

# Kroniek technologie en recht

Remy Chavannes, Dorien Verhulst & Anke Strijbos<sup>1</sup>

Alle traditionele rechtsgebieden zien zich inmiddels geconfronteerd met technische casuïstiek. Toch zijn er wel degelijk een aantal samenhangende (delen van) rechtsgebieden, waarvan de ontwikkeling momenteel wordt gedomineerd door technologische ontwikkelingen: de uitleg en handhaving van het auteursrecht op internet, allerlei aspecten van het privacyrecht, het recht op informatievrijheid en het aansprakelijkheidsregime voor internetbedrijven op basis van de e-Commercerichtlijn. Op het snijvlak van deze rechtsgebieden opereren grote technologiebedrijven als Apple, Facebook, Amazon en Google. Deze kroniek concentreert zich op enkele grote actuele digitale thema's.

## 1. Inleiding

Een jurist die zich bezig houdt met 'technologie en recht' is noodgedwongen van alle markten thuis. Alle traditionele rechtsgebieden kennen inmiddels technische casuïstiek. Van aansprakelijkheidskwesties bij zelfrijdende auto's,<sup>2</sup> een strafbeschikking ondanks elektronische hondenriem,<sup>3</sup> het gebruik van automatische nummerbordherkenning bij de fiscale controle van rittenregistraties van lease-auto's<sup>4</sup> tot de tweedehands verkoop van e-books.<sup>5</sup> Geen jurist is in al die rechtsvragen specialist. Dat neemt niet weg dat er wel degelijk een aantal samenhangende (delen van) rechtsgebieden zijn, waarvan de ontwikkeling momenteel wordt gedomineerd door technologische ontwikkelingen: de uitleg en handhaving van het auteursrecht op internet, allerlei aspecten van het privacyrecht, het recht op informatievrijheid en uiteraard het aansprakelijkheidsregime voor een scala aan internetbedrijven op basis van de e-Commercerichtlijn.

Op het snijvlak van deze rechtsgebieden opereren de grote technologiebedrijven van de 21<sup>e</sup> eeuw. Zij vormen het scharnierpunt van de digitale economie, ontworpen bestaande markten met technische innovaties

en zijn in al hun doen en laten voorwerp van maatschappelijk debat. Deze Apple's, Facebook's, Amazon's en Google's, maar ook de Adyen's en Blendle's van de wereld, opereren mondiaal. Zij zorgen wereldwijd voor nieuwe juridische vragen in het digitale domein, zowel traditioneel grensoverschrijdende vragen over rechtsmacht en de internationale reikwijdte van rechterlijke bevelen, als van oudsher nationale vragen over maatschappelijke zorgvuldigheid en de afweging van grondrechten. Zij vormen daarmee een logisch prisma om het digitale spectrum te bekijken en zijn een aanknopingspunt voor onze kroniek.

Ondanks de oneindig brede titel komt in deze kroniek dus veel niet aan bod. We concentreren ons op enkele grote actuele digitale thema's, bespreken alleen de belangrijkste ontwikkelingen, en dat op hoofdlijnen.<sup>6</sup> Daarmee blijven niet alleen allerlei non-thema's met een diffuus en onzelfstandig karakter ('big data', 'internet of things', 'value gap') grotendeels buiten beschouwing, maar ook hele rechtsgebieden die inmiddels een eigen kroniek zouden kunnen vullen; bijvoorbeeld het ICT-contracten- en consumentenrecht. De kroniekperiode bestrijkt de afgelopen twee jaar.<sup>7</sup>

### Auteurs

1. De auteurs zijn allen advocaat bij Brinkhof in Amsterdam. Zij danken Boukje van der Maazen voor haar bijdragen en suggesties. De kroniek beschrijft de periode oktober 2014 - september 2016.

### Noten

2. E. Tjong Tjin Tai & S. Boesten, 'Aansprakelijkheid, zelfrijdende auto's en andere zelfbestuurde objecten', *NJB* 2016/496, afl. 10.
3. B. Wallage & J. Slobbe, 'Een aantekening bij uitspraak over digitale hondenriem', *NJB* 2016/400, afl. 8.
4. Volgens A-G Niessen een inmenging in de

- persoonlijke levenssfeer van betrokkenen zonder de vereiste wettelijke grondslag, PHR 16 augustus 2016, ECLI:NL:PHR:2016:853 en ECLI:NL:PHR:2016:885.
5. Hof Amsterdam 20 januari 2015, ECLI:NL:GHAMS:2015:66 (*Tom Kabinet*).
  6. Zie voor een uitgebreide bespreking van

- digitale thematiek bijv. ook de preadviezen van de Nederlandse Juristenvereniging onder de noemer Homo Digitalis en de bespreking daarvan in het *NJB*, zie: *Handelingen NJV* 2016-1 en *NJB* 2016/1072 t/m 1075, afl. 22.
7. De vorige kroniek technologie en recht verscheen in 2014, *NJB* 2014/1836, afl. 35.

## 2. 'Digital Single Market'

### 2.1. Overzicht mededelingen en wetgevingsvoorstellen

In de loop van de verslagperiode heeft de Europese Commissie stapsgewijs een 'Strategie voor een digitale eenge-maakte markt voor Europa' gepresenteerd, in de wandel-gangen bekend als de 'Digital Single Market' – of DSM-strategie.<sup>8</sup> De voorstellen hebben vooral betrekking op auteursrecht en naburige rechten, maar waaieren uit naar onder meer mediaregulering en consumentenbe-scherming. Het element van digitale SM zit vooral in de hoeveelheid, omvang, en omslachtige benamingen van de opeenvolgende mededelingen en wetgevingsvoorstellen:

In mei 2015 publiceerde de Commissie een eerste DSM-mededeling, waarin zij haar strategie in (zeer) grote lijnen uiteenzette.<sup>9</sup>

In december 2015 volgde een mededeling over 'een modern, meer Europees kader voor auteursrechten'<sup>10</sup> en afzonderlijke wetgevingsvoorstellen over grensover-schrijdende portabiliteit van online-inhoudsdiensten,<sup>11</sup> overeenkomsten voor de levering van digitale inhoud;<sup>12</sup> en online-verkoop en andere verkoop op afstand van goederen.<sup>13</sup>

In mei 2016 kwamen een mededeling over online platforms<sup>14</sup> en wetgevingsvoorstellen om de Richtlijn audiovisuele mediadiensten te moderniseren;<sup>15</sup> en om geoblocking aan banden te leggen.<sup>16</sup>

## Afgaand op de eerste reacties zal de Commissie concluderen dat haar voorstellen kennelijk een redelijk evenwicht hebben gevonden: iedereen is boos

In september 2016 publiceerde de Commissie in september 2016 een mededeling over 'het bevorderen van een eerlijke, efficiënte en competitieve Europese op het auteursrecht gebaseerde economie'<sup>17</sup> vier wetgevings-voorstellen over auteursrecht in de DSM (de 'DSM-richt-lijn'),<sup>18</sup> de uitoefening van auteursrechten en naburige rechten van omroeporganisaties (de 'online omroep ver-ordening'),<sup>19</sup> en de implementatie van het Verdrag van Marrakesh inzake de rechten van blinden en slechtzienden;<sup>20</sup> en een studie naar de werking van de Satelliet- en Kabelrichtlijn.<sup>21</sup>

Het voorstellenpakket zal in Brussel ongetwijfeld een levendig wetgevingsproces ondergaan. Afgaand op de eerste reacties zal de Commissie concluderen dat haar voorstellen kennelijk een redelijk evenwicht hebben gevonden: iedereen is boos, van uitgevers en omroepen tot consumenten tot internettussenpersonen en -plat-forms. De reacties zijn echter meer dan een serie voor-spelbare lobbyreflexen: kritiek is er ook op de begripje-

lijkheid, coherentie en ambitie van de voorstellen. Van de stoere voornemens waarmee de huidige Commissie in 2014 aan haar mandaat begon – het neerhalen van silo's tussen rechtsgebieden en lidstaten, het hervormen van het auteursrecht voor de digitale revolutie<sup>22</sup> – is weinig terecht gekomen.

### 2.2. Consumentenbescherming

De in december 2015 gepresenteerde voorstellen inzake online-verkoop van goederen en verkoop van digitale inhoud beogen beide maximumharmonisatie en zijn al eerder besproken in het *NJB*.<sup>23</sup> Het voorstel over online-verkoop van goederen bouwt voort op Richtlijn 1999/44/EG en scherpt (met name) daarin gestelde regels omtrent non-conformiteit aan. Het tweede voorstel ziet op over-eenkomsten tot levering van digitale inhoud, waarover in veel EU-lidstaten wetgeving ontbreekt. Het begrip 'digitale inhoud' is diffuus. Uit de considerans blijkt dat het 'Inter-net of Things' er expliciet buiten valt en dat geldt ook voor digitale inhoud die als integraal deel van goederen functioneert. Belangrijk is dat de richtlijn ook van toepas-sing zal zijn op overeenkomsten waarbij de consument actief een andere tegenprestatie dan geld levert, bijvoor-beeld (persoons)gegevens.

Het voorstel voor een verordening tot totstandbren-ging van grensoverschrijdende portabiliteit van online-inhoudsdiensten moet consumenten in staat stellen om ook in het buitenland gebruik te maken van online-inhoudsdiensten waartoe zij thuis legaal toegang heb-ben. Dit 'Uitzending Gemist op de camping'-voorstel lijkt vooraansnog te kunnen rekenen op een relatief breed draagvlak, al waarschuwen omroepen en producenten dat het zal leiden tot afnemende investeringen in Europese programma's.

### 2.3. Platformregulering

De Platform-mededeling van mei 2016 werd voorafgegaan door een publieke consultatie ter evaluatie van het in de e-Commercerichtlijn neergelegde aansprakelijkheidsregi-me voor tussenpersonen.<sup>24</sup> Daaruit kwam onder meer naar voren dat het begrip 'platform' een eclecticische groep digitale diensten en dienstverleners omvat, die zich niet leent voor één alomvattende probleemanalyse of wetge-vingsaanpak. In de mededeling kondigde de Commissie aan de bestaande safe harbours vooraansnog te zullen handhaven, maar sprak zij wel een aantal concrete pun-ten van zorg uit, waaronder de 'verdeling van inkomsten voor het gebruik van auteursrechtelijk beschermd materi-aal'. Dat de Commissie in dit kader het aansprekende maar weinig precieze begrip 'value gap' hanteerde, was een opsteker voor de content-industrie wier knappe lobby-vondst het is.<sup>25</sup> Ondertussen vroeg ook het Nederlandse kabinet zich af hoe het beste met 'platforms' kan worden omgegaan; het zette een aantal studies uit. De koers lijkt vooraansnog ingezet op een sectorspecifieke benadering. Vlak voor het verschijnen van deze kroniek kondigde de ACM aan een marktstudie naar online video platforms te zullen houden.<sup>26</sup>

Het Commissie-voorstel tot wijziging van de Richt-lijn Audiovisuele Mediadiensten ('AVMS-richtlijn') brengt met zich mee dat de richtlijn voortaan ook van toepas-sing zal zijn op 'videoplatformdiensten'. De verplichtin-

gen voor deze categorie nieuwe normadressaten zijn vooralsnog beperkt: zij moeten passende maatregelen nemen om *hate speech* tegen te gaan en om minderjari-

## Er is weinig aanleiding te veronderstellen dat de existentiële crisis van nieuwsuitgevers wordt veroorzaakt door gebrek aan IE-rechten

gen te beschermen. De toekomst moet uitwijzen welke aanbieders in deze nieuwe categorie zullen vallen en hoe de nieuwe verplichtingen zich verhouden tot de systema-

tiek van de e-commercerichtlijn, die platformdiensten zonder kennis van problematische inhoud juist immunitet biedt en bovendien algemene monitoring verbiedt. Het voorstel brengt verder verplichtingen voor lineaire en on-demand mediadiensten meer op een lijn, enerzijds door flexibilisering van de reclameregels en anderzijds door bijvoorbeeld het quotum voor Europese producties van 20% voortaan ook toe te passen op de catalogus van een mediadienst op aanvraag.<sup>27</sup> Het Nederlandse kabinet staat kritisch tegenover de nieuwe regels voor videoplatformdiensten, zij pleit voor een 'level playing field' voor alle audiovisuele mediadiensten door middel van een vermindering van regels.<sup>28</sup>

### 2.4. Auteursrecht en naburige rechten

De in september 2016 voorgestelde DSM-richtlijn en online omroepverordening worden uitgebreid beschreven door Visser in een aankomend nummer van *NTER*.<sup>29</sup> De richtlijn bevat dwingendrechtelijke beperkingen voor onderwijs, onderzoek en erfgoedinstellingen; een verplichting voor grote hosting platforms om 'het functioneren' van 'overeenkomsten met rechthebbenden' te 'garanderen';<sup>30</sup> en een fel bekritiseerd nieuw naburig recht voor

8. Zie [ec.europa.eu/priorities/digital-single-market\\_enopen\\_in\\_new](http://ec.europa.eu/priorities/digital-single-market_enopen_in_new) en het persbericht van de Europese Commissie van 6 mei 2015, <https://goo.gl/IAf7W4>.

9. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité Van De Regio's: Strategie voor een digitale eengemaakte markt voor Europa, 6 mei 2015, COM(2015) 192 final.

10. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité Van De Regio's: Naar een modern, meer Europees kader voor auteursrechten, 9 december 2015, COM(2015) 626 final.

11. Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de totstandbrenging van grensoverschrijdende portabiliteit van online-inhoudsdiensten in de interne markt, 9 december 2015, COM(2015) 627 final.

12. Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud, 9 december 2015, COM(2015) 634 final.

13. Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de online-verkoop en andere verkoop op afstand van goederen, 9 december 2015, COM(2015) 635 final.

14. Mededeling van de Commissie over online platforms en de digitale eengemaakte markt, 25 mei 2016, COM(2016) 288 final.

15. Voorstel voor een Richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten in het licht van een veranderende marktsituatie, 25 mei 2016, COM(2016) 287 final.

16. Voorstel voor een Verordening van het Europees Parlement en de Raad inzake de aanpak van geoblocking en andere vormen van discriminatie van klanten op basis van nationaliteit, verblijfplaats of plaats van vestiging in de interne markt en tot wijziging van Verordening (EG) 2006/2004 en Richtlijn 2009/22/EG, 25 mei 2016, COM(2016) 289 final. Voor een bespreking zie: T. Weermeijer & N.C. Lodder, 'De Geoblocking-verordening: digitale EU-grenzen doorbroken?', *Tijdschrift voor Internetrecht* 2016/3.

17. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité Van De Regio's: Het bevorderen van een eerlijke, efficiënte en competitieve Europese op het auteursrecht gebaseerde economie in de digitale eengemaakte markt, COM(2016) 592 final.

18. Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016) 593 final.

19. Proposal for a Regulation laying down rules on the exercise of copyright and related rights applicable to certain online trans-

missions of broadcasting organisations and retransmissions, COM(2016) 594 final.

20. Proposal for a Regulation of the European Parliament and the Council on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print disabled, 14 september 2016, COM(2016) 595; Proposal for a Directive of the European Parliament and the Council on certain permitted uses of works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print disabled and amending Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, 14 september 2016, COM(2016) 596 final.

21. Survey and data gathering to support the evaluation of the Satellite and Cable Directive 93/83/EEC and assessment of its possible extension, 30 september 2016, SMART 2015/0075.

22. Zie o.a. de 'missiebriefen' van Commissievoorzitter Juncker aan verantwoordelijke commissarissen Anspij ([https://ec.europa.eu/commission/sites/cwt/files/commissioner\\_mission\\_letters/anspi\\_en.pdf](https://ec.europa.eu/commission/sites/cwt/files/commissioner_mission_letters/anspi_en.pdf)) en Oettinger ([https://ec.europa.eu/commission/sites/cwt/files/commissioner\\_mission\\_letters/oettinger\\_en.pdf](https://ec.europa.eu/commission/sites/cwt/files/commissioner_mission_letters/oettinger_en.pdf)).

23. Vanessa Mak, 'Op weg naar een Europese "Digital Single Market"',

*NJB* 2016/397, afl. 8.

24. Voor een bespreking zie: N. Helberger, 'Enkele reflecties op de Europese platformconsultatie', *Mediaforum* 2016-1, p. 1.

25. Mededeling van de Commissie over online platforms en de digitale eengemaakte markt, 25 mei 2016, COM(2016) 288 final. Zie voor een bespreking van verschillende standpunten over het al dan niet bestaan van een 'value gap' het verslag van L. Annemaet van 11 juli 2016 van het daaraan gewijde IE-Forum Zomercongres, IEF16092.

26. Nieuwsbericht ACM, 'Online video platforms onder de loep!', 21 september 2016, [www.acm.nl](http://www.acm.nl).

27. Voorstel voor een Richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten in het licht van een veranderende marktsituatie, COM(2016) 287 final. Zie voor een uitgebreide bespreking prof. L. Woods, 'The proposed new Audiovisual Media Services Directive: Key Features', [eulawanalysis.blogspot.nl](http://eulawanalysis.blogspot.nl), 26 mei 2016.

28. *Kamerstukken II* 2015/2016, 22112, 2170.

29. D.J.G. Visser, 'Viermaal auteursrecht in de digitale eengemaakte markt', verwacht in *NTER*.

30. Voorgesteld art. 13 DSM-richtlijn. Uit de tekst van de bepaling wordt niet duidelijk om welke overeenkomsten het gaat, en wie die op welke grond zou moeten sluiten.

nieuwsuitgevers.<sup>31</sup>

Er is weinig aanleiding te veronderstellen dat de existentiële crisis van nieuwsuitgevers wordt veroorzaakt door gebrek aan IE-rechten; ervaringen met soortgelijke nabuurrechtelijke regelingen in Spanje en Duitsland zijn bepaald geen aanbeveling. Aan het Commissievoorstel ging een openbare consultatie vooraf, maar wie de inzendingen<sup>32</sup> vergelijkt met het uiteindelijke voorstel moet zich afvragen hoeveel zin het heeft om aan zo'n consultatie mee te doen. Vlak voor het ter perse gaan van deze kroniek bekende verantwoordelijk Eurocommissaris Oettinger kleur, toen hij een bijeenkomst van Duitse uitgevers voorhield dat zij moesten 'uitzwermen' om zijn voorstellen te promoten, en hun online-journalisten moesten weerhouden van verdere kritiek daarop, omdat 'we anders met te weinig zullen zijn'.<sup>33</sup>

### 3. Digitaal auteursrecht, platforms en tussenpersonen

#### 3.1. Hyperlinks

In het arrest *GS Media*, over hyperlinks op *GeenStijl.nl* naar uitgelekte Playboy-foto's van Britt Dekker, boog het Hof van Justitie zich over de auteursrechtelijke kwalificatie van de hyperlink.<sup>34</sup> A-G Wathelet adviseerde dat een hyperlink naar een zonder toestemming van de rechthebbende gepubliceerd werk op internet géén nieuwe mededeling aan het publiek vormt, en zelfs überhaupt geen mededeling is.<sup>35</sup> Het Hof oordeelde daarentegen dat een hyperlink die weet of redelijkerwijs moet weten dat zijn link wijst naar een werk dat zonder toestemming op internet is gepubliceerd, dat werk daarmee mededeelt aan het publiek.<sup>36</sup> Wanneer de hyperlink naar een ongeautoriseerde publicatie is geplaatst met commercieel oogmerk, geldt een weerlegbaar vermoeden dat de hyperlinker wist dat er geen toestemming was. De uitspraak is daarmee goed nieuws voor rechthebbenden (en de stichting BREIN) in de strijd tegen grootschalige inbreuken door sites die volstaan met torrents en links naar gepirateerde streams van sportwedstrijden, die zich nu moeilijker kunnen verschuilen achter het standpunt dat zij slechts verwijzen naar inbreuken elders op internet.

Lastiger is de uitspraak voor professionele en minder professionele online-media. Als de aanwezigheid van reclame op de site voldoende is om 'commercieel oogmerk' aan te nemen, moeten journalisten, bloggers en twitteraars voorafgaand aan elke hyperlink onderzoeken of die niet verwijst naar een (pagina met een) werk dat zonder toestemming van de rechthebbende is gepubliceerd. In elk geval bij 'Groot Wereldnieuws' zullen zij een beroep kunnen doen op artikel 10 EVRM (geprezen zij de horizontale inbedding van het auteursrecht), maar dat laat een behoorlijk grijs, rechtsonzeker gebied, dat ongetwijfeld verder ontgonnen zal worden tijdens de komende verslagperiode.

Waar de hyperlinker geen commercieel oogmerk heeft, zal de rechthebbende moeten aantonen dat de hyperlinker wist of redelijkerwijs moest weten dat de link verwijst naar een zonder toestemming gepubliceerd werk. Daarmee wil het Hof een juist evenwicht verzeeken tussen de belangen van rechthebbenden en (niet-

commerciële) gebruikers. Deze kennis is volgens het Hof echter onder meer aanwezig als de rechthebbende aan de hyperlinker *meldt* dat de link verwijst naar een werk dat zonder toestemming is gepubliceerd. Zodoende lijkt het Hof het *notice & takedown* systeem uit de E-commerce richtlijn (artikel 6:196c lid 4 BW) te transporteren naar het openbaarmakingsrecht, evenwel zonder de in dat kader gehanteerde drempelvoorwaarde dat aan de juistheid van de kennisgeving redelijkerwijs niet valt te twijfelen.

### Het Hof lijkt het *notice & takedown* systeem uit de E-commerce richtlijn te transporteren naar het openbaarmakingsrecht

Verdere Europese jurisprudentie over hyperlinks is op korte termijn te verwachten in twee zaken die zijn geïnitieerd door de anti-piraterij-organisatie Stichting Brein. De Rechtbank Midden-Nederland vroeg in de *Film-speler*-zaak of sprake is van een mededeling aan het publiek bij de verkoop van een mediaspeler met 'add-ons' die hyperlinks bevatten naar websites waarop auteursrechtelijk beschermde werken zonder toestemming toegankelijk zijn gemaakt.<sup>37</sup> De Hoge Raad vroeg het Hof van Justitie of de exploitanten van The Pirate Bay, een zoekmachine voor links naar bittorrent-bestanden, een auteursrechtelijke mededeling aan het publiek verricht en, zo niet, of er dan nog een grondslag is voor een blokkade door internetaccessproviders.<sup>38</sup> Begrijpelijkerwijs zal de Stichting Brein zich in deze zaken enthousiast beroepen op het *GS Media*-arrest.<sup>39</sup>

#### 3.2. Overig digitaal auteursrecht

In de zaak *Nokia/Copydan* boog het Hof van Justitie zich over de vraag of een heffing op multifunctionele geheugendragers in het licht van de Auteursrechtlijn is toegelaten.<sup>40</sup> Het Hof leidt uit het eerdere *Padawan*-arrest af dat de geschiktheid van apparaten en dragers voor het maken van privékopieën een heffing reeds voldoende rechtvaardigt. Dat de geheugenkaarten ook andere functies vervullen, en vooral voor andere functies gebruikt worden, maakt dat niet anders, maar kan een rol spelen bij het bepalen van de hoogte van de heffing. In een Spaanse zaak oordeelde het Hof van Justitie dat de billijke vergoeding voor privékopieën niet uit de algemene middelen mag worden gefinancierd, nu dat niet waarborgt dat de kosten daarvoor uitsluitend gedragen worden door degenen die de privékopieën maken.<sup>41</sup> Het Hof van Justitie boog zich daarnaast over de Italiaanse privé-kopieregeling.<sup>42</sup> In Nederland bevestigde het Hof Den Haag dat Stichting de Thuis kopie ten onrechte een heffing voor alle blanco-dragers had geïnd, in plaats van

alleen voor aan particulieren geleverde cd's. Ongedifferentieerd heffen is niet toegestaan.<sup>43</sup> Negen filmproducenten en een aantal distributeurs kondigden aan de overheid aansprakelijk te zullen stellen voor diens lakse aanpak van illegaal downloaden en de schade die de filmindustrie daardoor lijdt.<sup>44</sup>

Het Rotterdams stadsarchief zette haar beeldbank (met 120 000 beelden) op zwart nadat zij een rechtszaak van Pictoright verloor. De Rechtbank Amsterdam oordeelde dat het archief bij het online presenteren inbreuk had gemaakt op de auteursrechten van een tiental fotografen. Het stadsarchief weigerde een afkoopsom van € 10 000 te betalen, onder andere omdat zij de achterban van Pictoright te klein achtte.<sup>45</sup> Het Hof Amsterdam bepaalde dat Tom Kabinet in beginsel een website mocht exploiteren waarop legale e-books worden doorverkocht.<sup>46</sup> Illegaal verkregen e-books mochten daarop echter niet worden doorverkocht, met als feitelijk gevolg dat de website uit de lucht moest. In een proefprocedure tussen de Vereniging van Nederlandse Bibliotheken en de Stichting Leenrecht kwam A-G Szpunar tot de conclusie dat het lenen van e-books onder het uitleenrecht valt.<sup>47</sup>

### 3.3. De positie van nieuwsplatforms

Het Hof van Justitie boog zich in de zaak *New Media Online* over de vraag wanneer een website met video-content van een Oostenrijkse krant onder de regels van de AVMS-richtlijn valt. Uit het arrest blijkt dat de cruciale vraag is of het video-gedeelte een autonome inhoud en functie heeft ten opzichte van de schriftelijke bijdragen van de online-krant. Als dat zo is, dan is sprake van

een mediadienst op aanvraag binnen de reikwijdte van de richtlijn.<sup>48</sup>

De vraag is of nieuwe platforms die lezers en media bij elkaar brengen, onderworpen zouden moeten worden aan mediaregulering. De Europese Commissie bracht Facebook, Twitter, YouTube en Microsoft ertoe om een gedragscode af te kondigen over de bestrijding van *hate speech* op internet.<sup>49</sup> Facebook oogstte eerst kritiek toen bleek dat zij zich actief bemoeide met de *trending topics* die haar gebruikers op hun tijdlijn te zien kregen, en vervolgens ook toen zij Nick Uts beroemde Vietnamfoto van het 'Napalmmeisje' verwijderde op basis van haar 'nude policy'.<sup>50</sup> Censureert 's wereld grootste editor nou teveel of juist te weinig? Vergeleken met een traditioneel telecom-platform bemoeit Facebook zich (te) veel met de inhoud. Voor een traditionele mediadienst doet zij dat juist weer (te) weinig. In een uitdagend blogbericht stelt Natali Helberger dat Facebook een nieuw soort *social editor* is, die niet onderworpen moet worden aan traditionele redactionele regels. Belangrijker is dat een platform als Facebook voldoende keuzemogelijkheden aan eindgebruikers biedt, zodat zij niet alleen automatisch in aanraking komen met alles wat tot de mainstream behoort, maar ook kunnen kiezen voor mensen met andere achtergronden en een meer divers mediadiet.<sup>51</sup>

### 3.4. Aansprakelijkheid en verantwoordelijkheden van tussenpersonen

Tijdens de verslagperiode verscheen een aantal zeer lezenswaardige studies over de aansprakelijkheid en verantwoordelijkheden van tussenpersonen, onder andere

31. Zie o.a.: European Copyright Society, The European Commission's public consultation on the role of publishers in the copyright value chain: a response by the European Copyright Society, *European Intellectual Property Review* 2016/10, p. 591-595; R.D. Chavannes, 'A neighbouring right for press publishers – the wrong solution to a serious problem', *Kluwer Copyright Blog* 13 juni 2016.

32. Synopsis reports and contributions of the results of the public consultation on the role of publishers in the copyright value chain and on the 'panorama exception', 14 september 2016, zie <https://ec.europa.eu>.

33. G. Oettinger, toespraak BDZV-congres 26 september 2016, zie [www.youtube.com/watch?v=qxz9X\\_6Zvqc](http://www.youtube.com/watch?v=qxz9X_6Zvqc).

34. HvJ EU 8 september 2016, zaak C-160/15, ECLI:EU:C:2016:644 (*GS Media/Sanoma c.s.*). Het kantoor van de auteurs treedt in deze zaak op voor GS Media.

35. Conclusie A-G M. Wathelet van 7 april 2016, C-160/15, ECLI:EU:C:2016:221 (*GS Media/Sanoma c.s.*).

36. Zie voor een bespreking van het openbaarmakingsrecht, in het bijzonder het nieuw-publiekriterium: S. van Velze, 'Het

nieuw publiek criterium hoort niet thuis in het Europese mededelingsrecht', *AMI* 2016/3, p. 57-66. Zie ook *ALAI Report and Opinion on a Berne-compatible reconciliation of hyperlinking and the communication to the public right on the internet*, [www.alai.org](http://www.alai.org).

37. Rb. Midden-Nederland 10 juni 2015, ECLI:NL:RBMNE:2015:4343, zaak C-527/15 (*Brein/Filmspeler.nl*). De rechtbank heeft daarnaast prejudiciële vragen gesteld over de toelaatbaarheid van streaming uit onrechtmatige bron.

38. HR 13 november 2015, ECLI:NL:HR:2015:3307 (*Brein/Ziggo & XS4All*); HvJ EU, zaak C-610/15. Over de achterliggende materie, zie ook R.D. Chavannes, 'Juist evenwicht' in de praktijk – De toelaatbaarheid van internetblokkades volgens het Hof van Justitie in UPC Telekabel Wien', *AMI* 2015/2.

39. Verslag Brein van het pleidooi inzake Filmspeler d.d. 29 september 2016, <http://stichtingbrein.nl/nieuws.php?id=415>.

40. HvJ EU 5 maart 2015, C-463/13, *NJ* 2016/186 (*Copydan/Nokia*), m.nt. PBH. Zie ook W.G.L. Düring, 'De billijke compensatie voor privé-kopiëren - een overzicht van de rechtspraak van het Hof van Justitie', *AMI*

2016/4, p. 81-92.

41. HvJ EU 20 juni 2016, C-470/14 (*EGEDA*); zie voor een bespreking J.P. Quintais, 'Private Copying and Payment of Fair Compensation through the General State Budget (Case C-470/14 – EGEDA and Others)', *Kluwer Copyright Blog*, 20 juni 2016.

42. HvJ EU 22 september 2016, ECLI:EU:C:2016:717 (C-110/15) (*Microsoft, voorheen Nokia/SIAE e.a.*).

43. Hof Den Haag 26 mei 2015, ECLI:NL:GHDHA:2015:3876, bevestigt: Rb. Den Haag 20 februari 2013,

ECLI:NL:RBDHA:2013:BZ1542 (*Imation Europe/Stichting de ThuisKopie*). De Rechtbank Den Haag was blijkens een tussenvonnis van 13 april 2016 voornemens prejudiciële vragen te stellen of, mede gezien het *Copydan*-arrest, in het Nederlandse rechtstelsel een vordering tot restitutie van teveel betaalde thuiskopieheffing alleen toekomt aan de eindverwerfer van de drager en niet aan de betalingsplichtige:

ECLI:NL:RBDHA:2016:3952.

44. J. Huijbregts, 'Nederlandse filmmakers stellen staat aansprakelijk voor schade door downloaden', 12 november 2015, zie <https://tweakers.net>.

45. Rb. Amsterdam 10 juni 2015,

ECLI:NL:RBAMS:2015:3590, *Mediaforum* 2015/5, p. 140 e.v., m.nt. M.M.M. van Eechoud.

46. Hof Amsterdam 20 januari 2015, ECLI:NL:GHAMS:2015:66 (*Tom Kabinet*).

47. Conclusie A-G M. Szpunar van 16 juni 2016, C-174/15 (*Vereniging Openbare Bibliotheken/Stichting Leenrecht*).

48. HvJ EU 21 oktober 2015, ECLI:EU:C:2015:709 (*New Media Online*).

49. [http://europa.eu/rapid/press-release\\_IP-16-1937\\_nl.htm](http://europa.eu/rapid/press-release_IP-16-1937_nl.htm).

50. Zie bijv. 'Mark Zuckerberg accused of abusing power after Facebook deletes "napalm girl" post', *The Guardian* 9 september 2016; "'Napalm Girl" Photographer Nick Ut Talks About the Facebook Controversy', <http://petapixel.com/2016/09/15/napalm-girl-photographer-nick-ut-talks-facebook-controversy/>.

51. Zie in detail: N. Helberger, 'Facebook is a new breed of editor. A social editor', *LSE Media Policy Project Blog* 15 september 2016, <http://blogs.lse.ac.uk>. Zie ook R. Broekstra, 'Private communicatiemachthebbers en onze uitingsvrijheid', *Mediaforum* 2015-1.

van Christina Angelopoulos,<sup>52</sup> Martin Husovec<sup>53</sup> en Jaani Riordan.<sup>54</sup> Angelopoulos betoogde dat de antwoorden niet gevonden moeten worden in sectorspecifieke regulering of grondrechtentoetsing, maar in het ouderwetse onrechtmatige-daadsrecht. Ook het Hof van Justitie zaagde aan de stoelpoten van het 'internetrecht' als zelfstandige discipline, door te bepalen dat het begrip 'tussenpersoon' ook ziet op ouderwetse analoge tussenpersonen zoals verhuurders van marktkramen.<sup>55</sup>

In het arrest *Delfi* van 16 juni 2015 oordeelde de Grote Kamer van het Europees Hof voor de Rechten van de Mens (EHRM) dat artikel 10 EVRM er niet aan in de weg staat dat de Estse nieuwssite Delfi aansprakelijk werd gesteld voor de inhoud van beledigende lezersreacties op een nieuwspagina. Daarbij leek het bedreigende en beledigende karakter van de reacties van beslissend gewicht, en speelde ook een rol dat de opgelegde schadevergoeding (€ 320) verwaarloosbaar was.<sup>56</sup> Die lijn werd vervolgens doorgezet en gematigd in de uitspraak *MTE*.<sup>57</sup> Het

### Wie stiekem hoopt dat dergelijke jurisprudentie het einde zal inluiden van lezersreacties onder artikelen op internet, kan dat resultaat overigens nu al met diverse adblockers bereiken

Hof verduidelijkt daarin onder meer dat het toelaten van ongefilterde comments op zichzelf nog geen reden is om de site waar die comments staan aansprakelijk te houden, zelfs niet als de site had moeten beseffen dat sommige daarvan mogelijk onrechtmatig zouden zijn. Ook stelt het hof dat de stijl die in veel comments wordt gebruikt deel uitmaakt van de uitingsvorm en dus ook wordt beschermd door de uitingsvrijheid. Het doorslaggevende verschil tussen de casusposities in *Delfi* en *MTE*, aldus het hof in de *MTE*-zaak, was dat het in de *Delfi*-zaak ging om lezersreacties die dusdanig extreem waren dat zij geen enkele bescherming genoten onder artikel 10 EVRM, terwijl het in de *MTE*-zaak ging om 'gewoon' diffamerende reacties. Dat onderscheid moge op papier elegant lijken, praktisch toepasbaar is het vermoedelijk niet, laat staan door de algoritmes en filters die de eerste lijn vormen in het weren van *hate speech* op *user-generated content sites*.<sup>58</sup> Wie stiekem hoopt dat dergelijke jurisprudentie het einde zal inluiden van lezersreacties onder artikelen op internet, kan dat resultaat overigens nu al met diverse adblockers bereiken.

In de zaak *Mc Fadden* stelde het Hof van Justitie vast dat een winkelier die zijn klanten een open (niet met wachtwoord afgeschermd) wifi-netwerk aanbiedt, zich kan

beroepen op de aansprakelijkheidsbeperking voor 'mere conduit' neergelegd in artikel 12 van de e-Commercerichtlijn wanneer een van die klanten via dat netwerk auteursrechtinbreuk pleegt.<sup>59</sup> Dat staat echter niet in de weg aan een rechterlijk bevel dat de aanbieder maatregelen neemt om inbreuken via zijn diensten te beëindigen. Een maatregel die vergt dat de aanbieder toezicht houdt op alle doorgegeven informatie is uitgesloten, en 'de internetaansluiting volledig (...) blokkeren' ook. Een maatregel die de aanbieder verplicht om de internetverbinding voortaan te beveiligen met een wachtwoord, dat de aanbieder alleen uitreikt aan een klant die zich heeft geïdentificeerd, kan echter een juist evenwicht vormen tussen enerzijds het belang van een effectieve handhaving en anderzijds de informatie- en ondernemingsvrijheid.

Het Hof staat in dit verband niet expliciet stil bij het recht op anonieme communicatie, en ook de uiteenlopende modaliteiten van een dergelijke wachtwoordbeveiliging blijven buiten beschouwing. Ook betreft het Hof het grondrecht op bescherming van persoonsgegevens niet bij zijn afweging, wat suggereert dat de aanbieder van een open wifi-netwerk niet geacht wordt klanten gebruiksgegevens te verzamelen en op verzoek aan rechthebbenden af te staan, maar dat eenmalige klantidentificatie voldoende is. Het is daarentegen onduidelijk hoe een dergelijke maatregel kan bijdragen aan de bescherming tegen auteursrechtinbreuk: als de aanbieder van het wifi-netwerk het verkeer over zijn netwerk niet mag monitoren, en (dus) niet kan associëren met individuele gebruikers, hoe kan hij dan inbreuk opsporen, identificeren of rapporteren?

Op nationaal niveau oordeelde de Rechtbank Amsterdam op 7 oktober 2015 in een geschil tussen Skyscanner en de Reclame Code Commissie (RCC) dat vergelijkingssites zelf verantwoordelijk zijn voor de juistheid van de door hen getoonde aanbiedingen, ook als die van derden afkomstig zijn. Aanbieders van vergelijkingssites moeten de informatie van derden, die zij met elkaar vergelijken, dus doorlopend controleren. Een beroep van Skyscanner op artikel 6:196c lid 4 BW faalde, omdat zij de informatie op haar website niet op verzoek van aanbieders opsloeg, maar die op eigen initiatief van een derde partij betrof.<sup>60</sup>

#### 3.5. Verstrekking van klantgegevens

Het opvragen van informatie bij internetproviders en andere dienstverleners, meestal in het kader van IE-handhaving of reputatiebescherming op internet, raakt steeds verder ingeburgerd. Omdat de internetgebruiker(s) wier informatie wordt gevorderd per definitie geen partij zijn in die procedures, blijft hun privacybelang doorgaans abstract. Het toetsingskader blijft vooralsnog het *Lycos/Pessers*-arrest.<sup>61</sup> De Rechtbank Den Haag volgde een procedurele constructie waarbij de internetgebruiker in kwestie genotificeerd werd over de op handen zijnde verstrekking en daarop een reactie kon geven.<sup>62</sup> In een procedure tegen Ziggo kon BREIN niet voldoende aannemelijk maken dat de desbetreffende Ziggo-klant doelbewust auteursrechtinbreuk faciliteerde en aanmoedigde.<sup>63</sup> Ook een bouwbedrijf dat had nagelaten een lastercampagne waarover zij klaagde deugdelijk te documenteren ving bot in een kort geding tegen de kabelaar.<sup>64</sup> Meer succes had een parfumwebwinkel tegen

Facebook,<sup>65</sup> die logischerwijs echter geen informatie over een Instagram-account kon en hoefde te verstrekken.<sup>66</sup>

Instagram werd daar in een geval van cyberpesten wel toe veroordeeld.<sup>67</sup> In een zaak over vermeende neprecensies moest Google NAW-gegevens verstrekken aan een kinderdagverblijf.<sup>68</sup> Ten slotte had de Eredivisie succes tegen hosting provider Global Layer, die niet alleen informatie moest verstrekken maar ook haar (volledige) dienstverlening aan de vermeende inbreukmaker moest staken.<sup>69</sup>

Verreweg de meeste aandacht trok echter het tamelijk schrijnende wraakporno-saga van Chantal uit Werkendam. Toen Facebook weigerde NAW-gegevens te verstrekken van een uploader van een wraakpornofilmje dagvaardde Chantal de sociale mediagigant. Vlak voor de zitting liet Facebook weten die gegevens niet meer te hebben. Dat achtte de Amsterdamse voorzieningenrechter zo ongeloofwaardig althans onsympathiek dat zij een technisch onderzoek bij het sociale mediaplatform gelastte om te kijken of de gegevens echt nergens meer te achterhalen waren.<sup>70</sup> Daarover kwam een moeizame schikking tot stand, waarna een IP-adres kon worden geïdentificeerd. Die leidde naar een schoolcomputer van het ROC West-Brabant, die echter weigerde mee te werken aan een onderzoek naar inloggegevens van haar leerlingen. De voorzieningenrechter in de Rechtbank Zeeland-West Brabant stelde de onderwijsinstelling in het gelijk. Volgens de rechtbank zijn er minder ingrijpende mogelijkheden om de identiteit van de uploader te achterhalen, zoals een voorlopig getuigenverhoor van zes vermoedelijke daders,

die ten onrechte onbenut zijn gebleven, en een nog altijd sluimerend strafrechtelijk onderzoek.<sup>71</sup> Chantal is dus aangewezen op de daadkracht van dezelfde politie die het aanvankelijk zo liet afweten.

#### 4. Netneutraliteit en cookies

Eind 2014 legde ACM boetes op aan KPN<sup>72</sup> en Vodafone<sup>73</sup> voor hun overtreding van de Nederlandse netneutraliteitsregels. In 2016 werden die Nederlandse regels ingehaald door een Europese verordening.<sup>74</sup> De verordening waarborgt voortaan 'open-internettoegang', wat onder andere inhoudt dat internettoegangsdiensten internetverkeer gelijk en niet-discriminerend moeten behandelen. Daarmee ontstond discussie over de vraag in hoeverre de Europese regels minder streng waren,<sup>75</sup> waarop BEREC richtsnoeren publiceerde.<sup>76</sup> Daaruit bleek dat 'zero-rating' op basis van de Europese regels niet altijd ongeoorloofd is.<sup>77</sup> Niettemin houdt de Nederlandse wetgever vooralsnog vast aan het nieuw voorgestelde artikel 7.4a lid 3 Tw, op basis waarvan zero-rating (in Nederland nog steeds) verboden zal zijn.<sup>78</sup> In april 2016 werd op Twitter een brief van de Europese Commissie gepubliceerd waaruit bleek dat artikel 5 lid 3 van de Privacyrichtlijn volgens haar ook van toepassing is op scripts die adblockers detecteren.<sup>79</sup> Na Kamervragen bleek dat deze praktijk door ACM onder de uitzondering van artikel 11.7a lid 3 Tw wordt geschaard.<sup>80</sup>

In de vorige kroniek werd al gesignaleerd dat de Nederlandse cookiewetgeving zeer gebruiksonvriendelijk uitpakt in de praktijk. Het wetsvoorstel dat bedoeld was

52. C.J. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (diss. Uva Amsterdam), 2016, <http://dare.uva.nl/document/2/172299>; en 'Sketching the outline of a ghost: the fair balance between copyright and fundamental rights in intermediary third party liability', info, vol. 17 iss. 6, p. 72-96.

53. M. Husovec, 'Accountable, Not Liable: Injunctions Against Intermediaries', TILEC Discussion Paper nr. 2016-012, [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2773768](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773768).

54. J. Riordan, *The Liability of Internet Intermediaries*, Oxford: Oxford University Press 2016.

55. HvJ EU 7 juli 2016, zaak C-494/15, *AMI* 2016-4, nr. 4 (Tommy Hilfiger e.a./Delta Center), m.nt. R.D. Chavannes.

56. EHRM 16 juni 2015, appl. nr. 64569/09 (Delfi), zie voor een uitgebreide bespreking: D. Voorhoof, 'De aansprakelijkheid van online nieuwsplatforms na Delfi', *Mediaforum* 2015/6, p. 194 e.v.

57. EHRM 2 februari 2016, IEF 15697; appl. nr. 22947/13 (MTE/Hongarije), *HRC* 2016/140, m.nt. T. McGonnagle.

58. Zie de serie blogposts van Stanford-hoogleraar Daphne Keller, 'Policy Debates over EU Platform Liability Laws: New

Human Rights Case Law in the Real World', <http://cyberlaw.stanford.edu/blog/2016/04/policy-debates-over-eu-platform-liability-laws-new-human-rights-case-law-real-world>.

59. HvJ EU 15 september 2016, ECLI:EU:C:2016:689 (Mc Fadden). Zie ook M. Husovec, 'Mc Fadden Drills Another Hole in the E-Commerce Directive', *Kluwer Copyright Blog* 29 september 2016.

60. Rb. Amsterdam 7 oktober 2015, ECLI:NL:RBAMS:2015:6507 (Skyscanner/RCC).

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

62. Rb. Den Haag (vzr.) 5 oktober 2015, ECLI:NL:RBDHA:2015:11408 (Brein/Google). Het kantoor van de auteurs trad in deze zaak op voor Google.

63. Rb. Midden-Nederland 16 december 2015, ECLI:NL:RBMNE:2015:8974 (Brein/Ziggo).

64. Rb. Midden-Nederland 27 januari 2016, ECLI:NL:RBMNE:2016:338 (Bouwbedrijf Casmond/Ziggo).

65. Rb. Den Haag 11 mei 2016, ECLI:NL:RBDHA:2016:5505 (Parfumwebwinkel/Facebook).

66. Rb. Noord-Holland 31 augustus 2016, IEF 16251, IT 2136 (Facebook/X).

67. Rb. Noord-Holland 5 juli 2016, ECLI:NL:RBNHO:2016:5536 (X/Instagram).

68. Rb. Amsterdam 29 februari 2016, ECLI:NL:RBAMS:2016:987 (Kinderdagverblijf/Google). Het kantoor van de auteurs trad in deze zaak op voor Google.

69. Rb. Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (Eredivisie/Global Layer). Het kantoor van de auteurs trad in deze zaak op voor Eredivisie.

70. Rb. Amsterdam (vzr.) 25 juni 2015, ECLI:NL:RBAMS:2015:3984 (Chantal/Facebook).

71. Rb. Zeeland-West-Brabant (vzr.) 21 september 2016, ECLI:NL:RBZWB:2016:5832.

72. Besluit van Autoriteit Consument en Markt tot het opleggen van een boete ter zake van overtreding van artikel 7.4a, lid 1 Telecommunicatiewet inzake netneutraliteit, ACM/DJZ/2014/207376, d.d. 18 december 2014 (KPN), beschikbaar via [acm.nl](http://acm.nl).

73. Besluit van Autoriteit Consument en Markt tot het opleggen van een boete ter zake van overtreding van art. 7.4a lid 3 Telecommunicatiewet inzake netneutraliteit, ACM/DJZ/2014/207383 (Vodafone), beschikbaar via [acm.nl](http://acm.nl).

74. Verordening 2015/2120 van het Europees Parlement en de Raad van 25 novem-

ber 2015 tot vaststelling van maatregelen betreffende open-internettoegang en tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten en Verordening 531/2012 betreffende roaming op openbare mobiele communicatienetwerken binnen de Unie. Zie ook *Kamerstukken I* 2015/16, 34379, A (Wijziging van de Telecommunicatiewet ter uitvoering van de netneutraliteitsverordening – Gewijzigd voorstel van wet).

75. A.J. Colenbrander, 'Van Netneutraliteit naar Open-Internettoegang: verdeeldheid en rechtsonzekerheid in de EU?', *Mediaforum* 2016/2, p. 30-37.

76. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127, beschikbaar via [berec.europa.eu](http://berec.europa.eu).

77. Idem., p. 11-15.

78. *Kamerstukken I* 2015/16, 34379, A.

79. Zie <https://twitter.com/alexanderhanff/status/722861362607747072>.

80. Beantwoording vragen over de uitspraak van de Europese Commissie over adblockers, 1 juni 2016, rijksverheid.nl.

om dat op te lossen is weliswaar wet geworden, maar de vraag is of de wijziging het gewenste effect (geheel) bereikt.<sup>81</sup> Nog steeds dient voor verreweg de meeste cookies geïnformeerde toestemming verkregen te worden. Door de strenge eisen die handhavers AP en ACM stellen aan het gebruik van cookies, kiezen steeds meer websites ervoor om een zogenaamde 'cookiewall' te gebruiken. De wetgever heeft bovendien verduidelijkt dat toestemming voor het plaatsen van cookies ook impliciet gegeven kan worden, bijvoorbeeld door verder te surfen op een website nadat de gebruiker op de hoogte is gesteld van het feit dat er dan cookies zullen worden geplaatst.<sup>82</sup> Van deze optie wordt door veel websites gebruik gemaakt. De Artikel 29 Werkgroep bevestigde eind 2014 dat de cookiewetgeving ook van toepassing is op andere, vergelijkbare technologieën, zoals *device fingerprinting*.<sup>83</sup> ACM publiceerde naar aanleiding van de gewijzigde wetgeving een update van het document 'Veelgestelde vragen over de cookiebepaling'<sup>84</sup> en een aankondiging dat zij de cookieregels voortaan actief zou gaan handhaven.<sup>85</sup> De handhaving van de cookiewetgeving werd tot die tijd vooral door de AP uitgevoerd.<sup>86</sup> ACM heeft tot nu toe, voor zover ons bekend, echter alleen handhavend opgetreden jegens NPO.<sup>87</sup>

### 5. Privacy, reputatiebescherming en surveillance

#### 5.1. Regelgeving

De inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming (de 'Verordening') is zonder twijfel de belangrijkste regulatoire privacyontwikkeling van de afgelopen twee jaar.<sup>88</sup> De Verordening wordt van toepassing met ingang van 25 mei 2018. Modernisering van de uit 1996 daterende Privacyrichtlijn was nodig, maar het is de vraag of met de nieuwe Verordening een regime tot stand is gekomen dat daadwerkelijk beter is toegesneden op technologische ontwikkelingen en de belangen van burgers, bedrijven en overheden.<sup>89</sup> De Verordening heeft nog grotendeels de structuur en inhoud van de huidige Privacyrichtlijn, maar bestaande verplichtingen zijn verder gespecificeerd en uitgebreid (de verordening is qua omvang een verdrievoudiging van de Privacyrichtlijn). De verordening is zwaar 'belobbed', kwam onder hoge politieke druk tot stand en zal juristen de komende jaren nog flink zal bezighouden.<sup>90</sup> Opinions van de Artikel 29 Werkgroep, omgedoopt tot 'Europees Comité voor gegevensbescherming' zullen daarbij moeten helpen.<sup>91</sup>

De belangrijkste wijzigingen die de verordening zal brengen zijn 1. een verruiming van het territoriale toepassingsgebied;<sup>92</sup> 2. de van toepassing verklaring van bestaande verplichtingen op zowel de verantwoordelijke als de verwerker (voorheen 'bewerker');<sup>93</sup> de aanwijzing van één toezichthoudende instantie, als one-stop-shop, in grensoverschrijdende zaken;<sup>94</sup> 3. een 'recht op vergetelheid';<sup>95</sup> 4. een recht op dataportabiliteit;<sup>96</sup> 5. strenge eisen aan de toestemming die een betrokkene geeft voor een gegevensverwerking;<sup>97</sup> 6. het vervallen van de meldplicht en introductie van de verplichting om een 'passend beleid' te voeren en een register van verwerkingsactiviteiten bij te houden; 7. de verplichting om voor sommige risicovolle verwerkingen een 'gegevensbeschermings-effectbeoordeling' (beter bekend als Privacy Impact Assess-

ment of PIA) uit te voeren en in sommige gevallen een functionaris voor de gegevensbescherming (beter bekend als Privacy Officer) aan te stellen voor intern toezicht.<sup>98</sup>

De Verordening bevat ook een meldplicht voor beveiligingsincidenten waarbij persoonsgegevens betrokken zijn. In Nederland is men daarop al vooruitgelopen door invoering van de meldplicht datalekken per 1 januari 2016,<sup>99</sup> waaraan in beleidsregels nadere invulling is gegeven.<sup>100</sup> De meldplicht geldt alleen als het gaat om datalekken die leiden tot '*een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens*'.<sup>101</sup> Het lek moet in beginsel binnen 72 uur na ontdekking gemeld worden bij de AP en in sommige gevallen ook aan betrokkenen.<sup>102</sup> Bij dezelfde wet is bepaald dat het College bescherming persoonsgegevens in het maatschappelijk verkeer voortaan wordt aangeduid als 'Autoriteit Persoonsgegevens' (hierna AP) en heeft zij een serieuze boetebevoegdheid gekregen.<sup>103</sup> Door de hoge boetes (tot € 820 000 of zelfs tot 10% van de jaaromzet per overtreding) en de korte termijn bij de meldplicht datalekken (72 uur) heeft *data security* in het bedrijfsleven en bij de overheid sinds begin dit jaar duidelijk een hoge prioriteit: bescherming van persoonsgegevens (althans: de risico's van tekortschietende bescherming van persoonsgegevens) heeft de boardroom bereikt.<sup>104</sup> Jacob Kohnstamm, tot 1 augustus 2016 voorzitter van de AP, sprak de hoop uit dat bedrijven daardoor sneller naar de rechter zullen stappen, en zo de rechtsvorming stimuleren.<sup>105</sup>

### Door de hoge boetes en de korte termijn bij de meldplicht datalekken heeft *data security* in het bedrijfsleven en bij de overheid sinds begin dit jaar duidelijk een hoge prioriteit

De verordening regelt niet de vertrouwelijkheid van online-communicatie of online-volgtechnieken zoals cookies, spam of het gebruik van locatie- en verkeersaanbieders door telecomaandieners. Deze onderwerpen worden bestreken door de e-Privacyrichtlijn, die de Europese Commissie wil herzien.<sup>106</sup> Een deel van deze verplichtingen geldt nu alleen voor traditionele telecomaandieners en de vraag rijst of die in de toekomst ook zouden moeten gelden voor OTT-dienstverleners zoals WhatsApp.<sup>107</sup>

#### 5.2. Gegevensverwerking door bedrijven

Veel van de onderzoeken die in de vorige kroniek werden gesignaleerd zijn inmiddels afgerond.<sup>108</sup> In december 2014 kondigde de AP een nieuw onderzoek naar de gewijzigde privacyvoorwaarden van Facebook aan.<sup>109</sup> Facebook stelde zich op het standpunt dat de Nederlandse toezichthouder niet bevoegd was en dat de Nederlandse Wbp niet van toe-



passing was.<sup>110</sup> Het onderzoek loopt echter nog steeds.<sup>111</sup> Online advertentiebedrijf YD vermeed een dwangsom van de AP door de verantwoordelijkheid voor de verwerking van persoonsgegevens naar een in het Verenigd Koninkrijk gevestigde vennootschap te verplaatsen.<sup>112</sup>

Het Hof van Justitie van de EU heeft zich sinds de vorige kroniek (waarin het *Costeja*-arrest over het 'recht om vergeten te worden' uitgebreid aan de orde kwam) nog twee keer gebogen over het vraagstuk van internationale bevoegdheid en toepasselijk recht. In het *Weltimmo*-arrest stelde het Hof vast dat het begrip vestiging in deze context

zeer ruim uitgelegd moet worden. Al bij één enkele vertegenwoordiger van de verantwoordelijke in een lidstaat kan sprake zijn van een vestiging. Tegenover deze ruime toepasselijkheid, staat de vaststelling van het Hof dat de nationale toezichthouder geen grensoverschrijdende bevoegdheden heeft. De nationale toezichthouder kan dus geen sancties opleggen buiten het grondgebied van de eigen lidstaat.<sup>113</sup> Deze verruiming is vastgelegd in een update van de opinie van de Artikel 29 Werkgroep over het toepasselijk recht.<sup>114</sup> In het meer recente *Amazon*-arrest formuleert het Hof het nog iets duidelijker: de verwerking van persoonsgegevens

81. L. Meij, 'Cookies, hebben we er nog trek in?', *Tijdschrift voor Internetrecht* 2015, afl. 5/6, p. 203-205; N. Wolters Ruckert, 'Aangepast cookieregime eindelijk wet', *Bedrijfsjuridische berichten* 2015/39, p. 135-138.
82. *Kamerstukken II* 2013/14, 33902, 3, p. 12-13.
83. Art. 29 Werkgroep, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224.
84. Nieuwsbericht ACM, 'Veelgestelde vragen over de cookiebepaling', 15 juni 2016, [www.acm.nl](http://www.acm.nl).
85. Nieuwsbericht ACM, 'ACM gaat nieuwe cookieregels actief handhaven', 11 maart 2015, [www.acm.nl](http://www.acm.nl).
86. Zie de rapporten over Philips Smart TV, Google, Snappet, YD, NPO en Nike en recente berichtgeving over ziekenhuiswebsites op [autoriteitpersoonsgegevens.nl](http://autoriteitpersoonsgegevens.nl).
87. 'Last onder dwangsom NPO voor overtreden cookieregels', 31 juli 2014, [www.acm.nl](http://www.acm.nl).
88. Verordening van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *PbEU* 2016, L 119/1.
89. Zie in kritische zin bijv.: E.M.L. Moerel & J.E.J. Prins, 'Privacy voor de homo digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van big data en Internet of Things', *Handelingen NJV*, 146e jaargang/2016-1, Deventer: Kluwer 2016, p. 9-136; N. van Eijk, 'Een normatief toetsingskader voor gegevensverwerking', *NJB* 2016/1072, afl. 22.; F. Zuiderveen Borgesius, 'Privacybescherming online kan beter: De mythe van geïnformeerde toestemming', *NJB* 2015/680, afl. 14.
90. Dat blijkt onder meer uit de op veel punten onduidelijke of inconsistente formulering van de artikelen en de vele fouten in de Nederlandse taalversie. De verordening

- laat op belangrijke punten ook nog ruimte voor nationale wetgeving.
91. Zie het werkprogramma 2016-2018 van de Artikel 29 Werkgroep en de toelichting daarop van 2 februari 2016, WP235 en WP 236, zie: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm).
92. Het territoriale toepassingsgebied van de verordening is veel ruimer dan dat van de Privacyrichtlijn: de verordening is ook van toepassing op elke verwerking van persoonsgegevens van betrokkenen die zich in de EU bevinden indien die verwerking verband houdt met het aanbieden van goederen of diensten aan die betrokkenen of het monitoren van het gedrag van die betrokkenen.
93. In de Privacyrichtlijn waren de verplichtingen voor de bewerker nog zeer beperkt.
94. Bij grensoverschrijdende verwerkingen moeten alle bevoegde toezichthouders samenwerken onder leiding van één leidende toezichthouder.
95. Het recht om vergeten te worden ('recht op vergetelheid') is specifiek omschreven en bevat ook uitdrukkelijke uitzonderingen, zoals de uitzondering op grond van het recht op informatievrijheid. In de context van het recht op vergetelheid is vooral opvallend dat de verordening een recht op beperking van de verwerking bevat. Dit recht lijkt te betekenen dat de betrokkene kan eisen dat gegevens worden verwijderd of ontoegankelijk gemaakt vóór dat de rechtmatigheid van het verzoek om vergetelheid is beoordeeld. Deze verplichting om preventief informatie te verwijderen zonder inhoudelijke toets lijkt ons evident in strijd met de uitsingsvrijheid omdat het geen enkele ruimte overlaat voor een proportionaliteitsafweging en daarom gemakkelijk kan worden misbruikt door betrokkenen om rechtmatige informatie snel (doch tijdelijk) verwijderd te krijgen.
96. Een betrokkene krijgt onder de verordening het recht op dataportabiliteit, hetgeen inhoudt dat de betrokkene de verantwoordelijke kan vragen om een export van zijn

- persoonsgegevens zodat hij die aan een andere verantwoordelijke kan verstrekken.
97. Overheidsinstanties kunnen onder de Verordening bovendien niet langer een beroep doen op de grondslag van gerechtvaardigd belang.
98. Zie voor een uitgebreidere bespreking van de verordening o.a.: H. De Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming, twee stappen vooruit, één stap terug', *NJB* 2016/1077, afl. 22; C.C.M. Kroeks-de Raaij, R.J.J. Westerdijk & G.J. Zwenne, 'De Algemene Verordening Gegevensbescherming', *Tijdschrift voor Internetrecht*, 2016, 2, p. 50 e.v.
99. Zie <https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken>.
100. Beleidsregels voor toepassing van art. 34a Wbp, *Stcrt.* 2015, 46128.
101. Daarvan is bijvoorbeeld sprake als het gaat om een lek dat veel personen treft of een lek van gevoelige gegevens, zoals informatie over iemands religie, gezondheid of seksuele leven. Ook inloggegevens, financiële en strafrechtelijke gegevens en kopieën van identiteitsbewijzen worden als gevoelig aangemerkt door de AP.
102. De AP heeft daarvoor een online meldingsformulier beschikbaar gesteld, zie [autoriteitpersoonsgegevens.nl](http://autoriteitpersoonsgegevens.nl).
103. Boetebeleidsregels Autoriteit Persoonsgegevens 2016, *Stcrt.* 2016, 2043 (nadien gewijzigd).
104. De AP heeft die boetebevoegdheid tot nu toe overigens nog niet gebruikt. In de meeste gevallen ligt een last onder dwangsom ook meer voor de hand, omdat de boete alleen kan worden opgelegd na een bindende aanwijzing van de AP of als de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid. Dat zal niet snel aan de hand zijn, alleen al omdat de Wbp veel open normen bevat waarvan de uitwerking in een specifieke casus niet altijd direct duidelijk is voor de verantwoordelijke. Jacob Kohnstamm, hoopte dat bedrijven voortaan sneller naar

- de rechter zouden stappen en zo de rechtsvorming zouden stimuleren.
105. Zie D. Tokmetzis & M. Martijn, "'Mischien moeten we het woord privacy niet meer gebruiken', zegt de man die er toezicht op hield", *De Correspondent*, 1 augustus 2016.
106. Zie Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive, 4 augustus 2016, <https://ec.europa.eu>.
107. Uit de publieke consultatie van de richtlijn blijkt dat het grootste deel van de respondenten daar voorstander van is. Zie Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive, 4 augustus 2016, <https://ec.europa.eu>.
108. Zie de verschillende nieuwsberichten op [autoriteitpersoonsgegevens.nl](http://autoriteitpersoonsgegevens.nl) over de onderzoeken naar Whatsapp, telecomaanbieders Tele2, T-Mobile en Vodafone, TP Vision en Google.
109. Nieuwsbericht AP, 'CBP onderzoekt nieuwe privacyvoorwaarden Facebook', 16 december 2014, zie [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).
110. Nieuwsbericht AP, 'CBP: Facebook verstrekt informatie na vordering van het CBP', 6 mei 2015, zie [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).
111. Nieuwsbericht AP, 'Autoriteit Persoonsgegevens: last onder dwangsom voor Facebook herroepen', 14 januari 2016, zie [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).
112. Nieuwsbericht AP, 'Autoriteit Persoonsgegevens: sanctie YD voor schending privacywet', 19 januari 2016, zie [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).
113. HvJ EU 1 oktober 2015 C-230/14 (*Weltimmo*); A.C.M. Meuwese, 'Europese bescherming persoonsgegevens is geen one-shop-stop', *Ars Aequi* december 2015, p. 998 e.v.
114. 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain', WP 179 Update, 16 december 2015.

wordt beheerst door het recht van het land waar een online-bedrijf zijn activiteiten op richt.<sup>115</sup>

Een tweede belangrijke ontwikkeling deed zich voor bij de export van persoonsgegevens naar de Verenigde Staten. In het *Schrems*-arrest stelde het Hof van Justitie het Safe Harbor Framework<sup>116</sup> per direct buiten werking, omdat het onvoldoende waarborgen zou bieden voor de bescherming van persoonsgegevens.<sup>117</sup> Daarmee ontstond grote rechtsonzekerheid in het bedrijfsleven, waar immers (o.a.) veel gebruik wordt gemaakt van Amerikaanse cloud-diensten. Bedrijven weken veelal uit naar Standard Contractual Clauses of Binding Corporate Rules. Het is echter nog onzeker of die instrumenten toekomstbestendig zullen blijken.<sup>118</sup> Op 12 juli 2016 kwam het EU-US Privacy Shield als vervangend instrument tot stand. De Artikel 29 Werkgroep juichte daarin aangebrachte verbeteringen toe, maar uitte ook nog punten van kritiek.<sup>119</sup> Max Schrems is van het nieuwe Privacy Shield niet onder de indruk, hij vindt dat de nieuwe regeling nog steeds niet aan de Europese wetgeving voldoet.<sup>120</sup>

### 5.3. Reputatiebescherming op internet

Reputatiebescherming op internet staat volop in de belangstelling, het bestrijden van 'hate speech' in het bijzonder.<sup>121</sup> In mei 2016 ondertekenden Facebook, Youtube, Twitter en Microsoft een Europese Hate Speech Code, een gedragscode met daarin onder meer het uitgangspunt dat klachten over hate speech binnen 24 uur worden onderzocht.<sup>122</sup>

## Max Schrems is van het nieuwe Privacy Shield niet onder de indruk, hij vindt dat de nieuwe regeling nog steeds niet aan de Europese wetgeving voldoet

Nederlanders van wie het centrum van belangen in eigen land ligt, kunnen niet alleen over (de volledige schade ontstaan door) internetpublicaties klagen bij de Nederlandse rechter,<sup>123</sup> maar kunnen daarvoor voortaan ook een beroep doen op Nederlands recht. In het arrest *Dahashiil* bevestigde de Hoge Raad namelijk dat het *eDate/Martinez*-criterium niet alleen in de context van de EEX-Verordening, maar ook in de context van de Rome II Verordening moet worden toegepast.<sup>124</sup> Minder principieel of verrassend was het oordeel van de Rotterdamse kantonrechter die een caféhouder verbood om een voormalige klant, met wie hij of zij nota bene een relatie had gehad, nog langer op Facebook uit te schelden.<sup>125</sup> Kritische uitlatingen over een thuiszorgorganisatie op Twitter en Facebook stond de Rotterdamse rechter in een andere zaak wel toe, gelet op het vluchtig karakter van het medium waarop berichten

relatief snel uit beeld verdwijnen en waarbij een gerichte zoekactie nodig was om van de litigieuze berichten kennis te kunnen nemen.<sup>126</sup> Geen succes had de wegens uitlokking van huurmoord veroordeelde Amsterdammer toen hij zijn pijlen richtte tegen een artikel in het Algemeen Dagblad en een nieuwsbericht op Blogspot.nl dat zijn voor- en de eerste letter van zijn achternaam bevatte.<sup>127</sup> Het Hof Den Bosch oordeelde dat van Google, als aanbieder van de dienst Blogger, mag worden verwacht dat zij een notice & takedown-verzoek voortvarend behandelt, maar dat daaruit niet een concrete beslisplicht met tijdsliemiet voor toekomstige verzoeken mag worden afgeleid.<sup>128</sup> Een tweet waarin Heerlens gemeenteraadslid Petermann een officier van justitie, betrokken bij de vervolging van Jos van Rey, vergeleek met een SS-kampbeul resulteerde in een veroordeling wegens belediging.<sup>129</sup>

Sinds het *Costeja*-arrest van het Hof van Justitie kunnen individuen onder bepaalde omstandigheden aanspraak maken op onderdrukking van zoekresultaten die verschijnen bij een zoekopdracht op hun naam, nog altijd hardnekkig aangeduid als 'het recht om vergeten te worden'. In de vorige kroniek berichtten we al over de eerste Nederlandse zaak, waarin de Amsterdamse voorzieningenrechter terughoudend was om beperkingen aan een zoekmachine op te leggen, vanwege de maatschappelijke functie daarvan. De voorzieningenrechter wees het verzoek in kwestie af met de overweging dat eiser recent een ernstig strafbaar feit had gepleegd, de daardoor ontstane publiciteit aan zichzelf had te danken, en dat zijn veroordeling in beginsel blijvend relevante informatie over zijn persoon vormde. Het Amsterdamse hof was het daarmee eens en bevestigde dat er minder ruimte voor een toewijzing is als de onwelgevallige zoekresultaten aan het eigen gedrag van de verzoeker te wijten zijn.<sup>130</sup>

Ook in daarop volgende 'vergeetzaken' stelde de Rechtbank Amsterdam het maatschappelijk belang van zoekmachines voorop. In een procedure aanhangig gemaakt door een KPMG-partner verduidelijkte de rechtbank dat een 'vergeetverzoek' aan een zoekmachine niet mag worden gebruikt om het bestaande juridische kader voor onrechtmatige perspublicaties te omzeilen. Bij de toepassing van het verwijderingsrecht op grond van artikel 36 en 40 Wbp gaat het derhalve alleen om de zoekresultaten zelf en niet om de vraag of de inhoud van berichten (waar die zoekresultaten naar verwijzen) al dan niet toereikend, relevant of bovenmatig is. Dat een onwelgevalig zoekresultaat ook na vele jaren nog relevant kan zijn bleek in een zaak die een freelance-journalist aanhangig maakte. Daarin wees de Rechtbank Amsterdam een vergeetverzoek af voor een zoekresultaat dat verwees naar een vijftien jaar oud krantenartikel over door de journalist gepleegd plagiaat, nu dat betrekking had op zijn professionele leven en hij nog altijd in dezelfde beroepsgroep werkzaam was.<sup>131</sup>

Een andere lijn koos de Rotterdamse rechtbank in een zaak over een zoekresultaat dat verwees naar een blogbericht over de strafrechtelijke veroordeling van een Nederlandse advocaat in een buurland voor verboden wapenbezit. De rechtbank oordeelde dat sprake was van een verwerking van bijzondere persoonsgegevens door Google, die op grond van artikel 16 Wbp verboden was. Voor een nadere belangenafweging was volgens de recht-

bank geen plaats.<sup>132</sup>

De Artikel 29 Werkgroep publiceerde richtsnoeren om lokale toezichthouders te helpen bij het beoordelen van vergeetverzoeken waarin zij gevraagd worden om te bemiddelen.<sup>133</sup> Die bevatten onder meer een lijst met gezichtspunten die een rol kunnen spelen bij de beoordeling van een vergeetverzoek. De AP rapporteerde recent over de 111 bemiddelingsverzoeken die zij in de twee jaar na het *Costeja*-arrest ontving over zoekresultaten van Google. In 61 gevallen ging het AP niet tot bemiddeling over, bijvoorbeeld omdat de beslissing van Google haar juist leek. In 32 gevallen ging het AP wel tot bemiddeling over, hetgeen in 24 gevallen tot heroverweging door Google leidde. In de overige gevallen nam het AP de verzoeken om formele redenen niet in behandeling, twee bemiddelingen liepen nog.<sup>134</sup>

Zowel Google<sup>135</sup> als Microsoft<sup>136</sup> publiceren statistieken over het aantal ontvangen en toegewezen verzoeken op grond van het recht om vergeten te worden. Of het nu toeval is of een voorheen onbekende natuurwet onthult, bij het sluiten van deze kroniek lag het toewijzingsper-

tage bij beide zoekmachines op 43%.

Het gevoelsmatige 'verlies aan controle' van overheden en individuen op internet is een van de thema's van de lijvige dissertatie waarop Hielke Hijmans begin 2016 promoveerde.<sup>137</sup> Hijmans is optimistisch, en ziet een grote rol weggelegd voor de Europese Unie als constitutionele waakhond van privacy en gegevensbescherming op internet.

#### 5.4. Surveillance

De discussie en rechtsontwikkeling met betrekking tot digitale surveillance loopt nog altijd volop. In de nasleep van de Snowden-onthullingen is omvangrijke wetenschappelijke en maatschappelijke discussie ontstaan over de handelwijze van de Amerikaanse inlichtingendiensten en het toezicht daarop.<sup>138</sup> Technologiebedrijven trekken ten strijde om de vrijheden van hun gebruikers te beschermen, Microsoft-jurist Brad Smith<sup>139</sup> en Apple-baas Tim Cook voorop.<sup>140</sup> Amerikaanse rechters buigen zich met enige regelmaat over principiële zaken, bijvoorbeeld over de reikwijdte van het Fourth Amendment en het doorzoeken van mobiele telefoons,<sup>141</sup> over rechtsmacht bij het

115. HvJ EU 28 juli 2016, zaak C-191/15, ECLI:EU:C:2016:612 (*Amazon*).

116. Het Safe Harbor Framework was een zelfreguleringsprogramma waarbij Amerikaanse bedrijven zich konden aansluiten. Als een Amerikaans bedrijf aangesloten was bij het Safe Harbor Framework, gold het verbod op doorgifte van persoonsgegevens naar landen buiten de EER niet en mochten Europese verantwoordelijken dus persoonsgegevens doorgeven aan het Amerikaanse bedrijf.

117. HvJ EU 6 oktober 2015, C-362/14 (*Schrems*); zie voor een bespreking o.a. L. Moerel, 'De betekenis van de Safe Harbor uitspraak van het Europese Hof voor data-doorgiftes naar de VS', *NJB* 2016/824, afl. 17, B. van der Sloot, 'Machtsstrijd over persoonsgegevens, De zaak Schrems v. Data Protection Commissioner van het Europees Hof van Justitie', *Ars Aequi* 2016, p. 248 e.v.; N.M. Wisman, 'Schrems ofte wel de "EU localisation laws"?', *P&I* 2015/6, p. 235 e.v. Specifiek voor advocaten: N. N. Gloudemans-Voogd, 'Hoe sla je je data veilig op? Saven na Schrems', *Advocatenblad* 2016/2, p. 40-42; O.L. van Daalen, 'Het Schrems/Facebook-arrest en de gevolgen voor internationale doorgifte', *NTER* mei 2016/3, p. 75 e.v.; zie ook de noot van N.A.N.M. van Eijk onder het arrest in *TvCH* 2016/4, p. 198-199.

118. De Artikel 29 Werkgroep heeft op 16 oktober 2015 laten weten dat zij onderzoek in hoeverre deze instrumenten een adequaat beschermingsniveau verzekeren. Zolang dat onderzoek nog loopt, kunnen de instrumenten gebruikt worden, maar dat betekent niet dat de toezichthouders niet

kunnen optreden in concrete zaken, bijv. naar aanleiding van klachten van betrokkenen, zie: [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2015/20151016\\_wp29\\_statement\\_on\\_schrems\\_judgement.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf).

119. Zie voor kritiek het persbericht van de Artikel 29 Werkgroep, [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2016/20160726\\_wp29\\_wp\\_statement\\_eu\\_us\\_privacy\\_shield\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf); en de eerdere uitgebreide analyse in *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision* van 13 april 2016, WP238. Deze kritiekpunten worden breder (bijvoorbeeld in de literatuur) gesignaleerd en zullen tijdens de jaarlijkse evaluatie van het Privacy Shield worden beoordeeld. L. Moerel, 'De betekenis van de Safe Harbor uitspraak van het Europese Hof voor datadoorgiftes naar de VS', *NJB* 2016/824, afl. 17.

120. Zie de verklaring van Schrems op: [http://europe-v-facebook.org/PA\\_PS.pdf](http://europe-v-facebook.org/PA_PS.pdf).

121. Voor een overzicht van relevante EHRM-jurisprudentie, zie de fact sheet hate speech van juni 2016, [www.echr.coe.int/Documents/FS\\_Hate\\_speech\\_ENG.pdf](http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf).

122. [http://europa.eu/rapid/press-release\\_IP-16-1937\\_en.htm](http://europa.eu/rapid/press-release_IP-16-1937_en.htm).

123. HvJ EU 25 oktober 2011, gev. zaken C-509/09 en C161/10, ECLI:EU:C:2011:685 (*eDate/Martinez*).

124. HR 3 juni 2016, ECLI:NL:HR:2016:1054 (*journalist/Dahabshii Transfer Services*). Het oordeel is sailant, omdat inbreuken op persoonslijke-rechten destijds juist expliciet van de

reikwijdte van de Rome II Verordening werden uitgezonderd (zie art. 1 lid 2 sub g Rome II Vo. 864/2007).

125. Rb. Rotterdam 29 oktober 2015, ECLI:NL:RBROT:2015:9169.

126. Rb. Rotterdam (vzr.) 16 oktober 2015, ECLI:NL:RBROT:2015:7637 (*Ambachtzorg/X*).

127. Rb. Den Haag (vzr.) 16 september 2015, IEF 15267 (*Blogspot*); bevestigd door Hof Den Haag 26 juli 2016, ECLI:NL:GHDHA:2016:2161; Rb. Den Haag (vzr.) 16 september 2015, MR 19044 (AD). Het kantoor van de auteurs treedt in deze zaak op voor Google.

128. Hof Den Bosch 6 oktober 2015, ECLI:NL:GHSHE:2015:3904. Het kantoor van de auteurs treedt in deze zaak op voor Google.

129. Rb. Limburg 22 augustus 2016, ECLI:NL:RBLIM:2016:7288.

130. Hof Amsterdam 31 maart 2015, ECLI:NL:GHAMS:2015:1123. De procedure is momenteel bij de Hoge Raad aanhangig. Het kantoor van de auteurs treedt in deze en de hierna nog te noemen 'vergeetzaken' op voor Google.

131. Rb. Amsterdam 24 december 2015, ECLI:NL:RBAMS:2015:9515.

132. Rb. Rotterdam 29 maart 2016, ECLI:NL:RBROT:2016:2395; annotatie van N.C. Lodder en M. Weij in *Tijdschrift voor Internetrecht* 2016, 2, p. 69 e.v.; zie ook F. Zuiderveen Borgesius, 'Het "right to be forgotten" en bijzondere persoonsgegevens', *Computerrecht* 2016/4, p. 220 e.v. Hoger beroep is aanhangig.

133. Artikel 29-Werkgroep, EU-Richtsnoeren voor behandeling van verzoeken aan

internetzoekmachines om 'vergeten te worden', 26 november 2014.

134. Nieuwsbericht AP, 'Bemiddeling AP bij verwijdering zoekresultaten door Google', 25 mei 2016, <https://autoriteitpersoonsgegevens.nl>.

135. [www.google.com/transparencyreport/removals/europeprivacy/](http://www.google.com/transparencyreport/removals/europeprivacy/).

136. [www.microsoft.com/about/csr/transparencyhub/crrr/](http://www.microsoft.com/about/csr/transparencyhub/crrr/).

137. H. Hijmans, *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU* (diss. UvA Amsterdam) 2016, <http://hdl.handle.net/11245/2.169421>.

138. Zie voor een bespreking daarvan bijv. het blog [www.justsecurity.org](http://www.justsecurity.org), van het Center for Human Rights and Global Justice van New York University School of Law.

139. Zie bijv. T. Simonite, 'Microsoft's Top Lawyer Becomes a Civil Rights Crusader', 8 september 2016, [www.technologyreview.com](http://www.technologyreview.com).

140. Zie bijv. de open brief naar aanleiding van de eis van de FBI dat Apple een verzwakte versie van het iOS-besturingssysteem zou ontwikkelen waarmee mogelijk de smartphone van de dader van een terreuraanslag in San Bernardino ontgrendeld zou kunnen worden: [www.apple.com/customer-letter/](http://www.apple.com/customer-letter/). Een zeer principieel aangezette rechtszaak tussen Apple en de FBI werd afgeblazen toen de FBI er langs andere weg alsnog in slaagde de telefoon te ontgrendelen.

141. *Riley/California*, No. 13-132, 573 U.S. \_\_\_ (2014).

opvragen van gegevens uit de cloud,<sup>142</sup> of over het verzwakken van encryptie en andere beveiligingsmaatregelen door tech-bedrijven.<sup>143</sup>

Aan onze kant van de oceaan zijn het Hof van Justitie, dat sinds 2009 kan toetsen aan het Handvest van de Grondrechten van de Europese Unie, en het EHRM in opeenvolgende uitspraken kritisch over grootschalige gegevensverzameling over burgers. In de vorige kroniek werd al besproken hoe het Hof van Justitie in een vernietigend arrest de *Dataretentierichtlijn* ongeldig verklaarde.<sup>144</sup> De vernietiging in de hiervoor besproken *Schrems*-zaak van de Safe Harbour-beschikking van de Europese Commissie was mede gebaseerd op het ontbreken van adequate waarborgen tegen gebruik daarvan door Amerikaanse inlichtingendiensten. Tegelijkertijd continueerde het Europees Hof voor de Rechten van de Mens zijn jurisprudentie over digitale surveillance in de uitspraken *Szabo* en *Zakharov*.<sup>145</sup> Ook de Artikel 29-werkgroep deed een duit in het zakje, met een analyse van (en eerdere opinie over) surveillance van elektronische communicatie voor inlichtingen- en veiligheidsdoelinden.<sup>146</sup> In Nederland volgde een dappere Haagse voorzieningenrechter de eerdere uitspraak van het Hof van Justitie door de nationale implementatie van de *Dataretentierichtlijn* buiten werking te stellen.<sup>147</sup> Toezichthouder Agentschap Telecom, dat de bewaarplicht na de vernietiging op Europees niveau gewoon was blijven handhaven,<sup>148</sup> maakte snel een draai van 180 graden: alle bewaarde gegevens moesten onmiddellijk worden geanonimiseerd of vernietigd.<sup>149</sup> De coalitie Burgers tegen Plasterk stelde hoger beroep in tegen het oordeel van de Rechtbank Den Haag dat – kort gezegd – de AIVD-gegevens met de Amerikaanse diensten mocht uitwisselen, en werd toegelaten om te interveniëren in de procedure die de Britse organisatie Big Brother Watch bij het EHRM heeft aangespannen vs. het Verenigd Koninkrijk.<sup>150</sup>

In Europa waait de politieke wind, gevoed door de recente terroristische aanslagen en opkomend populisme, ondertussen weer uit een andere hoek. In het Verenigd Koninkrijk codificeert de Investigatory Powers Bill de massale surveillancepraktijken die Edward Snowden aan het licht bracht.<sup>151</sup> Ook in Frankrijk werd in 2015 vergaande surveillancewetgeving aangenomen, die na de aanslagen van 2016 nog verder is verruimd.<sup>152</sup> In Duitsland publiceerde de hoogste privacytoezichthouder een vernietigend rapport waaruit bleek dat de Duitse inlichtingendienst op tal van punten de wet had geschonden en bovendien het onderzoek ernstig had gehinderd.<sup>153</sup> Kort daarna werd bekend dat 's werelds grootste internetknooppunt De-CIX de Duitse regering aanklaagt voor het onrechtmatig aftappen van haar systemen.<sup>154</sup> In Nederland is er momenteel een scala aan wetgevende activiteiten op dit terrein, waarvan de herziening van de Wet op de Inlichtingen- en Veiligheidsdiensten, het Wetsvoorstel Computercriminaliteit III, het voorstel voor een nieuwe bewaarplicht en een regeling voor het vastleggen en bewaren van kentekens de belangrijkste zijn. Na een positief en verstandig kabinetsstandpunt over encryptie<sup>155</sup> liet AIVD-baas Bartholee in een interview alvast weten dat hij de privacydiscussie 'beu' is en dat zijn dienst versleuteling altijd ongedaan moet kunnen maken.<sup>156</sup>

Het wetsvoorstel Computercriminaliteit III (hierna CC III) heeft een lange voorgeschiedenis en kwam in de

vorige kroniek al aan de orde.<sup>157</sup> Het ligt inmiddels bij de Tweede Kamer, in enigszins afgeslankte vorm.<sup>158</sup> Meest controversieel daarin is een omvangrijke hackbevoegdheid voor de officier van justitie, na machtiging van de rechter-commissaris, waarmee in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten voortaan iedere computer, tablet, telefoon, server of slimme thermostaat die 'in gebruik is bij een verdachte'<sup>159</sup> gehackt kan worden.<sup>160</sup> Het gehackte apparaat kan vervolgens onder surveillance worden geplaatst.<sup>161</sup> Daarbij geldt dat de autoriteiten Nederlandse rechtsmacht mogen aannemen, ook als niet bekend is waar de data waartoe toegang wordt verkregen zich bevinden.<sup>162</sup> Het CC III wetsvoorstel geeft iedere officier van justitie daarnaast de bevoegdheid om, met machtiging van een rechter-commissaris, iedere aanbieder van een communicatiedienst te bevelen informatie te blokkeren of te verwijderen ter beëindiging of voorkoming van een strafbaar feit.<sup>163</sup> Bits of Freedom boekte een overwinning door toegevoegd te krijgen dat een aanbieder voorafgaand aan een dergelijk notice & takedownbevel verplicht door de rechter-commissaris moet worden gehoord, met recht op bijstand door een advocaat.<sup>164</sup>

## In Nederland volgde een dappere Haagse voorzieningenrechter de eerdere uitspraak van het Hof van Justitie door de nationale implementatie van de *Dataretentierichtlijn* buiten werking te stellen

In april 2016 lekten een concept-wetsvoorstel en memorie van toelichting voor de herziene Wet op de Inlichtingen- en Veiligheidsdiensten (hierna Wiv 20xx) uit.<sup>165</sup> Controversieel is met name de voorgestelde bevoegdheid van AIVD en MIVD om kabelgebonden communicatie in bulk af te tappen, eufemistisch aangeduid als 'onderzoeksopdracht gerichte interceptie'.<sup>166</sup> In de toelichting wordt in populaire taal benadrukt dat de bevoegdheid niet overmatig of lichtvaardig zal worden ingezet<sup>167</sup> en in een parlementair debat sloot Minister Plasterk uit dat het volledige internetknooppunt AMS-IX zou worden afgetapt.<sup>168</sup> De wettekst bevat daartoe echter geen harde beperkingen, anders dan het vage criterium dat bulkinterceptie gekoppeld moet zijn aan een concrete 'onderzoeksopdracht'.<sup>169</sup> Voorbeelden daarvan geeft de toelichting nauwelijks. Duidelijk is wel dat tussen 2016 en 2020 vier 'access locaties' gereed worden gemaakt.<sup>170</sup> Veelzeggend was bovendien de gelekte brief van Minister Plas-

terk waarin hij telecomaandieners vroeg een kostenschattening te geven voor het aftappen van het communicatieverkeer tussen een fictieve stad met 400 000 inwoners en een niet nader genoemde applicatie, in de brief conservatief geschat op 200 eindgebruikers, en voor het aftappen van WiFi-hotspots.<sup>171</sup> De Wiv 20xx bevat daarnaast een uitgebreide set medewerkingsplichten.<sup>172</sup> Die zijn voortaan niet alleen meer op traditionele telecomaandieners van toepassing zijn, maar op iedere aanbieder van een private

of publieke communicatiedienst, of een verwante dienst (zoals *cloud-opslag*, *web hosting* en *over-the-top-diensten*).<sup>173</sup>

De Wiv 20xx voorziet, op een beperkte uitzondering voor de inzet van inlichtingenmiddelen tegen advocaten en journalisten na, niet in een systeem van rechterlijk toezicht.<sup>174</sup> In plaats daarvan is gekozen voor een tamelijk complexe en gefragmenteerde systematiek. Daarbij is voor de inzet van de zwaardere bevoegdheden vooraf

142. Zie: J. Daskal, 'Three Key Takeaways: The 2d Circuit Ruling in The Microsoft Warrant Case', 14 juli 2016, [www.justsecurity.org](http://www.justsecurity.org).

143. Zie de uitgebreide analyses van O. Kerr op 18, 19 en 24 februari 2016 over de *Apple/FBI*-zaak op het blog 'The Volokh Conspiracy' van de *Washington Post*, [www.washingtonpost.com/volokh-conspiracy](http://www.washingtonpost.com/volokh-conspiracy).

144. HvJ EU 8 april 2014, zaaknr. C-293/12, C-594/12, *Mediaforum* 2015/3 (*Digital Rights Ireland*), p. 112 e.v., m.nt. K. Irion, M-P. Granger en S.J. Eskens.

145. EHRM 4 december 2015 (*Roman Zakharov/Rusland*); EHRM 12 januari 2016 (*Szabó & Vissy/Hongarije*).

146. Art. 29 Werkgroep, Working Document on surveillance of electronic communications for intelligence and national security purposes, 5 december 2014. Zie ook: Opinion on surveillance of electronic communications for intelligence and national security purposes, 10 april 2014.

147. Rb. Den Haag (vzr.) 11 maart 2015, ECLI:NL:RBDHA:2015:2498. Voor commentaren zie: A. Diesfeldt & F. de Graaf, 'Dataretentie, alles of niets', *NJB* 2015/592, afl. 12; N. van Eijk, 'Dataretentie: beter ten halve gekeerd dan ten hele gedwaald', *Mediaforum* 2015, 3, p. 93, *Computerrecht* 2015/88, m.nt. F.C. van der Jagt.

148. A. Udo de Haes, 'Agentschap Telecom blijft bewaarplicht handhaven', *Webwereld* 11 april 2014, zie: <http://webwereld.nl/>.

149. Nieuwsbericht AT, 'Gevolgen buiten werking stelling Wet bewaarplicht telecommunicatiegegevens', 9 april 2015, [www.agentschaptelecom.nl](http://www.agentschaptelecom.nl).

150. 'Hoger beroep en Europese interventie in zaak Burgers tegen Plasterk (AIVD/NSA)', Nieuwsbericht Privacy First, 8 februari 2016, [www.privacyfirst.nl](http://www.privacyfirst.nl).

151. Zie o.a. de Briefing paper van de House of Commons Library van 11 maart 2016: <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7518>.

152. 'French State of Emergency: Overbidding Mass Surveillance', [www.laquadrature-dunet.net](http://www.laquadrature-dunet.net) 21 juli 2016.

153. A. Meister, 'Secret Report: German Federal Intelligence Service BND Violates

Laws And Constitution By The Dozen', [www.netzpolitik.org](http://www.netzpolitik.org) 2 september 2016.

154. K. McCarthy, 'World's largest internet exchange sues Germany over mass surveillance', [theregister.co.uk](http://theregister.co.uk) 16 september 2016.

155. *Kamerstukken II* 2015/16, 26642, 383.

156. "Ik vind bescherming van privacy ook uitermate belangrijk, maar zouden mensen die privacy als hoogste doel hebben dat net zo enthousiast nastreven als zij slachtoffer zijn van een aanslag? Als zij weten dat zij hebben toegestaan dat zoiets gebeurd is?", aldus Bertholee in: H. Modderkolk, "Dreiging is in jaren niet zo groot geweest", Rob Bertholee, hoofd van veiligheidsdienst AIVD', *de Volkskrant* 17 september 2016. [www.privacynieuws.nl/images/001-Yatta/Docs/VK-AIVD.pdf](http://www.privacynieuws.nl/images/001-Yatta/Docs/VK-AIVD.pdf).

157. Zie voor een bespreking ook: P.J.D.J. Muijen, 'Wetsvoorstel Computercriminaliteit III, To boldly go where no man has gone before', *P&I* 2016, 3, p. 104 e.v.

158. *Kamerstukken II*, 34372, 1-6. Zie ook: J. Nan, 'Kroniek van het Strafprocesrecht', *NJB* 2016/740, afl. 15.

159. Uit de memorie van toelichting (p. 98-99) blijkt dat het daarbij niet alleen gaat om telefoons en computers, maar ook 'het deel van' de cloud dat 'in gebruik is bij' een verdachte. Dat laatste is technisch en daarom problematisch. Het is maar de vraag of een dergelijke beperkte toegang technisch mogelijk is, of dat daarvoor feitelijk een volledige cloud-dienst gehackt moet worden. Opvallend is ook dat in dat verband nergens gerept wordt over de inbreuk op de vrijheid van onderneming en het eigendomsrecht van de cloud-aanbieder in een dergelijk geval.

160. Wetsvoorstel Computercriminaliteit III, *Kamerstukken II* 2015/16, 34372.

161. *Kamerstukken II* 2015.16, 23372, 3, p. 21 e.v. Daarbij kan niet alleen toegang worden verkregen tot gegevens opgeslagen in het apparaat, maar ook tot alle gegevens die worden uitgewisseld via alle communicatiekanalen en gegevens opgeslagen in de cloud. Daarbij kan bijvoorbeeld gebruik worden gemaakt van een keylogger en

kunnen GPS of microfoon heimelijk worden aangezet, vergelijk memorie van toelichting, p. 24-25.

162. Zie: par. 2.8 van de memorie van toelichting. Gelet op bijvoorbeeld het decentrale karakter van cloud-diensten, brengt dat in potentie een enorme extraterritoriale werking met zich mee.

163. Wetsvoorstel Computercriminaliteit III, *Kamerstukken* 2015/16, 34 372, voorgesteld 125p Sv. Meewerken aan een 'take-down-bevel' is voor aanbieders van communicatiediensten verplicht en voorwaarde voor een geslaagd beroep op de vervolgingsuitsluitingsgrond van art. 54a Sr. Of dat laatste in overeenstemming is met de e-Commercerichtlijn (2000/31/EG) is de vraag.

164. Voorgesteld art. 125p lid 4 Sv, MvT, p. 97.

165. Het betrof een aangepaste versie van het wetsvoorstel dat in de zomer van 2015 geconsulteerd was en dat tot honderden kritische reacties leidde. Het gelet ontwerp lijkt de kabinetsversie te zijn die voor advies aan de Raad van State is toegestuurd en die op korte termijn bij de Tweede Kamer zal worden ingediend, zie voor de volledige tekst: <http://vkplusmobilebackend.persgroep.net/rest/content/assets/13a3edbf-7dfb-4515-99b1-2d6abd32f832>.

166. Op die manier verkregen datasets mogen in ongeëvalueerde vorm met buitenlandse inlichtingendiensten worden gedeeld en kunnen met geautomatiseerde data-analysetechnieken worden onderzocht.

167. Zie bijv. para. 1.7 ('Wat gaan wij nu wel en niet doen') van de MvT: 'Wij gaan niet op zoek naar mensen die het woord "bom" of "ISIS" gebruiken in hun e-mails. Wij trekken niet in bulk internetverkeer naar binnen om te kijken welke mensen op zoek zijn naar kunststempels (...) Wat doen we wel? Onderzoekopdracht gericht interceptie zal te allen tijde een zeer klein percentage betreffen van het totaal aan nationaal en internationaal dataverkeer (...)'.  
168. 'Plasterk: AIVD gaat niet hele AMS-IX aftappen', 11 februari 2015, [www.security.nl](http://www.security.nl).

169. Als enige voorbeelden worden in de toelichting genoemd het onderscheppen van telecommunicatie met betrekking tot een missiegebied of van metadata tussen een gebied in handen van terroristen en Nederland, zie bijv. MvT, p. 127.

170. MvT, p. 21.

171. J. Schellevis, 'Plasterk denkt na over aftappen chat-apps en wifi-hotspots', 20 april 2016, [www.nos.nl](http://www.nos.nl).

172. Aanbieders kunnen op basis van de herziene Wiv 20xx worden verplicht om informatie te verschaffen over aftapmogelijkheden, moeten meewerken aan een tap en daarvoor geïnstalleerde faciliteiten een jaar na gebruik in stand houden. Aanbieders kunnen daarnaast worden verplicht om allerlei informatie te verstrekken, waaronder informatie uit de cloud met betrekking tot een specifiek target, metadata met betrekking tot een specifiek(e) nummer, gebruiker of locatie, gebruikersgegevens en kunnen verplicht worden mee te werken aan decryptie.

173. Het ligt voor de hand dat veel van deze aanbieders niet in Nederland gevestigd zullen zijn, zodat de vraag rijst of toepassing van de wet tot het nationale grondgebied beperkt is. Op het eerste gezicht is dat het geval: de memorie van toelichting expliciteert dat de herziene wet geen extraterritoriale werking heeft. Daar wordt echter cryptisch aan toegevoegd dat de Wet bescherming persoonsgegevens mogelijk een aanknopingspunt biedt om, ook waar het de Wiv 20xx betreft, rechtsmacht uit te oefenen jegens aanbieders die in het buitenland gevestigd zijn, zie: MvT, p. 302-303.

174. Parallel houdt minister Plasterk hardnekkig vast aan zijn weigering om voor de AIVD tapstatistiek vrij te geven, ondanks het oordeel van de Raad van State dat hij die weigering beter moest motiveren. Zie: 'Plasterk wil tapstatistiek AIVD opnieuw niet vrijgeven', 12 mei 2016, [www.security.nl](http://www.security.nl), met verwijzing naar ABRvS 13 januari 2016, ECLI:NL:RVS:2016:48.

gaande ministeriële toestemming vereist, waarvan de rechtmatigheid getoetst wordt door een nieuwe toetsingscommissie.<sup>175</sup> De procedure bij deze commissie is echter niet op tegenspraak en er wordt geen *public interest attorney* of technisch expert aangewezen.<sup>176</sup> Zittingen van de commissie zijn niet openbaar en het is onduidelijk of uitspraken dat wel zijn. Daarnaast is er toezicht achteraf door de CTIVD, dat haar werk doet via het publiceren van rapporten, het onderzoeken van meldingen van klokkenluiders en in een klachtprocedure. Die laatste procedure staat open voor een ieder 'jegens wie' door de diensten is opgetreden. Het is niet expliciet verduidelijkt of dat ook aanbieders van communicatiediensten omvat. De door de CTIVD toe te passen norm is vaag, namelijk of de diensten 'behoorlijk' gehandeld hebben. Het is onduidelijk of dat een beoordeling van de geschiktheid en effectiviteit van een ingezette maatregel omvat en of naast het belang van een klager, ook het

### Als het Hof van Justitie die conclusie volgt, dan is een nationale bewaarplicht die daadwerkelijk verenigbaar is met het EU Handvest eerder een theoretische mogelijkheid dan eenvoudige realiteit

algemeen belang meeweegt.

Intussen ligt de principiële vraag naar de bestaanbaarheid van een algemene (nationale) bewaarplicht van communicatiegegevens bij het Europese Hof van Justitie voor.<sup>177</sup> A-G Saugmandsgaard kwam tot de conclusie dat een nationale bewaarplicht voor opsporingsdoelinden op zich verenigbaar kan zijn met Europese fundamentele rechten, mits daarbij in een reeks strikte waarborgen wordt voorzien.<sup>178</sup> De Nederlandse regering stuurde daarop, na een publieke consultatie,<sup>179</sup> en ondanks een negatief advies van de AP,<sup>180</sup> een wetsvoorstel voor een nieuwe bewaarplicht naar de Tweede Kamer.<sup>181</sup> Bits of Freedom liet daarop weten die niet onder haar gebruikelijke privacyloep te zullen nemen: er zijn teveel voorgestelde surveillancemaatregelen tegelijkertijd en de waakhond van onze digitale burgerrechten is onderbezet.<sup>182</sup> Een zorgelijke ontwikkeling en goede reden om de digitale burgerrechtenorganisatie (alsnog) te steunen.

Bij de nieuwe Nederlandse bewaarplicht moeten te bewaren verkeersgegevens voortaan in Nederland of een andere EU-lidstaat worden opgeslagen.<sup>183</sup> Het Agentschap Telecom krijgt voortaan de bevoegdheid om de opgeslagen gegevens in te zien en zelfstandig vast te stellen of de beveiliging op orde is.<sup>184</sup> Toegang tot bewaarde gegevens is alleen mogelijk met voorafgaande machtiging

van de rechter-commissaris,<sup>185</sup> die daardoor zo'n 42 000 extra vorderingen per jaar zal zien.<sup>186</sup> De rechter-commissaris heeft per vordering ongeveer 15 minuten de tijd om te beoordelen of het opvragen van verkeersgegevens wordt gerechtvaardigd door de ernst van het misdrijf in kwestie en het belang van het onderzoek. Concrete(re) handvatten voor die beoordeling zijn er niet.<sup>187</sup> Het college van procureurs-generaals en de politie vinden de nieuwe rechterlijke toets – door het Hof van Justitie zo wezenlijk geacht<sup>188</sup> – zonder 'bijzondere meerwaarde' en vrezende vertragingen; alsof rechtstatelijke waarborgen alleen toelaatbaar zijn als zij geen tijd of inspanning vergen.<sup>189</sup> Een aanvankelijk gehanteerd onderscheid, waarbij voor zwaardere misdrijven over een langere periode in bewaarde gegevens mocht worden teruggekeken dan voor lichtere misdrijven is geschrapt. Bewaarde gegevens zijn gedurende de volledige opslagtermijn (twaalf maanden voor telefonie, zes maanden voor internettoegang) opvraagbaar.<sup>190</sup>

Als het opslaan van de metadata van het telefoon- en internetgedrag van alle Nederlandse burgers *an sich* toelaatbaar blijkt, dan is het nog maar de vraag of het huidige wetsvoorstel voorziet in alle waarborgen die het Hof van Justitie daarvoor heeft geformuleerd.<sup>191</sup> Volgens A-G Saugmandsgaard zijn die waarborgen zelfstandig verplicht én cumulatief en kan een bewaarverplichting die aan deze checklist voldoet toch nog disproportioneel zijn.<sup>192</sup> Als het Hof van Justitie die conclusie volgt, dan is een nationale bewaarplicht die daadwerkelijk verenigbaar is met het EU Handvest eerder een theoretische mogelijkheid dan eenvoudige realiteit.<sup>193</sup>

Hoewel voormalig Minister Opstelten dat anders zag,<sup>194</sup> heeft de verwachte uitspraak over de toelaatbaarheid van de bewaarplicht voor communicatiegegevens ook betekenis voor een grootschalige opslag, en het gebruik, van kentekens door politie en de belastingdienst. Met ANPR-camera's langs de Nederlandse snelwegen worden jaarlijks drie miljard kentekenfoto's real time naar de politie en belastingdienst gestuurd.<sup>195</sup> In drie procedures over het gebruik van dergelijke foto's ter controle van een rittenregistratie van de 'auto van de zaak' concludeerde A-G Niessen recent dat deze systematische en permanente vastlegging van alle Nederlandse weggebruikers een inbreuk op artikel 8 EVRM vormt, waarvoor de vereiste wettelijke grondslag ontbreekt.<sup>196</sup> Het bij de Tweede Kamer aanhangige wetsvoorstel ANPR beoogt dat te veranderen en voorziet voor kentekenfoto's in een bewaartermijn van vier weken.<sup>197</sup> Anders dan zijn voorganger, ziet minister van der Steur wel enige overeenkomst met de bewaarplicht van communicatiegegevens, die net als de kentekengegegevens voor opsporingsdoelinden worden opgeslagen. Hij besloot daarom in het wetsvoorstel de toegang tot bewaarde kentekengegegevens afhankelijk te stellen van een voorafgaand bevel van de officier van justitie.<sup>198</sup>

## 6. Afsluiting

Net als in onze vorige kronieken over technologie en recht vallen er weinig algemene conclusies te trekken. De Algemene Privacyverordening laat zien hoe moeizaam de Europese Unie compromissen bereikt over controversiële onderwerpen op het snijvlak van recht, techniek en

maatschappij. Terwijl het bedrijfsleven zich de komende verslagperiode instelt op dit lange, tegenstrijdige en soms onbegrijpelijke gedrocht, zal in Brussel een volgen-de lobby- en wetgevingsstrijd woeden rondom de DSM-voorstellen van de Europese Commissie. Op het spel

staat het evenwicht tussen oude en nieuwe industrieën; tussen intellectuele eigendom, uitingvrijheid en priva-cy; en tussen burgers, makers, adverteerders en de plat-forms waarop zij samenkomen. Het wordt ongetwijfeld een mooie show. •

**175.** De toetsingscommissie heeft drie leden, maar ieder lid is bevoegd zelfstandig te oordelen, zodat de rechtmatigheid van een ministeriële toestemming in principe door één persoon kan worden getoetst. Leden moeten ten minste zes jaar rechterlijke ervaring hebben (maar hoeven dus niet per se rechter te zijn). Zij worden benoemd in een procedure met zeggenschap van het parlement en de rechterlijke macht, maar met beslissende macht van de regering.

**176.** Een probleem dat in de Verenigde Staten voor het beruchte FISA-court wel werd aangepakt met de Freedom Act, zie voor een overzicht: [www.washingtonpost.com/graphics/politics/usa-freedom-act/](http://www.washingtonpost.com/graphics/politics/usa-freedom-act/).

**177.** HvJ EU zaaknr. C-203/15 en C-698/15 (*Tele2 en Tom Watson*).

**178.** Conclusie A-G Saugmandsgaard 19 juli 2016 in gevoegde zaken C-203/15 en C-698/15 (*Tele2 en Tom Watson*). Ook de voorzieningenrechter die de Nederlandse wet bewaarplicht telecommunicatiegegevens buiten werking stelde achtte een algeme-nere bewaarplicht niet per se ontoelaatbaar of onevenredig, Rb. Den Haag (vzr.)

11 maart 2015, ECLI:NL:RBDHA:2015:2498, r.o. 3.5-3.7.

**179.** Conceptwetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens, [www.internetconsultatie.nl/dataretentie](http://www.internetconsultatie.nl/dataretentie). Zie voor een bespreking van het geconsulteerde wetsvoorstel G. Bierma, 'Opinie. Bewaarplicht 2.0 (de bètaversie)', *Tijdschrift voor Internetrecht* 2015, 8, p. 54-55; C. Cuypers & S. van Schendel, 'Het bewaren van dataretentie in Nederlands', *Tijdschrift voor Internetrecht* 2015, 8, p. 47-53.

**180.** Volgens de AP was de noodzaak van de bewaarplicht onvoldoende onderbouwd, zie: 'CBP adviseert over bewaarplicht tele-comgegevens', 16 februari 2015, [autoriteit-persoonsgegevens.nl](http://autoriteit-persoonsgegevens.nl).

**181.** Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in ver-band met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunica-tiegegevens, *Kamerstukken II* 2015/16, 34537, 1-4.

**182.** D. van der Kroft, 'Waarom wij de bewaarplicht niet gaan tackelen', 13 sep-tember 2016, <https://bof.nl/2016/09/13/waarom-wij-de-bewaarplicht-niet-gaan-tackelen/>.

**183.** Voorgesteld art. 13.5 lid 3 Tw.

**184.** Voorgesteld art. 18.7 lid 2 Tw. Momenteel bestaat het toezicht op de beveiliging en vernietiging van gegevens alleen uit systeemtoezicht, waarbij het AT alleen kan toezien op een juiste uitvoering van bedrijfsprocessen.

**185.** Voorgesteld lid 3 bij art. 126n, 126u en 126zh Sv.

**186.** *Kamerstukken II* 2015/16, 34537, 3, p. 30.

**187.** Idem, p. 12.

**188.** HvJ EU 8 april 2014, gevoegde zaken C-293/12 en C-594/12, r.o. 62 (*Digital Rights Ireland*).

**189.** *Kamerstukken II* 2015/16, 34537, 3, p. 13.

**190.** Volgens de memorie van toelichting is het aan de rechter-commissaris om de peri-ode waarop een bevraging ziet af te zetten tegen de ernst van het delict en het onder-

zoeksbelang in kwestie, idem, p. 32.

**191.** HvJ EU 8 april 2014, gevoegde zaken C-293/12 en C-594/12, r.o. 62 (*Digital Rights Ireland*), r.o. 59-68.

**192.** Conclusie A-G Saugmandsgaard 19 juli 2016 in gevoegde zaken C-203/15 en C-698/15 (*Tele2 en Tom Watson*), r.o. 221 jo. r.o. 262.

**193.** Zie voor een gedetailleerde bespreking van de conclusie van A-G Saugmandsgaard, prof. L. Woods, 'Human Rights and National Data Retention Law: the Opinion in Tele 2 and Watson', 20 juli 2016, <http://eulawanalysis.blogspot.nl>.

**194.** Y. Nijs, 'Arrest Hof om bewaarplicht heeft geen gevolgen voor opslaan kente-kengegevens', 11 april 2014, [tweakers.net](http://tweakers.net).

**195.** 'Fiscus en politie maken 3 miljard kente-kenfoto's per jaar', 2 oktober 2015, [www.security.nl](http://www.security.nl).

**196.** PHR 16 augustus 2016, ECLI:NL:PHR:2016:853 en ECLI:NL:PHR:2016:885.

**197.** *Kamerstukken II*, 33542, 1-20.

**198.** *Kamerstukken II* 2015/16, 33542, 20.