

# Kroniek technologie en recht

Remy Chavannes en Niels van der Laan<sup>1</sup>

Tijdens de verslagperiode brachten de onthullingen van Edward Snowden over de digitale spionageprogramma's van de Amerikaanse en Britse veiligheidsdiensten een maatschappelijk debat teweeg over de verhouding tussen veiligheid en (digitale) grondrechten. De kritische aandacht voor de al dan niet vrijwillige medewerking van grote Amerikaanse technologiebedrijven aan surveillance en hun eigen omgang met persoonsgegevens,<sup>2</sup> was onderdeel van een bredere tegenreactie onder de noemer 'de Oude Wereld laat zich niet langer koloniseren door Silicon Valley'. Nederlandse internetaanbieders werden massaal bevolen de toegang tot de *file sharing* website *The Pirate Bay* te blokkeren, maar toen dat geen effect bleek te hebben op inbreukmakende bestandsuitwisseling werd de blokkade weer opgeheven. Het auteursrecht speelde ondertussen nog iets verder weg door het elektronisch vergiet.<sup>3</sup>

## 1. Inleiding

De grootste ontwikkeling van de afgelopen twee jaar is echter misschien wel de toegenomen invloed op de rechtsontwikkeling van het Hof van Justitie. Het Hof benadert juridische problemen in het technologie- en informatierecht al langer als botsingen van conflicterende grondrechten, waaronder met name vrijheid van meningsuiting, privacy, intellectuele eigendom en vrijheid van onderneming. Waar het Hof zich in het verleden vaak beperkte tot de opdracht dat nationale wetgevers en rechters een juist evenwicht moesten verzekeren,<sup>4</sup> is het in toenemende mate geneigd om zelf knopen door te hakken. Alleen al in de eerste helft van 2014 heeft het Hof privé-downloads uit illegale bron verboden,<sup>5</sup> *hyperlinken* toegestaan,<sup>6</sup> de Richtlijn bewaarplicht telecommunicatiegegevens vernietigd<sup>7</sup> en in de bestaande Privacyrichtlijn uit 1995 een recht om door zoekmachines 'vergeten te worden' gelezen waarvan de mogelijke invoering in een toekomstige Priva-

cyverordering nog voorwerp was van verhit debat.<sup>8</sup>

In onze vorige kroniek hebben wij 'technologie en recht' omschreven als een tijdelijke wachtkamer voor ontwikkelingen die nog niet door hun eigen rechtsgebied zijn opgehaald,<sup>9</sup> en ook de in deze kroniek beschreven ontwikkelingen laten zich weer voor een groot deel kwalificeren als in wezen *commune* kwesties met toevallig technische casuïstiek. Wij blijven dus sceptisch over de waarde van 'technologie en recht' als ordenend thema. In het *NJB* en andere bladen verschenen tijdens de kroniekperiode regelmatig artikelen over de juridische status van een bepaalde nieuwe dienst, product of ontwikkeling, zoals de auteursrechtelijke aspecten van online massacursussen,<sup>10</sup> de privacyrechtelijke aspecten van drones,<sup>11</sup> strafrechtelijke aansprakelijkheid voor handelen onder invloed van een gehackt hersenimplantaat<sup>12</sup> en een *NJB*-themanummer over *neurolaw*,<sup>13</sup> zonder dat daarmee een beeld ontstaat van een samenhangend, objectief af te bakenen rechtsge-

### 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 Tineke van de Bunt (Brinkhof), Marilyn Fikenscher (De Roos & Pen), Brendan Newitt (De Roos & Pen) en Axel Armbak (Instituut voor Informatierecht) voor hun bijdragen respectievelijk suggesties.

### Noten

2. Zie bijv. 'Big Tech at Bay', *Financial Times* 14 september 2014, <http://on.ft.com/1qDAQqu>.

3. E.J. Dommering, 'Het auteursrecht spoelt weg door het elektronisch vergiet', *Computerrecht* 1994, p. 109-113.

4. Zie bijv. HvJ EU 29 januari 2008, C-275/06, *NJ* 2009/551, m.nt. PBH, (*Pro-musicae*). Zie voor een recente Nederlandse toepassing van horizontale afweging van informatiegondrechten: Rb. Amsterdam (vzr.) 10 april 2013, *Mediaforum* 2013/20, afl. 7/8, m.nt. R.D. Chavannes, (*Four One Media vs. Staat*: toestemming Staat vereist voor gebruik politiestrepen in TV-serie?).

5. HvJ EU 10 april 2014, C-435/12, (*ACI Adam vs. ThuisKopie*).

6. HvJ EU 13 februari 2014, C-466/12, *AMI* 2014/7, p. 85 m.nt. K.J. Koelman, (*Svensson vs. Retriever*).

7. HvJ EU 8 april 2014, C-293/12, (*Digital Rights Ireland*).

8. HvJ EU 13 mei 2014, C-131/12, *Computerrecht* 2014/115 m.nt. P. Van Eecke & A. Cornette (*Google Spanje vs. Costeja*).

9. Zie nader onze vorige kroniek *NJB* 2012/2022, afl. 35, p. 2512.

10. D.J.G. Visser & C.J.S. Vrendenburg, 'Net

als in de film: Massive Open Online Courses (MOOCs) en auteursrecht', *NJB* 2013/2449, afl. 42, p. 2912-2919.

11. B.W. Schermer & M. van der Heide, 'Privacyrechtelijke aspecten van drones', *NJB* 2013/1605, afl. 27, p. 1773-1779.

12. J. Slobbe, B. Wallage & S. Verberk, 'Culpa in causa in technica: een verkenning van de schuldvraag in het strafrecht bij een gehackt hersenimplantaat', *Computerrecht* 2014/114.

13. *NJB*-themanummer 'Neurolaw in Nederland', *NJB* 2013/2611-2618, afl. 45,

bied. Technologische ontwikkelingen raken alle onderdelen van maatschappij en recht, van televisie<sup>14</sup> tot toezicht,<sup>15</sup> maar niet op een dermate eenvormige snelheid of wijze dat een horizontale benadering voor de hand ligt. Zelfs een beperkter deelgebied zoals 'internetrecht' omvat vooral ontwikkelingen die ook aan de orde komen in de traditionele kronieken van onder meer het vermogensrecht, strafrecht, procesrecht, bestuursrecht, intellectuele eigendom en grondrechten. De 'internetjurist' zou dus van al die markten thuis moeten zijn; aangezien geen jurist dat kan zijn, heeft ieder zijn eigen internetrecht. Het is niet evident dat de rechtsvraag of *bitcoin* moet worden aangemerkt als geld of als ruilmiddel,<sup>16</sup> behoort tot hetzelfde rechtsgebied als de auteursrechtelijke kwalificatie van een *embedded hyperlink*.<sup>17</sup> Het diffuse en onzelfstandige karakter van het internetrecht blijkt, om dezelfde redenen, uit de uiteenlopende afbakening die in verschillende kronieken wordt gehanteerd: waar sommigen de nadruk leggen op ontwikkelingen op het gebied van IT-, contracten- en consumentenrecht, concentreren anderen zich op ontwikkelingen op het gebied van auteurs-, media- en privacyrecht.<sup>18</sup>

### Juist waar de casuïstiek door technologische innovatie razendsnel verandert, moeten rechtsbeoefenaren steeds terug naar de basis van hun vakgebied

Omgekeerd roepen belangrijke technologische ontwikkelingen doorgaans (rechts)vragen op die zich niks aantrekken van bestaande grenzen tussen rechtsgebieden, zodat een multidisciplinaire analyse vereist is. En wat er ook zij van het bestaansrecht, het nut of de reikwijdte van technologierecht, internetrecht e.d. als zelfstandig vakgebied, 'nieuwe technologie' is op zich een instructieve lens voor de beschouwing van ontwikkelingen in de verschillende rechtsgebieden. Juist waar de casuïstiek door technologische innovatie razendsnel verandert, moeten rechtsbeoefenaren steeds terug naar de basis van hun vakgebied. Iedere nieuwe digitale distributietechniek roept opnieuw de vraag op: waar is het auteursrecht voor bedoeld? Iedere nieuwe opsporingstechniek roept opnieuw de vraag op: hoe verhoudt de vrijheid van het individu zich tot de veiligheid van het collectief? Terugnereende vragen over de medewerkings- en informatieplichten van internetaanbieders roepen de klassieke civielrechtelijke vraag op: in hoeverre is men rechtens verplicht behulpzaam te zijn? Het is geen toeval dat het Hof van Justitie steeds de belangenafweging vooropstelt. En juist waar conflicterende belangen moeten worden afgewogen, komt het veelal aan op proportionaliteit en waarborgen; in alle gevallen valt een verstandige en duurzame beslissing daarom alleen te nemen met verstand van de werking en consequenties van de desbetreffende techniek.

Om overlap met andere kronieken enigszins te beperken hebben wij in deze kroniek de nadruk gelegd op technische ontwikkelingen die wezenlijke rechtsvragen oproepen en juridische ontwikkelingen die een interessant licht werpen op de receptie van technologische innovatie in het gewone recht. Dat betekent relatief veel aandacht voor rechtsgebieden waarin de huidige rechtsontwikkeling grotendeels wordt bepaald door technologische ontwikkelingen, zoals auteursrecht en privacyrecht, en nagenoeg geen aandacht voor rechtsgebieden die naar hun aard bestaan uit de regulering van techniek, zoals octrooirecht en telecommunicatierecht. Ook overigens hebben wij noodgedwongen vele onderwerpen onbesproken gelaten die onder enige definitie van 'technologie en recht' behandeld hadden kunnen worden.

#### 2. Auteursrecht

Hoe om te gaan met nieuwe reproductie- en distributietechnieken is een terugkerend thema in de geschiedenis van het auteursrecht.<sup>19</sup> Op het jubileumcongres van het Instituut voor Informatierecht (IvIR) in juli 2014 analyseerde de Google-auteursrechtjurist Fred von Lohmann de discrepantie in auteursrechtelijke behandeling van bepaalde functionaliteiten (zoals dataopslag of tv-opname), al naar gelang die wordt geleverd als fysiek product (harde schijf, videorecorder) of als clouddienst (online opslagdienst, netwerk-PVR).<sup>20</sup> De volgende dag citeerde prof. James Boyle (Duke Law) uit verhitte toespraken over de auteursrechtelijk status van een nieuwe reproductietechniek.<sup>21</sup> Ze bleken te komen uit debatten over de fonogram uit 1906, maar zowel de toon als de inhoud hadden naadloos gepast in hedendaagse debatten over het 'downloadverbod' of de auteursrechtelijke status van clouddiensten. Volgens Boyle was het huidige internet er niet geweest als de VS en de EU in de jaren negentig niet op het laatste moment hadden afgezien van het plan om internettussenpersonen rechtstreeks aansprakelijk te houden voor alle openbaarmakingen en veelevoudigingen via hun netwerken. Min of meer toevallig zijn zij toen uitgekomen op de nu nog vigerende aanpak, zoals verankerd in de Richtlijn Elektronische handel, waarbij neutrale tussenpersonen worden gevrijwaard van aansprakelijkheid en technische beschermingsmaatregelen een extra juridische bescherming krijgen. Volgens Boyle laat de huidige strijd over auteursrecht en auteursrechtshandhaving op internet zich begrijpen als een poging van de rechthebbers om een nieuw evenwicht te forceren.

Het Europese auteursrechtbeleid is er al geruime tijd op gericht om zowel 'digitale creatie' als 'de digitale economie' te stimuleren, maar ondertussen brokkelt het gezag van het auteursrecht verder af, zeker onder jongere internetgebruikers die het auteursrecht steeds meer zien als een archaische hindernis. Eurocommissaris Kroes heeft in verschillende speeches, waaronder tijdens hetzelfde IvIR-congres,<sup>22</sup> gewezen op de dreigende irrelevantie van het auteursrecht, maar heeft geringe concrete vooruitgang kunnen boeken. De ruim 9500 reacties op een Commissieconsultatie over de Europese auteursrechtwetgeving bieden ook weinig uitzicht op spontane consensus tussen makers, gebruikers en tussenpersonen.<sup>23</sup> De nieuwe Commissievoorzitter Jean-Claude Juncker heeft zijn vicevoorzitter voor de Digitale Interne Markt, Andrus Ansip, in zijn *mission letter* de ambitieuze en in potentie revolutionaire opdracht mee-

gegeven om nationale silo's in telecomregulering, auteursrecht- en privacywetgeving te doorbreken. Tegelijkertijd blijkt de gevoeligheid en tweeslachtigheid van Ansips taak uit zijn opdracht op auteursrechtgebied: 'modernising copyright rules in the light of the ongoing digital revolution – taking full account of Europe's rich cultural diversity.'<sup>24</sup>

### 2.1 Reikwijdte van het digitale openbaarmakingsrecht

Een van de vragen in de Commissie-consultatie betrof de auteursrechtelijke status van *hyperlinken* en ook op dit punt antwoordden de verschillende categorieën van respondenten in overeenstemming met hun eigen belang: individuele en institutionele gebruikers en tussenpersonen vinden dat *hyperlinken* (vrijwel) altijd moet kunnen, individuele en collectieve rechtenhouders menen dat het (in elk geval in sommige gevallen) onder hun verbodsrecht valt. De Nederlandse rechtspraak worstelde ondertussen met de relevantie en toepassing van de criteria 'interventie', 'nieuw publiek' en 'winstoogmerk', die het Hof van Justitie had geïntroduceerd in een reeks arresten over het concept 'mededeling aan het publiek'. De Haagse voorzieningenrechter oordeelde eind 2012 dat een webportal met *embedded* links naar de audiostreams van alle Nederlandse radiozenders een inbreukmakende openbaarmaking opleverde.<sup>25</sup> Dat de browser van de gebruiker na het aanklikken van een link de desbetreffende radiostreams zelf ophaalde bij de mediaservers van de omroepen maakte volgens de rechtbank niet uit, omdat de website *Nederland.FM* zo was ingericht dat de radiostreams vervolgens werden beluisterd 'in het kader van' die website en dus door die website aan het publiek werden 'gepresenteerd'.

In 2013 oordeelde het Hof Amsterdam in twee verschillende zaken dat het aanbrenge van een hyperlink naar inbreukmakend materiaal elders op het internet (uitwerkingen van wiskundeopgaven respectievelijk een voorzichtige uitgelekte *Playboy*-reportage van Britt Dekker) géén

auteursrechtinbreuk opleverde, maar wel een onrechtmatige daad.<sup>26</sup> In beide gevallen legt het Hof aan zijn beslissing ten grondslag dat de gedaagde (een wiskundeleraar respectievelijk *GeenStijl*) het materiaal niet zelf op internet heeft gezet en evenmin door bijzondere technische faciliteiten mogelijk heeft gemaakt dat derden ervan kennis nemen (geen openbaarmaking); maar wel onzorgvuldig handelt door internetgebruikers in vergaande mate behulpzaam te zijn (in de *Playboy*-zaak: te faciliteren en enthousiasmeren) bij het raadplegen van het materiaal. Begin 2014 hakte het Hof van Justitie enkele knopen door, door in het *Svensson*-arrest te oordelen dat een hyperlink weliswaar een 'mededeling aan het publiek' was, maar niet onder het verbodsrecht van de rechthebbende viel omdat deze geen 'nieuw publiek' bereikt.<sup>27</sup> De wijze van *hyperlinken* – 'gewoon', 'embedded', of anders – maakt niet uit. De stellige interpretatie van Visser in zijn IE-kroniek, dat uit het *Svensson*-arrest volgt dat hyperlinks naar materiaal dat niet met toestemming van de rechthebbenden is gepubliceerd *dus* inbreukmakend zouden zijn, berust ons inziens op een onjuiste lezing van het arrest. De hyperlink-controverse is maar één verschijningsvorm van een veel ruimere onduidelijkheid over de reikwijdte van het openbaarmakingsbegrip (in de terminologie van de Auteursrechtrichtlijn: 'mededeling aan het publiek'), die Visser uitgebreid behandelt.

## 3. Internettussenpersonen

### 3.1 Aansprakelijkheid

In het internettussenpersonenrecht gaat het veelal om de vragen a. wanneer een tussenpersoon aansprakelijk is voor eigen handelen, b. wanneer een tussenpersoon aansprakelijk is voor het handelen van zijn klanten, en c. wanneer een niet-aansprakelijke tussenpersoon verplicht is een derde behulpzaam te zijn.<sup>28</sup> De logische voorvraag is

p. 3129-3161.

14. [www2.deloitte.com/nl/nl/pages/Over%20Deloitte/articles/technologie-verander-tv-sector-radicaal.html](http://www2.deloitte.com/nl/nl/pages/Over%20Deloitte/articles/technologie-verander-tv-sector-radicaal.html).

15. B. Leeuw, F.L. Leeuw & M. Morawski, 'Evidence-based toezicht en internet: goed gereedschap is het halve werk', *Tijdschrift voor Toezicht* 2013/4, afl. 3, p. 67-75.

16. Rb. Overijssel 14 mei 2014, ECLI:NL:RBOVE:2014:2667. Het antwoord is overigens dat bitcoin slechts een ruilmiddel is. Dat maakte nogal wat uit, omdat de eiser daardoor geen koerswijzigingsschade kon claimen. De zaak ging over de aankoop van 2750 bitcoin, waarvan de 'ruilwaarde' tijdens de duur van de procedure opliep van ruim € 22 000 tot (momenteel) bijna € 1 miljoen.

17. Rb. Den Haag (vzr.) 19 december 2012, *IER* 2013/38 (*Buma Stemra vs. X, Nederland.FM*), waarover nader in par. 2.1.

18. Zie bijv. H.A.J. de Jong & G.C.J. Erents, 'Online Overeenkomsten en meer', *Tvl* 2013-5/6, p. 141-152; de Kroniek Internetrecht 2012-2013 van Amout Engelfiet

(<http://blog.iusmentis.com/kroniek-internetrecht-201213/>); en het Jaaroverzicht Internetrecht 2013 van advocatenkantoor SOLV ([www.solv.nl/weblog/jaaroverzicht-internetrecht-2013/19733](http://www.solv.nl/weblog/jaaroverzicht-internetrecht-2013/19733)).

19. Voor een mooie verzameling historische voorbeelden, zie: B. Sherman & L. Wiseman (red.), *Copyright and the Challenge of the New*, Alphen a/d Rijn: Kluwer 2012. De meest recente ontwikkelingen worden behandeld door D.J.G. Visser in zijn 'Kroniek intellectuele eigendom', *NJB* 2014/794, afl. 15, p. 1008-1010.

20. F. von Lohmann, 'Copyright as innovation policy', lezing op *Information Influx* congres op 3 juli 2014, [www.youtube.com/watch?v=p87w0vyMTW0](http://www.youtube.com/watch?v=p87w0vyMTW0), mede onder verwijzing naar de recente Aereo-beslissing van de US Supreme Court inzake Aereo van 25 juni 2014: 573 US, 2014, (*American Broadcasting Cos. vs. Aereo, Inc.*).

21. J. Boyle, 'Intellectual property: two pasts and a future', lezing op *Information Influx* congres op 4 juli 2014, [www.youtube.com/watch?v=gFDA-G\\_VqHo](http://www.youtube.com/watch?v=gFDA-G_VqHo).

[watch?v=gFDA-G\\_VqHo](http://www.youtube.com/watch?v=gFDA-G_VqHo).

22. Neelie Kroes, 'Our single market is crying out for copyright reform', lezing op *Information Influx* congres op 2 juli 2014, [http://europa.eu/rapid/press-release\\_SPEECH-14-528\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-14-528_en.htm).

23. Europese Commissie, DG Interne Markt, 'Report on the responses to the Public Consultation on the Review of the EU Copyright Rules', juli 2014, [http://ec.europa.eu/internal\\_market/consultations/2013/copyright-rules/docs/contributions/consultation-report\\_en.pdf](http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/docs/contributions/consultation-report_en.pdf).

24. *Mission Letter* van Jean-Claude Juncker aan Andrus Ansip d.d. 10 september 2014, [http://ec.europa.eu/about/juncker-commission/docs/ansip\\_en.pdf](http://ec.europa.eu/about/juncker-commission/docs/ansip_en.pdf).

25. Rb. Den Haag (vzr.) 19 december 2012, *IER* 2013, 38 (*Buma Stemra vs. X, Nederland.FM*).

26. Hof Amsterdam 15 januari 2013, *IER* 2013, 39 (*X vs. Noordhoff*); Hof Amsterdam 19 november 2013, *Computerrecht* 2014/39 m.nt A.R. Lodder. Co-auteur Chavannes

treedt in deze zaak op voor *GeenStijl*.

27. HvJ EU 13 februari 2014, C-466/12, *AMI* 2014/7, p. 85 m.nt. K.J. Koelman (*Svensson vs. Retriever*).

28. Zie o.a. T. van der Linden, 'Het is niet goed of het deugt niet: de juridische positie van internet tussenpersonen is onbevredigend!', *Tvl* 2014/1 p. 4-9; J.B. Nordemann, 'Liability for Copyright Infringements: Host Providers (Content Providers) – The German Approach', 2011, *JIPITEC* 37; A. Tsoutsanis, 'Privacy and piracy in cyberspace: justice for all', *Journal of Intellectual Property Law & Practice* 2013, vol. 8, issue 12, p. 952-956. U. Kohl, 'Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)', *International Journal of Law and Information Technology*, vol. 21, no. 2, 2013, p. 187-234; en 'Google: the rise and rise of online intermediaries in the governance of the Internet and beyond – Connectivity Intermediaries', 2012, *26 International Review of Law, Computers & Technology* 185.

steeds of een bepaalde onderneming wel kwalificeert als tussenpersoon, of veeleer zelf informatieaanbieder is.

Het EHRM wees een controversieel arrest over de aansprakelijkheid van een nieuwswebsite voor onder een bericht geplaatste lezersreacties.<sup>29</sup> De website publiceerde een genuanceerd en zorgvuldig artikel over een veerdienstbedrijf en haar eigenaar L. Daaronder plaatsten vervolgens zo'n 200 veelal minder genuanceerde lezers reacties. Delfi verwijderde er zo'n twintig op verzoek van L., maar L. eiste ook schadevergoeding. Na een slepende nationale rechtsgang, waarin het vooral ging over de toepasselijkheid van het vrijwaringsregime voor diensten van de informatiemaatschappij (vergelijk artikel 6:196c BW), werd uiteindelijk een immateriële schadevergoeding toegekend van € 320. Delfi klaagde bij het Hof dat de beslissing om haar aansprakelijk te houden voor berichten van haar gebruikers een schending opleverde van artikel 10 EVRM.

In zijn arrest gaat het EHRM de vraag over de toepasselijkheid van de E-commerce richtlijn uit de weg: zijn taak is niet de interpretatie van nationale of EU-wetgeving over te doen, maar te oordelen of die interpretatie door de nationale rechter verenigbaar is met het EVRM. Het onderkent dat de boete een beperking is van artikel 10 EVRM, maar meent dat die dient ter bescherming van de reputatie van eigenaar L.; de beoordeling van de noodzakelijkheid van de inmenging is een kwestie van belangenafweging. Het Hof stelt vast dat de desbetreffende lezersreacties diffamerend waren, oordeelt dat Delfi had kunnen weten dat het artikel (over staking van bepaalde veerdiensten) de nodige boze reacties zou kunnen oproepen en dat er dus een bovengemiddeld hoog risico op diffamerende reacties was, en koppelt daaraan het gevolg dat Delfi bovengemiddeld waakzaam had moeten zijn. Onder die omstandigheden was een (deels geautomatiseerd) *notice-and-takedown* systeem niet noodzakelijkerwijs voldoende. Het Hof hecht ook belang aan de zeer lage toegekende schadevergoeding van € 320 en concludeert:

*'Based on the above elements, in particular the insulting and threatening nature of the comments, the fact that the comments were posted in reaction to an article published by the applicant company in its professionally-managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to avoid damage being caused to other parties' reputations and to ensure a realistic possibility that the authors of the comments will be held liable, and the moderate sanction imposed on the applicant company, the Court considers that in the present case the domestic courts' finding that the applicant company was liable for the defamatory comments posted by readers on its Internet news portal was a justified and proportionate restriction on the applicant company's right to freedom of expression.'*

De uitspraak oogstte felle kritiek van (online) uitgevers en uitingsvrijheidsactivisten. Volgens Dirk Voorhoof 'doorprijkt [het Hof] de illusie dat uitgevers of forumbeheerders van aansprakelijkheid gevrijwaard blijven als zij onrechtmatige of strafbare inhoud na kennisgeving onmiddellijk van hun site verwijderen'.<sup>30</sup> De zaak is inmiddels verwezen

naar de Grote Kamer en aldaar op 9 juli bepleit.<sup>31</sup> Een interessante interventie van de *European Information Society Institute* vraagt aandacht voor de moeizame positie van (zeer) kleine internettussenpersonen en -platforms als de door de Estlandse rechters aangenomen eigen aansprakelijkheid voor reacties van derden wordt geaccepteerd.<sup>32</sup>

Meer recent heeft ook het Hof van Justitie een arrest gewezen over de verhouding tussen nieuwswebsites en de E-commerce richtlijn.<sup>33</sup> Het Hof bevestigt dat ook een indirect (via reclame) gefinancierde informatiedienst een 'dienst van de informatiemaatschappij' kan zijn en dat een krantenwebsite geen beroep toekomt op de vrijwaringen voor 'mere conduit' of 'hosting' omdat de uitgever van zo'n website actieve controle uitoefent over de aangeboden informatie.

Dichter bij huis oordeelde het Hof Amsterdam, anders dan de rechtbank, dat Usenet-aanbieder NSE zich voor wat betreft de doorgifte en opslag van inbreukmakende *binaries* van auteursrechtelijk beschermde werken kon beroepen op de vrijwaringen voor 'mere conduit' respectievelijk 'hosting' (artikel 6:196c lid 1 respectievelijk 4 BW) en dus niet aansprakelijk was voor auteursrechtinbreuk door haar abonnees. Wel zag het Hof aanleiding om NSE op grond van artikel 6:196c lid 5 BW te bevelen een effectieve *notice-and-takedown* procedure te hanteren; daarover mogen partijen zich nu uitlaten.<sup>34</sup>

### 3.2 Medewerkingsplichten

#### 3.2.1 Blokkeren en filteren

Een andere grondslag voor het opleggen van medewerkingsplichten aan internettussenpersonen is artikel 26d Auteurswet, dat bepaalt dat de rechter 'op vordering van de maker, tussenpersonen wier diensten door derden worden gebruikt om inbreuk op het auteursrecht te maken, [kan] bevelen de diensten die worden gebruikt om die inbreuk te maken, te staken.' Het Hof Den Haag oordeelde in januari 2014 dat internetaanbieders Ziggo en XS4ALL niet langer gehouden zijn om de toegang tot de website van The Pirate Bay op grond van artikel 26d Aw te blokkeren voor hun abonnees.<sup>35</sup> Hoewel Nederland daarmee enigszins uit de pas loopt met andere landen,<sup>36</sup> is het oordeel van het hof gebaseerd op relatief omvangrijke empirische data over de periode sinds de providers begin 2012 op last van de rechtbank waren begonnen met filteren.<sup>37</sup> Volgens het hof bleek uit de data weliswaar dat minder mensen The Pirate Bay (rechtstreeks) hadden bezocht, maar was geen sprake van een significante afname in het aantal auteursrechtinbreuken dat door de abonnees van Ziggo en XS4ALL wordt gepleegd. Sinds het arrest hebben ook de andere internetaanbieders die The Pirate Bay op bevel van de rechtbank hadden geblokkeerd, de toegang weer hersteld.<sup>38</sup>

Brein heeft inmiddels cassatie ingesteld tegen het arrest van het Hof Den Haag en voert daarin (onder meer) aan dat het hof een onjuiste effectiviteitsmaatstaf heeft aangelegd door te kijken naar het effect van een filter op het totale volume aan illegale bestandsuitwisseling. Zij beroept zich op het in maart 2014 gewezen arrest *UPC Telekabel Wien* van het Hof van Justitie.<sup>39</sup> In dit arrest, dat volgt op twee eerdere arresten over filterverplichtingen van tussenpersonen,<sup>40</sup> oordeelde het Hof van Justitie dat

een aanbieder van internettoegang die zijn klanten toegang verschaft tot auteursrechtelijk beschermde werken die een derde op een website beschikbaar heeft gesteld zonder toestemming van de rechthebbende, kwalificeert als een tussenpersoon van wie de diensten worden gebruikt om inbreuk te maken op het auteursrecht. Voor een blokkeringsbevel aan een dergelijke internetprovider hoeft naar oordeel van het Hof van Justitie o.a. niet te worden aangetoond dat de klanten van de aanbieder zich daadwerkelijk toegang verschaffen tot de beschermde werken op website van de derde, aangezien een bevel ook preventief van aard kan zijn.

Het Hof oordeelt verder dat de betrokken grondrechten, zoals de vrijheid van onderneming van de internetprovider, niet voorschrijven dat de rechter in zijn bevel preciseerd welke maatregelen de internetprovider moet nemen dan wel aangeeft dat de internetprovider kan ontkomen aan dwangsommen wegens schending van dit bevel door aan te tonen dat hij alle redelijke maatregelen heeft genomen. Het kan dus aan de tussenpersoon worden overgelaten om de technische parameters van de blokkeringsmaatregel vast te stellen. Tegelijkertijd overweegt het Hof dat die blokkeringsmaatregel géén rechtmatig materiaal mag tegenhouden, omdat dan de informatievrijheid zou worden geschonden. Het Hof verlangt dat er een aparte procedure beschikbaar is waarin de tussenpersoon vóór verbeurte van boetes kan laten vaststellen of de voorgenomen maatregelen voldoende blokkeert, én dat er een procedure wordt ingericht waarin internetgebruikers kunnen klagen dat de voorgestelde maatregel te véél blokkeert. Hoe deze vereisten kunnen worden verzoend, en hoe deze procedurele voorschriften zich verhouden tot de processuele autonomie van de lidstaten, is niet duidelijk.

### 3.2.2 Overige medewerkingsplichten

Niet alleen klassieke internettussenpersonen kwamen in aanraking met tussenpersonenrecht. Ook ING Bank werd geconfronteerd met een eis van de Stichting Brein om NAW-gegevens te verstrekken van rekeninghouders die mogelijk betrokken waren bij file-sharing website FTD World.<sup>42</sup> De uitspraak bevat een verrassende overweging 4.2, die erop lijkt neer te komen dat artikel 8 sub f Wbp een grondslag zou kunnen zijn voor *verplichte* gegevensverwerking door een verantwoordelijke. Vervolgens past

de rechtbank echter alsnog een alleszins navolgbare belangenafweging toe, die weliswaar is geïnspireerd op *Lycos vs. Pessers*<sup>43</sup> maar ook oog heeft voor de eigen positie van de bank. De rechtbank overweegt dat de bank niet 'instrumenteel' is bij het plegen van de (beweerde) auteursrechtinbreuken door FTD World of het faciliteren hiervan door FTD World. De rol van een bank is bovendien 'wezenlijk anders' dan die van een *access of hosting provider*, omdat de dienstverlening van de bank geen *conditio sine qua non* is voor de inbreuk en de ING Bank niet in

## Het kan dus aan de tussenpersoon worden overgelaten om de technische parameters van de blokkeringsmaatregel vast te stellen

een positie verkeert om de rechtmatigheid van de desbetreffende website te kunnen beoordelen. Nu Brein de overige mogelijkheden om achter de gegevens te komen nog niet heeft uitgeput, er ook een strafrechtelijke weg open staat en de bank een bijzondere positie heeft als het gaat om het garanderen van de vertrouwelijkheid van betalingsverkeer, krijgen de belangen van ING Bank de doorslag. De uitspraak zet daarmee een voorzichtige rem op de in onze vorige kroniek gesignaleerde neiging om in *Lycos vs. Pessers* een algemene informatieverstrekkingsverplichting te lezen, ondanks de overweging van de Hoge Raad in dat arrest dat het Hof juist 'niet een algemene regel [had] geformuleerd dat ieder die kennis bezit van bepaalde informatie verplicht is deze te verschaffen aan degene die bij kennisneming van die voor hem onbekende informatie een redelijk belang heeft'. Voor een verdere analyse van de uitspraak, de verhouding met de eerdere uitspraak *Brein vs. Techno Design* waarin een financiële tussenpersoon wel werd verplicht gegevens te verstrekken,<sup>43</sup> en de houdbaarheid van *Lycos vs. Pessers* in het licht van de *Sabam*-arresten van het Hof van Justitie, zij verwe-

29. EHRM 10 oktober 2013, nr. 64569/09, EHRC 2014-1, nr. 14 m.nt. B. van der Sloot (*Delfi vs. Estland*).

30. D. Voorhoof, 'ISP of online-uitgever: Delfi naar de Grote Kamer?', *Mediaforum* 2014/1 p. 1.

31. Voor de videostream van de pleidooien, zie: <http://goo.gl/r2ciug>.

32. EISI, Third Party Intervention Submission In re *Delfi AS vs. Estonia*, appl. no. 64569/09, [www.eisionline.org/images/EISI-Delfi-Intervention.pdf](http://www.eisionline.org/images/EISI-Delfi-Intervention.pdf).

33. HvJ EU 11 september 2014, C-291/13 (*Papasavas*).

34. Hof Amsterdam 19 augustus 2014, ECLI:NL:GHAMS:2014:3435 (*NSE vs. Brein*).

35. Hof Den Haag 28 januari 2014, ECLI:NL:GHDHA:2014:88 (*Ziggo c.s. vs. Stichting Brein*).

36. Zie o.a. M. Husovec, 'European Cases on Ordering ISPs to Block Certain Websites', [www.husovec.eu/2011/11/european-cases-on-ordering-isps-to.html](http://www.husovec.eu/2011/11/european-cases-on-ordering-isps-to.html). Er zijn ook in de periode die deze kroniek bestrijkt diverse interessante artikelen geschreven over dit onderwerp, zie bijv.: M. Husovec, 'Injunctions against Innocent Third Parties: The Case of Website Blocking', *JIPITEC* 2013, 4/2; A.R. Lodder & N.S. van der Meulen, 'Evaluation of the Role of Access Providers. Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness,

Effectiveness, Costs, Relevance, and Time', *JIPITEC* 2013, 4/2.

37. Rb. Den Haag 11 januari 2012, ECLI:NL:RBSGR:2012:BV0549 (*Stichting Brein vs. Ziggo c.s.*).

38. Het betreft access providers KPN, Tele2, T-Mobile en UPC, die The Pirate Bay blokkeerden op grond van Rb. Den Haag (vzr.) 10 mei 2012, ECLI:NL:RBSGR:2012:BW5387 (*Stichting Brein vs. UPC c.s.*). Co-auteur Chavannes trad op voor twee van de betrokken access providers.

39. Hof van Justitie EU, 27 maart 2014, C-314/12 (*UPC Telekabel Wien*). Zie voor het standpunt van Stichting Brein [www.anti-piracy.nl/nieuws.php?id=321](http://www.anti-piracy.nl/nieuws.php?id=321).

40. Zie daarover R.D. Chavannes, 'Belangenafweging in het informatierecht: het arrest Scarlet/SABAM en de botsing tussen auteursrecht en ondernemingsvrijheid, uitingsvrijheid en privacy', in: *25 jaar Mediaforum, een blik vooruit via de achteruitkijkspiegel. 25 jaar rechtspraak media- en communicatierecht*, Amsterdam: Otto Cramwinckel 2013, <http://blog.chavannes.net/2013/12/vmc-scarlet/>.

41. Rb. Amsterdam (vzr.) 14 mei 2013, *IER* 2013 m.nt. S. Kulk.

42. HR 25 november 2005, *NJ* 2009/550, m.nt. PBH (*Lycos vs. Pessers*).

43. Rb. Den Haag (vzr.) 6 december 2011, *IEPT* 20111206 (*Brein vs. Techno Design*).

zen naar de lezenswaardige noot van Kulk in *IER*.

### 3.3 Netneutraliteit

Alle overeenkomsten voor de levering van internettoegangsdiensten die op of na 1 januari 2013 zijn gesloten, moeten voldoen aan het netneutraliteitsvereiste zoals neergelegd in artikel 7.4a Telecommunicatiewet (Tw). Ter verduidelijking van het begrip internettoegangsdienst is een concept Beleidsregel definitie internettoegangsdienst in de zin van artikel 7.4a Tw geconsulteerd. De beleidsregel preciseert dat de levering van één losse dienst via internet<sup>44</sup> niet kwalificeert als internettoegangsdienst, waardoor artikel 7.4a Tw niet op deze levering van toepassing is.<sup>45</sup> Overigens lijkt de Nederlandse netneutraliteit in Europa navolging te gaan krijgen: op 14 april 2013 heeft het Europees Parlement ingestemd met een voorstel van Eurocommissaris Kroes om netneutraliteit in Europa in te voeren.<sup>46</sup>

### 4. Privacy en vrijheid van meningsuiting

Voor ontwikkelingen en vindplaatsen verwijzen wij in de eerste plaats naar de jaarlijkse grondrechtenkronieken in dit blad van Janneke Gerards.<sup>47</sup> Voor wat betreft uitspraken van het EHRM heeft de persafdeling het de lezer en de kroniekschrijvers gemakkelijk gemaakt door een nieuwe *Fact Sheet* te publiceren met bondige samenvattingen van de belangrijkste arresten op het gebied van 'New technologies'.<sup>48</sup>

Ook overigens verschenen tijdens de kroniekperiode diverse interessante publicaties over het raakvlak tussen online privacy en vrijheid van meningsuiting.<sup>49</sup>

#### 4.1 Het 'recht om vergeten te worden'

Al enige jaren wordt in Brussel onderhandeld en gelobbyd over een nieuwe Privacyverordening, ter vervanging van de uit de klassieke *Netscape*-tijd daterende Privacyrichtlijn 95/46/EG, in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens. Een van de meest controverse onderwerpen was de vraag of het EU-recht expliciet moet voorzien in een 'recht om vergeten te worden': een recht voor datasubjecten om in bepaalde gevallen te verlangen dat hun persoonsgegevens worden gewist van websites, zoekresultaten, archieven, sociale media, enz.<sup>50</sup> Met name de Franse, Italiaanse en Spaanse privacytoezichthouders ijverden al enige tijd voor erkenning van zo'n recht, maar de Artikel 29 Werkgroep van Europese privacytoezichthouders had daar in haar opinie over zoekmachines over gezwegen.<sup>51</sup>

Nog voordat de Brusselse discussie over toekomstig recht was afgerond, oordeelde het Hof van Justitie in mei 2014 dat de bestaande Privacyrichtlijn al voorziet in een recht om door zoekmachines vergeten te worden.<sup>52</sup> Op verzoek van datasubjecten moeten zoekmachine-exploitanten bepaalde zoekresultaten bij een zoekopdracht naar de naam van het datasubject onderdrukken. Dat moet met name wanneer de informatie waarnaar wordt verwezen 'gelet op het geheel van de omstandigheden van het onderhavige geval, ontoereikend, niet of niet meer ter zake dienend of bovenmatig' is in relatie tot het datasubject, of 'wegens zwaarwegende en gerechtvaardigde redenen betreffende [zijn] bijzondere situatie'. Dit recht geldt ook indien deze naam of deze informatie niet vooraf of gelijktijdig van deze webpagina's is gewist en, in voorko-

mend geval, zelfs wanneer de publicatie ervan op deze webpagina's op zich rechtmatig is'. Wanneer aan de genoemde voorwaarde is voldaan, krijgen de rechten van het datasubject 'in beginsel voorrang niet enkel op het economische belang van de exploitant van de zoekmachine, maar ook op het belang van [het] publiek om deze informatie te vinden wanneer op de naam van deze persoon wordt gezocht. Dit zal echter niet het geval zijn indien de inmenging in de grondrechten van de betrokkene wegens bijzondere redenen, zoals de rol die deze persoon in het openbare leven speelt, wordt gerechtvaardigd door het overwegende belang dat het publiek erbij heeft om, door deze opneming, toegang tot de betrokken informatie te krijgen.'

## Enkele weken na het arrest heeft Google een apart formulier beschikbaar gesteld dat mensen kunnen gebruiken om gemotiveerde 'vergeetverzoeken' in te dienen

Volgens annotator Van Hoboken, gepromoveerd op het aansprekende onderwerp zoekmachinesvrijheid, bevat het arrest een doorwrochte en overtuigende analyse van de privacybelangen die op het spel staan als het gaat om de vindbaarheid van persoonlijke informatie via zoekmachines; de daartegenover staande belangen van informatievrijheid en ondernemingsvrijheid, en de positieve en wezenlijke rol die zoekmachines spelen, worden daarentegen amper onderzocht.<sup>53</sup> Opmerkelijk vindt hij ook de overweging van het Hof (r.o. 38) dat de bescherming van privacybelangen 'volledig' dient te zijn: juist in situaties waar botsende, grondrechtelijk genormeerde belangen tegen elkaar moeten worden afgewogen, zal het per definitie niet mogelijk zijn alle rechten 'volledig' te beschermen. Christopher Kuner publiceerde een uitgebreide analyse van de uitspraak en de mogelijke implicaties ervan, met name voor de toekomstige Algemene Privacyverordening.<sup>54</sup> Hij bekritiseert de op het oog eenzijdige wijze waarop privacy en uitingsvrijheid worden afgewogen en pleit ervoor om de totstandkoming van de Verordening aan te grijpen om een 'recht om vergeten te worden' te regelen met meer duidelijkheid, coherentie en nuance dan het Hof in een enkel arrest kan doen.

Enkele weken na het arrest heeft Google een apart formulier beschikbaar gesteld dat mensen kunnen gebruiken om gemotiveerde 'vergeetverzoeken' in te dienen.<sup>55</sup> Daarmee zijn inmiddels meer dan 120 000 verzoeken ingediend. De Artikel 29 Werkgroep heeft in juli 2014 overleg gevoerd met Google, Microsoft en Yahoo over de praktische implementatie van het *Costeja*-arrest en verwacht in het najaar richtsnoeren te publiceren.<sup>56</sup> Een door

Google in het leven geroepen Adviesraad over het recht om vergeten te worden houdt openbare bijeenkomsten in een aantal Europese steden, 'over hoe het recht van één persoon om vergeten te worden, in balans moet worden gebracht met het recht op informatie van het grote publiek'.<sup>57</sup>

#### Eerste Nederlandse uitspraak

Ondertussen is de eerste Nederlandse kort geding uitspraak over het recht om vergeten te worden een feit.<sup>58</sup> De eiser was in 2012 veroordeeld voor poging tot uitlokking van een huurmoord, mede op basis van verborgencamera-beelden die de vermeende huurmoordenaar maakte van zijn gesprekken met eiser. De zaak en de beelden waren voorwerp geweest van een uitzending van Peter R. de Vries, waarover vooraf in twee instanties was geoordeeld.<sup>59</sup> De eis tot verwijdering van zoekresultaten over de eiser, onder meer naar een (deels fictief, deels feitelijk) boek over hem, wordt door de rechtbank afgewezen. De rechtbank stelt voorop dat terughoudendheid is geboden bij het opleggen van beperkingen aan de werking van zoekmachines, die een belangrijke maatschappelijke functie vervullen om internetgebruikers informatie te laten vinden in de 'oceaan van informatie'. De functie van catalogus, die de zoekmachine in feite is, zou ernstig worden belemmerd indien strenge beperkingen aan de werking ervan zou worden opgelegd en daarmee zou de zoekmachine aan geloofwaardigheid inboeten. Met betrekking tot het 'vergeetverzoek' overweegt de rechtbank:

'4.11. Aangenomen moet dus worden dat eiser recentelijk een ernstig strafbaar feit heeft gepleegd. Dat heeft tot veel publiciteit aanleiding gegeven, onder meer een televisie-uitzending, diverse perspublicaties en een op de gebeurtenissen gebaseerd, deels fic-

tief, boek. Thans heeft eiser de gevolgen van zijn eigen handelen te dragen. Het plegen van een misdrijf heeft nu eenmaal tot gevolg dat men op zeer negatieve wijze in het nieuws kan komen en dit laat ook op het internet – mogelijk zelfs zeer langdurig – zijn sporen na. Het Costeja-arrest beoogt personen niet te beschermen tegen alle negatieve berichten op internet, maar alleen tegen het langdurig 'achtervolgd worden' door berichten die 'irrelevant', 'buitensporig' of 'onnodig diffamerend' zijn. De veroordeling voor een ernstig misdrijf zoals het onderhavige en de negatieve publiciteit als gevolg daarvan zijn in het algemeen blijvend relevante informatie over een persoon. De negatieve kwalificaties die daarbij kunnen voorkomen zullen slechts in zeer uitzonderlijke gevallen 'buitensporig' of 'onnodig diffamerend' zijn. Gedacht zou kunnen worden aan de situatie dat het gepleegde feit zonder duidelijke aanleiding opnieuw aan de orde wordt gesteld met kennelijk geen ander doel dan de betrokkene te schaden of de situatie dat niet zozeer van zakelijke berichtgeving sprake is, maar van een 'scheldpartij'. Ten aanzien van de zoekresultaten die eiser verwijderd wil zien is in de dagvaarding in het geheel niet onderbouwd (behalve met de in 4.9 reeds weerlegde argumenten) waarom deze 'irrelevant', dan wel 'buitensporig' of 'onnodig diffamerend' zouden zijn.'

#### 4.2 Gegevensverwerking door bedrijven

Tijdens de verslagperiode heeft het College bescherming persoonsgegevens diverse onderzoeken uitgevoerd naar het privacybeleid van technologiebedrijven.<sup>60</sup> Daarbij ging het onder meer om het gebruik van contactgegevens door Whatsapp,<sup>61</sup> de inzet van *deep packet inspection* door mobiele telefonie-aanbieders,<sup>62</sup> de verzameling van kijkge-

44. Dus uitdrukkelijk niet in combinatie met een internettoegangsdienst.

45. Zie [www.internetconsultatie.nl/netneutraliteit](http://www.internetconsultatie.nl/netneutraliteit).

46. Voor de aangenomen tekst wordt verwezen naar [www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN](http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN).

47. J.H. Gerards, 'Kroniek van de grondrechten', *NJB* 2012/2015, afl. 35, p. 2443-2452 en *NJB* 2013/2113, afl. 35, p. 2420-2430.

48. [www.echr.coe.int/Documents/FS\\_New\\_technologies\\_ENG.pdf](http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf).

49. Zie o.a. R.D. van Leek, 'De Wbp als toetssteen van uitingen op internet: een jurisprudentieanalyse van Kleintje Muurkrant tot nu', *Tijdschrift voor internetrecht* 2014/3, p. 75-79; Emiel Jurjens, 'Hof Amsterdam legt lijfsdwang op voor herhaalde onrechtmatige uitingen', *MediaReport MR* 2014/051 onder verwijzing naar Hof Amsterdam 1 april 2014, ECLI:NL:GHAMS:2014:1104; A. Flanagan, 'Defining 'journalism' in the age of evolving social media: a questionable EU legal test',

*International Journal of Law and Information Technology*, vol. 21, no. 1, 2012, p. 1-30;

R. van der Zaal, 'Social mediaverbod: onnodig beperking van de uitingsvrijheid?', *Tvl* 2013/1, onder verwijzing naar Rb. Amsterdam 4 december 2012, ECLI:NL:RBAMS:2012:BY9149; M. Richardson, 'Honour in a Time of Twitter', 2013, 5(1) *Journal of Media Law*, p. 45-56; A. Vamialis, 'Online Defamation: confronting anonymity', *International Journal of Law and Information Technology*, vol. 21, no. 1, 2012, p. 31-65.

50. Zie J.V.J. van Hoboken, 'The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment', juni 2013, <http://goo.gl/0BwVTQ>.

51. Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, <http://goo.gl/oNXMP>.

52. HvJ EU 13 mei 2014, C-131/12, *Computerrecht* 2014/115 m.nt. P. Van Eecke en

A. Cornette (*Google Spanje vs. Costeja*).

Vanwege de betrokkenheid bij dit onderwerp aan de zijde van Google van co-auteur Chavannes beperken wij ons tot een weergave van de kernoverwegingen en enkele commentaren van derden. Voor een uitgebreid overzicht van juridische commentaren, zie: [www.cambridge-code.org/googespain.html](http://www.cambridge-code.org/googespain.html).

53. J.V.J. van Hoboken, Case Note, CJEU 13 May 2014, C-131/12 (*Google Spain*), <http://goo.gl/ozqKbv>. Andere commentaren op het arrest zijn o.a. te vinden via het Institute for Ethics & Emerging Technologies (<http://ieet.org/index.php/IEET/more/is20140912>).

54. C. Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges', [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2496060](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496060).

55. [https://support.google.com/legal/contact/lr\\_eudpa?product=websearch&hl=nl](https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=nl).

56. Persbericht Artikel 29 Werkgroep d.d. 25 juli 2014, <http://goo.gl/tc9i3z>.

57. [www.google.com/advisorycouncil/](http://www.google.com/advisorycouncil/).

58. Rb. Amsterdam (vzr.) 18 september 2014, ECLI:NL:RBAMS:2014:6118 (*Google vs. X*). Co-auteur Chavannes trad in deze zaak op voor Google.

59. Rb. Amsterdam (vzr.) 14 april 2012, ECLI:NL:RBAMS:2012:BW2460; Hof Amsterdam 22 mei 2012, ECLI:NL:GHAMS:2012:BW6242, (*X en Y vs. SBS Broadcasting en Endemol*).

60. Het kantoor van co-auteur Chavannes treedt op voor een aantal van de betrokken ondernemingen.

61. Persbericht 28 januari 2013: 'Overtredingen WhatsApp deels beëindigd na onderzoek CBP en Canadese privacytoezichthouder' met link naar rapport van bevindingen, [http://www.cbpweb.nl/Pages/pb\\_20130128-whatsapp.aspx](http://www.cbpweb.nl/Pages/pb_20130128-whatsapp.aspx).

62. Persbericht 4 juli 2013: 'Telecomaanbieders passen data-analyse aan na onderzoek CBP. Resultaten onderzoek CBP naar packet inspection door telecomaanbieders' met link naar rapporten van bevindingen, [www.cbpweb.nl/Pages/pb\\_20130704-onderzoek-analyse-gegevens-mobiel-dataverkeer.aspx](http://www.cbpweb.nl/Pages/pb_20130704-onderzoek-analyse-gegevens-mobiel-dataverkeer.aspx).

# In sommige gevallen was een korte mediahype voldoende om voorgenomen gegevensverwerkingen te voorkomen, zoals de plannen van Equens om pintransacties te vermarkten

gegevens via smart-tv's van TP Vision,<sup>63</sup> de nieuwe privacyvoorwaarden van Google<sup>64</sup> en, meest recentelijk, de Okki Gekke-bekken-club tandenpoetsapp voor kinderen.<sup>65</sup> Ook overigens is er steeds meer aandacht voor de privacy- en overige juridische aspecten van mobiele applicaties (apps).<sup>66</sup> Emre Yildirim won in 2012 de Internetscriptieprijs met een onderzoek naar de verzameling van persoonsgegevens door mobiele apps.<sup>67</sup> De Artikel 29 Werkgroep publiceerde er begin 2013 een opinie over,<sup>68</sup> naast andere opinies over onder meer slimme energiemeters,<sup>69</sup> de effectiviteit en beperkingen van verschillende anonimiserings technieken<sup>70</sup> en privacyaspecten van met het internet verbonden gadgets, sensoren en domotica (het 'Internet of Things').<sup>71</sup> In sommige gevallen was een korte mediahype voldoende om voorgenomen gegevensverwerkingen te voorkomen, zoals de plannen van Equens om pintransacties te vermarkten<sup>72</sup> en van de ING om advertenties te personaliseren op basis van betaalgedrag.<sup>73</sup>

In ruimere zin is *big data* een thema geworden. Bij de presentatie van zijn jaarverslag 2013 waarschuwde het Cbp voor de risico's van het op geavanceerde wijze verwerken van enorme hoeveelheden persoonsgegevens en pleit te het voor zo veel mogelijk anonimisatie van gegevens:

'Uit de grote berg gegevens kunnen bedrijven en overheden verbanden en behoeften destilleren waardoor zij toekomstig gedrag van mensen kunnen voorspellen, zónder dat mensen dit zelf ook maar kunnen vermoeden. Organisaties kunnen hierdoor mensen anders behandelen dan anderen. Dit kan grote impact hebben op iemands leven. "Voor veel doelen waarvoor big data wordt ingezet, zijn tot de persoon herleidbare gegevens helemaal niet nodig. De gegevens moeten dan onomkeerbaar worden geanonimiseerd."<sup>74</sup>

De meest leesbare verhandeling over het thema is wellicht die van Deirdre Mulligan en Cynthia Dwork<sup>75</sup> en op basis daarvan kan de vraag gesteld worden of de door het Cbp voorgestelde anonimisering zo effectief is: het gaat niet alleen om herleidbaarheid, maar heel sterk om selectie in categorieën en in- en uitsluiting op basis daarvan.

### 4.3 Gegevensverwerking door (semi-)overheden

Ook (semi-)overheden waren regelmatig voorwerp van Cbp-onderzoeken. De Rotterdamse vervoerder RET bereikte een schikking en vernietigde reisgegevens van Studenten OV-chipkaarten.<sup>76</sup> De websites van de publieke omroep zouden de cookieregels schenden.<sup>77</sup> De Belastingdienst werd gedwongen minder inkomensgegevens te verwerken bij de uitvoering van de inkomensafhankelijke huurverhoging.<sup>78</sup>

Interessanter was een andere procedure die de Belastingdienst voerde tegen de parkeerdienst SMSParking. In het kader van onderzoek naar privégebruik van zakelijke

auto's eiste de Belastingdienst op grond van artikel 53 AWR (Algemene wet inzake rijksbelastingen) verstrekking van alle parkeergegevens (kenteken, datum, locatie en tijd) van SMSParking klanten over het jaar 2012 in het kader van een controle naar 2,5 miljoen zakelijk gebruikte auto's. SMSParking weigerde en beriep zich met name op de privacy van haar klanten. De Voorzieningenrechter vond het verzoek op zich vallen onder de reikwijdte van artikel 53 AWR, maar met een voor de Belastingdienst onheilspellende motivering: 'Wie maar genoeg gegevens over het feitelijk gebruik van veel auto's verzamelt, zal ongetwijfeld iets vinden dat voor de belastingheffing van belang is.'<sup>79</sup> Inderdaad volgt daarop een principiële verwoorde afwijzing van de eis wegens schending van artikel 8 EVRM:

'Artikel 8 EVRM bevat een belangrijk beginsel in de verhouding tussen de overheid (het openbaar gezag) en de burgers. De tot het openbaar gezag gerichte en ter bescherming van de burgers strekkende hoofdregel in artikel 8 EVRM luidt voor zover in dit geval relevant: 'een ieder heeft recht op respect voor privéleven' en 'geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht'. Dit uitgangspunt in de relatie tussen burger en overheid is niet het veelgehoorde 'wie niets te verbergen heeft, heeft ook niets te vrezen' maar 'het dagelijks doen en laten van de burgers gaat de overheid niets aan'. [...] Iedere burger moet in beginsel een auto kunnen parkeren op een door die burger verkozen plaats in Nederland, zonder dat de overheid behoeft te weten dat hij dat doet en waarom hij dat doet.'

In reactie op het beroep dat de Belastingdienst deed op het arrest-*Stad Rotterdam* uit 1974<sup>80</sup> overwoog de Voorzieningenrechter:

'De gegevens van SMSParking waar het hier om gaat zijn een voorbeeld van de vele elektronisch vastgelegde gegevensbestanden die in 1974 nog niet of nauwelijks bestonden. Die bestanden bevatten veel informatie die eenvoudig is te relateren aan gedrag van individuele burgers in hun privésfeer en die gegevens blijken zich te lenen voor analyse en gebruik door het openbaar gezag dat zich de belangen als verwoord in artikel 8 lid 2 EVRM zegt aan te trekken. Dat doet in de samenleving de vraag ontstaan naar begrenzing onder meer, maar niet uitsluitend, ten aanzien van de gegevens die mogen worden gebruikt en de wijze waarop het openbaar gezag dat mag doen. Anders gezegd, waar de vastgelegde informatie over burgers enorm is toegenomen, dringt zich in het maatschappelijk debat steeds meer de vraag op: wat is de hoofdregel van artikel 8 EVRM voor de burger nog waard?'

In hoger beroep tapte het Hof Den Bosch uit een heel ander vaatje: het achtte het opvragen van alle parkeergegevens 'alleszins proportioneel'. Het alternatief om voertuigbewegingen met camera-auto's te volgen werd, als niet minder belastend, terzijde geschoven. Dat de Staat met deze methode geautomatiseerde inzage krijgt in exact gedateerde locatiegegevens van alle negen miljoen Nederlandse autobezitters, kwam niet aan de orde.<sup>81</sup> Het Hof lijkt aan te nemen dat parkeergegevens geen persoonsgegevens zijn en hanteert daarbij een herleidbaarheids criterium dat haaks staat op de beschikkingenpraktijk van het CBP:

'3.5.3. [...] De betreffende gegevens zijn niet dadelijk te herleiden naar de persoon van het aldus gebruikte voertuig. Voor zover die gegevens bij SMSParking wel bekend zijn door het gebruik van het bij haar aangeelde klantcontact, wordt niet om deze persoonlijke gegevens door de Belastingdienst aan SMSParking gevraagd.'

Ongetwijfeld zal de Belastingdienst de kentekengegevens echter onmiddellijk koppelen aan de bestuurder (of in elk geval de kentekenhouder) van de desbetreffende auto: het Hof stelt als uitgangspunt vast dat de Belastingdienst voornemens is 'alle van SMS Parking te verkrijgen parkeergegevens op basis van kentekeninformatie te filteren op fiscale relevantie'. Hoe dat ook zij, de parkeerbedrijven

hebben inmiddels besloten hun bewaartermijnen terug te brengen tot dertien weken, zodat de Belastingdienst alsnog verstoken blijft van complete jaargegevens.

#### 4.4 Snowden

De verzameldrift van de Belastingdienst valt uiteraard in het niet vergeleken met die van de geheime diensten van onder meer de Verenigde Staten en het Verenigd Koninkrijk. De door ex-NSA-medewerker Edward Snowden geïnitieerde onthullingen over PRISM en andere surveillanceprogramma's waren misschien wel hét nieuwsverhaal van 2013 en hebben het debat over de verhouding tussen veiligheid en (digitale) grondrechten nieuw leven ingeblazen.

De juridische literatuur is nog betrekkelijk schaars.<sup>82</sup> Het Europees Parlement publiceerde een zeer kritisch rapport,<sup>83</sup> mede op basis van een getuigenverklaring van Snowden zelf<sup>84</sup> en een grondig onderzoek van het Centre for European Policy Studies naar de surveillancepraktijken van een aantal EU-landen waaronder Nederland.<sup>85</sup> Lezenswaardig is ook de *expert opinion* van Ian Brown (Oxford Internet Institute) in de zaak die Big Brother Watch bij het EHRM aanspande tegen het Verenigd Koninkrijk.<sup>86</sup> De bredere discussie gaat niet alleen over de activiteiten van inlichtingen- en opsporingsdiensten, maar ook over de al dan niet vrijwillige medewerking daaraan door telecom- en internetbedrijven en hun recht daarover transparant te zijn.<sup>87</sup> De onthullingen lieten ook Nederland niet onberoerd. De Commissie-Dessems publiceerde een kritisch rapport

63. Persbericht 22 augustus 2013: 'CBP: persoonsgegevens via smart tv's verzameld in strijd met wet. TP Vision niet transparant over verzamelen en bewaren gegevens online kijkgedrag' met link naar rapport van bevindingen, [www.cbweb.nl/Pages/pb\\_20130822-persoonsgegevens-smart-tv.aspx](http://www.cbweb.nl/Pages/pb_20130822-persoonsgegevens-smart-tv.aspx).

64. Persbericht 28 november 2013: 'CBP: Privacyvoorwaarden Google in strijd met de wet' met link naar rapport van bevindingen, [www.cbweb.nl/Pages/pb\\_20131128-google-privacybeleid.aspx](http://www.cbweb.nl/Pages/pb_20131128-google-privacybeleid.aspx).

65. Persbericht 11 september 2014: 'Overtredingen kinderapp beëindigd na onderzoek CBP' met link naar rapport van bevindingen, [www.cbweb.nl/Pages/pb-20140911-okki-app.aspx](http://www.cbweb.nl/Pages/pb-20140911-okki-app.aspx).

66. Gewezen wordt o.a. op D.M. Sithigh, 'App law within: rights and regulation in the smartphone age', *International Journal of Law and Information Technology* 2013, 21/2.

67. E. Yildirim, *Mobile Privacy: is there an app for that? On smart mobile devices, apps and data protection*, [www.internetscriptie-prijs.nl/archief/jaar/2012/](http://www.internetscriptie-prijs.nl/archief/jaar/2012/).

68. Article 29 Working Party, Opinion 02/2013 on apps on smart devices, 27 februari 2013, <http://goo.gl/CyqsQ>.

69. Article 29 Working Party, Opinion 07/2013 on the Data Protection Impact

Assessment Template for Smart Grid and Smart Metering Systems, <http://goo.gl/GF1yf>.

70. Article 29 Working Party, Opinion 05/2014 on anonymisation techniques, <http://goo.gl/0FQC8c>.

71. Article 29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, <http://goo.gl/1w0A4b>.

72. Zie [www.solv.nl/weblog/equens-plan-nen-verkoop-van-pingegevens/19431](http://www.solv.nl/weblog/equens-plan-nen-verkoop-van-pingegevens/19431).

73. Zie o.a. <http://fd.nl/ondernemen/546161-1403/ing-geeft-adverteerderinzicht-in-klantgedrag>; [www.nu.nl/economie/3722010/ing-houdt-privacygevoelige-proef-met-klantgegevens.html](http://www.nu.nl/economie/3722010/ing-houdt-privacygevoelige-proef-met-klantgegevens.html); [www.volkskrant.nl/vk/nl/2680/Economie/article/detail/3616281/2014/03/17/ING-stelt-proef-commercieel-gebruik-klantgegevens-uit.dhtml](http://www.volkskrant.nl/vk/nl/2680/Economie/article/detail/3616281/2014/03/17/ING-stelt-proef-commercieel-gebruik-klantgegevens-uit.dhtml).

74. [www.cbweb.nl/Pages/jv\\_2013.aspx](http://www.cbweb.nl/Pages/jv_2013.aspx).

75. C. Dwork & D.K. Mulligan, 'It's Not privacy and It's Not Fair', 66 *Stan. L. Rev. Online* 35. ([www.stanfordlawreview.org/online/privacy-and-big-data/its-not-privacy-and-its-not-fair](http://www.stanfordlawreview.org/online/privacy-and-big-data/its-not-privacy-and-its-not-fair)). Zie ook het verslag dat D. Verhulst maakte van het congres 'Big Data and privacy' in september 2013 (<http://goo.gl/7MUT6p>) en de overige bijdragen aan de bijbehorende thema-uitgave van *Stanford Law Review* ([www.stanfordlawreview.org/](http://www.stanfordlawreview.org/)

[online/privacy-and-big-data](http://online/privacy-and-big-data)).

76. Persbericht 3 februari: 'CBP: procedure RET over bewaartermijnen reisgegevens Studenten OV-chipkaart via schikking beëindigd. RET heeft reisgegevens vernietigd', [www.cbweb.nl/Pages/med\\_20140203-bewaartermijnen-reisgegevens-ovchip-ret.aspx](http://www.cbweb.nl/Pages/med_20140203-bewaartermijnen-reisgegevens-ovchip-ret.aspx).

77. Persbericht 8 juli 2014: 'CBP: Volgen bezoekers omroepwebsites met cookies in strijd met de wet' met link naar rapport van bevindingen, [www.cbweb.nl/Pages/pb\\_20140708\\_npo-cookies-publieke-omroep.aspx](http://www.cbweb.nl/Pages/pb_20140708_npo-cookies-publieke-omroep.aspx).

78. Persbericht 12 juni 2014: 'CBP: Belastingdienst beëindigt overtreding gebruik huurdersgegevens. Verstrekking inkomensgegevens huurders in 2014 niet langer in strijd met de wet', [www.cbweb.nl/Pages/pb\\_20140612\\_belastingdienst-inkomensgegevens-scheefwonen.aspx](http://www.cbweb.nl/Pages/pb_20140612_belastingdienst-inkomensgegevens-scheefwonen.aspx).

79. Rb. Oost-Brabant (vzr.) 26 november 2013, *Computerrecht* 2014/78 m.nt. T.H.A. Wisman.

80. HR 10 december 1974, *NJ* 1975/178.

81. Hof Den Bosch 19 augustus 2014, ECLI:NL:GHSHE:2014:2803 (*Staat vs. SMS Parking*).

82. Zie o.a. B. van der Sloot, 'Privacy in het post NSA-tijdperk: Tijd voor een fundamentele herziening?', *NJB* 2014/866, afl. 17, p. 1172-1179.

83. Zie o.a. Committee on Civil Liberties, Justice and Home Affairs, *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, A7-0139/2014, aangenomen op 21 februari 2014.

84. <http://goo.gl/ZC5E2A>.

85. Centre for European Policy Studies, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, CEPS Papers in Liberty & Security in Europe, no. 62, november 2013, <http://goo.gl/ew4xRX>.

86. Witness statement of Dr Ian Brown, 27 september 2013, <http://goo.gl/BRZCby>. Zie verder [www.privacynotprism.org.uk/](http://www.privacynotprism.org.uk/).

87. Zie o.a. N. van der Laan en B.W. Newitt, 'Tap secret: de strijd tussen transparantie en geheimhouding. De strijd tussen transparantie en geheimhouding', *Computerrecht* 2014/151. Over de steun van de Europese Commissie aan Microsoft in haar strijd om in Europa opgeslagen gegevens van Europese gebruikers niet aan de Amerikaanse autoriteiten te hoeven afgeven, zie T. Ring, 'European Commission backs Microsoft in privacy fight with US', *SC Magazine* 12 augustus 2014, <http://goo.gl/ZheDx9>.

over de verenigbaarheid van het werk van de diensten met de huidige Wet op de inlichtingen- en veiligheidsdiensten, en pleitte voor een nieuwe, stevig in de wet verankerde balans tussen het effectief kunnen opereren van de diensten en de rechtsstatelijke waarborgen.<sup>88</sup> De voor de veiligheidsdiensten verantwoordelijke minister Plasterk kwam in het nauw nadat hij zowel in de Kamer<sup>89</sup> als bij *Nieuwsuur* onjuiste informatie had verschaft over het verzamelen van 1,8 miljoen Nederlandse telefoongegevens.<sup>90</sup> De betreffende *metadata* waren niet zoals eerder door hem gesteld door de NSA verzameld, maar door de Nederlandse Nationale Sigint Organisatie (NSO) en later door Nederland gedeeld met de Verenigde Staten.<sup>91</sup> Plasterk overleefde uiteindelijk het debat.<sup>92</sup> De kwestie kwam aan het rollen door een procedure tegen de Nederlandse Staat waarin onder meer werd geëist dat de Staat stopt met het gebruik van gege-

### Alle kritiek ten spijt, een initiatiefwetsvoorstel van Groenlinks om de bewaarplichtwet in te trekken heeft weinig vooruitgang geboekt en het Agentschap Telecom laat weten de wet gewoon te handhaven

vens die niet in overeenstemming met het Nederlandse recht zijn verkregen.<sup>93</sup> De rechtbank stelde de Staat echter in het gelijk.<sup>94</sup> Hoewel zij vaststelde dat de mogelijkheid bestaat dat Nederlandse autoriteiten informatie ontvangen van buitenlandse diensten die is vergaard op wijzen die de Nederlandse diensten niet zouden zijn toegestaan, is het ontvangen (en gebruiken) daarvan niet in strijd met de Nederlandse wetgeving. De zaak loopt in hoger beroep.

#### 4.5 Vernietiging Dataretentierichtlijn

Tegen deze achtergrond moest het Hof van Justitie oordelen over de verenigbaarheid met privacyrechten van de Europese Dataretentierichtlijn, die lidstaten opdraagt telecombedrijven te verplichten om verkeersgegevens te bewaren voor opsporingsdoeleinden.<sup>95</sup> Waar de eerder genoemde arresten over afweging van conflicterende grondrechten zich afspeelden in horizontale situaties tussen burgers onderling, is hier sprake van een meer 'ouderwetse', verticale toetsing van een beperking door de staat van grondrechten van burgers. Het Hof kan daarom betrekkelijk eenvoudig de klassieke voorwaarden voor beperkingen van grondrechten (artikel 52 lid 1 EU-Handvest) aflopen.<sup>96</sup> vormt de richtlijn een inmenging in de privacy- en gegevensbeschermingsrechten van burgers (ja, een 'zeer ruime en bijzonder zware inmenging'); beantwoordt de inmenging werkelijk aan een doel van algemeen belang (ja, bestrijding van ernstige criminaliteit); en

is de inmenging evenredig?

De evenredigheidstoets valt uiteen in de vraag of de wettelijke regeling geschikt is (ja, de te bewaren gegevens kunnen nuttig zijn); of zij blijft binnen de grenzen van het strikt noodzakelijke; en of de regeling 'duidelijke en precieze regels bevat betreffende de draagwijdte en de toepassing van de betrokken maatregel, die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens.' Op al deze punten zakt de richtlijn door het ijs: de richtlijn is algemeen van toepassing op ieders telecomgegevens, ongeacht het bestaan van enige verdenking en ook op gegevens van geheimhouders; vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid; de richtlijn bevat geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen; en bevat geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan.

De Nederlandse wet tot implementatie van de Dataretentierichtlijn is in 2009 alleen door de Eerste Kamer gekomen omdat het moest van Brussel. Onder leiding van Hans Franken, in eerdere debatten verklaard tegenstander van de bewaarplicht en overigens een van de grootvaders van technologie en recht, hielp de CDA-fractie deze 'domme wet' toen aan een meerderheid met de beroemd geworden onderbouwing dat 'politieke opportuniteit zwaarder weegt dan wetenschappelijke rationaliteit'.<sup>97</sup> Juist vanwege deze historie rees na het arrest-*Digital Rights Ireland* onmiddellijk de vraag welke gevolgen het wegvallen van de richtlijn zou hebben voor de Nederlandse bewaarplicht. De regering, destijds en nu voorstander van de bewaarplicht, heeft kans gezien die urgent gestelde vraag langdurig in beraad te nemen en voor advies voor te leggen aan de Raad van State en het Cbp. Critici wezen op het opmerkelijke contrast met de situatie toen het Hof van Justitie, twee dagen na het arrest-*Digital Rights Ireland*, oordeelde dat een privékopie niet uit illegale bron mocht komen, en de staatssecretaris binnen een week liet weten dat het arrest onmiddellijke werking had in Nederland.<sup>98</sup> Alle kritiek ten spijt, een initiatiefwetsvoorstel van Groenlinks om de bewaarplichtwet in te trekken heeft weinig vooruitgang geboekt<sup>99</sup> en het Agentschap Telecom laat weten de wet gewoon te handhaven.<sup>100</sup> In andere EU-landen heeft het arrest inmiddels wel geleid tot opschorting of vernietiging van de nationale bewaarplichtwetgeving.<sup>101</sup>

#### 4.6 Cookieregels

De strenge Nederlandse cookiewetgeving is pas per 1 januari 2013 volledig inwerking getreden, maar staat alweer op het punt om gewijzigd te worden.<sup>102</sup> De nieuwe cookiebepaling blijkt – zoals verwacht – in de praktijk zeer

gebruiksvriendelijk, aangezien internetgebruikers als gevolg van de ruime omvang van artikel 11.7a Tw ook geïnformeerd worden over en om toestemming worden gevraagd voor relatief onschuldige cookies zoals *analytics cookies*, *affiliate cookies* en *A/B testing cookies* die niet (ook) gebruikt worden om bijvoorbeeld unieke interesseprofielen van unieke internetgebruikers op te stellen. Om dit geconstateerde ongemak te verhelpen, heeft de regering een conceptwetsvoorstel geconsulteerd tot aanpassing van de cookiebepaling, als gevolg waarvan de internetgebruiker niet langer hoeft te worden geïnformeerd en om toestemming te worden gevraagd als met het plaatsen of lezen van een cookie informatie wordt verkregen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij, mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de internetgebruiker.<sup>103</sup> De regering heeft de aanpassing bovendien aangegrepen om de cookiebepaling te verduidelijken. Het wetsvoorstel ligt op dit moment ter behandeling bij de Tweede Kamer.<sup>104</sup> Eerder had de Artikel 29 Werkgroep van Europese privacytoezichthouders een (niet-bindende) opinie gepubliceerd over de wijze van verkrijgen van toestemming voor cookies.<sup>105</sup>

#### 4.7 Meldplichten datalekken

Sinds de vorige kroniek is Nederland een meldplicht rijker. Sinds 1 november 2013 geldt voor een certificatie-dienstverlener de verplichting om onverwijld na iedere veiligheidsinbreuk die of ieder integriteitsverlies dat aanzienlijke gevolgen heeft of kan hebben voor de betrouwbaarheid van door hem aangeboden of afgegeven gekwalificeerde certificaten dat te melden bij de ACM.<sup>106</sup>

Ook zit er een tweetal meldplichten in de pijplijn. In de eerste plaats is er een wetsvoorstel ingediend voor een

meldplicht voor verantwoordelijken in de zin van de Wbp om beveiligingsinbreuken waarvan redelijkerwijs kan worden aangenomen dat die leiden tot een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens te melden bij Cbp, alsook bij betrokkene(n) indien de inbreuk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.<sup>107</sup> In de tweede plaats is er van 22 juli tot 17 september 2013 een meldplicht bij de Minister van Veiligheid en Justitie geconsulteerd voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving, indien de inbreuk tot gevolg heeft of kan hebben dat die beschikbaarheid of betrouwbaarheid in belangrijke mate wordt onderbroken.<sup>108</sup> In de literatuur is uitgebreid stilgestaan bij de verschillende (aankomende) meldplichten, waarnaar hier kortheidshalve wordt verwezen.<sup>109</sup>

Per 5 juni 2012 rustte op aanbieders van een openbare elektronische communicatiedienst op grond van artikel 11.3a Tw al de verplichting om de ACM onverwijld in kennis te stellen van beveiligingsinbreuken die nadelige gevolgen hebben voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie. Wanneer dergelijke inbreuken waarschijnlijk ongunstige gevolgen zullen hebben voor de persoonlijke levenssfeer voor degene(n) wiens persoonsgegevens de beveiligingsinbreuk betreft, rust op de aanbieder bovendien de plicht deze individu(en) onverwijld van de inbreuk in kennis te stellen.<sup>110</sup> Op grond van de Uitvoeringsverordening 611/2013 van 24 juni 2013 moet de onverwijld kennisgeving aan de ACM plaatsvinden binnen 24 uur en de kennisgeving aan de individu zonder onnodige vertraging.<sup>111</sup>

88. Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002: Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 2 december 2013, <http://goo.gl/GUHWgt>.

89. Bijvoorbeeld in *Kamerstukken II* 2013/14, 30977, 71 en *Kamerstukken II* 2013/14, 30977, 77.

90. Dit naar aanleiding van een grafiek in Der Spiegel dat gebaseerd op de gelekte informatie van Snowden een aantal van 1,8 miljoen Nederlandse telefoongegevens toonde.

91. Brief van minister Plasterk (BZK) en minister Hennis-Plasschaert (Defensie) d.d. 4 februari 2014 aan de Tweede Kamer met een reactie op een bericht in Der Spiegel over 1,8 miljoen records metadata die de Nationale Sigint Organisatie (NSO) heeft verzameld in het kader van terrorismebestrijding en militaire operaties in het buitenland. Zie [www.rijksoverheid.nl](http://www.rijksoverheid.nl).

92. *Kamerstukken II* 2013/14, 30977, 82.

93. Zie dagvaarding op [www.bureaubrand-eis.com](http://www.bureaubrand-eis.com).

94. Rb. Den Haag 23 juli 2014,

ECLI:NL:RBDHA:2014:8966.

95. Zie over de voorgeschiedenis par. 8.2 van onze vorige kroniek, *NJB* 2012/2022, afl. 35, p. 2512.

96. HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ireland*). Zie G.-J. Zwenne en F. Simons, 'Daar kon je op wachten: richtlijn bewaarplicht ongeldig verklaard', *Tijdschrift voor internetrecht* 2014/3, p. 70-74.

97. *Handelingen I* 2008/09, 39 (6-7-2009), p. 1807. Ook de daarop volgende toelichting, interrupties en reacties behoren nog altijd tot de klassiekers van *Handelingen I*.

98. HvJ EU 10 april 2014, C-435/12 (*ACI Adam vs. Thuiskopie*); brief van staatssecretaris Teeven aan de Tweede Kamer van 17 april 2014, *Kamerstukken II* 2013/14, 29838, 72.

99. Voorstel van wet van het lid Van Tongeren tot intrekking van de Wet bewaarplicht telecommunicatiegegevens, *Kamerstukken II* 2013/14, 33939.

100. <http://webwereld.nl/overheid/82140->agentschap-telecom-blijft-bewaarplicht-handhaven.

101. Zie o.a. het arrest van het Oostenrijkse *Verfassungsgerichtshof* van 27 juni 2014, G

47/2012, <http://goo.gl/kteht5>, Engelse vertaling <http://goo.gl/LxjNe3>. De Zweedse toezichthouder heeft laten weten de wet voorlopig niet te handhaven: <http://goo.gl/8smXIO>.

102. G.H.G.M. van Berkel, 'Alweer aanpassing 'cookiewet' voorgesteld: beter ten halve gekeerd', *NJB* 2013/386, afl. p. 480-482.

103. Zie [www.internetconsultatie.nl/cookie-bepaling](http://www.internetconsultatie.nl/cookie-bepaling).

104. Wijziging Telecommunicatiewet in verband met toevoegen uitzondering op 'cookiebepaling', *Kamerstukken II* 2013/14, 33902, 2.

105. *Opinie* 02/2013 van de Artikel 29 Werkgroep met richtsnoeren voor het verkrijgen van toestemming voor cookies van 2 oktober 2013.

106. Besluit van 17 september 2013 tot wijziging van het Besluit elektronische handtekeningen in verband met een meldingsplicht voor veiligheidsinbreuken en integriteitsverlies betreffende gekwalificeerde certificaten.

107. Het wetsvoorstel wordt op het moment van schrijven van deze kroniek behandeld

door de Tweede Kamer (*Kamerstukken II* 2014/2015, 33662).

108. Zie [www.internetconsultatie.nl/meldplicht\\_ict\\_inbreuken](http://www.internetconsultatie.nl/meldplicht_ict_inbreuken).

109. Zie o.a. F. van der Jagt, 'lets te melden? De diverse datalek meldplichten in kaart gebracht', *NJB* 2012/1415; J.M. van Essen, 'Nieuwe meldplichten in privacyland', *P&I* 2013/5; H.A.J. de Jong & G.C.J. Erents, 'Online Overeenkomsten en meer', *Tvl* 2013, afl. 5/6; F.J. Zuiderveen Borgesius, 'De meldplicht voor datalekken in de Telecommunicatiewet', *Computerrecht* 2011/4.

110. F.J. Zuiderveen Borgesius, 'De meldplicht voor datalekken in de Telecommunicatiewet', *Computerrecht* 2011/4.

111. Zie artikelen 2 en 3 van de Verordening (EU) nr. 611/2013 van de commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.

Hoewel de meldplichten als paddenstoelen uit de grond lijken te schieten, is het maar de vraag of meldplichten in de praktijk effectief zijn en incidenten als bijvoorbeeld het Diginotar incident zullen voorkomen, gelet op de ingrijpende consequenties voor een bedrijf als een incident uitkomt (getuigt het faillissement van Diginotar).<sup>112</sup>

### 5. IT-, contracten- en consumentenrecht

#### 5.1 Licenties bij faillissement

Op 11 juli 2014 heeft de Hoge Raad een interessant arrest gewezen over de bevoegdheden van de curator na het uitspreken van een faillissement, dat ook interessant is voor de licentiepraktijk.<sup>113</sup> In het *Berzona*-arrest oordeelt de Hoge Raad dat het uitspreken van een faillissement niet tot gevolg heeft dat de curator 'actief' vorderingen of bevoegdheden toekomt die niet worden toegekend door de wet of de overeenkomst, aangezien een andere opvatting in strijd zou komen met het beginsel dat het faillissement geen invloed heeft op bestaande wederkerige overeenkomsten. Als voorbeeld van een dergelijke actieve bevoegdheid noemt de Hoge Raad een bevoegdheid tot ontruiming of opeising van een gehuurde onroerende zaak als de huurovereenkomst nog loopt, maar evengoed zou kunnen worden gedacht aan het verbieden van het gebruik van software door een licentienemer. De curator mag naar het oordeel van de Hoge Raad enkel uit de overeenkomst voortvloeiende verbintenissen die uit of ten laste van de boedel moeten worden voldaan (bijv. betalingen) 'passief' niet nakomen. Eerder werd in de praktijk wel aangenomen dat een curator bij faillissement ook de (actieve) bevoegdheid zou hebben om bijv. softwarelicenties te beëindigen,<sup>114</sup> aangezien de Hoge Raad in 2006 in het *Nebula*-arrest heeft geoordeeld dat de curator niet gebonden is aan voor het faillissement verleende contractuele rechten op een onroerende zaak.<sup>115</sup>

#### 5.2 Consumentenbescherming

##### 'Gratis' mobiele telefoon

De Hoge Raad oordeelde in een prejudiciële procedure dat de levering van een 'gratis' mobiel toestel als onderdeel van een (duur) telefonieabonnement moet worden aangemerkt als een koop op afbetaling, waarvoor diverse bijzondere regels gelden ter bescherming van consumenten.<sup>116</sup> De Hoge Raad benadrukt dat gekeken moet worden naar de strekking van de overeenkomst. De gebezigde vormgeving, benaming en formulering van de overeenkomsten – die door de aanbieder worden bepaald en niet door de consument – zijn niet beslissend, omdat anders de beoogde bescherming van de consument zou kunnen worden ontgaan. De Hoge Raad formuleert vervolgens als uitgangspunt dat de overeengekomen, door de consument te betalen maandbedragen niet alleen betrekking hebben op de vergoeding voor de door deze af te nemen telecommunicatiediensten, maar mede strekken tot afbetaling van een koopprijs voor de mobiele telefoon. Dat brengt mee dat een telefoonabonnement inclusief toestel ter zake van de mobiele telefoon in beginsel is aan te merken als een koop op afbetaling, en tevens als een krediettransactie dan wel kredietovereenkomst.

De provider had nog aangevoerd dat toepasselijkheid

van (met name) de wettelijke regelingen inzake krediettransactie dan wel kredietovereenkomst, en daarmee ook van de Wft, ingrijpende en kostbare gevolgen heeft voor aanbieders van telefoonabonnementen. De Hoge Raad is daarvan niet onder de indruk en speelt de bal door naar de wetgever om desgewenst te voorzien in relevante uitzonderingen.

##### Implementatiewet richtlijn consumentenbescherming

Een belangrijke ontwikkeling op het gebied van de (digitale) consumentenbescherming is de inwerkingtreding van de Implementatiewet richtlijn consumentenbescherming op 13 juni 2014.<sup>117</sup> De implementatiewet richtlijn consumentenbescherming implementeert de op 25 oktober 2011 tot stand gekomen Richtlijn consumentenrechten<sup>118</sup> in boek 6, 7 en 7A van het Burgerlijk Wetboek, de Wet handhaving consumentenbescherming, de Wet op het financieel toezicht en de Overgangswet nieuw Burgerlijk Wetboek. De implementatiewet voorziet in intrekking van de Colportagewet, die daarmee het zoveelste slachtoffer van de digitalisering lijkt. De implementatiewet ziet echter, net als de richtlijn, op alle overeenkomsten die tussen handelaren en consumenten zijn gesloten: op afstand (bijvoorbeeld via internet), buiten verkooppunten (bijvoorbeeld colportage) dan wel anders dan op afstand en buiten verkooppunten (bijvoorbeeld in de winkel).

Deze kroniek leent zich er niet toe de implementatiewet richtlijn consumentenrechten uitgebreid te behandelen.<sup>119</sup> Belangrijke wijzigingen als gevolg van de implementatiewet zijn de uitbreiding van de bestaande informatieplichten voor handelaren en de verlenging van het bestaande herroepingsrecht van de consument. Om de uitoefening van het herroepingsrecht te vereenvoudigen, is bovendien een standaardformulier voor de herroeping ontwikkeld. De informatieplicht en het herroepingsrecht zijn ook van toepassing op het aanbieden van digitale inhoud, een begrip dat door de richtlijn consumentenrechten is geïntroduceerd. Opvallend is dat de implementatiewet de bepalingen over consumentenkoop ook van overeenkomstige toepassing verklaart op de levering van digitale inhoud die niet op een materiële drager is geleverd aan een consument (enkele uitzonderingen daargelaten).<sup>120</sup>

### 6. Strafrecht en strafvordering

#### 6.1 Cybercrime

Dit jaar berekende McAfee dat cybercrime de Nederlandse economie € 8,8 miljard per jaar kost, ongeveer 1,5 procent van het bruto nationaal product.<sup>121</sup> Dat beeld volgt ook uit het door minister Opstelten gepresenteerde rapport 'Cybersecuritybeeld Nederland'.<sup>122</sup> Hierin wordt geconcludeerd dat de impact van cyberaanvallen toeneemt, waarbij het gebrek aan ICT duurzaamheid een risico vormt voor de maatschappelijke veiligheid. De grootste dreiging gaat uit van beroeps-criminelen en staten. Opmerkelijk is het verband dat het rapport legt tussen de toenemende risico's van cybercrime en de (maatschappelijke) druk op privacybelangen. De uit een behoefte naar veiligheid en controle ontstane grootschalige dataverzamelingen vormen namelijk een risico voor onze cyberveiligheid. Kortom: een vicieuze cirkel.

De strijd tegen cybercrime is dweilen met de kraan open, zo vond het hoofd van het European Cybercrime

Center Troels. Opsporing en vervolging is zinloos. Het duurt lang, kost handen vol geld en aan het eind van de rit blijken de verdachten veelal ongrijpbare Russische criminelen. 'Disruption' van de activiteiten is in zijn beleving

## De levering van een 'gratis' mobiel toestel als onderdeel van een (duur) telefonie-abonnement moet worden aangemerkt als een koop op afbetaling

zinnvoller.<sup>123</sup> Het kabinet blijft desalniettemin investeren in de bestrijding van cybercrime, zo bleek op Prinsjesdag.<sup>124</sup> Dat is ook nodig, want de Nederlandse politie worstelt. Ondanks de invoering van het *High Tech Crime Team*, het *National Cyber Security Center*, het *Computer Emergency Response Team* en gespecialiseerde officieren<sup>125</sup> wordt

gepleit voor reorganisatie van de politie in de strijd tegen cybercrime.<sup>126</sup>

### 6.2 Wetsvoorstel versterking bestrijding computercriminaliteit III

De wetgever maakt haast met de herintroductie van het 'wetsvoorstel versterking bestrijding computercriminaliteit' ('Computercriminaliteit III') dat in mei 2013 in consultatie ging.<sup>127</sup> Het voorstel heeft als doel de toenemende bedreigingen en kwetsbaarheden op het terrein van computercriminaliteit het hoofd te bieden door het juridisch instrumentarium aan te passen naar aanleiding van (technologische) ontwikkelingen. In het kort biedt het wetsvoorstel de opsporingsdiensten de mogelijkheden om op afstand geautomatiseerde werken binnen te dringen en om software te plaatsen voor de opsporing van ernstige vormen van cybercrime waarmee op afstand gegevens in een geautomatiseerd werk kunnen worden doorzocht en ontoegankelijk gemaakt (ook wel: 'terughacken'<sup>128</sup>). Daarnaast wordt heling van computergegevens strafbaar en kunnen verdachten van bepaalde misdrijven worden verplicht mee te werken aan het openen van versleutelde bestanden op hun computer (het zogenaamde decryptiebevel).

Het was de tweede maal dat het wetsvoorstel in consultatie ging. De vorige consultatieronde had jaren geleden zoveel kritiek opgeleverd dat herbezinning noodzakelijk bleek.<sup>129</sup> Voornaamste kritiek was de angst voor

112. Zie B. Nieuwenhuizen, *The legal position and social effects of security breach notification laws*, winnaar van de Internetscriptieprijs 2013. De scriptie is te downloaden op de website [www.internetscriptieprijs.nl](http://www.internetscriptieprijs.nl) en in boekvorm verschenen bij DeLex.

113. HR 11 juli 2014, *NJB* 2014/1439 (*ABN vs. Berzona*).

114. Zie bijv. M. Weij, 'De Nebula-storm is overgewaaid: rust in escrowland'; D. van Engelen, 'De Hoge Raad keert op zijn Nebula-schreden terug in *ABN AMRO v Berzona*', *B913118*; De Brauw Blackstone Westbroek, 'Licensees slightly better off in bankruptcy of Dutch licensor – but not out of the woods'. Kritisch over het gevolg van het *Nebula* arrest voor IE-licenties: H. Struik, 'Nebula in het licht van Oracle vs. UsedSoft. Softwarelicenties in faillissement nader beschouwd', *NJB* 2013/2507, afl. 43, p. 2994-3000.

115. HR 3 november 2006, *NJ* 2006/155 (*Nebula*). Voor een uitgebreide analyse van dit arrest wordt verwezen naar Th.C.J.A. van Engelen, 'E-Goederenrecht', Utrecht: Uitgeverij Boek 9 2013, p. 429-442.

116. HR 13 juni 2014, *NJB* 2014/1236, *JOR* 2014/206 m.nt. J.M. van Poelgeest & J.W.A. Biemans.

117. Wet van 12 maart 2014 tot wijziging van de Boeken 6 en 7 van het Burgerlijk Wetboek, de Wet handhaving consumentenbescherming en enige andere wetten in verband met de implementatie van Richtlijn

2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad (*PbEU* L 304/64) (Implementatiewet richtlijn consumentenrechten).

118. Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad (*PbEU* L 304/64).

119. Voor meer informatie over de Implementatiewet richtlijn consumentenrechten wordt daarom verwezen naar: C. Jeloschek & V. van Druenen, 'De implementatie van het nieuwe regime voor overeenkomsten op afstand. Is de wetgever te ver doorgeschoten wat betreft de levering van digitale inhoud?' *Tvl* 2013/2; M.Y. Schaub, 'Het herroepingsrecht bij overeenkomsten op afstand', *NTBR* 2014/23; A.L.M. Keirse, S.A. Krusinga & M.Y. Schaub 'Nieuws uit Europa: Twee nieuwe wetgevingsinstrumenten: de Richtlijn Consumentenrechten en het gemeenschappelijk Europees kooprecht', *Contracteren*

2012/1; J.W. Rutgers, Kroniek van het Europees privaatrecht, *NJB* 2014/800, afl. 15, p. 1073-1081.

120. C. Jeloschek & V. van Druenen, 'De implementatie van het nieuwe regime voor overeenkomsten op afstand. Is de wetgever te ver doorgeschoten wat betreft de levering van digitale inhoud?' *Tvl* 2013, afl. 2; R. Rinzema & F. Melis, 'Wat betekent het kooprecht voor zakelijke softwarelicenties?', *Computerrecht* 2013/43, afl. 2, p. 88-97; H.A.J. de Jong & G.C.J. Erents, 'Online Overeenkomsten en meer', *Tvl* 2013, afl. 5-6.

121. Center for Strategic and International Studies/McAfee, 'Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II', juni 2014 ([www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf](http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf)). Overigens kan kritisch naar dergelijke cijfers worden gekeken aangezien ze berekend zijn door een bedrijf dat geld verdient aan computerbeveiliging. Desgevraagd kon minister Opstelten de cijfers ook niet bevestigen: Kamervragen aan Minister van Veiligheid en Justitie Opstelten d.d. 13 augustus 2014, 2014Z10959.

122. Jaarrapportage Cybersecuritybeeld Nederland, van Nationaal Cyber Security Centrum, juli 2014.

123. The Register, 'Cuffing darknet-dwelling cyberscum is tricky. We'll 'disrupt' crims

instead, warns top cop', 29 april 2014, [www.theregister.co.uk](http://www.theregister.co.uk).

124. 'Opstellen en Teeven zetten veiligheidsbeleid met kracht voort', zie [www.rijksoverheid.nl](http://www.rijksoverheid.nl).

125. Zie o.a. antwoorden Kamervragen aan Minister van Veiligheid en Justitie Opstelten d.d. 13 augustus 2014, 2014Z10959.

126. Daartoe pleit Hoofd Landelijke Recherche Wilbert Paulissen in 'Onderwereld ontdekt in hoog tempo internet', *Het Financieel Dagblad* 12 juli 2014.

127. Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III).

128. Over de definitie van hacken was overigens het een en ander te doen. Het OM stelde in een campagne dat hacken 'het zonder toestemming inbreken in computers' was, waartegen diverse hackers in een open brief ageerden. Zij voelden zich gecriminaliseerd omdat hacken niet altijd zonder toestemming gebeurt en er ook niet altijd ergens wordt ingebroken. Zie open brief van diverse hackersorganisaties d.d. 26 augustus 2014 op [www.computervrede.nl](http://www.computervrede.nl).

129. Zie bijv.: Advies van de Raad voor de rechtspraak van 30 september 2010 over het wetsvoorstel bestrijding computercriminaliteit, gepubliceerd op [www.rechtspraak.nl](http://www.rechtspraak.nl) onder nr. 2010/38.

censuur als gevolg van de invoering van een verwijderingsbevel door de officier van justitie van internetcontent gericht aan internettussenpersonen, zonder tussenkomst van de rechter-commissaris. Aan die kritiek is de regering tegemoet gekomen. Het is echter de vraag of die 'winst' ook van feitelijke waarde zal zijn voor de bescherming van de vrijheid van meningsuiting. In de praktijk blijkt het Openbaar Ministerie niet zelden het rechterlijke toestemmingsvereiste te omzeilen door uit te gaan van een (te) beperkte definitie van het begrip 'tussenpersoon'. Menig serviceprovider kiest daardoor (in de onjuiste veronderstelling dat het geen strafrechtelijke immuniteit geniet voor *third-party content* ex artikel 54a Sr<sup>130</sup>) eieren voor zijn geld en haalt op (dreigend) verzoek van de officier van justitie content offline.<sup>131</sup>

Hoe dan ook, de kansen voor het hernieuwde wetsvoorstel lijken (mede door de tegemoetkomingen) te zijn toegenomen. Dat wil niet zeggen dat het huidige voorstel kritiekloos wordt omarmd; met name het decryptiebevel stuit op verzet. Dat is niet verwonderlijk, omdat een dergelijk bevel al in de jaren negentig werd overwogen maar uiteindelijk werd geschrapt, omdat het afbreuk deed aan het zwijgrecht.<sup>132</sup> Tijden veranderen.<sup>133</sup>

Ook het voorstel om in het kader van de opsporing 'terug te hacken' krijgt niet bij iedereen de handen op elkaar. Zo is het College Bescherming Persoonsgegevens kritisch omdat het wetsvoorstel onvoldoende blijk geeft van een zorgvuldige afweging binnen de grondwettelijke kaders, met name daar waar het gaat om de vraag of wel een dringende noodzaak (in het licht van artikel 8 EVRM) bestaat.<sup>134</sup> De moeite die het de wetgever al jaren kost om het wetsvoorstel door het parlement te loodsen lijkt overigens mede de voedingsbodem voor een in juni van dit jaar aangekondigde stelselvernieuwing van het Wetboek van Strafvordering. Speerpunt is de behoefte om het strafvorderlijke legaliteitsbeginsel in te perken opdat formele wetgeving voldoende ruimte biedt voor lagere regelgeving (zoals amvb's, ministeriele regelingen en aanwijzingen van het College van procureurs-generaal) waarmee sneller kan worden ingespeeld op maatschappelijke ontwikkelingen en behoeften uit de praktijk. Uitdrukkelijk worden daaronder door de minister ook de technologische ontwikkelingen geschaard.<sup>135</sup>

Overigens lijken de opsporingsdiensten een voorshot te nemen op de toekomstige bevoegdheden. Volgens Bits of Freedom bezit de politie actieve licenties van software waarmee veel digitale opsporingshandelingen uit kunnen worden gevoerd waar de huidige wetgeving nog niet uitdrukkelijk in voorziet.<sup>136</sup>

### 6.3 Technisch opsporen

De moeizame invoering van het wetsvoorstel Computercriminaliteit III toont aan dat wetgeving de technische

ontwikkelingen niet kan bijbenen. Discussies over de toelaatbaarheid zijn het gevolg. Toch blijven eveneens oude technische opsporingsbevoegdheden in zwang.

#### 6.3.1 Taps

Ook deze kroniekperiode staat Nederland weer in de top van de wereldwijde telefoontap statistieken. In 2012 werden er 25 487 telefoontaps aangelegd, een toename van 3%.<sup>137</sup> Het aantal ip-taps steeg nog explosiever: in 2012 werden er 16 676 internettaps geplaatst, het jaar daarvoor waren dat er 3331.<sup>138</sup> Deze forse stijging wordt door minister Opstelten (deels) toegeschreven aan de toename van het aantal smartphones. Ook het aantal bevragingen van historische gegevens neemt jaarlijks toe. In 2012 gebeurde dit 56 825 keer, een stijging van 10% op jaarbasis. Zorgelijke cijfers, zo vindt het College voor de Rechten van de Mens die het kabinet al in 2012 opriep onderzoek te doen; een oproep die dit jaar werd herhaald.<sup>139</sup> Het nut van de telefoontaps staat echter ter discussie. Een ouderwets telefoongesprek voert bijna niemand meer.<sup>140</sup> Het – al dan niet versleuteld – versturen van informatie via internet is veel populairder, waardoor de politie wordt overspoeld door terabytes aan informatie waar zij zich geen raad mee weet.<sup>141</sup>

#### 6.3.2 Technische hulpmiddelen (IMSI-catcher en stille sms)

Discussie was er deze kroniekperiode (opnieuw) over de (legaliteit) van de inzet van de *IMSI-catcher* en de *'stealth sms'*, twee opsporingsmethoden die niet expliciet in de wet zijn geregeld en waarmee de locatie van een verdachte kan worden achterhaald.<sup>142</sup> Over de toelaatbaarheid werd zeer wisselend gedacht,<sup>143</sup> maar de Hoge Raad oordeelde dat de grondslag voor de inzet van deze opsporingsmiddelen kon worden gevonden in artikel 3 Politiewet in combinatie met de artikelen 141 en 142 Sv.<sup>144</sup> Overigens betekent dit niet dat de inzet onder alle omstandigheden is toegestaan. Dit hangt af van de duur en intensiteit van de inzet en van het beeld dat van de bewegingen van de verdachte wordt verkregen. Minister Opstelten lichtte toe dat het gebruik van de stille sms dient te worden verantwoord in een (verplicht) proces-verbaal waarin de duur en de frequentie van de inzet worden geverbaliseerd.<sup>145</sup>

#### 6.3.3 Keylogger

Nieuwe onenigheid valt te verwachten over de inzet van de *keylogger*, software die het mogelijk maakt om o.a. *real-time* informatie, zoals toetsaanslagen, screenshots en muisbewegingen, van een computer op te slaan en te monitoren. Voor zover bekend werd hiervan in Nederland dit jaar voor het eerst gebruik gemaakt in de *Amanda Todd* zaak.<sup>146</sup> De wettelijke basis voor de keylogger is diffuus. Daarbij speelt mee dat de keylogger bij uitstek 'terug-hack' software lijkt zoals voorgesteld in het wetsvoorstel Computercriminaliteit III. Daaruit zou kunnen volgen dat de inzet vooralsnog niet is toegestaan.

#### 6.3.4 Drones

Onbemande luchtvaartuigen die op afstand worden bestuurd zijn niet meer weg te denken uit het straat-, of beter gezegd, luchtbeeld. Het is niet alleen leuk speelgoed, maar ook een ideaal middel voor toezicht en opsporing.

**De implementatiewet voorziet in intrekking van de Colportagewet, die daarmee het zoveelste slachtoffer van de digitalisering lijkt**

Reeds in 2013 zei de Minister van Justitie en Veiligheid dat drones van Defensie door de politie werden ingezet in opsporingsonderzoeken en voor de (handhaving van) de openbare orde.<sup>147</sup> De inzet van drones ten behoeve van de opsporing is echter met schimmigheid omgeven.<sup>148</sup> Onlangs werd door de politierechter de behandeling van een strafzaak aangehouden om meer informatie te verkregen over de inzet van een drone.<sup>149</sup>

Dit jaar is een wetsvoorstel aangenomen waardoor gemeenten de bevoegdheid krijgen gebruik te maken van flexibel cameratoezicht.<sup>150</sup> Voor de centrale overheid ontbreekt evenwel regelgeving, hetgeen leidde tot Kamervragen.<sup>151</sup> Privacy, aansprakelijkheid en wettelijke bevoegdheden zijn daarbij terugkerende thema's. Het vliegen met een drone voor particulieren is geregeld in de Luchtvaartwet en de daarbij behorende Regeling modelvliegen die per 1 juli 2013 is gewijzigd.<sup>152</sup> Sindsdien is het verboden om bedrijfsmatig met een drone te vliegen, tenzij hiertoe een ontheffing is verleend.<sup>153</sup>

### 6.3.5 Aanwijzing handhaving Telecommunicatiewet

Per 1 juli 2014 is de Aanwijzing handhaving Telecommunicatiewet in werking getreden.<sup>154</sup> Deze aanwijzing geeft regels voor de opsporing en vervolging bij overtredingen van de Telecommunicatiewet, bijv. het gebruik van *jam-mers* (blokkeerzenders van mobiele-telefonie en GPS signalen) en de verstoring van frequentieruimte in radio-signalen door etherpiraten of marifoons zonder vergunning.

### 6.4 Delen van terroristisch beeldmateriaal

Weinig onderwerpen hebben de discussie over de uitingsvrijheid zo aangewakkerd als het op sociale media delen van de video waarop de Amerikaanse journalist James Foley door jihadisten wordt onthoofd. De video werd al kort na plaatsing vele duizenden malen gedeeld. Na ontstane ophef hebben zowel YouTube als Twitter actief stappen ondernomen tegen gebruikers die de video deelden.<sup>155</sup> In Groot-Brittannië waarschuwde de politie zelfs dat het delen, downloaden en bekijken van de video strafbaar zou zijn onder de antiterrorwetgeving.<sup>156</sup> Ook in de Tweede Kamer werd (mede) naar aanleiding van de onthoofdingsvideo gedebatteerd over de wenselijkheid van strafbaarstelling van dergelijk beeldmateriaal. Een motie om de verheerlijking van terrorisme strafbaar te stellen redde het echter niet.<sup>157</sup> De aanpak van dergelijke video's valt in Nederland mogelijk onder de strafbaarstelling van opruiing (tot een terroristisch misdrijf) op basis van artikel 131 lid 2 Sr. Zonder opzet op het aanzetten tot een misdrijf of agressie tegen het gezag lijkt echter het enkele delen van de beelden daar niet snel onder te vallen.

### 6.5 Rechtspraak

De Hoge Raad oordeelde in 2013 dat een inbraak op een router met een gekraakt wachtwoord, het 'meesurfen met de burens', onder omstandigheden computervrederebreuk kan opleveren. Het hof had de verdachte vrijgesproken omdat een router niet geschikt is om zowel gegevens op te slaan, als te verwerken en over te dragen, de drie cumu-

130. Anders dan de civielrechtelijke immuniteit van aansprakelijkheid voor *third party content* voor 'tussenpersonen', is de strafrechtelijke immuniteit absoluut. Uit artikel 54a Sr volgt dat een tussenpersoon geen verplichting heeft content te verwijderen zo lang geen bevel tot verwijdering (na machtiging van de rechter-commissaris) is ontvangen. De in par. 3.2 besproken uitspraken die de civielrechtelijke immuniteit beperken hebben derhalve geen invloed op de strafrechtelijke immuniteit van tussenpersonen.

131. Dat artikel 54a Sr niet geheel van onwaarde blijkt en in de praktijk soms nog wel van de verwijderingsbevoegdheid gebruik werd gemaakt bleek in HR 15 april 2014 ECLI:NL:HR:2014:908 waarin de Hoge Raad bepaalde dat de procedure ex artikel 552a Sv niet openstond voor beklag tegen een bevel zoals bedoeld in artikel 54a Sr.

132. *Kamerstukken II 1998/99*, 26671, 3, p. 26.

133. Zie voor kritiek op het voorstel en mogelijke strijd met het *nemo tenetur* beginsel: Advies van de Raad voor Rechtspraak d.d. 4 juli 2013 over het wetsvoorstel Computercriminaliteit III, gepubliceerd op [www.rechtspraak.nl](http://www.rechtspraak.nl) onder nr. 2013/27.

134. Brief College Bescherming Persoonsgegevens aan de Minister van Veiligheid en

Justitie d.d. 17 februari 2014, gepubliceerd op [www.cbppweb.nl](http://www.cbppweb.nl).

135. Toespraak minister Opstelten tijdens het congres Modernisering Wetboek van Strafvordering van 19 juni 2014, gepubliceerd op [www.rijksoverheid.nl](http://www.rijksoverheid.nl).

136. Zie 'Is het hack straks van de dam', op [www.bof.nl](http://www.bof.nl).

137. Brief van de minister aan de Tweede Kamer, 'Tapstatistiek 2012', 18 juli 2013.

138. G. Odinet, 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.

139. Mensenrechten in Nederland 2012, jaarlijkse rapportage van het College voor de Rechten van de Mens.

140. G. Odinet, 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, p. 152.

141. G. Odinet, 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, p. 155-167.

142. Artikel 126nb Sv regelt weliswaar de inzet van de IMSI-catcher, maar alleen voor zover hiermee het telefoonnummer van een

verdachte (en dus niet zijn locatie) wordt achterhaald.

143. Voor rechtspraak omtrent de IMSI-catcher: zie Rb. Utrecht 23 januari 2009, ECLI:NL:RBUTR:2009:BH0748 en ook Gerechtshof Arnhem 24 januari 2012, ECLI:NL:GHARN:2012:BV3076. Voor uitspraken over de stealth sms zie: Gerechtshof Den Bosch 15 augustus 2013,

ECLI:NL:GHSHE:2013:4046 (kritisch over de beheersbaarheid van de inzet), Gerechtshof Arnhem-Leeuwarden 7 juli 2013,

ECLI:NL:GHARL:2013:5849; Rb. Amsterdam 8 maart 2011,

ECLI:NL:RBAMS:2011:BQ9049, Rb. 's-Hertogenbosch 14 juni 2012, ECLI:NL:RBSHE:2012:BW8633; Rb. Amsterdam 31 mei 2011,

ECLI:NL:RBAMS:2011:BQ9049. Zie verder: ECLI:NL:RBSHE:2012:BW8610, ECLI:NL:RBSHE:2012:BW8620, ECLI:NL:RBSHE:2012:BW8629, ECLI:NL:RBAMS:2011:BP7233.

144. Hoge Raad 1 juli 2014, ECLI:NL:HR:2014:1562 (IMSI); Hoge Raad 1 juli 2014, ECLI:NL:HR:2014:1569 en Hoge Raad 1 juli 2014, ECLI:NL:HR:2014:1563 (stealth).

145. *Aanhangsel handelingen II 2013/14*, 1906.

146. 'OM zette keylogger in bij Todd-zaak',

NOS 25 juni 2014, [www.nos.nl](http://www.nos.nl). In deze zaak werden tientallen meisjes afgeperst en gedwongen tot seksuele handelingen voor de webcam.

147. *Aanhangsel Handelingen II 2012/13*, 1847.

148. Zie ook: Brief 'Besluit wob-verzoek drones/UAV', Politie Zeeland-West-Brabant 1 mei 2013, en Brief 'Besluit op uw WOB-verzoek', Politie Noord-Holland 27 augustus 2013, [www.politie.nl](http://www.politie.nl).

149. 'Rechtbank: opheldering over drone boven Arnhem', Omroep Gelderland 4 augustus 2014.

150. *Kamerstukken II 2012/13*, 33582, 2.

151. Zie bijv.: *Aanhangsel handelingen II 2013/14*, 1574.

152. *Stcr.* 2013, 17149.

153. Regeling sluiting luchtruim boven Den Haag en kasteel Drakensteijn, Regeling sluiting luchtruim Scheveningen en Regeling sluiting luchtruim nationale herdenkingen.

154. Aanwijzing handhaving Telecommunicatiewet (2014A003).

155. 'Viewing or sharing beheading video could be a criminal offence police warn', *The Telegraph* 20 augustus 2014.

156. 'Police warn sharing James Foley killing video is a crime', *The Guardian* 20 augustus 2014.

157. *Kamerstukken II 2013/14*, 29754, 255.

latieve vereisten voor een geautomatiseerd werk. Een onderdeel dat de Hoge Raad weliswaar deelde, maar desondanks casseerde omdat ook een geheel netwerk (dus computer(s) en of router(s) samen) aangemerkt kunnen worden als 'geautomatiseerd werk'.<sup>158</sup>

Veelbesproken was de aanval op Spamhaus dat slachtoffer werd van wat in de media 'de grootste cyberaanval ooit' werd genoemd.<sup>159</sup> Geruime tijd waren delen van het internet niet of lastiger te bereiken. In april 2013 werd in Spanje een Nederlander aangehouden als hoofdverdachte, dit naar aanleiding van een Europees aanhoudingsbevel van het Nederlandse Openbaar Ministerie.

Een andere relevante zaak voor het hacken van 2000 computers.<sup>160</sup> Hij gebruikte o.a. een computer van een derde voor het bekendmaken van het VWO-eindexamen Frans 2013, dat nog moest worden afgenomen. Mede hierdoor kwam de diefstal van eindexamens bij de Ibn Ghal-donschool aan het licht.

Dat Russen (zie de uitspraak van Troels in par. 6.1) niet altijd de dans ontspringen bleek uit de uitspraak van de rechtbank die de uitlevering toestond van Vladimir Drinkman aan zowel de Verenigde Staten, als Rusland.<sup>161</sup> Drinkman werd verdacht van het deel uitmaken van een groep van vijf hackers die 160 miljoen creditcardgegevens zou hebben buitgemaakt waarmee meer dan 300 miljoen dollar zou zijn gestolen. De minister mag nu bepalen waar deze verdachte als eerste wordt berecht.

### 6.6 Digitalisering binnen rechterlijke macht en OM

In de rechtspraak wordt tegenwoordig niet alleen gedeeld over digitale (strafbare) feiten, de digitale wereld bereikt nu langzaam ook de zittende en staande magistratuur zelf. Zo werd in september 2013 het Slachtoffer Informatie Portaal geopend<sup>162</sup> en startte het OM begin 2014 het Digitaal Loket Verkeer.<sup>163</sup> Ook kunnen burgers sinds dit jaar online een rechtszaak starten bij de eKantonrechter.<sup>164</sup> Videorechtspraak, waarbij sprake is van een videoverbinding tussen de zittingszaal en de locatie van de verdachte, is ook in opkomst.<sup>165</sup> Sinds september dit jaar is een start gemaakt met de Advocatenportaal waarop strafrechtadvocaten digitaal dossiers kunnen downloaden afkomstig uit

GPS (Geïntegreerd Processysteem Strafrecht).

Toch gaat de ontwikkeling traag. GPS kreeg in deze kroniekperiode bijvoorbeeld de nodige kritiek te verduren; de kosten van de ontwikkeling en invoering zouden veel hoger zijn uitgevallen dan vooraf begroot en de doelstellingen werden niet gehaald.<sup>166</sup> Om die reden wordt nog veelvuldig COMPAS gebruikt, software die stamt uit 1988 en draait op MS DOS.<sup>167</sup> Je zou er bijna nostalgisch van worden.

## 7. Afsluiting

De hier voorgaande verkenning illustreert de veelzijdige en gevarieerde interactie tussen technologische innovatie en recht. Nieuwe technieken doen per definitie hun intrede voordat het recht heeft bedacht hoe ze te kwalificeren en (eventueel) reguleren. Volgens James Boyle is dat maar

## Ook deze kroniekperiode staat Nederland weer in de top van de wereldwijde telefontapstatistieken

goed ook, en doen we er verstandig aan nieuwe technieken eerst een decennium of wat hun gang te laten gaan voordat we ze in wetgeving proberen te vangen. Daarmee wil hij niet zeggen dat (aanbieders van) nieuwe technieken ondertussen ongestoord hun gang mogen gaan, maar dat de eerste jaren altijd – ook in juridisch opzicht – rommelig verlopen. Wat dat betreft verloopt de juridische receptie van de voortwoekerende informatierevolutie geheel volgens plan. Dat rommelige proces moeten we vrolijk zijn gang laten gaan, ook als de gevestigde orde vraagt om beteugeling van vernieuwing die het vertrouwen evenwicht verstoort en comfortabele business-modellen bedreigt. •

<sup>158</sup>. HR 26 maart 2013,

ECLI:NL:HR:2013:BY9718.

<sup>159</sup>. Daarop was ook de nodige kritiek, zie: 'Nederlander coördineert "grootste cyberaanval ooit" NOT', NOS.

<sup>160</sup>. Rb. Rotterdam 4 september 2014, ECLI:NL:RBROT:2014:7379.

<sup>161</sup>. Rb. Rotterdam 16 april 2014,

ECLI:NL:RBROT:2014:7371 en

ECLI:NL:RBROT:2014:7370, alsmede HR 26 augustus 2014, ECLI:NL:HR:2014:2458.

<sup>162</sup>. 'Uitbreiding slachtofferzorg OM met online informatieportaal', Openbaar Ministerie, 4 september 2013, [www.om.nl](http://www.om.nl).

<sup>163</sup>. 'Digitaal in beroep tegen verkeersboetes', Openbaar Ministerie 27 januari 2014,

[www.om.nl](http://www.om.nl).

<sup>164</sup>. 'Nu ook online rechtspraak voor burgers bij de eKantonrechter', de Rechtspraak, 3 juni 2014, [www.rechtspraak.nl](http://www.rechtspraak.nl).

<sup>165</sup>. 'De rechtspraak start als eerste rechtbank met videorechtspraak vanuit gemeentehuis', de Rechtspraak 7 mei 2014, [www.rechtspraak.nl](http://www.rechtspraak.nl).

<sup>166</sup>. 'Voorganger problematisch justitiesysteem GPS draait nog', *Binnenlands Bestuur* 27 juni 2013, [www.binnenlandsbestuur.nl](http://www.binnenlandsbestuur.nl).

<sup>167</sup>. P. Langbroek & M. Tjaden, 'ICT in de strafrechtketen, de ontwikkeling en implementatie van nieuwe systemen bij het Openbaar Ministerie', *Proces* 2008/1, p. 2-8; en: *Handelingen II* 2013/14, 109, item 6, p. 4.