier en de klant voor het gebruik van die kopie kwalificeert, tezamen beschouwd, als verkoop. Voorwaarde is wel dat de kopie met de licentie onbeperkt bruikbaar is en dat een redelijke vergoeding is betaald. Eerder had de Hoge Raad in het *Beeldbrigade*-arrest[105] geoordeeld dat het kooprecht van toepassing is op de aanschaf van standaardsoftware voor onbeperkte tijd en tegen betaling van een bepaald bedrag. Zowel het Hof als de Hoge Raad achtten het irrelevant of de kopie aan de klant beschikbaar is gesteld door een download of op fysieke drager. Het Hof heeft daarbij uitgemaakt dat de tweede verkrijger van de kopie en iedere verdere verkrijger kwalificeren als 'rechtmatig verkrijger' van de kopie in de zin van art. 5 lid 1 van de richtlijn en dat zij de – eventueel verbeterde en bijgewerkte – kopie op hun computer mogen downloaden. Het Hof stelt wel duidelijke grenzen aan de uitputtingsregeling van art. 4 lid 2 van de richtlijn: de uitputtingsregeling strekt zich niet uit tot onderhoudsovereenkomsten en geldt alleen als de eerste verkrijger de gehele licentie aan *UsedSoft* verkoopt als ook zijn eigen kopie van de software onbruikbaar maakt.

Deze twee arresten zullen vermoedelijk verregaande gevolgen hebben voor bedrijven die standaardsoftware verkopen met een eeuwigdurende gebruikslicentie tegen een passende vergoeding. Bedrijven zullen moeten toestaan dat rechtmatige verkrijgers een kopie van hun software met de gebruikslicentie mee doorverkopen aan derden, die op hun beurt ook weer rechtmatig verkrijger worden en als rechtmatige verkrijger de software mogen downloaden. Contractuele bedingen en de betiteling van de overeenkomst als 'licentieovereenkomst' kunnen tegen wederverkoop geen uitkomst bieden, omdat dit het effect van de uitputtingsregel teniet zou doen. Het arrest zal voor bedrijven de overstap naar het *software as a service*-model bij standaardsoftware mogelijk aantrekkelijk maken, aangezien bij dit model niet geraakt wordt door UsedSoft.

Bedrijven zullen moeten toestaan dat rechtmatige verkrijgers een kopie van hun software met de gebruikslicentie doorverkopen aan derden, die op hun beurt weer rechtmatig verkrijger worden en als rechtmatige verkrijger de software mogen downloaden

6.3 Elektronisch verkeer en elektronische handtekening

Op 1 juli 2010 is de Wet schriftelijkheid en elektronisch verkeer[106] in werking getreden. Per 1 juli 2011 is het Besluit elektronische mededelingen in het kader van een verzekeringsovereenkomst,[107] dat het besluit uit 2008 vervangt in verband met de nieuwe wet, in werking getreden. Als gevolg van de wetswijziging kunnen onder meer onderhandse aktes elektronisch worden opgemaakt en zijn de voorwaarden voor het ter beschikkingstellen van algemene voorwaarden langs elektronische weg verruimd.[108] De verruiming van het ter beschikking stellen algemene voorwaarden blijft grenzen kennen. In het arrest-*First data/Attingo*[109] heeft de Hoge Raad uitgemaakt dat een gebruiker aan de wederpartij geen redelijke mogelijkheid tot kennisneming van de algemene voorwaarden (in casu de Fenit-voorwaarden) langs elektronische weg heeft geboden wanneer de algemene voorwaarden op internet kunnen worden gevonden, bijvoorbeeld door een zoekopdracht.

De rechtbank Rotterdam heeft in de zaak-*Bizner*[110] bepaald dat – bij afwezigheid van een andersluidend contractueel beding – het risico van misbruik van een elektronische sleutel (de zogenoemde 'Biz Key') met bijbehorende inlogcodes, die wordt gebruikt als hulpmiddel voor het plaatsen van een (niet-gekwalificeerde) elektronische handtekening, in beginsel voor de gebruiker van de elektronische handtekening is. Dit ligt alleen anders als de gebruiker stelt en bewijst dat het misbruik niet te wijten is aan zijn onzorgvuldigheid,[111] hetgeen vooralsnog niet snel wordt aangenomen.[112]

De kwetsbaarheid van het elektronisch dienstenverkeer werd pijnlijk duidelijk met de hack van certificaatdienstverlener Diginotar. Na de hack van Diginotar beëindigde OPTA haar registratie. OPTA gunde gebruikers vrijblijvend een termijn van twee weken voordat de door Diginotar uitgegeven certificaten werden intrekken. Als gevolg daarvan moesten o.a. advocaten, notarissen en gerechtsdeurwaarders binnen korte tijd een nieuwe certificaatdienstverlener vinden om hen van nieuwe certificaten te voorzien. Een verzoek van de beroepsorganisaties van notarissen en gerechtsdeurwaarders aan OPTA om een langere termijn toe te staan werd door OPTA afgewezen. Ook bij de voorzieningenrechter Den Haag vingen de beroepsorganisaties bot, mede gelet op het belang van veilige en betrouwbare certificaten dat zwaarder weegt dan een tijdelijke kostenstijging.[113]

6.4 Domeinnamen

Op het gebied van het 'domeinnaamrecht' zijn, zeker in vergelijking tot eerdere verslagperioden, weinig baanbrekende ontwikkelingen te melden. In pers- en IE-zaken komt regelmatig een domeinnaam kijken, maar dat leidt doorgaans niet tot bijzondere discussies. De meest interessante zaken zijn misschien wel die waarin geen duidelijke grondslag valt aan te wijzen voor overdracht van een domeinnaam, terwijl het (rechts)gevoel wel zegt dat dat moet gebeuren. De registrant van de domeinnaam ministerpresidentrutte.nl gebruikte deze om door te leiden naar een andere door hem beheerder website, waarop hij diverse vermeende misstanden aan het licht wilde brengen. De rechter oordeelde dat hij zo verwarring veroorzaakte bij mensen die via deze domeinnaam informatie over de Minister-President verwachtten te krijgen, terwijl niet aannemelijk was dat het voor zijn doel noodzakelijk was om juist deze domeinnaam te gebruiken. Daarom kwalificeerde de voorzieningenrechter de registratie en instandhouding van de domeinnaam als misbruik van recht in de zin van art. 3:13 BW en werd de registrant bevolen deze over te dragen.[114]

7. Technologie en strafrecht

7.1 Het begrip 'goed'

Op strafrechtelijk gebied was de beslissing van de Hoge Raad in de *RuneScape*-zaak waarschijnlijk het belangrijkste 'technologische' nieuws binnen deze kroniekperiode. Ondanks de jurisprudentie inhoudende dat 'gegevens' geen 'goed' zijn in vermogensrechtelijke zin,[115] oordeelde de Hoge Raad dat een virtueel amulet en masker in het computerspel RuneScape kunnen worden aangemerkt als een 'goed' en diefstal hiervan mogelijk is.[116] Doorslaggevend was dat een bepaalde mate van 'beschikkingsmacht' bestond en de voorwerpen een

92. Zie voor een gedetailleerde bespreking: G.J. Zwenne, M. van Hooidonk, 'Enige kanttekeningen bij de handhaving van telemarketingregels', *Mediaforum* 2012/6, p. 186-192.
93. CBb 15 juni 2011, *LJN* BQ8708, *JB* 2011/182 m.nt. prof. mr. G. Overkleeft-Verburg; eerder oordeelde het CBb al over rechtsvragen met betrekking tot de handhaving van het spamverbod door OPTA, zie ook: CBb 2 juli 2010, *LJN* BN0534 en CBb 22 januari 2009, *LJN* BH 6932 (over het aan het boetebesluit ten grondslag gelegde feitenmateriaal).
94. Zie o.a.: S. Sanders en L. Wildeboer, 'Toezicht en handhaving bij sms-geschillen', *Mediaforum* 2010/4, p. 117-125.
95. Zie: www.smsgedragscode.nl.
96. *Kamerstukken II* 2009/10, 31 412, nr. 14 en 21.
97. *Stcrt.* 3 maart 2011, nr. 3687.
98. *Stcrt.* 10 juli 2012, nr. 13915.
99. *Kamerstukken II* 33 186.
100. HvJ EU 5 juli 2012, zaak C-49/11, *WPNR* 2012/6932 (*Content Services/Bundesarbeitskammer*).
101. M. Loos, 'Harmonisatie van het consumentencontractenrecht', *NJB* 2011/342; K. Boele-Woelki, A. Keirse, S. Kruisinga, 'Naar een contractenrecht voor de Unie', *NJB* 2011/27; A.L.M. Kierse, S.A. Kruisinga, M.Y. Schaub, 'Nieuws uit Europa: Twee nieuwe wetgevingsinstrumenten: de Richtlijn Consumentenrechten en het gemeenschappelijk Europees kooprecht', *Contracteren* maart 2012/nr. 1; H.A.J. de Jong & G.C.J. Erents, 'Online overeenkomstenrecht 2009-2011', *Tijdschrift voor Internetrecht* 2011/6, p. 172.
102. HvJ EG 2 mei 2012, zaak C-406/10, *Computerrecht* 2012/121 m.nt. M. Truyens (*SAS Institute*).
103. HvJ EU 3 juli 2012, zaak C-128/11 (*UsedSoft*).
104. Richtlijn 2009/24/EG van het Europees parlement en de Raad van 23 april 2009 betreffende de rechtsbescherming van computerprogramma's.
105. HR 27 april 2012, *LJN* BV1301, *NJB* 2012/1107, *NJ* 2012/293 (*De Beeldbrigade/Hulskamp*). Zie ook: R. Rinzema, 'Pleidooi voor het kopen van standaardsoftware', *NJB* 1012/1601.
106. *Stb.* 2010, 222.
107. *Stb.* 2011, 20.
108. Voor een uitgebreide bespreking, zie: R.E. van Esch, 'De Wet schriftelijkheid en elektronisch verkeer en online shopping door consumenten', *Tijdschrift voor Internetrecht*, december 2010/p. 184-187; H.A.J. de Jong & G.C.J. Erents, 'Online overeenkomstenrecht 2009-2011', *Tijdschrift voor Internetrecht* december 2011/p. 172.
109. HR 11 februari 2011 *LJN* BO7108, *NJB* 2011/420 (*First data /Attinga*).
110. Rb. Rotterdam 20 april 2011, *Computerrecht* 2011/159 (*Bizner*).
111. Vgl. HR 19 november 1993, *NJ* 1994/622.
112. Zowel in deze zaak als in een tweede *Bizner*-zaak (Rb. Zutphen 22 februari 2012, *LJN* BX1620) oordeelde de rechtbank dat de zorgplicht was geschonden.
113. Rb. Den Haag (vzr.) 27 september 2011, *NJF* 2011/471.
114. Zie voor een vergelijkbare uitspraak, dit keer over de domeinnaam www.112.nl: Hof Amsterdam 31 juli 2008, *Mediaforum* 2008-11/12, nr. 37 m.nt. R.D. Chavannes (*Staat/Heerink*).
115. HR 3 december 1996, *NJ* 1997/574.
116. HR 31 januari 2012, *LJN* BQ9251.

waarde vertegenwoordigden. Tegelijk met deze uitspraak oordeelde de Hoge Raad dat ook het ontvreemden van sms- en beltegoed als diefstal kan worden gekwalificeerd[117] en in vervolg daarop werd geoordeeld dat ook 'credits' (gebruikseenheden voor mobiele telefonie) gestolen en/of verduisterd kunnen worden.[118]

Het begrip 'goed' is met deze uitspraken definitief op de helling, al betekent deze jurisprudentie nog geenszins dat ieder digitaal 'gegeven' dus ook een 'goed' is. Het is dan ook niet voor niets dat in het wetsvoorstel Computercriminaliteit III, waarvan zoals gezegd al geruime tijd niets meer is vernomen, een bepaling is opgenomen (art. 139e) waarin het bezit van illegaal verkregen gegevens, die nog niet als 'goed' kwalificeren onder de helingbepaling, strafbaar wordt.[119]

Het begrip 'goed' is met deze uitspraken definitief op de helling, al betekent deze jurisprudentie nog geenszins dat ieder digitaal 'gegeven' dus ook een 'goed' is

7.2 Phising en grooming

'Nieuw' in deze kroniekperiode zijn de strafbaarstellingen voor phishing (art. 326 Sr) en grooming (art. 248e Sr). Het is dan ook interessant om te zien hoe daarmee in de praktijk wordt omgegaan. Conclusie: de strijd tegen de vollopende e-mailboxen lijkt moeizaam van de grond te komen (de gepubliceerde uitspraken terzake phising zijn op een hand te tellen) terwijl daarentegen grooming getuige de vele gepubliceerde veroordelingen[120] een interessant en bruikbaar kapstokartikel (b)lijkt voor lastig bewijsbare zedenzaken. Art. 248e Sr, een uitvloeisel van het verdrag van Lanzarote inzake de bescherming van kinderen tegen seksuele uitbuiting uit 2007,[121] stelt strafbaar het benaderen van minderjarigen via internet om een ontmoeting voor te stellen met het oogmerk ontuchtige handelingen te plegen. Daadwerkelijk ontuchtige handelingen hoeven niet te worden bewezen. De strafbaarstelling betreft enkel de communicatiefase, de voorbereiding van (eventueel later) seksueel misbruik.[122]

7.3 Internet en social media

Dat de groei van internet in het algemeen en social media in het bijzonder een nieuwe dimensie geeft aan het strafrecht ondervond Bert Brussen die zich voor even in de vuurlinie van het OM bevond nadat hij een bedreiging aan het adres van Geert Wilders had geretweet, of in dit geval gecopypastet. Weliswaar seponeerde het OM,[123] maar aangetoond werd dat wisselend kan worden gedacht over strafrechtelijke aansprakelijkheid voor internetcontent. De oorspronkelijke schrijver kreeg overigens een werkstraf.[124] Hetzelfde overkwam de twitteraar die de koningin enige onvriendelijke woorden had toegevoegd.[125]

Ook bij een zaak tegen de beheerder van de anti-Wilders Hyve stond de vraag naar de reikwijdte van strafrechtelijke aansprakelijkheid. Onder het groepslogo, een weinig flatteuze foto van de PVV leider, hadden diverse leden van de site bedreigende teksten geplaatst. De beheerder had deze niet verwijderd omdat hij naar eigen zeggen niet wist dat het mogelijk was te reageren op het logo. De rechtbank sprak de beheerder vrij. Nalatigheid levert nog geen strafrechtelijke aansprakelijkheid op, aldus de rechtbank.[126]

Hyves bracht ook een ander juridisch vraagstuk aan het licht, te weten of smaad (art. 261 Sr) gepleegd kan worden via een profiel. Voor smaad is immers 'ruchtbaarheid' noodzakelijk, maar hoeveel 'hyvesvrienden' moet je hebben alvorens het aldus kwalificeert? De meningen waren daarover verdeeld, 12 vrienden was te weinig,[127] 25 was genoeg. De Hoge Raad oordeelde uiteindelijk dat het aantal vrienden irrelevant is, de ruchtbaarheid volgt uit het semi-openbare karakter van de website waarbij de ontvanger van het bericht 'naar eigen inzicht en zonder enige restrictie over de uitlating konden beschikken'.[128]

Overigens is het strafrechtelijk geen bezwaar om te twitteren, hyven, of facebooken via de WiFi van de buren, zo oordeelde het gerechtshof Den Haag in maart 2011 in de zogenoemde *4chan*-zaak.[129] Het meesnoepen met een openstaande verbinding is volgens het hof weliswaar maatschappelijk ongewenst, maar niet strafbaar.

7.4 Hacken

Het spanningsveld tussen maatschappelijk ongewenst en strafbaarheid is, zij het in een spiegelbeeldsituatie, ook aan de orde bij 'hacken'. Strafbaar? Meestal wel. Maatschappelijk ongewenst? Niet altijd. Vermeldenswaard is in dat kader de nieuwe Europese richtlijn over 'aanvallen op informatiesystemen'.[130] De richtlijn maakt een onderscheid tussen crimineel hacken en ethisch hacken.[131] Daar waar de richtlijn beoogt de straffen voor crimineel hacken te verhogen zou de (rechts) bescherming voor ethisch hacken juist moeten worden verbeterd. Het roept de vraag op hoe diverse spraakmakende 'hacks' uit de afgelopen kroniekperiode moeten worden gekwalificeerd. Weinig discussie zal er zijn over de ov-chipkaart kraak,[132] of de hack op het Playstation-Network in 2011. Ook de DigiNotar inbraak zal niet snel als 'ethisch hacken' worden ingedeeld. Minder eenvoudig te beoordelen is de inbraak via een botnet in de mailbox van Jack de Vries door het tijdschrift *Revu*. De scheidslijn tussen ethisch hacken en strafbaar hacken kwam daarin helder aan het licht. De hoofdredacteur werd enerzijds ontslagen van rechtsvervolging t.a.v. de gepleegde computervredebreuk (hetgeen volgens de rechtbank was toegestaan op grond van art. 10 EVRM) maar anderzijds veroordeeld voor het doorsturen van de e-mails.[133]

In de *Toxbot*-zaak werd betoogd dat de beveiliging van de geïnfecteerde computers dermate slecht was (Windows XP kwam er niet goed vanaf), dat geen sprake was van het doorbreken van een beveiliging. Het Hof vond van wel, en de Hoge Raad liet dat oordeel in stand.[134]

De genoemde DigiNotar blies de discussie over de beveiliging van persoonsgegevens overigens nieuw leven in.[135] In reactie hierop nam de Tweede Kamer een motie aan om te komen tot een zogenoemde 'security breach notification'.[136] Wetgeving hiertoe is inmiddels in voorbe-

reiding.[137] Dat de DigiNotar-kwestie slechts een van de vele cybersecurityincidenten van de afgelopen tijd was, bracht het Nationaal Cyber Security Centrum aan het licht in zijn rapport uit juni 2012.[138] Digitale spionage, malwarebesmetting, spam en digitale (identiteits)fraude blijken nog immer een grote bedreiging te vormen voor de overheid en (private) organisaties.

8. Technologie en strafvordering

8.1 Digitaal strafdossier

Dat de rechterlijke macht de technologische ontwikkelingen niet allemaal kan bijbenen blijkt alleen al uit het feit dat er, ondanks diverse pilots, weinig schot lijkt te zitten in de invoering van het elektronische strafdossier. Want hoewel de hoeveelheid papier die nog steeds in strafzaken wordt geproduceerd menig milieuactivist slapeloze nachten zal bezorgen, lijkt een volledig digitale zitting nog ver weg. Voor eenvoudige zaken zit daarin overigens, met de invoering van het Geïntegreerd Processysteem Strafrecht (GPS), meer schot. Via GPS worden strafdossiers steeds meer digitaal aangemaakt en behandeld. Met het gebruik van GPS hangt overigens ook de invoering begin 2011 van het elektronisch opmaken van een proces-verbaal samen.[139] In de nieuwe Wet Processtukken[140] wordt trouwens voor het eerst gerept over digitale verstrekking en kennisname van dossierstukken.

De digitalisering van procesvoering, zowel in het strafrecht als daarbuiten, is een van de kernthema's van de (volgens sommige auteurs weinig innovatieve) Innovatieagenda Rechtsbestel die de minister in oktober 2011 publiceerde.[141]

8.2 Bewaarplicht verkeersgegevens

Dat het spanningsveld tussen enerzijds privacy en anderzijds het bestrijden van criminaliteit een terugkerend thema is bleek tijdens deze kroniekperiode (onder meer) uit de discussie over de bewaarplicht van verkeersgegevens. Ondanks de definitieve invoering van de twaalf maanden bewaarstermijn in september 2009 bleef dit ook in Nederland (zeker in verkiezingstijd) een bediscussieerd onderwerp.[142] Ook het rapport van de Europese Commissie begin 2011 droeg daar aan bij. De bewaarplicht zou weinig opleveren en onvoldoende zou blijken of hiermee daadwerkelijk criminaliteit werd bestreden.[143] De bewaarplicht is overigens ook niet Europabreed ingevoerd. In Duitsland en Roemenië werd deze onwettig verklaard terwijl Oostenrijk en Zweden vanwege privacy-bezwaren de bewaarplicht überhaupt niet hebben geïmplementeerd. Ook de Nederlandse wetgever bleek niet geheel ongevoelig voor de kritiek. Bij wet van 6 juli 2011 is de bewaartermijn in de Telecomunicatiewet voor internetgegevens verkort tot zes maanden.[144]

8.3 Technisch opsporen

De snelle technische ontwikkelingen van de afgelopen jaren hebben ertoe geleid dat bij 'technisch opsporen' opsporingsinstanties steeds vaker de grenzen van haar wettelijke bevoegdheden opzoeken. Een van de oorzaken is het feit dat de factoren die door de wetgever en de jurisprudentie zijn ontwikkeld om de grenzen van opsporingsbevoegdheden aan te geven geënt zijn op voorbeelden uit de fysieke ruimte. Daardoor is het onduidelijk waar concreet de grenzen liggen en hoever men bijvoorbeeld mag gaan in het observeren via of van internet. Zo zijn bijvoorbeeld de meningen verdeeld over de (ongelimiteerde en niet in de wet voorziene) inzet van 'crawlers' of 'spiders' die het internet afstruinen op zoek naar strafbare feiten.[145] Dat dit grijze gebied tot ietwat hilarische situaties kan leiden bleek toen een opsporingsambtenaar in een fraudezaak achterhaalde dat twee gele 'Bubble Club fauteuils' die

'Hacken' strafbaar? Meestal wel Maatschappelijk ongewenst? Niet altijd

117. HR 31 januari 2012, *LJN* BQ6575.
118. HR 17 april 2012, *LJN* BV9064.
119. Zie voor het wetsvoorstel en de Memorie van Toelichting hierop: http://www.rijksoverheid.nl/regering/het-kabinet/ministerraad/persberichten/2010/07/28/hirsch-ballin-versterkt-aanpak-computercriminaliteit.html.
120. Bijvoorbeeld: Rb. Rotterdam 23 augustus 2012, BX5571, Hof Leeuwarden 15 september 2011, BT1553, Rb. Utrecht, 25 oktober 2011, *LJN* BU3200, Rb. 's-Hertogenbosch, 28 december 2011, *LJN* BU9341, Hof 's-Hertogenbosch 7 maart 2012, *LJN* BV8018, Rb. Middelburg, *LJN* BO 2782.
121. Raad van Europa, Verdrag inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, gesloten op 25 oktober 2007, *Trb*. 2008/58.
122. Kool, R. 'Better safe than sorry? Over de legitimiteit van strafbaarstelling van seksueel corrumperen van minderjarigen en grooming', *Delikt en Delinkwent*, december 2010, nr. 10.
123. Zie persbericht OM: http://www.om.nl/actueel-0/nieuws-persberichten/@155743/seponeert-zaak-bert/.
124. Rb. 's-Gravenhage 9 juni 2011, *LJN* BQ7588.
125. Rb. 's-Hertogenbosch 24 augustus 2012, *LJN* BX5364.
126. Rb. Amsterdam 27 augustus 2012, *LJN* BX5755.
127. Hof 's-Hertogenbosch 12 oktober 2009, *LJN* BK5777.
128. Hof Leeuwarden 3 november 2009, *LJN* BK1897. Hoge Raad 5 juli 2011, *LJN* BQ2009.
129. Hof 's-Gravenhage 9 maart 2011, *LJN* BP7080.
130. Richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/*JBZ* van de Raad' De voorgestelde richtlijn is te vinden op: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF.
131. Zie ook Koops, B.J., 'De ethiek van de hacker', *Informatie: Maandblad voor de Informatievoorziening* 2000/42.
132. Rb. Utrecht 8 december 2010, *LJN* BO6723.
133. Rb. 's-Gravenhage 23 november 2009, *LJN* BK4065.
134. HR 22 februari 2011, *LJN* BN9287, ro. 2.4.
135. Zie ook Friederike van der Jagt, 'Iets te melden?', *NJB* afl. 25, p.1713
136. *Kamerstukken* 2011/12, 26 643 nr. 202.
137. Zie brief minister d.d. 6 juli 2012, Meldplicht en interventiemogelijkheden, 251200075/nctv/2012.
138. *Cybersecuritybeeld Nederland*, rapport van het Nationaal Cyber Security Centrum.
139. *Stb*. 2011, 15.
140. Zie voor Kamerstukken omtrent de wijziging van het Wetboek van Strafvordering i.v.m. de herziening regels betreffende de processtukken in strafzaken: *Kamerstukken II* 2009/10, 32 468.
141. 'Innovatieagenda rechtsbestel (#innovatierechtsbestel)', bijlage bij *Kamerstukken II* 2011/12, 33 071, nr. 5; I. Giesen en L.M. Coenraad, 'Innovaties in de (civiele) rechtspleging', *NJB* 2012/882.
142. Wet bewaarplicht telecommunicatiegegevens, *Stb*. 2009, 333.
143. Evaluation report on the Data Retention Directive 2006/24/EC, COM(2011) 225
144. Wet van 6 juli 2011 tot wijziging van de Telecommunicatiewet (…), *Stb*. 2011, 350.
145. Zie J.J. Oerlemans en B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen Politie* anno 2012/p.35 e.v.

De meningen zijn verdeeld over de (ongelimiteerde en niet in de wet voorziene) inzet van 'crawlers' of 'spiders' die het internet afstruinen op zoek naar strafbare feiten

zakelijk waren aangeschaft blijkens Google Earth bij de verdachte thuis in de achtertuin stonden.[146]

Ook de inzet van technische hulpmiddelen in de 'fysieke wereld' zijn vaak niet onomstreden. Zo blijven de meningen verdeeld over de inzet van de IMSI-catcher, een apparaat waarmee opsporingsautoriteiten enerzijds het telefoonnummer van een verdachte kunnen achterhalen indien diens verblijfplaats bekend is, maar anderzijds ook de verblijfplaats kunnen achterhalen indien het telefoonnummer bekend is. Daar waar de bevoegdheid tot het verkrijgen van het telefoonnummer expliciet is geregeld in art. 126nb Sv, ontbreekt een specifieke bevoegdheid voor de spiegelbeeldsituatie. Die wordt door menig rechtbank 'ingelezen' in art. 2 Politiewet, nu een dergelijke inzet wordt vergeleken met een niet-stelselmatige observatie.[147]

Ook de inzet van de 'stealth-sms' roept discussie op. Het betreft een stil smsje dat wordt gestuurd naar een verdachte (wiens telefoon vaak ook getapt wordt), zonder dat deze dit in de gaten heeft. Het doel van zo'n sms is het lokaliseren van een mobiele telefoon. Ook hier worstelen rechters zichtbaar met de wettelijke basis voor de inzet van het middel. De ene rechtbank ziet deze in art. 2 Politiewet,[148] al dan niet aangevuld met art. 141 Sv,[149] terwijl andere rechtbanken menen dat art. 126n of 126m Sv hiervoor grondslag biedt.[150]

Ophef ontstond er in deze kroniekperiode over het gebruik van spysoftware door opsporingsdiensten waarmee heimelijk kan worden meegekeken met een webcam. Het gebruik hiervan kwam aan het licht nadat hierover in Duitsland een politieke rel was ontstaan. In reactie op Kamervragen zei de minister niet veel meer dan dat de software werd gebruikt;[151] de gebruikte software moet geheim worden gehouden om een optimale inzet van het middel te garanderen. De wettelijke basis voor de inzet van deze software is echter onduidelijk. Volgens de minister kan deze worden gevonden in art. 126l Sv (het opnemen van vertrouwelijke communicatie) maar totdat een rechter zich hierover heeft uitgelaten blijft dat standpunt slechts een standpunt.

Dat het OM vaker worstelt met de juridische (on)mogelijkheden van het wetboek van strafvordering bleek ook in de zaak van de Europese Internetbeheerder RIPE NCC. RIPE NCC ontving in november 2011 een bevel tot bevriezing van diverse IP-registraties in het belang van een Amerikaans strafrechtelijk onderzoek naar een DNS-changer botnet. Een bevel dat niet zozeer was gericht op het opsporen van strafbare feiten, maar met name op het voorkomen (en herstellen) hiervan. Bij gebreke van enige specifieke wettelijke basis grondde het OM haar bevel op het kapstokartikel 2 Politiewet. In de bodemprocedure die RIPE NCC is begonnen zal blijken in hoeverre een dergelijk bevel rechtmatig is.[152]

Tot slot kan de inzet van de telefoontap niet onbesproken blijven in deze kroniek. Ook dit jaar weer is Nederland, zo bleek ook uit een rapport van het WODC, koploper telefoontap. In 2011 werden er 24 718 taps geplaatst, een lichte stijging ten opzichte van het jaar 2010.[153] Ter vergelijking: in de Verenigde Staten werden over dezelfde periode in totaal 2 732 taps aangelegd[154] en een kleine rekensom leert dan ook dat Nederland per inwoner bijna honderd keer meer tapt dan de VS. De minister erkent dat het steeds moeilijker wordt om volledige informatie via de tap te verkrijgen omdat er steeds meer (nieuwe) vormen van communicatie ontstaan. Desalniettemin oordeelt hij dat nut en noodzaak van de telefoontap nog altijd vaststaan, dat de telefoontap omgeven wordt door voldoende wettelijke waarborgen en mogelijkheden voor de inzet van de telefoontap verder uitgebreid dienen te worden.[155]

9. Afsluitende opmerkingen

Over een niet bestaand rechtsgebied als technologierecht kunnen moeilijk alomvattende conclusies worden getrokken. De technologische vooruitgang bezorgde de uitvoerende, wetgevende en rechtsprekende machten veel moeilijke vragen en de respons was wisselend en aarzelend. Het is geen toeval dat bij de afgelopen verkiezingen steeds meer partijen een forse internetparagraaf in hun verkiezingsprogramma hadden opgenomen, waarin een 'open en vrij internet' meer aandacht krijgt dan 'handhaving'. Er dient zich een generatie *digital natives* aan, van burgers die met internet zijn opgegroeid en zich afvragen waarom die digibete stenentijdperkjuristen zoveel dode bomen nodig hebben om met hopeloze analogieën vragen te lijf te gaan die zij op basis van eigen kennis en intuïtie al kunnen beantwoorden. De komende verslagperioden zullen zij hun stempel zetten op de complexe afwegingen van botsende (grond)rechten die in de digitale informatiesamenleving onvermijdelijk zijn. •

146. Rb. Den Haag 23 december 2011, *LJN* BU9409.

147. Voor rechtspraak omtrent de IMSI-catcher: zie *LJN*: BH0748 en ook Hof Arnhem 24 januari 2012, *LJN* BV3076.

148. Rb. Amsterdam, 8 maart 2011, *LJN* BQ9049, Hof Arnhem, 24 juni 2012 *LJN* BV3076.

149. Rb. 's-Hertogenbosch 14 juni 2012 *LJN* BW8633.

150. Rb. Amsterdam 31 mei 2011, *LJN* BQ9049. Zie verder over de stealth-sms: *LJN* BW8610, BW8620, BW8629, *LJN* BP7233.

151. Brief minister inzake Beantwoording Kamervragen over het gebruik van spysoftware, 194389.

152. http://www.ripe.net/internet-coordination/news/dagvaarding-ripe-ncc-staat. De auteurs treden in deze zaak op voor RIPE NCC.

153. G. Odinot, D. de Jong, J.B.J. van der Leij, C.J. de Poot, E.K. van Straalen, *Het gebruik van de telefoon- en internettap in de opsporing*, Boom Lemma Uitgevers 2012.

154. http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table7.pdf.

155. Brief van de Minister van Justitie, Evaluatie van hoofdstuk 13 van de Telecommunicatiewet, 30 517 nr. 25.