

COMPUTERRECHT

TIJDSCHRIFT VOOR INFORMATIETECHNOLOGIE EN RECHT

Editorial

Aandacht voor grondrechten, ook in crisistijd!

F.J. Zuiderveen Borgesius

Artikel

De 'aanbieder van een onlinedienst voor het delen van content' in de Richtlijn 'Digital Single Market' **Platformen, gebruikers, auteursrecht en aansprakelijkheid**

S. Depreeuw

Artikel

Content Filtering Technologies under the new copyright liability regime for content Sharing service providers and Fundamental Rights: the clash with Data Protection

E. Ellyne

Artikel

Introducing an Ancillary Right for Press Publishers: A European Law-Making Ambition for the Press - but also on Hyperlinking

A.-C. Lorrain

3/2020

NP/COMPREC-MI20003



Wolters Kluwer

Colofon

Computerrecht Tijdschrift voor Informatietechnologie en Recht

Redactie

Prof. dr. mr. S. Depreeuw, **Université Saint Louis
Brussel, advocate bij Daldewolf te Brussel, senior-onderzoeker bij Law Science, Technology and Society aan de Vrije Universiteit Brussel**

Prof. dr. A. Drahmman, hoofddocent Instituut
Publiekrecht, Universiteit Leiden

Prof. dr. mr. P. Van Eecke, hoofddocent Universiteit
Antwerpen, visiting professor Queen Mary University
of London en advocaat bij DLA Piper te Brussel

Mr. L.J. van Eymeren, legal counsel bij CarNext.com
te Amsterdam

Mr. dr. T.J. de Graaf, hoofddocent Instituut voor
Privaatrecht en eLaw, Universiteit Leiden

Prof. dr. mr. R. van den Hoven van Genderen, do-
cent Computer Law Institute, VU Amsterdam, professor
University of Lapland Rovaniemi, associate partner
Switchlegal advocaten Amsterdam

Prof. dr. mr. E. Kindt, associate professor eLaw,
Universiteit Leiden, onderzoeker CiTiP KU Leuven en
advocaat te Brussel

Mr. M. De Koning, advocaat bij Kennedy Van der Laan
te Amsterdam

Mr. A.P. Meijboom, advocaat bij Kennedy Van der
Laan te Amsterdam

Prof. mr. dr. J.J. Oerlemans, bijzonder hoogleraar bij
het Moutain Centrum en Willem Pompe Instituut
van de Universiteit Utrecht

Mr. dr. A.D. Reiling, senior rechter (gepensioneerd) in
de Rechtbank Amsterdam

Dr. S. Royer, onderzoeker CiTiP KU Leuven

Mr. S. De Schrijver, advocaat bij Astrea te Brussel

Mr. K. Stas, advocaat bij Crowell & Moring te Brussel

Mr. dr. W. Steenbruggen, advocaat bij Bird & Bird te
Den Haag

Dr. D. Stevens, voorzitter

Gegevensbeschermingsautoriteit te Brussel

Prof. mr. M.J.M. Taeymans, lector Thomas More
University College Mechelen, rechter in de
Ondernemingsrechtbank Antwerpen

Mr. E. Valgaeren, advocaat bij Stibbe te Brussel

Prof. dr. F.J. Zuiderveen Borgesius, docent, iCIS
Institute for Computing and Information Sciences,
Radboud Universiteit Nijmegen; onderzoeker bij het
IViR Instituut voor Informatierecht, Universiteit van
Amsterdam

Redactiesecretariaat

Prof. mr. M.J.M. Taeymans,
redactiecomputerrecht@telenet.be

Uitgever

Mr. drs. N.J.T. Duin,
Nicolai.Duin@wolterskluwer.com

Citeerwijze

Computerrecht jaar/publicatienummer, paragraaf-
nummer

Bijvoorbeeld: *Computerrecht* 2020/1, par. 3.4

Verschijsning

6 afleveringen per jaar

Abonnementen

Raadpleeg voor de abonnementsmogelijkheden en de
bijbehorende prijzen: www.wolterskluwer.nl/shop.

Klantenservice

Onze klantenservice kunt u bereiken via:
www.wolterskluwer.nl/klantenservice

Aanvullende informatie

Het tijdschrift Computerrecht wordt uitgegeven door de
V.Z.W. Jurimetrie

Auteursrecht

Alle rechten in deze uitgave zijn voorbehouden aan Wolters
Kluwer Nederland B.V. Niets uit deze uitgave mag worden
verveelvoudigd, opgeslagen in een geautomatiseerd gegevens-
bestand, of openbaar gemaakt, in enige vorm of op enige
wijze, hetzij elektronisch, mechanisch, door fotokopieën,
opnamen, of enige andere manier, zonder voorafgaande
schriftelijke toestemming van Wolters Kluwer. Voor zover
het maken van kopieën uit deze uitgave is toegestaan op
grond van art. 16h t/m 16m Auteurswet jo. Besluit
van 27 november 2002, Stb. 575, dient men de daarvoor
wettelijk verschuldigde vergoeding te voldoen aan de
Stichting Reprorecht te Hoofddorp (Postbus 3051, 2130 KB).

Disclaimer

Hoewel aan de totstandkoming van deze uitgave de uiterste
zorg is besteed, aanvaarden de auteur(s), redacteur(en) en
Wolters Kluwer geen aansprakelijkheid voor eventuele
fouten en onvolkomenheden, noch voor gevolgen hiervan.

Algemene voorwaarden en privacy statement

Op alle aanbiedingen en overeenkomsten van Wolters
Kluwer Nederland B.V. zijn van toepassing de Algemene
Voorwaarden van Wolters Kluwer Nederland B.V. U kunt
deze raadplegen via:
www.wolterskluwer.nl/algemene-voorwaarden. Indien
Wolters Kluwer Nederland B.V. persoonsgegevens verkrijgt is
daarop het privacybeleid van Wolters Kluwer Nederland B.V.
van toepassing. Dit is raadpleegbaar via:
www.wolterskluwer.nl/privacy-cookies.

Standaardpublicatievoorwaarden

Op iedere inzending van een bijdrage of informatie zijn van
toepassing de Standaardpublicatievoorwaarden van Wolters
Kluwer Nederland BV, gedeponeerd ter griffie van de
Rechtbank Amsterdam onder nr. 121/2004. De
Standaardpublicatievoorwaarden kunt u raadplegen via:
www.wolterskluwer.nl/algemene-voorwaarden.

ISSN 0771-7784

www.wolterskluwer.nl



Inhoudsopgave

EDITORIAL

- 80 **Aandacht voor grondrechten, ook in crisistijd!** / p. 141
F.J. Zuiderveen Borgesius

ARTIKELEN

- 81 **De ‘aanbieder van een onlinedienst voor het delen van content’ in de Richtlijn ‘Digital Single Market’ Platformen, gebruikers, auteursrecht en aansprakelijkheid** / p. 143

In deze bijdrage wordt onderzocht op welke manier de recente Richtlijn inzake auteursrechten en naburige rechten in de digitale eengemaakte markt de “aanbieder van een onlinedienst voor het delen van content” aansprakelijk maakt voor een bijzonder recht van mededeling aan het publiek tenzij hij binnen een speciaal regime van beperking van aansprakelijkheid valt. Eerst wordt gekeken naar de rechtspraak van het Hof van Justitie van de Europese Unie over het geharmoniseerde recht van mededeling aan het publiek (sub II). Vervolgens wordt het regime voor het “gebruik van beschermde content door aanbieders van een onlinedienst voor het delen van content” onderzocht (sub III), waarbij deze nieuwe figuur wordt geanalyseerd, het principe van de mededeling aan het publiek wordt uiteengezet en vervolgens de voorwaarden besproken worden waaraan voldaan moet zijn opdat de aansprakelijkheid van de aanbieder beperkt zou zijn. Tot slot wordt dit bijzondere regime gekaderd binnen ruimere evolutie van de aansprakelijkheid van de tussenpersonen in andere domeinen (sub IV).
S. Depreuw

- 82 **Content Filtering Technologies under the new copyright liability regime for content Sharing service providers and Fundamental Rights: the clash with Data Protection** / p. 154

On the 17th of April 2019, the DSM (Digital Single Market) directive was adopted. This directive was the subject of much attention, not to say scorn, on behalf of internet technology companies on the one hand and freedom of expression activists on the other. It has become infamous for, inter alia, a new copyright reform affecting the liability regime applicable to online content-sharing service provider (OCSSP). OCSSPs are content sharing platforms, such as YouTube, Facebook, Instagram, Twitter. These platforms have come to play central roles in our day-to-day lives and contribute not only to public debate but also, the evolution of art and culture. The DSM has enacted a new copyright liability regime for OCSSPs, which has overturned the previous ‘notice and take-down’ approach into a ‘notice and stay-down’ model. This new liability regime incentivizes the use of content filtering technologies. This article analyses the use of technologies in light of personal data protection and privacy. This article will start by briefly explaining (1) the new liability regime, (2) the legal questions raised by filtering technologies (3) the ECJ case law on balancing of fundamental rights with regard to filtering mechanisms (4) the filtering mechanism and the GDPR and, will end with some (5) general conclusions.
E. Ellyne

- 83 **Introducing an Ancillary Right for Press Publishers: A European Law-Making Ambition for the Press – but also on Hyperlinking** / p. 164

This paper aims at giving an overview on the “ancillary” right for the protection of press publications concerning

online uses, introduced by the Directive on Copyright in the Digital Single Market (Directive 2019/790). Through the successive amendments of the European Commission’s proposal, first by the European Parliament and then during the inter-institutional negotiations, the then Article 11, now Article 15, of the Directive has drawn a lot of attention considering its regulatory ambition and its potential impact on the daily use of online news by internet users. How will this new neighbouring right, designed for a specific category of right holders and for specific uses of content, be implemented in practice within the current copyright legal framework, in light of the existing – and evolving – related case-law, but also at national level? The discussion among the three European institutions – the Commission, the Parliament and the Council – during the so-called “trilogue” negotiations revealed some risks for legal uncertainty that could not be entirely lifted by the final inter-institutional agreement reached in February 2019. Whereas the ancillary right for the protection of press publications concerning online uses is about to be implemented in the Member States, and whereas the dominant online platforms using news extracts (such as Google and Facebook) have promptly reacted to the introduction of this new right, it is useful to look back at the genesis of Article 15 from within the law-making process. While giving an overview on the “ancillary” right for press publishers as provided by the Copyright Directive, this paper will therefore aim to analyse its law-making process, in the purpose of explaining the – legal, but also economic and political – motivations behind it. Such an exercise will lead to attempting to assess the robustness of the “ancillary” right vis-a-vis technological and economic realities.

A.-C. Lorrain

RECHTSPRAAK

NEDERLAND

- 84 **HR 27 september 2019, ECLI:NL:HR:2019:1445, m.nt. mr. R.J.J. Westerdijk** / p. 171
Browse-wrapping: het aanvaarden van algemene voorwaarden voor gebruik van gegevens gepubliceerd op een website vindt rechtens niet plaats door een mededeling in die algemene voorwaarden van aanvaarding daarvan door het gebruik van de website. Oordeel naar lers recht, maar ook geldig onder Nederlands recht.

- 85 **Rb. Amsterdam 18 december 2019, ECLI:NL:RBAMS:2019:9635, m.nt. mr. W.F.R. Rinzema** / p. 173
Als professionele IT-dienstverlener {dienst Smart Connection} een CRM-systeem op te leveren dat voldoet aan de verwachtingen die een gemiddelde klant daaraan mag ontleen. Zelfs als dit dus niet met zoveel woorden in de overeenkomst is opgenomen (die hier overigens slechts een presentatie betreft, waaruit dus sowieso de daadwerkelijke afspraken slecht af te leiden zijn), mag een klant immers van een deskundige ICT-dienstverlener die daarvoor marktconforme prijzen in rekening brengt, verwachten dat deze een systeem levert waarmee door de gemiddelde werknemer kan worden gewerkt. En ook als een ISO-norm niet met zoveel woorden is overeengekomen, mag de klant verwachten dat zijn professionele dienstverlener werkt met inachtneming van de normen die binnen de branche gebruikelijk zijn.

(Zie vervolg op omslag 3)

Aandacht voor grondrechten, ook in crisistijd!

Computerrecht 2020/80

Editorial

De redactie van *Computerrecht* hoopt dat u en uw naasten gezond zijn in deze coronacrisis. We leven in vreemde tijden. Velen van ons werken vanuit huis, vaak terwijl de kinderen ook thuis zijn. Een enorme stroom coronanieuws komt elke dag op ons af.

Op het gebied van grondrechten, ICT en recht gebeurt er ondertussen ook veel, ook in verband met de coronacrisis. Zo staat het recht op privacy onder druk. Op het moment van schrijven (april 2020) is er bijvoorbeeld veel discussie in Nederland en daarbuiten over het gebruik van apps om de coronacrisis te helpen indammen. De Nederlandse regering heeft gevraagd om voorstellen voor 'slimme digitale oplossingen', waaronder apps in de strijd tegen corona, maar wel met voldoende aandacht voor privacy.

Niet alleen privacy wordt bedreigd door maatregelen om het coronavirus tegen te gaan. Er wordt soms geopperd dat mensen een soort ik-ben-immuun-pas zouden moeten krijgen. Zo'n maatregel zou een bedreiging vormen voor het recht op bewegingsvrijheid en het recht op vereniging, als bepaalde locaties alleen toegankelijk zijn met zo'n pas. Er is ook een risico op discriminatie van mensen die niet immuun zijn.

Haastige maatregelen als reactie op een crisis kunnen langdurig onze grondrechten aantasten, leert het verleden. Zo werd in Europa in reactie op terroristische aanslagen in Londen en Madrid de Dataretentierichtlijn aangenomen in 2006. De EU-richtlijn verplichtte landen om dataretentiewetten aan te nemen. Die wetten moesten telecommunicatiebedrijven verplichten alle metadata van hun klanten op te slaan voor een periode van zes tot achttien maanden. Metadata laten bijvoorbeeld zien wie u belde op welk moment, en waar u uw mobieltje gebruikte. De bedoeling was dat nationale autoriteiten, zoals de politie, toegang tot die metadata konden krijgen als dat nodig was in de strijd tegen terrorisme en zware criminaliteit.

Velen vonden de richtlijn te ver gaan. De toenmalige European Data Protection Supervisor, Peter Hustinx, noemde de richtlijn de meest privacybedreigende maatregel die de EU ooit had genomen. Na nationale juridische procedures vroegen uiteindelijk rechters uit Ierland en Oostenrijk aan het Hof van Justitie van de Europese Unie of de richtlijn wel verenigbaar was met fundamentele rechten.

Het Europese Hof verklaarde de richtlijn ongeldig in 2014.² Het Hof zei dat de strijd tegen terrorisme en zware criminaliteit belangrijk was. Maar de inbreuk op de fundamentele rechten op privacy en de bescherming van persoonsgegevens was te groot. Het Hof verklaarde daarom de richtlijn ongeldig. EU-lidstaten waren dus niet meer verplicht een dataretentiewet te hebben.

Je zou kunnen zeggen: het systeem van *checks and balances* heeft gewerkt, en het Hof van Justitie van de EU heeft grondrechten beschermd tegen overijverige beleidsmakers.

Maar het heeft wel acht jaar geduurd voor de Dataretentierichtlijn ongeldig werd verklaard. In Nederland duurde het overigens nog langer voor we van de dataretentiewet verlost waren. De Nederlandse regering koos ervoor om de dataretentiewet te handhaven, zelfs nadat het Europese Hof beslist had dat een dataretentieverplichting te ver ging.

¹ Prof. dr. Frederik Zuiderveen Borgesius is frederikzb@cs.ru.nl.

² HvJ EU 8 april 2014, C-293/12, ECLI:EU:C:2014:238, *Computerrecht* 2014/76.

Uiteindelijk stelde de Nederlandse rechter ook de Nederlandse dataretentiewet buiten werking.³

Kortom, haastig aangenomen crisiswetten kunnen onze grondrechten voor lange tijd aantasten, zelfs in gevallen waarin een rechter uiteindelijk ingrijpt om de burger te beschermen.

We kunnen lessen trekken uit de dataretentiezaak, ook voor maatregelen in de strijd tegen het coronavirus. Eén les is bijvoorbeeld dat maatregelen geen disproportionele beperking op grondrechten met zich mogen brengen, zelfs niet als een zwaarwichtig algemeen belang wordt nagestreefd zoals het tegengaan van terrorisme of een pandemie.

Een tweede belangrijke les is: wetten die aangenomen worden als antwoord op een crisis, zoals in dit geval de coronacrisis, moeten altijd een horizonbepaling hebben. Met andere woorden, de crisiswet moet vanzelf ongeldig worden na een bepaalde periode (bijvoorbeeld zes maanden), tenzij de wetgever dan expliciet beslist om de geldigheid van de wet te verlengen. Ook in crisistijden moeten we onze grondrechten blijven beschermen.

3 Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498, *Computerrecht* 2015/88.

De ‘aanbieder van een onlinedienst voor het delen van content’ in de Richtlijn ‘Digital Single Market’ Platformen, gebruikers, auteursrecht en aansprakelijkheid

Computerrecht 2020/81

In deze bijdrage wordt onderzocht op welke manier de recente Richtlijn inzake auteursrechten en naburige rechten in de digitale eengemaakte markt de “aanbieder van een onlinedienst voor het delen van content” aansprakelijk maakt voor een bijzonder recht van mededeling aan het publiek tenzij hij binnen een speciaal regime van beperking van aansprakelijkheid valt. Eerst wordt gekeken naar de rechtspraak van het Hof van Justitie van de Europese Unie over het geharmoniseerde recht van mededeling aan het publiek (sub II). Vervolgens wordt het regime voor het “gebruik van beschermde content door aanbieders van een onlinedienst voor het delen van content” onderzocht (sub III), waarbij deze nieuwe figuur wordt geanalyseerd, het principe van de mededeling aan het publiek wordt uiteengezet en vervolgens de voorwaarden besproken worden waaraan voldaan moet zijn opdat de aansprakelijkheid van de aanbieder beperkt zou zijn. Tot slot wordt dit bijzondere regime gekaderd binnen ruimere evolutie van de aansprakelijkheid van de tussenpersonen in andere domeinen (sub IV).

I. Inleiding

1. Op 17 april 2019 werd de langverwachte Richtlijn inzake auteursrechten en naburige rechten in de digitale eengemaakte markt aangenomen.² Een van de meest controverseele bepalingen was “art. 13” (intussen art. 17), dat de “value gap” moest herstellen die met de komst van moderne contentplatformen gegroeid was.

Kort gezegd had de Europese wetgever vastgesteld dat beschermde werken en prestaties (uitvoeringen, opnames) door gebruikers via platformen geupload en met

andere gebruikers gedeeld werden, waardoor een bepaalde waarde gegenereerd werd voor de gebruikers (namelijk toegang tot beschermde inhoud voor de ontvanger, cultureel of sociaal kapitaal voor de deler, in sommige gevallen zelfs een financiële vergoeding) en voor de platformen (namelijk een geïnteresseerd publiek, toegang tot persoonsgegevens en advertentie-inkomsten). De auteurs en houders van naburige rechten bleven echter vreemd aan deze lucratieve deals.³

Met zijn ingrijpen had de Europese wetgever de bedoeling om deze situatie te corrigeren en de rechthebbenden juridische middelen te geven om over een vergoeding te onderhandelen voor het gebruik van de beschermde inhoud of, bij gebrek aan een akkoord, het gebruik te verbieden.

2. De notie “platform” is complex en kan verschillende technische of commerciële begrippen omvatten. Een eenduidige juridische definitie is er voorlopig niet, maar voor deze bijdrage wordt onder “platform” begrepen een platform om inhoud te delen (“content sharing platforms”), meer bepaald een digitale applicatie (bijv. webapplicatie of een mobiele applicatie) die door personen gebruikt kan worden om inhoud te uploaden (actieve gebruiker) of om inhoud te bekijken of te beluisteren (passieve gebruiker). Belangrijk is dat de gebruiker op eigen initiatief handelt, zonder a priori onder controle van het platform te staan. Typische voorbeelden van deze platformen zijn YouTube, Soundcloud of Facebook.

Daarentegen zijn de applicaties die contentdistributeurs gebruiken om muziek of video (onder hun eigen merk) bij het publiek te brengen geen “platformen” voor deze bijdrage: de gebruikers hebben geen aansprakelijkheid om het aanbod via deze diensten te beïnvloeden, zodat de auteursrechtelijke problematiek anders gesteld wordt. Typische voorbeelden zijn de contentdiensten van omroepen (zoals VRT Nu of VTM Go), van teleco-aanbieders of van nieuwe spelers (zoals Netflix).

3. In deze bijdrage zal worden onderzocht op welke manier het gebruik van beschermde inhoud via online platformen auteursrechtelijk geregeld wordt. Eerst zal

¹ Sari Depreeuw is advocate bij het kantoor DALDEWOLF (Brussel) en professor Intellectuele Rechten en Mediarecht aan de Université Saint-Louis Bruxelles.

² Richtlijn (EU) 2019/790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG, *PbEU* L 130 van 17 mei 2019, (92) (ook wel de “Digital Single Market” genoemd en hierna “DSM-richtlijn” of “DSM”) heeft het Hof van Justitie verzocht om de DSM-richtlijn, met name art. 17 lid 4 onder (b) en (c) te vernietigen wegens strijdigheid met de vrijheid van meningsuiting (art. 11 Handvest Grondrechten EU). Beroep ingesteld op 24 mei 2019, *Republiek Polen/Europees Parlement en Raad van de Europese Unie*, zaak C-401/19.

³ Hierna zal voor de leesbaarheid slechts naar “auteurs” en “auteursrechten” verwezen worden. De regels gelden evenwel ook voor de houders van naburige rechten (uitvoerende kunstenaars, producenten van fonogrammen en eerste vastleggingen van films), tenzij anders aangegeven.

kort worden nagegaan hoe de rol van deze platformen in het auteursrecht gezien werd vooraleer de DSM-richtlijn aangenomen werd (sub II), daarna zal onderzocht worden hoe de toegang tot beschermde inhoud via online platformen in de DSM-richtlijn geregeld wordt (sub III) en tot slot zal nagegaan worden of deze regeling een algemene evolutie inluidt in de perceptie van platformen (sub IV).

II. 'Mededeling aan het publiek' en de rol van platformen voor de DSM-richtlijn

4. De vraag naar de verantwoordelijkheid van platformen voor de auteursrechtelijke inbreuken die met hun diensten begaan werden, werd al gesteld lang voor van de DSM-richtlijn sprake was. Op Europees niveau moet niet alleen rekening gehouden worden met de harmonisering van het auteursrecht, maar ook met de beperking van de aansprakelijkheid van bepaalde tussenpersonen in de Richtlijn e-commerce⁴ en de mogelijkheid om ten aanzien van tussenpersonen een stakingsmaatregel op te leggen, onafhankelijk van hun aansprakelijkheid voor deze inbreuk (art. 8 lid 3 InfoSoc-richtlijn en art. 11 Handhavingsrichtlijn).⁵

Een eerste vraag is of het delen van beschermde inhoud via platformen een inbreuk op het recht van mededeling aan het publiek maakt, in hoofdte van de gebruiker en/of het platform. Een tweede vraag is of het platform zijn eventuele aansprakelijkheid voor de mededelingsdaad kan ontlopen door de beperking van de aansprakelijkheid die de E-commercerichtlijn ten voordele van bepaalde tussenpersonen heeft ingesteld.

5. Vaste rechtspraak

Sinds de harmonisering van de auteursrechtelijke vermogensrechten⁶ heeft het Hof van Justitie van de Europese Unie (HvJ EU) zich al verschillende keren uitgesproken over de interpretatie van het recht van mededeling aan

het publiek.⁷ Zo heeft zich een vaste, steeds complexere rechtspraak gevormd rond het mededelingsrecht dat wordt voorzien in art. 3 van de InfoSoc-richtlijn en art. 8 van de Verhuurrichtlijn.

Een handeling kan als een mededeling aan het publiek gekwalificeerd worden indien aan twee cumulatieve voorwaarden voldaan is: er is een "mededeling" en een "publiek".⁸ Dit recht vergt een "geïndividualiseerde beoordeling", in functie van "meerdere niet-autonome en onderling afhankelijke, elkaar aanvullende criteria", die "zowel individueel als in hun onderling verband worden toegepast, aangezien deze criteria in verschillende concrete situaties met een zeer wisselende intensiteit een rol kunnen spelen".⁹ Hiermee houdt het Hof de handen vrij om het synthetisch geformuleerde mededelingsrecht toe te passen op zeer uiteenlopende situaties.

Toch moet de rechter uitgaan van een "hoog beschermingsniveau" voor de auteur, hem een "passende vergoeding" kan toekomen.¹⁰ Tegelijkertijd moet de rechter ook een evenwicht nastreven tussen de fundamentele rechten die zowel de intellectuele eigendomsrechten (krachtens art. 17 Handvest van de grondrechten van de Europese Unie) als de vrijheid van meningsuiting (krachtens art. 11 Handvest) toekomen.¹¹

6. Een "mededeling" kan worden vastgesteld wanneer de gebruiker "met volledige kennis van de gevolgen van zijn handelwijze, intervenieert om zijn klanten toegang te verlenen tot beschermd werk, met name daar deze klanten zonder een dergelijke interventie in beginsel geen, of slechts moeilijk, toegang zouden hebben tot het verspreide werk".¹² De gebruiker speelt zo een centra-

4 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel"), *PbEG* L 178 van 17 juli 2000 (0001).

5 Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, *PbEG* L 167 van 22 juni 2001, (10) (hierna "InfoSoc-richtlijn"); Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten, *PbEG* L 157 van 30 april 2004, (45) (hierna "Handhavingsrichtlijn").

6 Richtlijn 2006/115/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende het verhuurrecht, het uitleenrecht en bepaalde naburige rechten op het gebied van intellectuele eigendom (gecodeerde versie), *PbEU* L 376 van 27 december 2006, (28) (hierna "Verhuurrichtlijn").

7 Zie hierover o.a. S. Depreeuw, *The Variable Scope of the Exclusive Economic Rights in Copyright*, Kluwer Law International, 2014, 364 e.v.; F. Brison & S. Depreeuw, 'Het recht van mededeling aan het publiek' in: J. Cabay, V. Delforge, V. Fossoul & M. Lambrecht (ed.), *20 ans de nouveau droit d'auteur – 20 jaar nieuw auteursrecht*, Limal, Anthemis, 2015, 69-117; S. Depreeuw, 'De 'mededeling aan het publiek' in de rechtspraak van het Hof van Justitie van de Europese Unie', *I.R. D.J.* 2015, 4 (310) 310-330; F. Brison & S. Depreeuw, 'The right of "communication to the public" in the European Union' in: P. Torremans (ed.), *Research Handbook on Copyright Law*, Edward Elgar, 2017, 96-134; E. Rosati, *The CJEU Pirate Bay Judgment and Its Impact on the Liability of Online Platforms*, SSRN, 2017, 23, <https://ssrn.com/abstract=3006591> (zie ook: *European intellectual property review* 2017, vol. 39, nr. 12).

8 Zie o.a. HvJ EU 31 mei 2016, *Reha Training Gesellschaft für Sport- und Unfallrehabilitation mbH/Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte eV (GEMA)*, C-117/15, ECLI:EU:C:2016:379, punt 37; HvJ EU 19 november 2015, *SBS Belgium NV/Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM)*, C-325/14, ECLI:EU:C:2015:764, punt 15; HvJ EU 26 april 2017, *Stichting Brein/Jack Frederik Willems ("Filmspeler")*, C-527/15, ECLI:EU:C:2017:300, punt 29; HvJ EU 14 juni 2017, *Stichting Brein/Ziggo, XS4ALL Internet ("Pirate Bay")*, C-610/15, ECLI:EU:C:2017:456, punt 24.

9 Zie o.a. HvJ EU 8 september 2016, *GS Media/Sanoma Media Netherlands BV e.a.*, C-160/15, ECLI:EU:C:2016:644, punt 34; HvJ EU, *Filmspeler*, punt 30; HvJ EU, *Stichting Brein (Pirate Bay)*, punt 25.

10 Zie o.a. HvJ EU, *GS Media*, punt 30; HvJ EU, *Filmspeler* punt 28.

11 HvJ EU, *GS Media*, punt 31.

12 HvJ EU, *GS Media*, punt 35; HvJ EU, *Filmspeler*, punt 31; HvJ EU, *Stichting Brein (Pirate Bay)*, punt 26.

le rol, ~~zijn~~ haar interventie is “weloverwogen”. De gebruiker heeft “kennis” van de gevolgen van ~~zijn~~ interventie, een vereiste die van toepassing is, ongeacht of het gaat om een gebruiker of een platform.¹³

Het begrip “mededeling” omvat ook de “beschikbaarstelling” aan het publiek, wat betekent dat leden van het publiek toegang hebben tot het werk op een moment en op een plaats die zij individueel gekozen hebben, ongeacht of zij gebruikmaken van de toegang om het beschermd materiaal ook effectief te downloaden, bekijken of beluisteren.¹⁴

7. Verder moet de mededeling gericht zijn op een “publiek”, te weten een “onbepaald aantal potentiële ontvangers”, maar wel een “vrij groot aantal personen”. Deze de-minimisdrempel wordt beoordeeld, rekening houdend met de cumulatieve effecten van de beschikbaarheid voor download, i.e. de mensen die gelijktijdig en achtereenvolgens toegang hebben tot een werk.¹⁶ Het geharmoniseerde mededelingsrecht viseert alleen een publiek op afstand, i.e. een publiek dat niet aanwezig is op de plaats waar de mededeling tot stand gebracht wordt.

In het geval van een beschikbaarstelling is relevant dat het beschermde werk via een “openbaar toegankelijke site” aangeboden wordt, het wordt aangeboden aan een “publiek” – de eigenlijke transmissie komt pas later tot stand, op vraag van de ontvanger, of komt helemaal niet tot stand.¹⁷ Het “publiek” bestaat in dat geval uit “verschillende personen tussen wie geen onderlinge relatie bestaat” (i.e. de leden van het publiek), die “individueel op verschillende plaatsen en tijdstippen toegang kunnen verkrijgen tot een werk dat het publiek op een website kan

raadplegen, en dat het publiek bestaat uit de individuele leden ervan”.¹⁸

8. De mededelingshandeling kan met verschillende technologische middelen tot stand gebracht worden. Het HvJ EU gaat volgens vaste rechtspraak na of de mededeling aan het publiek volgens een “specifieke technische werkwijze” tot stand wordt gebracht: als het werk meege-deeld wordt op een wijze die verschilt van werkwijzen die tot nu toe werden gebruikt (bijv. streaming na uitzending), volstaat de vaststelling dat het werk aan een “publiek” gericht wordt.

Wordt de mededeling echter voorafgegaan door een mededeling volgens dezelfde werkwijze (bijv. tweemaal streaming), dan moet zij gericht zijn tot een “nieuw publiek”, i.e. “een publiek dat door de houders van het auteursrecht nog niet in aanmerking werd genomen toen zij toestemming verleenden voor de oorspronkelijke mededeling van hun werk aan het publiek”.¹⁹

Tot slot is het criterium van het winsttoogmerk volgens het HvJ EU “niet zonder belang” (al wordt deze dubbele negatie niet verder ingevuld).²⁰

9. Het Hof van Justitie heeft het recht van mededeling aan het publiek op verschillende exploitatiewijzen in een digitale context toegepast, zoals de online streaming van televisieprogramma's,²¹ hyperlinking,²² het installeren van een filmspeler die het afspelen van online beschikbare films vergemakkelijkt²³ of het indexeren, het organiseren en promoten van content via een peer-to-peernetwerk²⁴ of het uitwisselen van e-books.²⁵

In het licht van de latere DSM-richtlijn is de *Pirate Bay*-zaak interessant. Met betrekking tot het peer-to-peerplatform “The Pirate Bay” heeft het HvJ EU geoordeeld dat beschermde werken beschikbaar worden gesteld aan het publiek, zodat deze on demand toegankelijk zijn, ook al

13 Opmerkelijk is de vereiste dat de gebruiker “kennis” heeft van de gevolgen van zijn interventie. Dit element zaait verwarring over de aard van de aansprakelijkheid: in geval van inbreuken op auteursrecht (i.e. primaire aansprakelijkheid) wordt uitgegaan van een objectieve aansprakelijkheid, waarbij het volstaat dat de gebruiker toegang verleent tot het werk – ongeacht of hij zich bewust is van het inbreuk makende karakter van de mededeling en ongeacht of hij een fout begaan heeft ten aanzien van een algemene zorgvuldigheidsnorm. Zie hierover F. George & J.-B. Hubin, ‘Les prestataires intermédiaires de la société de l'information face au droit commun de la responsabilité extracontractuelle’, *A&M* 2017, 3 (208) 208-237; S. Lens & B. Vanbrabant, ‘La réparation du dommage résultant d'atteintes aux droits intellectuels’ in: J. Cabay & A. Strowel (ed.), *Les droits intellectuels, entre autres droits. Intersections, interactions et interrogations*, Larcier, 2019, 109 e.v. Het element van “kennis” wordt daarentegen veelal gebruikt voor indirecte of secundaire aansprakelijkheid voor de daden van een derde (“secondary” of “contributory” liability). Zie hierover C. Angelopoulos, ‘Communication to the public and accessory copyright infringement’, *The Cambridge Law Journal* 2017, (496) 498; C. Angelopoulos & J.P. Quintais, ‘Fixing Copyright Reform: A Better Solution to Online Infringement’, *JIPITEC* 2019, 2 (147) 153.

14 HvJ EU 19 december 2019, *Nederlands Uitgeversverbond, Groep Algemene Uitgevers/Tom Kabinet Internet BV, Tom Kabinet Holding BV, Tom Kabinet Uitgeverij BV*, C-263/18, ECLI:EU:C:2019:1111, punt 63.

15 HvJ EU, *GS Media*, punt 36; HvJ EU, *Filmspeler*, punt 32; HvJ EU, *Stichting Brein (Pirate Bay)*, punt 27.

16 HvJ EU, *Filmspeler*, punt 44; HvJ EU, *Stichting Brein (Pirate Bay)*, punt 41; HvJ EU, *Tom Kabinet*, punt 68.

17 HvJ EU, *Tom Kabinet*, punt 64.

18 HvJ EU, *Tom Kabinet*, punt 67.

19 Zie o.a. HvJ EU, *GS Media*, punt 37; HvJ EU, *Filmspeler*, punt 33; HvJ EU, *Stichting Brein (Pirate Bay)*, punt 28.

20 Zie o.a. HvJ EU, *GS Media*, punt 38; HvJ EU, *Filmspeler*, punt 34; HvJ EU, *Stichting Brein (Pirate Bay)*, punt 29. In het arrest *GS Media* heeft het winsttoogmerk wel een bijzondere rol gespeeld, aangezien het winsttoogmerk van de gebruiker een weerlegbaar vermoeden doet ontstaan dat de gebruiker op de hoogte was dat de inhoud waarnaar een link verwijst onrechtmatig is geplaatst en dus toch een mededeling aan het publiek vastgesteld kan worden in geval van hyperlinking; HvJ EU, *GS Media*, punt 51.

21 HvJ EU 7 maart 2011, *ITV Broadcasting Ltd, ITV 2 Ltd, ITV Digital Channels Ltd, Channel 4 Television Corporation, 4 Ventures Ltd, Channel 5 Broadcasting Ltd, ITV Studios Ltd/TVCatchup Ltd*, C-607/11, ECLI:EU:C:2013:147.

22 HvJ EU 13 februari 2014, *Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd/Retriever Sverige AB*, C-466/12, ECLI:EU:C:2014:76; HvJ EU 21 oktober 2014, *BestWater International GmbH/Michael Mebes and Stefan Potsch*, C-348/13, ECLI:EU:C:2014:2315; HvJ EU 26 maart 2015, *C More Entertainment AB/Linus Sandberg*, C-279/13, ECLI:EU:C:2015:199; HvJ EU, *GS Media*.

23 HvJ EU, *Filmspeler*.

24 HvJ EU, *Stichting Brein (Pirate Bay)*.

25 HvJ EU, *Tom Kabinet*, punten 24-26.

waren het niet de beheerders van het platform, maar de gebruikers ervan die de werken uploaden.

Toch achtte het Hof dat “deze beheerders [van het platform The Pirate Bay], door het beschikbaar stellen en het beheer van een online platform voor de uitwisseling van bestanden (...) zich welbewust van de gevolgen van hun gedrag, handelen om toegang te verschaffen tot de beschermde werken door het op dat platform indexeren en inventariseren van de torrent-bestanden, waarmee de gebruikers van het platform deze werken kunnen lokaliseren en delen in het kader van een peer-to-peernetwerk”.²⁶ Zonder het platform zouden de gebruikers de werken niet of moeilijker kunnen delen op internet. De platformbeheerders moesten gezien worden als “onontkoombare actoren” bij de beschikbaarstelling van de werken, doordat zij het platform beschikbaar maakten en beheerden en zo aan de gebruikers toegang boden tot de werken die de gebruikers onderling met elkaar deelden.²⁷

The Pirate Bay kon niet gezien worden als een loutere “beschikbaarstelling van fysieke faciliteiten om een mededeling mogelijk te maken of te verrichten” die geen mededeling aan het publiek zou uitmaken (ov. 27 InfoSoc-richtlijn). Dit platform nam immers een actievare rol aan met de indexering van de torrent-bestanden van de gedeelde werken, die de bestanden vindbaar (via een zoekmotor en via een index volgens categorieën) en dus downloadbaar maakte, en met een controle op de kwaliteit van de bestanden en hun classificatie.

Met de vaststelling dat een publiek, zelfs een nieuw publiek, bereikt werd en dat The Pirate Bay een winstoogmerk had, kwam het HvJ EU tot de conclusie dat “het beschikbaar stellen en het beheer, op internet, van een platform voor de uitwisseling van bestanden dat, door de indexering van meta-informatie inzake beschermde werken en de verstrekking van een zoekmotor, de gebruikers van dit platform in staat stelt deze werken te vinden en deze in het kader van een peer-to-peernetwerk te delen” een mededeling aan het publiek uitmaakt.

10. Hiermee was wel duidelijk dat de beheerders van The Pirate Bay zelf aansprakelijk zijn voor de inbreuk op het mededelingsrecht, op basis van hun eigen gedrag, ook al werd het beschermd materiaal niet door hen maar door de platformgebruikers geüpload en uitgewisseld.²⁸ Het ging niet om een indirecte of secundaire aansprakelijkheid van de platformbeheerders voor het inbreukmakende gedrag

van de platformgebruikers, maar om een directe, primaire aansprakelijkheid voor een eigen mededelingshandeling.²⁹

Opmerkelijk was wel dat het HvJ EU de rol van de eindgebruiker niet heeft geanalyseerd en dus niet heeft onderzocht hoe de verhouding tussen de eindgebruiker en de platformbeheerders lag bij de aansprakelijkheid voor de inbreuk op het mededelingsrecht.

In november 2018 werden twee prejudiciële vragen gesteld aan het HvJ EU die verder ingaan op deze vragen, te weten of YouTube dan wel Cyando een mededeling aan het publiek doen van beschermde werken door hun platform ter beschikking van gebruikers te stellen en, indien dit niet het geval is, of zij van de beperking van aansprakelijkheid van art. 14 E-commercerichtlijn gebruik kunnen maken.³⁰

III. Gebruik van beschermde content door aanbieders van onlinedienst voor het delen van content in de DSM-richtlijn

11. Intussen werd de DSM-richtlijn aangenomen waarin de rol van bepaalde platformen bij de exploitatie van beschermde content geregeld wordt. Bijzonder aan dit vraagstuk is dat (net als in het *Pirate Bay*-arrest) de beheerder van het platform zelf geen beschermde werken aanbiedt maar aan de gebruikers de mogelijkheid biedt om beschermd materiaal (zoals muziek en video) te uploaden en te bekijken of te beluisteren. Het is de gebruiker die bepaalt welk materiaal (al dan niet beschermd en al dan niet door de gebruiker bewerkt) via het platform voor de andere gebruikers toegankelijk is, maar de gebruiker kan deze content alleen maar uploaden, vinden, organiseren, bekijken en beluisteren dankzij de infrastructuur van het platform.

De regeling is een complexe combinatie van regels van auteursrecht en aansprakelijkheid die slechts voor bepaalde platformen geldt. Kort gezegd wordt uitgegaan van het principe dat de platformuitbater direct aansprakelijk is voor een mededelingshandeling wanneer hij een platform uitbaat waar gebruikers beschermd materiaal kunnen delen. Deze principiële aansprakelijkheid wordt beperkt wanneer aan bepaalde voorwaarden voldaan is.

Met deze bijzondere regeling wordt weliswaar één vraag beantwoord (doet het platform een mededeling aan het publiek wanneer zijn gebruikers beschermd materiaal up-

²⁶ HvJ EU, *Stichting Brein (Pirate Bay)*, punt 36.

²⁷ HvJ EU, *Stichting Brein (Pirate Bay)*, punt 37.

²⁸ E. Rosati, *The CJEU Pirate Bay Judgment and Its Impact on the Liability of Online Platforms*, sectie 3.1; C. de Callatay & S. Depreeuw, ‘La responsabilité des intermédiaires à la lumière de la nouvelle Directive “Digital Single Market”’ in: J. Cabay & A. Strowel (ed.), *Les droits intellectuels, entre autres droits. Intersections, interactions et interrogations*, Larcier, 2019, 135 e.v.

²⁹ Deze ruime toepassing van het mededelingsrecht is te verklaren door de wens om dit aspect zoveel mogelijk te harmoniseren. De aansprakelijkheid voor de daden van derden, zoals de indirecte of secundaire aansprakelijkheid, wordt bepaald onder nationaal recht, terwijl de omschrijving van het mededelingsrecht geharmoniseerd werd, met de beperking van de aansprakelijkheid van bepaalde tussenpersonen. Zie conclusie van advocaat-generaal M. Szpunar van 8 februari 2017 in zaak C-610/15, *Stichting Brein/Ziggo BV en XS4All Internet BV*, ECLI:EU:C:2017:99, punt 3.

³⁰ Prejudiciële vragen in gevoegde zaken C-682/18 (*LF/Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH*) en C-683/18 (*Elsevier Inc./Cyando AG*).

loaden en met andere gebruikers delen?), maar rijzen meteen vele nieuwe vragen (wanneer kan het platform aan zijn eigen aansprakelijkheid voor deze mededeling ontsnappen? Hoe moeten de verschillende middelenverbintenissen geïnterpreteerd worden en hoe verhouden ze zich tot elkaar? Hoe verhouden de aansprakelijkheden van gebruikers en platform zich tot elkaar? Is er een filterverplichting en hoe verhoudt deze verplichting zich tot de afwezigheid van een algemene toezichtsverplichting?).

A. De "aanbieder van een onlinedienst voor het delen van content"

12. De bijzondere regeling van art. 17 DSMR is van toepassing op de "aanbieder van een onlinedienst voor het delen van content", een nieuwe figuur in het auteursrecht.

Deze "aanbieder van een onlinedienst voor het delen van content" ("online content-sharing service provider" of "OCSSP") wordt gedefinieerd als "een aanbieder van een dienst van de informatiemaatschappij die als belangrijkste of een van de belangrijkste doelstellingen heeft een grote hoeveelheid door de gebruikers van de dienst geüploade auteursrechtelijk beschermde werken of andere beschermde materialen op te slaan en toegankelijk te maken voor het publiek, waarbij hij deze werken en materialen ordent en promoot met een winstoogmerk" (art. 2 lid 6 DSMR).

13. Het gaat om een aanbieder van een **informatiemaatschappij**, i.e. "elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht" (art. 2 lid 5 DSMR, met verwijzing naar art. 1 lid 1 onder (b) Richtlijn (EU) 2015/1535).³¹

14. **Omschrijven** Deze aanbieder heeft als "belangrijkste doel" een "grote hoeveelheid" beschermd materiaal op te slaan en toegankelijk te maken voor het publiek. De bedoeling is de online platformen te vatten die een "belangrijke rol spelen op de markt voor online-content door te concurreren met andere online-contentdiensten, zoals online audio- en video-streamingdiensten, om hetzelfde publiek" (r.o. 62 DSMR).

Platformen zoals YouTube of Vimeo vallen dus zonder veel twijfel onder deze definitie. Voor andere diensten is dit misschien minder duidelijk, met name wanneer dit aspect van content delen "bijkomstig" is. In de praktijk en uit de rechtspraak zal moeten blijken wat een "grote hoeveelheid" content is. Bijvoorbeeld onlinemarktplaatsen geven de gebruikers de mogelijkheid om bepaalde content te delen (beoordelingen, commentaren), maar de belangrijkste

doelstelling is de verhandeling van goederen, niet het toegankelijk maken van auteursrechtelijk beschermde werken. Voor sociale netwerken is dit aspect misschien minder voor de hand liggend: is hun hoofddoel het onderhouden van sociale contacten of is het delen van beschermd materiaal toch meer dan "bijkomstig"? Elektronische communicatiediensten vallen buiten het toepassingsgebied en ook collaboratieve platforms, zoals platforms voor het ontwikkelen en delen van opensourcesoftware, worden uitdrukkelijk uitgesloten (art. 2 lid 6 DSMR).

15. Platform en gebruiker spelen el **rol**: de gebruikers uploaden beschermde werken, de OCSSP slaat deze op, ordent en promoot ze en maakt ze toegankelijk voor het publiek. De gebruiker maakt de selectie van de toegankelijke werken, terwijl de OCSSP voor de opslag, ordening, zoek- en vindbaarheid en toegankelijkheid voor het publiek zorgt. Dit aspect van opslag, het optimaliseren van de manier waarop de content wordt getoond of waarop deze bevorderd wordt, kan ook teruggevonden worden in het arrest *eBay*,³² net als in het arrest *The Pirate Bay*.³³

Het is duidelijk dat OCSSP's het verschil kunnen maken wanneer zij performante algoritmes hebben die de interesses van hun gebruikers goed begrijpen en dus relevante content kunnen voorstellen, waardoor zij een groter publiek kunnen aantrekken en dus meer winst kunnen halen, veelal uit advertenties (r.o. 62 DSMR).

Cyberlockers of andere clouddiensten die **principe** gebruikt worden om materiaal voor eigen (persoonlijk of professioneel) gebruik toegankelijk te maken, vallen in principe dus niet onder deze definitie (art. 2 lid 6 DSMR).

16. Verder moet de aanbieder van de onlinecontentdienst een **winstoogmerk** hebben. Online-encyclopedieën, onderwijs- of wetenschappelijke databanken zonder winstoogmerk vallen dus niet onder het bijzondere regime. Het begrip "winstoogmerk" wordt niet nader omschreven, nochtans een notoir complex begrip in het auteursrecht. Waar het Hof van Justitie in zijn vaste rechtspraak herhaaldelijk heeft gesteld dat het winstoogmerk "niet zonder relevantie" is, heeft de Europese wetgever hier duidelijk stelling ingenomen: alleen de dienstenaanbieders met een winstoogmerk vallen onder het toepassingsgebied van de richtlijn.

Het winstoogmerk van de OCSSP is relevant, maar ook het winstoogmerk van de gebruiker is pertinent om de strek-

³¹ Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij, *PbEU* L 241 van 17 september 2015, (1-15) (hierna "Richtlijn informatiemaatschappij").

³² HvJ EU 12 juli 2011, *L'Oréal SA e.a./eBay International AG e.a.*, C-324/09, ECLI:EU:C:2011:474, punt 116. Het Hof oordeelde in deze merkenzaak dat eBay, als platform, geen louter neutrale rol had maar een actieve rol speelde waardoor hij kennis had van de gegevens betreffende de aanbiedingen en hierover ook controle had, waardoor hij de beperking van aansprakelijkheid voor hosting providers verloor.

³³ HvJ EU, *Stichting Brein (Pirate Bay)*, punt 38.

king van de toestemming aan het platform te bepalen (art. 17 lid 2 DSMR).

17. **uitsluiting**

Tot slot wordt in de overwegingen opgemerkt dat dienstverleners die “hoofdzakelijk tot doel hebben schendingen van het auteursrecht te plegen of te bevorderen” niet onder de mechanismes van aansprakelijkheidsbeperking vallen (r.o. 62 DSMR).

Of een dienst al dan niet als een OCSSP gezien kan worden, moet geval per geval beoordeeld worden, rekening houdend met een “combinatie van factoren, zoals het publiek van de dienst en het aantal door de gebruikers van de dienst geüploade bestanden met auteursrechtelijk beschermd content” (r.o. 63 DSMR).

Belangrijk is dat de definitie van de “aanbieder van een onlinedienst voor het delen van content” het toepassingsgebied van dit bijzondere regime bepaalt. Dienstverleners die niet onder deze definitie vallen (dus ook de repositories voor wetenschappelijke artikelen of de niet-commerciële online encyclopedieën), zullen onder het algemene auteursrecht (inbegrepen de generieke definitie van het mededelingsrecht) vallen zonder dat zij van de bijzondere aansprakelijkheidsbeperking kunnen genieten.

B. **Principe: mededeling aan het publiek**

18. **principe**

Het principe wordt duidelijk gesteld in art. 17 DSMR: de OCSSP verricht een handeling van mededeling aan het publiek of een handeling van beschikbaarstelling voor het publiek, wanneer hij het publiek toegang verleent tot auteursrechtelijk beschermd werken die door de gebruikers ervan zijn geüpload.

Het gaat dus om een directe aansprakelijkheid van het platform voor deze nieuwe mededelingshandeling, niet om een indirecte aansprakelijkheid voor de inbreuk makende handelingen van de gebruiker.³⁴ Het platform moet bijgevolg de toestemming verkrijgen van de auteur en houders van naburige rechten om het beschermd materiaal aan het publiek mee te delen.

Om een mededelingshandeling te stellen, volstaat het dus dat de OCSSP aan het publiek toegang verleent tot beschermd materiaal, dat de gebruiker van de OCSSP geselecteerd en geüpload heeft. Het “toegang geven” aan het publiek wordt niet gedefinieerd in de richtlijn, maar kan

gelezen worden in het verlengde van de rechtspraak van het Hof van Justitie over het mededelingsrecht (supra sub n). Het zo wordt het “publiek” niet gedefinieerd, maar kan in de zin van de vaste rechtspraak van het Hof van Justitie begrepen worden.

Anders dan in de vaste rechtspraak van het HvJ EU is het element van “volle kennis” die de gebruiker heeft van de gevolgen van zijn handelswijze, geen voorwaarde in art. 17 DSMR. Het volstaat dus dat het platform de facto gebruikt wordt om het publiek toegang te geven tot beschermd materiaal, zonder dat in concreto aangetoond moet worden dat de OCSSP weet dat het platform hiervoor gebruikt kan worden of, voor specifieke werken, gebruikt wordt.

Kennis is dus niet uitdrukkelijk opgenomen als constitutieve voorwaarde van deze mededelingshandeling. Deze kennis is wellicht wel impliciet verondersteld in de definitie van de “aanbieder van een onlinedienst voor het delen van content”, die de werken “ordent en promoot”.³⁵ De nieuwe richtlijn lijkt dus een regime van objectieve aansprakelijkheid voor te schrijven, zonder dat een fout aangetoond moet worden.

19. De *aansprakelijkheid* van de OCSSP is dus altijd in de kiem aanwezig en kan getriggerd worden door de upload van beschermd werken door de gebruiker. Het bestaan van een mededelingshandeling hangt dus samen met de handelingen van de gebruikers, die al dan niet beschermd content kunnen opladen, al dan niet met de toestemming van de rechthebbenden, al dan niet gedekt door een uitzondering.

Opmerkelijk is dat de wetgever de verhouding tussen de verantwoordelijkheid van de OCSSP en die van de gebruiker niet verder geduid heeft. Het lijkt erop dat de platformbeheerder en de gebruiker elk een eigen mededelingshandeling stellen, eerder dan een hoofdelijke verantwoordelijkheid voor één mededelingshandeling te delen.³⁶

De beperking van aansprakelijkheid voor hosting providers in art. 14 E-commercerichtlijn is niet toepasselijk op deze mededelingshandelingen (art. 17 lid 3 DSMR) – al kan deze “safe harbour” wel toepasselijk zijn op andere handelingen van de platformaanbieder. Dit is een logisch gevolg van het principe van de primaire, objectieve aansprakelijkheid van de OCSSP voor zijn eigen mededelingshandeling.

³⁴ M. Senftleben, *Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market* (4 april 2019), SSRN, 2019, 1-18, <https://ssrn.com/abstract=3367219> or <http://dx.doi.org/10.2139/ssrn.3367219>;

C. Angelopoulos & J.P. Quintais, ‘Fixing Copyright Reform’, 148. Deze laatste pleiten voor de uitwerking van een geharmoniseerd systeem van indirecte aansprakelijkheid van het platform voor de inbreuken door de gebruiker.

³⁵ Dit element maakte dat het Hof in *eBay* oordeelde dat eBay een actieve rol speelde: HvJ EU 12 juli 2011, *L’Oréal SA e.a./eBay International AG e.a.*, C-324/09, ECLI:EU:C:2011:474, punt 116.

³⁶ Dit kan o.a. blijken uit het feit dat voor beide handelingen de toestemming van de rechthebbende nodig is – ook al bepaalt de richtlijn in art. 17 lid 2 dat de toestemming aan de OCSSP de toestemming voor de niet-commerciële gebruiker inhoudt.

20. Toestemming

De OCSSP stelt een handeling van mededeling of van beschikbaarstelling aan het publiek en moet bijgevolg de toestemming van auteurs en houders van naburige rechten krijgen (art. 17 lid 1, tweede alinea DSMR).³⁷

Deze toestemming kan verkregen worden door middel van een individueel onderhandelde licentie (zoals gesteld in art. 17 lid 1 onder 2 DSMR), maar dit is slechts een van de mogelijkheden zodat ook collectieve licenties (op basis van vrijwillig, uitgebreid of verplicht collectief beheer) of, volgens sommige auteurs, zelfs wettelijke licenties tot de mogelijkheden behoren.³⁸

Deze verplichting stelt de OCSSP voor een logisch probleem: het is niet hij die bepaalt welke content via het platform gedeeld wordt, maar de gebruiker die de content uploadt.³⁹ Het is voor de OCSSP dus moeilijk of zelfs onmogelijk om de toestemming te verkrijgen vooraleer de mededeling plaatsvindt.⁴⁰ Vrijwillige collectieve licenties kunnen een oplossing zijn,⁴¹ maar het zal onmogelijk zijn om voor alle mogelijke werken en naburige prestaties voor de relevante territoria op voorhand de rechten te verwerven. Uiteindelijk behoudt de rechthebbende de mogelijkheid om de licentie niet te geven (bijvoorbeeld in het kader van een exclusieve distributieovereenkomst, om een bepaalde reputatie te bewaren of om hogere vergoedingen te onderhandelen).

De toestemming die de rechthebbenden aan de beheerder van de OCSSP geven, dekt ook de mededelingshandelingen van de gebruikers, voor zover deze gebruikers niet op commerciële basis handelen of indien hun activiteiten geen significante inkomsten genereren (art. 17 lid 3 DSMR). Heeft de gebruiker daarentegen een “commercieel” oogmerk (een notoir vaag begrip) of haalt hij “significante inkomsten” uit zijn online activiteit, dan zal hij een eigen licentie moeten aanschaffen. De richtlijn geeft geen verdere indicaties om deze noties nader te bepalen.

Omgekeerd, wanneer de gebruiker toestemming gekregen heeft om het werk te uploaden via een platform, wordt de mededeling aan het publiek door de OCSSP toegestaan “binnen de werkingssfeer van de door de rechthebbende verleende toestemming”. De OCSSP mag er evenwel niet zomaar van uitgaan dat de gebruiker alle rechten verkrijgt (ov. 69 DSMR).

C. Beperking van aansprakelijkheid

21. Het feit dat het platform geen toestemming bekomen heeft voor de eigen mededelingshandelingen betekent echter niet noodzakelijk dat het aansprakelijk is voor inbreuken op het auteursrecht.

De nieuwheid van art. 17 DSMR bestaat inderdaad in de beperking van de aansprakelijkheid van de OCSSP's: zij zijn aansprakelijk voor de niet-toegestane mededeling *tenzij* aan een aantal voorwaarden voldaan is, namelijk zij hebben (i) “alles in het werk gesteld” om toestemming te krijgen, (ii) “alles in het werk gesteld” om ervoor te zorgen dat bepaalde content niet beschikbaar is via het platform, dit op basis van informatie die door de rechthebbenden verstrekt wordt, en (iii) prompt opgetreden om de toegang tot beschermde content te deactiveren of deze “van hun websites” te verwijderen en *hebben* “alles in het werk gesteld” om de toekomstige uploads ervan te voorkomen. Voor startups zijn deze voorwaarden bovendien verzacht (art. 17 lid 6 DSMR).

De DSM-richtlijn legt zo twee *inspanningsverplichtingen* (“best effort”, “meilleurs efforts”) op aan de OCSSP, die *haar* best moet doen om de nodige toestemmingen te krijgen en om te voorkomen dat de door de rechthebbende te identificeren content beschikbaar wordt. Daarnaast heeft hij de verplichting om “prompt op te treden” om niet-toegelaten content te verwijderen, maar ook dat leidt niet tot een resultaatsverbintenis dat de content definitief verwijderd is of in de toekomst niet meer opgeladen zal worden.

22. De articulatie van deze verbintenissen in de pre- en post-uploadfasen is bijzonder. Pre-upload heeft de OCSSP de verplichting om de beste inspanningen te leveren om te voorkomen dat het geïdentificeerd beschermd, niet-toegestaan materiaal via het platform beschikbaar wordt. Lukt dit niet, is hij aansprakelijk voor het specifieke materiaal dat toch via het platform toegankelijk is *tenzij*

37 Deze verwijzing naar de InfoSoc-richtlijn en de Verhuurrichtlijn geeft aan dat de wetgever dit nieuwe recht ziet als een species van het generieke mededelingsrecht dat bij de Richtlijn informatiemaatschappij geharmoniseerd werd.

38 In die zin M. Husovec & J.P. Quintais, *How to license Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms*, 2019, 27, <https://ssrn.com/abstract=3463011> or <http://dx.doi.org/10.2139/ssrn.3463011>. Zie ook M. Senftleben, *Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market*, (4 april 2019), 3-4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3367219.

39 Een parallel kan hier gemaakt worden met de situatie van de kabeloperatoren die zowel in geval van kabeldoorgifte als van directe injectie, een essentiële rol spelen bij de verdeling van televisieprogramma's. In het geval van de kabeldoorgifte voltrekken zij een autonome mededelingshandeling. In het geval van de directe injectie bestaat een wederzijdse afhankelijkheid tussen de “omroep” en de kabeloperator, voor een unieke mededeling aan het publiek per directe injectie. In beide gevallen bepaalt de omroep welke programma's volgens een bepaald schema meegedeeld worden, maar heeft de kabeloperator zijn eigen verantwoordelijkheid in de mededeling. Zowel in het geval van de kabeldoorgifte als voor de directe injectie, is er verplicht collectief beheer en moet de kabeloperator de licentie via de collectieve beheersvennootschappen verkrijgen (art. XI.226 lid 1 en art. XI.227 WER). Dit type van regeling werd niet opgelegd in de DSM-richtlijn.

40 Het mededelingsrecht is een verbodsrecht, waarvoor dus toestemming verkregen moet worden vooraleer de mededeling uitgevoerd wordt. Zie HvJ EU, *Filmstrijder*, punt 25; HvJ EU, *Stichting Brein (Pirate Bay)*, punt 20.

41 De bereidheid om per collectieve licentie te werken hangt ook af van de sector en de gangbare businessmodellen. In de muzieksector bestaat een uitgebreid systeem van collectieve licenties, terwijl de exploitatie van audiovisuele inhoud eerder gebaseerd is op exclusieve distributie. Dit blijkt ook uit de stakeholderdialogen die de Commissie organiseert: zie hierover ook P. Keller, *Article 17 stakeholder dialogue: What we have learned so far – Part 1*, Kluwer Copyright Blog, 13 januari 2020, <http://copyrightblog.kluweriplaw.com/2020/01/13/article-17-stakeholder-dialogue-what-we-have-learned-so-far-part-1/>.

hij kan aantonen dat hij “alles in het werk [heeft] gesteld overeenkomstig de strenge sectorale normen op het gebied van professionele toewijding” om de upload te voorkomen (ov. 66 DSMR).

Post-upload is hij aansprakelijk voor de mededelingshandeling indien hij niet “prompt” handelt om de werken onbeschikbaar te maken en indien hij niet alles in het werk heeft gesteld om nieuwe uploads te voorkomen. Deze verplichting van de OCSSP komt overeen met de verplichting van de hosting provider om prompt te handelen om informatie te verwijderen of de toegang daartoe onmogelijk te maken (art. 14 lid 1 onder (b) E-commercerichtlijn) en met de verplichting om toekomstige inbreuken te vermijden die het Hof van Justitie op basis van art. 11 van de Handhavingsrichtlijn heeft ontwaard.⁴²

Deze derde verplichting van take-down en keep-down geldt, ongeacht of de OCSSP aan de pre-upload inspanningsverplichting voldaan heeft en ongeacht of de rechthebbende in de pre-uploadfase de nodige identificatie-informatie heeft bezorgd (ov. 66 DSMR). De rechthebbende die in de pre-uploadfase onvoldoende of geen informatie heeft bezorgd om de upload te voorkomen, kan post-upload dus nog informatie bezorgen om de werken te laten weghalen of om toekomstige heruploads te voorkomen. De OCSSP loopt zo het risico om voor een inbreuk op het publiek mededelingsrecht aansprakelijk gehouden te worden wanneer hij zich onvoldoende inspent om de upload van niet-toegestane werken te voorkomen, reeds geuploade werken te verwijderen en om de herupload van niet-toegestane werken te vermijden.

De verplichtingen die op de OCSSP rusten zijn **aanvaard**, reden waarom een soepeler regime werd voorzien voor startups of jonge onderneming (art. 17 lid 6 DSMR).

23. Rond de maatregelen die de contentdeeldienst moet nemen om aan zijn aansprakelijkheid te ontsnappen bestaat nog heel wat onzekerheid, die mettertijd uitgeklaard zal moeten worden. De richtlijn legt als dusdanig geen automatische filterverplichting op maar de facto zal de OCSSP dergelijke systemen installeren, gelet op de enorme hoeveelheid materiaal die minuut per minuut geupload wordt. Om te bepalen welke maatregelen verwacht kunnen worden, kan wel gekeken worden naar de rechtspraak van het Hof van Justitie over filtermaatre-

gelen (in het kader van art. 14 E-commercerichtlijn, art. 8 lid 3 InfoSoc-richtlijn of art. 11 Handhavingsrichtlijn).⁴³

Terwijl ook de DSM-richtlijn geen algemene toezichtsverplichting oplegt (art. 17 lid 8 DSMR),⁴⁴ zal de OCSSP toch inspanningen moeten doen om de verspreiding van beschermd materiaal te voorkomen of te beëindigen en zal hij hierop beoordeeld worden in functie van verschillende factoren, in de eerste plaats het evenredigheidsbeginsel (art. 17 lid 5 DSMR).

De maatregelen moeten doeltreffend zijn “met het oog op de nagestreefde doelstellingen” (i.e. de handhaving van het auteursrecht), maar mogen niet verder gaan dan wat “nodig” is om ervoor te zorgen dat niet-toegestane werken niet of niet langer beschikbaar zijn (ov. 66 DSMR). Volgens het Hof van Justitie wordt verwacht dat filtermaatregelen op basis van art. 3 van de Handhavingsrichtlijn “billijk en evenredig moeten zijn en niet overdreven kostbaar”⁴⁵ en moet een afweging gemaakt worden tussen de bescherming van de verschillende grondrechten, zoals de bescherming van de intellectuele rechten (inbegrepen het auteursrecht), de vrijheid van ondernemerschap, de vrijheid van meningsuiting en de bescherming van de persoonsgegevens.⁴⁶ Het loutere feit dat beschermde inhoud, ondanks een stakingsbevel, nog steeds aange troffen kan worden op een platform, leidt dus niet automatisch tot aansprakelijkheid van het platform.⁴⁷

Verder kan ook gekeken worden naar het type, het publiek en de omvang van de diensten en het soort content dat door de gebruikers van de dienst is geupload en de beschikbaarheid van passende en doeltreffende middelen en de kosten daarvan voor dienstverleners. Hiermee schijnt de wetgever de kosten voor de beschermingsmaatregelen bij de platformuitbater te leggen.⁴⁸ De platformuitbater moet de ontwikkelingen van de stand van de techniek volgen en zo de bestaande middelen en mogelijke toekomstige ontwikkelingen onderzoeken. Welke middelen “pas-

42 HvJ EU, *L'Oréal e.a.*, punten 131 en 141; HvJ EU 24 november 2011, *Scarlet Extended SA/Société Belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771, punt 31; HvJ EU 27 maart 2014, *UPC Telekabel Wien GmbH/Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, ECLI:EU:C:2014:192, punt 37.

43 Voor een uitgebreider overzicht: P. Campolini, S. Hermoye & F. Lejeune, ‘Droit d’auteur et contrefaçon dans l’environnement internet: les injonctions contre les intermédiaires’, *A&M* 2017, 3 (238) 246 e.v.; C. de Callatay & S. Depreeuw, ‘La responsabilité des intermédiaires à la lumière de la nouvelle Directive “Digital Single Market”’ in: J. Cabay & A. Strowel (ed.), *Les droits intellectuels, entre autres droits. Intersections, interactions et interrogations*, Larcier, 2019, 150 e.v.

44 Zie hierover HvJ EU, *L'Oréal e.a.*, punt 139; HvJ EU, *Scarlet Extended*, punt 36 e.v.: een tussenpersoon (een platform of een internetprovider) kan niet verplicht worden actief toezicht te houden op alle gegevens van ieder van zijn klanten om elke toekomstige inbreuk op intellectuele rechten te voorkomen.

45 HvJ EU, *L'Oréal e.a.*, punt 139; HvJ EU, *Scarlet Extended*, punt 36.

46 HvJ EU, *Scarlet Extended*, punten 41-53. Zie hierover de bijdrage van E. Ellyne, *Computerrecht* 2020/82.

47 HvJ EU, *UPC Telekabel Wien*, punt 58. Voor de OCSSP zou dit betekenen dat hij niet automatisch het voordeel van de beperking van de aansprakelijkheid van art. 17 lid 4 DSMR verliest.

48 Dit was niet noodzakelijk het geval voor de filtermaatregelen die als stakingsmaatregel opgelegd werden in toepassing van art. 8 lid 3 Richtlijn informatiemaatschappij of art. 11 van de Handhavingsrichtlijn, waarvoor de aansprakelijkheid van de tussenpersoon niet noodzakelijk is.

send en evenredig” zijn kan afhangen van het type materiaal, waardoor het “niet [kan] worden uitgesloten dat niet-toegestane content in sommige gevallen pas na kennisgeving door de rechthebbenden kan worden vermeden” (ov. 66 DSMR).⁴⁹

De inspanningen van het platform zullen worden beoordeeld naar “strenge sectorale normen op het gebied van professionele toewijding”, met referentie aan de “zorgvuldige exploitant” en de maatregelen die deze genomen zou hebben om te voorkomen dat niet-toegestane werken op zijn website (sic) beschikbaar zijn, rekening houdend met de “beste sectorale praktijken en de doeltreffendheid van de genomen maatregelen in het licht van alle relevante factoren en ontwikkelingen, alsook met het evenredigheidsbeginsel” (ov. 66 DSMR).

24. De verplichtingen van de OCSSP om de content onbeschikbaar te maken of te verwijderen zijn afhankelijk van de informatie die hij van de rechthebbende ontvangt. Dit leidt tot de vreemde situatie dat de onlinecontentdeeldienst dus de verplichting heeft de toestemming te bekomen voor de mededeling die hij zelf stelt (art. 17 lid 1, tweede alinea DSMR), terwijl het beschermd materiaal pas geïdentificeerd wordt om de upload te voorkomen.

De rechthebbenden moeten de beschermde inhoud identificeren en de “nodige toepasselijke informatie” verstrekken vooraleer de OCSSP de upload kan verhinderen (art. 17 lid 4 onder (b) DSMR). Om content te laten deactiveren, verwijderen of de herupload te verhinderen moeten de rechthebbenden een “voldoende onderbouwde melding” doen (art. 17 lid 4 onder (c) DSMR).

De rechthebbende wordt dus geacht “relevante en noodzakelijke informatie [te] verstrekken, waarbij onder meer rekening wordt gehouden met de omvang van de rechthebbenden en de aard van hun werken en andere materialen” (ov. 66 DSMR). Toch lijkt deze beperking niet zo ver te gaan dat de OCSSP een filterverplichting zou hebben, ondanks het feit dat de rechthebbende (gelet op haar beperkte middelen) onvolledige informatie zou hebben bezorgd.

Krijgt de OCSSP niet de nodige informatie, dan kan hij niet aan zijn verplichtingen tegemoetkomen en kan hij niet aansprakelijk gesteld worden voor een inbreuk op het mededelingsrecht betreffende “dergelijke niet-geïdentificeerde werken” (ov. 66 DSMR).

Dit schijnt niet zozeer een probleem te zijn om de beschermde inhoud (werken, prestaties en opnames) te iden-

tificeren, maar wel om betrouwbare informatie te bezorgen of auteursrecht op. De auteursrechtelijke vermogensrechten kunnen zonder formaliteiten en zonder registratie vervreemd of in (exclusieve of niet-exclusieve) licentie gegeven worden en nog eens opgesplitst worden per territorium of per exploitatiewijze. Het is voor de OCSSP dus moeilijk om de informatie over het houderschap te verifiëren.

Op basis van de beschikbare technologieën is het “matchen” van geüploade content en content die de rechthebbenden identificeren geen onoverkomelijk probleem. Verschillende platformen (zoals Facebook en YouTube) hebben hun eigen technologie, naast de technologie van derden.⁵⁰ Daarentegen is de beoordeling of een upload een inbreuk uitmaakt op de exclusieve auteursrechten een niet-opgelost probleem.

25. Grondrechten van gebruikers

Een risico dat platformen, gebruikers en consumentenverenigingen met veel verve hebben benadrukt is dat de OCSSP's al de inhoud op hun platformen zouden filteren en zo de vrijheid van meningsuiting van de gebruikers in gevaar zouden brengen.⁵¹

OCSSP's hebben technologie voorhanden om beschermd materiaal (meer bepaald opnames) te identificeren op basis van de informatie die de rechthebbenden hen bezorgen. Daarentegen is het moeilijk om te beoordelen of de mededeling van het materiaal al dan niet rechtmatig is, bijvoorbeeld omdat een uitzondering van toepassing is. Mensen hebben hiermee al moeite, automatische systemen die voorlopig blind zijn voor context zijn hier helemaal niet toe in staat.

Gelet op het risico dat de DSM-richtlijn met art. 17 lid 1 nu uitdrukkelijk aansprakelijkheid bij de OCSSP legt, zou de OCSSP geneigd zijn om het geüploade materiaal te verwijderen en te blokkeren, eerder dan de gebruiker het voordeel van de twijfel te geven.

De DSM-richtlijn voorziet in dat verband dat de “samenwerking” tussen de OCSSP en de rechthebbenden niet leidt tot “het voorkomen van de beschikbaarheid” van door gebruikers geüploade werken die “geen inbreuk maken” op het auteursrecht of wanneer deze werken vallen onder een uitzondering of beperking. Meer bepaald moeten de uitzonderingen van citaat, kritiek, recensie en van karikatuur, parodie of pastiche (geharmoniseerd in de InfoSoc-richtlijn) gelden.

49 Deze formulering lijkt te suggereren dat het platform toch auteursrechtelijke inbreuken moet opsporen, los van de aangifte van de rechthebbende en dus strijdig met het principe dat de OCSSP geen algemene toezichtsverplichting heeft (art. 17 lid 8 DSMR).

50 Dit bleek ook uit de stakeholderdialogen: P. Keller, *Article 17 stakeholder dialogue (Part 1)*, Kluwer Copyright Blog.

51 Zie ook M. Senftleben, *Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market* (4 april 2019), 5 e.v., <https://ssrn.com/abstract=3367219>.

De richtlijn stelt niet uitdrukkelijk dat de mededelingshandeling van de OCSSP (onderscheiden van de mededelingshandeling van de gebruiker) ook onder deze uitzonderingen valt. Deze uitzonderingen worden gemotiveerd door de vrijheid van meningsuiting van de eindgebruiker: deze vrijheid zou echter bedreigd worden indien de uitzondering slechts toegepast kon worden als de OCSSP ook binnen de voorwaarden van dezelfde uitzondering zou vallen (hij uit immers geen mening) of indien hij de toestemming zou moeten bekomen. Logischerwijze zou dus moeten volstaan dat de platformgebruiker binnen een uitzondering valt. Overigens wordt bevestigd dat de DSM-richtlijn geen gevolgen mag hebben voor het rechtmatig gebruik, inbegrepen op basis van uitzonderingen of beperkingen, een principe dat de OCSSP's in hun contractuele voorwaarden moeten herhalen (art. 17 lid 9, derde en vierde alinea DSMR). Jammer genoeg laat de tekst ruimte voor interpretatie,⁵² gelet op het feit dat de OCSSP een eigen mededelingshandeling stelt, onafhankelijk van de gebruiker.

26. De OCSSP heeft een *informatieverplichting* ten aanzien van de rechthebbenden en moet "passende informatie" verstrekken over de werking van de verschillende maatregelen die de OCSSP treft om de inbreuk makende content te verwijderen, ontoegankelijk te maken en te houden en over het gebruik van content die onder eventueel afgesloten licenties valt (art. 17 lid 8, tweede alinea DSMR).

Opmerkelijk is dat de gebruikers (of representatieve organisaties) geen equivalent recht hebben om zicht te krijgen op eventuele filterpolitiek.⁵³

Wel zouden zij toegang moeten hebben tot een klachten- en beroepsmechanisme, ingericht door de OCSSP (art. 17 lid 9 DSMR). Wanneer een OCSSP op verzoek van een rechthebbende bepaalde content ontoegankelijk maakt, kan de uploader zich hiertegen verzetten, bijvoorbeeld omdat hij ervan uitgaat dat het gebruik wel onder een uitzondering voor parodie valt en dus ten onrechte geblokkeerd werd. De rechthebbenden moeten motiveren waarom zij verzoeken om toegang tot hun specifieke werken te deactiveren of deze te verwijderen. De richtlijn voorziet

evenwel niet op welke basis de OCSSP zelf positie moet innemen (behalve dat er een snelle behandeling moet zijn en dat blokkeringsbeslissingen door een mens getoetst moeten worden), noch wordt een "by default" positie bepaald in geval de partijen niet tot een akkoord bewogen kunnen worden. Gelet op het arsenaal van sancties kan vermoed worden dat de OCSSP het risico op aansprakelijkheid voor een auteursrechtelijke inbreuk zal vermijden en eerder zal blokkeren dan in het voordeel van de gebruiker te beslissen.

Tot slot moeten de lidstaten zorgen voor buitengerechtelijke en gerechtelijke geschillenbeslechtsprocedures.

27. Sinds de DSM-richtlijn werd aangenomen heeft de Commissie al een aantal stakeholderdialogen georganiseerd, waar de betrokken belanghebbende partijen (platformen, rechthebbenden en collectieve beheersorganisaties, gebruikersorganisaties, (...)) overleggen over de praktische uitwerking van de verschillende beschermingsmechanismen. De bedoeling is om richtsnoeren uit te werken die een minimale rechtszekerheid tot stand kunnen brengen.

IV. Perspectief

28. Met de nieuwe regeling voor OCSSP's heeft de DSM-richtlijn een onuitgegeven constructie vooropgesteld voor een vastgesteld probleem van value gap. Er werd gekozen voor een duidelijk principe van primaire, objectieve aansprakelijkheid in hoofde van de OCSSP (platform stelt handeling van mededeling aan het publiek). Dit principe wordt getemperd door de beperking van de aansprakelijkheid van de OCSSP (voor **haar** eigen primaire mededelingshandeling), indien aan bepaalde voorwaarden voldaan is. Dit regime is een originele blend van elementen uit het mededelingsrecht en de uitgebreide rechtspraak van het Hof van Justitie rond het mededelingsrecht, de stakingsbevelen (inbegrepen filtermaatregelen) en de beperking van aansprakelijkheid van internettussenpersonen.

Het voluntarisme van de Europese wetgever kan bewonderd worden, al is nog maar de vraag of deze theoretisch elegante constructie ook de gewenste effecten zal hebben, namelijk de rechthebbenden een vergoeding bezorgen voor de geëxploiteerde content, of hen controle geven over de distributiekanaal en dus niet-toegestane inhoud onbeschikbaar maken en houden.

29. Met de toegenomen verantwoordelijkheid van de OCSSP volgt de wetgever een tendens die ook in andere Europese wetgeving ontwaard kan worden. Deze evolutie is niet onverwacht, gelet op het toegenomen belang van platformen en de verbluffende resultaten waartoe de datagedreven technologieën in staat zijn.

Het pad van de principiële onverantwoordelijkheid van de E-commercerichtlijn werd al sterk genuanceerd in de

52 Art. 17 lid 7 vermeldt dat de "gebruikers" in elke lidstaat gebruik moeten kunnen maken van de genoemde uitzonderingen (voor citaat, kritiek, recensie en voor karikatuur, parodie en pastiche) wanneer zij "door gebruikers van [OCSSP] gegenereerde content uploaden en beschikbaar maken". Deze paragraaf verwijst naar de "gebruiker", niet de OCSSP, waar in art. 17 lid 1 "gebruiker" doelt op de platformgebruiker; en naar de "upload" en het "beschikbaar maken", terwijl naar de bewoording van art. 17 lid 1 de platformgebruiker het werk uploadt en de OCSSP toegang tot het werk verleent. Dit slordig taalgebruik is te betreuren en kan tot onnodige discussies leiden.

53 Dit blijkt inderdaad een pijnpunt in de stakeholderdialoog: P. Keller, *Article 17 stakeholder dialogue: What we have learned so far – Part 2*, Kluwer Copyright Blog, 14 januari 2020, <https://copyrightblog.kluweriplaw.com/2020/01/14/article-17-stakeholder-dialogue-what-we-have-learned-so-far-part-2/>.

rechtspraak, recent nog met een arrest in de zaak *Glawischnig-Piesczek* waarin het Hof geoordeeld heeft dat een maatregel om lasterlijke inhoud te verwijderen betrekking kan hebben op inhoudelijk identieke informatie maar ook op informatie die “inhoudelijk overeenstemt” met de lasterlijke uiting⁵⁴ en dat de uitwerking van een eventueel rechterlijk bevel zelfs wereldwijde werking kan hebben.

Ook in nieuwe wetgeving worden aan platformen verplichtingen opgelegd die verdergaan dan de principes van de E-commercerichtlijn. Uiteraard zijn de platformen ook **boden** door de verplichtingen uit de Algemene verordening Gegevensbescherming.⁵⁵ Ook worden de verplichtingen voor “videoplatformdiensten” in de nieuwe AVMS-richtlijn aangescherpt⁵⁶ en moeten zij “passende maatregelen” nemen, o.a. ter bescherming van minderjarigen of van het algemene publiek tegen aanzet tot geweld of aanzet tot terroristische misdrijven. Ook in het Voorstel van verordening om de online verspreiding van terroristische inhoud tegen te gaan worden preciezere verplichtingen opgelegd aan de hosting serviceprovider om “terroristische inhoud” te verwijderen en in sommige gevallen de herupload te voorkomen.⁵⁷

Naast de “verticale” regulering (inzake audiovisuele content, auteursrechten en terroristische inhoud) zal de Commissie vermoedelijk een transversaal instrument voorstellen, een “Digital Service Act”, waarmee de E-commercerichtlijn hervormd wordt. Volgens een gelekte nota⁵⁸ zou het de bedoeling zijn om het uitgangspunt van een geharmoniseerde en voorwaardelijke uitsluiting van aansprakelijkheid te behouden en het toepassingsgebied aan te passen aan de nieuwe soorten van diensten die er sinds het aannemen van de E-commercerichtlijn in 2000 bij gekomen zijn. Ook het principiële verbod van een algemene toezichtsverplichting zou aangehouden worden, maar dan wel met bijzondere bepalingen voor algorit-

mes voor geautomatiseerde filtertechnologieën. De takedownregels zouden zo verder geharmoniseerd worden. Interessant is overigens dat de Commissie blijkbaar de mogelijkheid onderzoekt om een regulator op te richten, met een focus op grensoverschrijdende problemen, richtlijnen en ondersteuning (gelet ook op de technische aard van de vragen). De (gecentraliseerde of gedecentraliseerde) vorm van deze regulator en de bevoegdheden zijn nog open vragen.

30. Dit betekent dat de “platformen” in een complexer reglementair kader zullen moeten opereren. Afhankelijk van het toepassingsgebied, de definitie van het type platform waarop de regels van toepassing zijn of de functie van het platform die gereguleerd wordt, zullen de platformen verschillende “gepaste” maatregelen moeten treffen die telkens een impact kunnen hebben op hun aansprakelijkheid voor content die door hun gebruikers (actief) gedeeld of (passief) geconsumeerd wordt.

Wat betreft het auteursrecht is het nu uitkijken naar de manier waarop de lidstaten art. 17 in hun nationaal recht omzetten en in welke mate zij van hun marge gebruik zullen maken om een aantal onduidelijke punten weg te werken (zoals de inspanningsverbintenissen). De platformen en gebruikers zouden gebaat zijn met meer rechtszekerheid, maar zouden – bij divergentie – geconfronteerd kunnen worden met nieuwe fragmentering in de toepasselijke regelgeving, wat de hele DSM-richtlijn moest voorkomen.

54 HvJ EU 3 oktober 2019, *Eva Glawischnig-Piesczek/Facebook Ireland Limited*, C-18/18, ECLI:EU:C:2019:821, punt 41. De rechter moet een aantal specifieke gegevens aanduiden die in de “overeenstemmende informatie” terug te vinden zijn, zoals de naam van de belasterde persoon, de omstandigheden waarin deze inbreuk is vastgesteld en een inhoud die overeenstemt met de eerder onwettig verklaarde inhoud. Van de hosting-provider kan echter niet verwacht worden dat hij die inhoud autonoom beoordeelt: HvJ EU, *Glawischnig-Piesczek*, punt 45.

55 Zie hierover de bijdrage van E. Ellyne, *Computerrecht* 2020/82.

56 Art. 28bis-ter van Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 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 (Richtlijn audiovisuele mediadiensten) in het licht van een veranderende marktsituatie, *PbEU* L 303 van 28 november 2018, (69-92).

57 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM(2018) 640 final, 2018/0331 (COD), https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf.

58 Zie A. Fanta & T. Rudl, *Leaked document: EU Commission mulls new law to regulate online platforms*, 16 juli 2019, <https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/>.

Content Filtering Technologies under the new copyright liability regime for content Sharing service providers and Fundamental Rights: the clash with Data Protection

Computerrecht 2020/82

On the 17th of April 2019, the DSM (Digital Single Market) directive was adopted.² This directive was the subject of much attention, not to say scorn, on behalf of internet technology companies on the one hand and freedom of expression activists on the other. It has become infamous for, inter alia, a new copyright reform affecting the liability regime applicable to online content-sharing service provider (OCSSP). OCSSPs are content sharing platforms,³ such as YouTube, Facebook, Instagram, Twitter. These platforms have come to play central roles in our day-to-day lives and contribute not only to public debate but also, the evolution of art and culture.

The DSM has enacted a new copyright liability regime for OCSSPs, which has overturned the previous 'notice and take-down' approach into a 'notice and stay-down' model. This new liability regime incentivizes the use of content filtering technologies. This article analyses the use of technologies in light of personal data protection and privacy.

This article will start by briefly explaining (1) the new liability regime, (2) the legal questions raised by filtering technologies (3) the ECJ case law on balancing of fundamental rights with regard to filtering mechanisms (4) the filtering mechanism and the GDPR and, will end with some (5) general conclusions.

1. The new OCSSP liability regime

The new liability regime under article 17 DSM is set out in detail in another contribution to this journal.⁴ This is just a very brief overview of the principles that are of interest for the present contribution.

Under the new regime, OCSSPs are supposed to obtain the necessary authorizations from copyright rights-holders, this means concluding licensing agreements.⁵

In the absence of obtaining the necessary authorizations – despite the OCSSP's best efforts –, the OCSSP can avoid liability, to the extent that they can demonstrate having made, *in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the right-holders have provided the service providers with the relevant and necessary information...*⁶

In determining whether the OCSSP can benefit from this liability carve-out or and whether it has met its 'best efforts', the nature of the service and the type of uploaded content, as well as *the availability of suitable and effective means and their cost for service providers*, shall be taken into account.

How will OCSSPs be able to detect infringing content and ensure the *unavailability* of works, based on *suitable and effective means*? Automated upload and content recognition/filtering technologies are the answer.⁷ There are different varieties of such filtering technologies, overall the main premise is that they work on the basis of automated content identification, matching and

¹ Erika Eva Ellyne is ...

² DIRECTIVE (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (DSM Directive).

³ OCSSP are defined as a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes. See article 2 (6) of the DSM Directive.

⁴ S. Depreeuw, "De 'aanbieder van een onlinedienst voor het delen van content' in de Richtlijn 'Digital Single Market' Platformen, gebruikers, auteursrecht en aansprakelijkheid", (complete citation).

⁵ Provided an OCSSP obtains the necessary authorizations, this shall also cover any user's behaviour (constituting an act of communication to the public or an act of making available to the public an act of communication to the public or an act of making available to the public) so long as they are not acting on a commercial basis or where their activity does not generate significant revenues.

⁶ The law adds a third obligation for the OCSSP to remove content upon notice by the copyright holder: the OCSSP must "act expeditiously, upon receiving a sufficiently substantiated notice from the right-holders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point". Article 17.4(c) DSM Directive.

⁷ Generally speaking, authors have thought that the regime will inevitably give rise to upload and content filtering technology. C. Callatay & S. Depreeuw, op. cit., p. 153; F. Brison, S. Hermoye, M. Sahagun et D. Borgniet, op. cit.; Husvec, "The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?", Columbia Journal of Law & the Arts, 2018, 42(1), p. 53-84, p. 55, 63, p. 55, 62, and 63; Spoerri, On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market, JIPITEC, 2019; see also previous version of article 17 DSM Directive: article 13 stated "Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate." Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, COM (2016) 593 final (Sept. 14, 2016), <https://perma.cc/8KNK-WCSB>.

control mechanism.⁸ When a user uploads a piece of original content, it will be identified and generate a tag, against which all content uploaded to the platform will be checked.⁹

The regime set up by article 17 directly incentivizes the use of content recognition technologies.¹⁰ This is because, to prove that the OCSSP undertook its best efforts to ensure the unavailability of works, “*account should be taken of whether the service provider has taken all the steps that would be taken by a diligent operator to achieve the result of preventing the availability of unauthorized works [...] taking into account best industry practices and the effectiveness of the steps taken [...] as well as the principle of proportionality. For the purposes of that assessment, a number of elements should be considered, such as the size of the service, the evolving state of the art as regards existing means, including potential future developments, to avoid the availability of different types of content and the cost of such means for the services.*”¹¹ In this regard, large OCSSPs such as Facebook and YouTube already use such technologies, so the industry standard will likely be to continue the development of such technologies.¹² In essence, companies will be de facto required to use such filtering mechanisms to demonstrate their “best efforts”, remain in line with “industry standard” and compliant with the new safe harbour set up by article 17.

Despite that fact, that the DSM Directive provides that the new regime shall not lead to any identification of individual users nor to the processing of personal data, except in accordance with EU regulation,¹³ the use of content upload filtering technologies leads to a number of legal questions, in particular with regard to data protection. This is discussed next.

2. Content upload filtering technologies and data protection

Much ink has been spilt on the impact that the new safe-harbour regime will have on users’ freedom of

expression.¹⁴ Every bit as worrisome is the impact the filtering technologies will have on individuals’ personal data rights and privacy interests.

As YouTube explains itself with regard to its Content User ID and copyright matching software: “*Content ID will match a user’s reference content against every upload to YouTube*” and “*When you upload your original video to YouTube, we’ll scan all the videos that are uploaded after yours to check if any of them match.*”¹⁵

This means that all content being uploaded to the platform is being *monitored* all the time and all the users’ doing this uploading, their *personal data*, such as their IP address, is being processed for such monitoring. Monitoring of user content and indiscriminate personal data processing raises legal questions with regard to the conformity with the GDPR and the very nature of the regime as it may or may not be compliant with fundamental rights, particularly in light of the Scarlet and Netlog case-law (see section 3.3).

OCSSP can only process (use) individuals’ personal data within the boundaries of the law, in particular the EU Charter¹⁶ and GDPR.¹⁷ This means that any processing activities have to, inter alia, comply with data protection processing principles and most notably have a justifiable legal basis for processing. The legal grounds and further compatibility questions under the GDPR are discussed in more detail in the section 4.

However, more than just complying with the legal regime for processing personal data under the GDPR, the use of filtering technologies begs the question of the lawfulness of the regime as such, inasmuch as it opposes the right to personal property on the one hand and data protection

⁸ https://en.wikipedia.org/wiki/Automatic_content_recognition#Fingerprints_and_watermarking.

⁹ As YouTube describes itself for its Content ID program: *Videos uploaded to YouTube are scanned against a database of files that have been submitted to us by content owners*. More generally for copyright matching mechanisms: *When you upload your original video to YouTube, we’ll scan all the videos that are uploaded after yours to check if any of them match.* <https://support.google.com/youtube/answer/2797370?hl=en> and https://support.google.com/youtube/answer/7648743?hl=en&ref_topic=9282364.

¹⁰ T. Spoerri, op. cit.

¹¹ Recital 66 DSM directive.

¹² T. Spoerri, op. cit., n° 18; The numbers refer to the status in 2018, it can be assumed that the number has increased since then (see Paul Sawers, YouTube: We’ve invested \$100 million in Content ID and paid over \$3 billion to rightsholders (November 7, 2018), available at: <https://venturebeat.com/2018/11/07/>); Husvec, op. cit.

¹³ Directive 2002/58/EC and Regulation (EU) 2016/679.

¹⁴ It is immediately apparent how the use of filtering technologies function as a censoring mechanism to limit or curtail freedom of speech. M. Senftleben, “Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright on the Digital Single Market”, 2019, available at SSRN: <https://ssrn.com/abstract=3367219> or <http://dx.doi.org/10.2139/ssrn.3367219>.

¹⁵ See also footnote 16; “Videos uploaded to YouTube are scanned against a database of files that have been submitted to us by content owners” <https://support.google.com/youtube/answer/2797370?hl=en>, https://support.google.com/youtube/answer/7648743?hl=en&ref_topic=9282364, and https://support.google.com/youtube/answer/1311402?hl=en&ref_topic=9282364; “As explained above, content recognition technologies are today used for two purposes: to pre-emptively detect infringements by right holders (Scenarios 3, 4, 5) and by intermediaries (Scenario 6) and to automatically review the notifications received by right holders (Scenarios 2 and 4).” Husvec, op. cit., p. 74.

¹⁶ Article 8 of the EU Charter and article 7 of the ECHR on the right to a private life.

¹⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

and privacy on the other. This is examined next, through case law, in section 3.

3. Balancing of fundamental rights and content filtering mechanisms in ECJ case law

3.1 The Prohibition of Imposing a Monitoring Obligation Under the E-Commerce Directive

Under article 15.1 of the e-Commerce Directive 2000/31/EC, Member States are prohibited from imposing a general obligation on intermediaries, which would require that they monitor the information which they transmit or store, or actively seek out illegal activity.¹⁸ Such general monitoring obligations are seen as disproportionate and excessively costly for the intermediaries.¹⁹ In the *L'Oréal* case the ECJ ruled that measures applied to the intermediaries “cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider’s website. Furthermore, a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly.”²⁰

However, this has not stopped industry and commercial actors from voluntarily adopting such measures: YouTube has the most developed tool: “Content ID”, which according to some authors, effectively repeals article 15 of the e-commerce directive.²¹

Article 17.8 DSM seeks to uphold this prohibition, where it states that the application of article 17 *shall not lead to any general monitoring obligation*. However, it is difficult to conceive of how this could be avoided. As described by Bridy, the most prevalent content upload filtering technologies “work by screening every piece of user-uploaded content in real time against that universe of works. No file escapes the systems surveillance. If such functionality does not amount to general monitoring, it is hard to imagine what would.”²²

These content filtering technologies raise questions with regard to other fundamental rights, in particular freedom of expression, data protection and privacy. Any measures adopted by the OCSPPs will be subject to a proportionality assessment between protection of property on the one

hand and the respect for data protection on the other hand. This is further discussed below.

3.2 Proportionality

Member States are supposed to protect IP rights,²³ however, copyright protection should respect other fundamental rights, data protection and privacy included. The ECJ’s approach in reconciling conflicting fundamental rights is to apply a proportionality test. Numerous authors have tried to rationalize the approach.²⁴ Here is a brief recap.

The limitation must:

- i. Pursue a legitimate aim.²⁵
- ii. Be suitable: the measure is adapted to the context in order achieve the pursued aim.²⁶
- iii. Be necessary: there is no other less restrictive option available to meet the objective.
- iv. Be proportionate (*stricto sensu*): means that the infringement regarding the right in question of the measure does not outweigh the benefits, i.e. the measures does *not upset a fair balance between the conflicting rights and/or destroy the essence of the right that is restricted*.²⁷

In context of the two fundamental rights in opposition to each other, the focus of the proportionality assessment is on the last step of the test: ensuring an appropriate balance of rights and that the limitation in question does not overstep the ‘essence’ of the right being protected.²⁸

3.3 Balancing Fundamental Rights

In the *Scarlet* and *Netlog* cases, the ECJ set out the principle that the injunction measures requested by SABAM had to comply with the *requirements that stem from the protection of the applicable fundamental rights*.²⁹ The Court condemned the injunction measures in question (ordering *Scarlet* / *Netlog* to implement measures to block access to content or cease file sharing of protected

18 Article 15.1 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘e-Commerce Directive’)

19 *L’Oreal Case C-324/09*, ECLI:EU:C:2011:474 (*L’Oréal*), para 139; *Sabam v Scarlet C-70/10*, ECLI:EU:C:2011:771 (*Scarlet*), para 36.

20 *L’Oréal*, para. 139.

21 A. Bridy, “EU Copyright Reform: Grappling With the Google Effect”, *Vanderbilt Journal of Entertainment & Technology Law*, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3412249, p. 16.

22 A. Bridy, op. cit., p. 15.

23 Articles Article 8(3) of Directive 2001/29 and 1 of Directive 2004/48.

24 P. Teunissen, *The Balance Puzzle: the ECJ’s Method Of Proportionality Review for Copyright Injunctions*, *European Intellectual Property Review*, 2018, vol. 40, n° 9, available at: <https://repository.ubn.ru.nl/handle/2066/194106>; J. Cabay & M. Lambrecht, “Les droits intellectuels, entre autres droits fondamentaux: la Cour de justice à la recherche d’un «juste équilibre» en droit d’auteur”, *Les droits intellectuels, entre autres droits*, J. Cabay & A. Strowel (ed.) Bruxelles, Larcier, 2019, p. 304.

25 It meets an objective of general interest recognised by the Union or the need to protect the rights and freedoms of others Article 52.1 of the EU Charter of Fundamental Rights.

26 “The notion presumes that a measure possesses a minimum degree of effectiveness, as an ineffective measure cannot benefit the pursued aim.” Teunissen, op. cit., p. 6.

27 Teunissen, op. cit. n° 3.2; Cabay & Lambrecht, op. cit., p. 222.

28 Cabay & Lambrecht, op. cit., p. 220.

29 *Scarlet* para 41; *Sabam v Netlog*, C-360/10, ECLI:EU:C:2012:85 (*Netlog*), para 39.

content),³⁰ because the measures would require that the intermediaries actively monitor the content linked to all their users to prevent future intellectual property violations, which amounted to imposing a general monitoring obligation contrary to article 15 of the e-commerce directive.³¹

The ECJ did not stop there and went on to assess the requested measures in light of the balance to be struck with other fundamental rights. The Court found that the measures did not strike a fair balance between the competing fundamental rights,³² as the measures i) were too costly for the intermediaries and thus infringed their freedom to conduct business,³³ ii) involved the systematic analysis of information linked to the user profiles and the collection and identification of users' IP addresses, which are all types of protected personal data, and iii) they risked infringing the user's freedom of information.³⁴ In fine, the measures were not sufficiently targeted.³⁵ Moreover, in both cases, the ECJ explicitly condemns the measures as contrary to the intermediary's right to conduct its business, it does not however, explicitly state that the measures would be contrary to data protection³⁶ or the

freedom to information in and of themselves, the Court merely highlights the risks for these rights.³⁷

In the UPC Telekabel case,³⁸ an Austrian judge had ordered UPC Telekabel to forbid its customers access to a particular website at issue.³⁹ Although UPC Telekabel contested that the means were too costly, the injunction was deemed to be acceptable, seeing as it did not *infringe the very substance* of the intermediary's right to conduct its business. This is because the injunction left it up to the intermediary to decide the particular technical measures to be adopted to achieve a particular result (blocking of a website) and it allowed for it to avoid liability by proving that it had taken all reasonable measures.⁴⁰ The Court further ordered that the national judge take into account the user's freedom of information and assess that any blocking measures be *strictly targeted*, in the sense that they serve to bring an end to a third party's infringement of copyright, but without affecting the internet users' lawful access to information, *failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued*.⁴¹ Data protection was absent from the ECJ's ruling.

In 2019, the ECJ recently upheld an order enjoining Facebook⁴² to block access to and remove certain content declared illegal for reasons of defamation and reputational harm, as well as essentially similar content.⁴³ The ECJ deemed that such a measure was proportionate, seeing as the measure at hand concerned *monitoring 'in a specific case'*. This is because it concerned particular content which had been deemed illegal by a court.⁴⁴ The ECJ also held that the order should not overly burden the intermediary, particularly in regard to the order to remove information with equivalent content, the court injunction must contain the specific content and elements properly identified, such that the intermediary need not conduct its own assessment of the content. This was the case at

30 "SABAM also sought an order requiring Scarlet to bring such infringements to an end by blocking, or making it impossible for its customers to send or receive in any way, files containing a musical work using peer-to-peer software without the permission of the right-holders, on pain of a periodic penalty." Scarlet para 50; In Netlog, SABAM requested that "Netlog be ordered immediately to cease unlawfully making available musical or audio-visual works from SABAM's repertoire"... "as the granting of such an injunction could result in the imposition of an order that it introduce, for all its customers, in abstracto and as a preventative measure, at its own cost and for an unlimited period, a system for filtering most of the information which is stored on its servers in order to identify on its servers electronic files containing musical, cinematographic or audio-visual work in respect of which SABAM claims to hold rights, and subsequently that it block the exchange of such files." Netlog para 20, 24.

31 The ECJ found that the particular orders/measures requested were found to require that the intermediary: a) identify, within all of the electronic communications data of all its customers, the files relating to intellectually protected works; b) identify, which of those files are being shared unlawfully; c) prevent those files from being made available unlawful. Scarlet para 20, 38; Netlog para 21, 36.

32 In this respect, the court balanced the fundamental right to property against the intermediaries right to freedom to conduct business, as well as the customers' fundamental rights to the protection of their personal data and their freedom to receive or impart information. Scarlet para 47; Scarlet para 45-46 and 50; Netlog para 43-44 and 48; "In the present case, the injunction requiring the installation of the contested filtering system involves monitoring all the electronic communications made through the network of the ISP concerned in the interests of those right-holders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also future works that have not yet been created at the time when the system is introduced."

33 Netlog para 46; Scarlet para 48.

34 Seeing as, that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Scarlet para 51-53; Netlog para 38, 49-50.

35 P. Campolini, "Droit d'auteur et contrefaçon dans l'environnement internet: les injonctions contre les intermédiaires", *A&M* 2017, p. 238-263, p. 248.

36 The Court does not conduct any proportionality assessment.

37 Scarlet para 49-52, Netlog para 47-51.

38 C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, ECLI:EU:C:2014:192 (*UPC Telekabel*).

39 Making available illicit content.

40 UPC Telekabel para 51-54.

41 UPC Telekabel para 56; To summarize: provided that (i) they do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that they have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right. UPC Telekabel para 63.

42 C-18/18 of Eva Glawischnig-Piesczek v Facebook Ireland Limited, ECLI:EU:C:2019:821 (*Facebook*).

43 Information with equivalent meaning.

44 Recital 47 e-commerce directive; Facebook para 35; Moreover, the Court took into account the nature of social networks, including the swift flow of information and genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network. Facebook para 36.

hand, *since the (intermediary) had recourse to automated search tools and technologies.*⁴⁵

The driving force underlying a finding that an injunction (ordering content filtering) be deemed disproportionate appears to be intermediaries' freedom to conduct business and the cost that would be occasioned to them, as well as the risk to users' freedom of speech. Data protection is used as an additional element to tip the scales of an already unbalanced measure. It does not serve as a determinative factor of disproportionality and is not addressed in depth by the ECJ.

3.4 The Essence of Data Protection and Privacy

As explained in section 4.2 and as illustrated above the ECJ carries out a proportionality assessment regarding the different fundamental rights in question: balancing the rights, examining the proportionality of the measures, but also addressing the essence of the fundamental right in question.

One doctrine, in fact, distinguishes the proportionality test from the essence test. This doctrine argues that every fundamental right has a 'hard nucleus', which cannot be trespassed upon:

"a measure that compromises the essence of a fundamental right is automatically disproportionate. Nevertheless, the fact that a measure respects the essence of a fundamental right does not automatically mean that it complies with the principle of proportionality."⁴⁶

In any event, it is clear from the case law that a measure limiting a fundamental right must be proportionate and not infringe its essence. So, what is the essence of data protection and privacy?

In the Digital Rights Ireland Case on the 2006/24/EC Directive regarding the retention of electronic communications data (Data Retention Directive), the ECJ touched upon the 'essence' of data protection and privacy rights. The ECJ held that the interference with the right to privacy was 'particularly serious', but it did not as such *adversely affect the essence of those rights given that...the directive does not permit the acquisition of knowledge of the content of the electronic communications* as such."⁴⁷ Nor did the retention of data infringe on the essence of the fundamental right to the protection of personal data, seeing as the directive set out obligations with respect to the principles of data protection and data security, i.e., requiring appropriate technical and organisational

measures protecting against accidental or unlawful destruction, accidental loss or alteration of the data.⁴⁸

However, the retention regime fell short of the necessity test, as the directive did not "*lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter... In particular, the regime didn't provide for adequate safeguards in light of the data protection risk.*"⁴⁹

In the Tele 2 Watson case, again the essence of data protection was not impacted, but the proportionality/necessity of the measures fell short.⁵⁰ Another recent opinion by the Advocate General regarding the Data Retention Directive, opined similarly, that the essence of data protection and privacy were not infringed, but the 'general and indiscriminate' data retention obligations failed with regard to the proportionality test as the regime was insufficiently targeted and lacked adequate safeguards.⁵¹

In the Schrems case the Court held that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.*"⁵² When it came to addressing data protection, the Court seemed to insist more on the

⁴⁵ Facebook para 45-46.

⁴⁶ K. Lenaerts, "Limits on Limitations: The Essence of Fundamental Rights in the EU", German Law Review, 2019, p. 779-793, p. 781, 785.

⁴⁷ Digital Rights Ireland, Joined Cases 293 & 594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), para 39.

⁴⁸ Digital Rights Ireland para 40.

⁴⁹ Digital Rights Ireland para 64-69.

⁵⁰ The ECJ pursued, the "national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data must ensure...that such access does not exceed the limits of what is strictly necessary...a data retention measure must...lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data... that national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data." *Tele 2 Sverige v Watson and others*, C-203/15 et C-698/15, EU:C:2016:97 (*Tele 2 Watson*), para 109, 110, and 118.

⁵¹ Advocate General's Opinions in Joined Cases C-511/18 *La Quadrature du Net and Others*, and C-512/18 *French Data Network and Others*, ECLI:EU:C:2020:6, para 155. In the AG's opinion in *Ordre des barreaux francophones et germanophone and Others*, C-520/18, ECLI:EU:C:2020:7, the AG cites notably that regarding the authorities requests to access data, there should be, save in the case of urgency, judicial oversight, information to the data subject when suitable, and sufficient security obligations with regard to the service provider, para 60.

⁵² Case C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650 (*Schrems*), para 94.

failure of the necessity test and the lack of procedural safeguards in place.⁵³

It appears from the case law, that ECJ's essence approach to data protection calls for tailored limitations, with strict procedural guarantees and adequate safeguards. As to the essence of privacy, it is more ambiguous, though seems to revolve around a limited sphere of intimacy protected by a privacy expectation.

This is confirmed in the ECJ's opinion on the EU Canada PNR agreement:

"As regards the essence of the fundamental right to respect for private life, enshrined in Article 7 of the Charter, even if PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information is limited to certain aspects of that private life, in particular, relating to air travel between Canada and the European Union. As for the essence of the right to the protection of personal data, enshrined in Article 8 of the Charter, the envisaged agreement limits... the purposes for which PNR data may be processed and lays down... rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing."⁵⁴

This case law regarding the essence of personal data protection and privacy will be applied in the following sections 3.5 and 4.2 with respect to the content filtering technologies and data protection.

3.5 Compatibility Assessment of the Directive and Implementing Legislation with Personal Data Protection and Privacy

With regard to the question of the proportionality of article 17 itself, in light of the fundamental right of data protection, it will likely not be deemed – in and of itself – disproportionate. Despite the fact that article 17 does

implicitly incite the use of content filtering technologies,⁵⁵ which rely on the systematic processing of personal data, the DSM Directive does not prescribe explicitly any specific infringement/limitation on data protection rights.⁵⁶

Moreover, in light of the ECJ's approach with regard to the essence of privacy and data protection in relation to the data retention directive, it seems quite unlikely that article 17 be deemed to infringe the essence of privacy and data protection. As Lenaerts explains *"in order to determine whether a measure compromises the essence of a fundamental right, one must not only examine the intensity, but also the extent, of the limitation at issue. A measure that limits the exercise of certain aspects of a fundamental right, leaving others untouched, or that only applies in a specific set of circumstances regarding the individual conduct of the person concerned, is not such as to compromise the essence of that fundamental right."*⁵⁷ Looking at article 17, the infringement on privacy and data protection is not explicit but purely context dependent (i.e. best efforts in light of industry standard), any potential infringement would be limited to a particular sphere/activity, and the DSM Directive does call for a series of safeguards (i.e. dispute mechanisms and the respect for data protection regulation). Thus, a finding that article 17 be deemed contrary to personal data protection and privacy rights, is not expected.

More important, will be the Member States implementation or that of industry actors (the latter being discussed in section 5.2). Depending on the design and content of national measures, the national implementing legislation/and injunction risks failing with regard to the "necessity" test. Member States authorities (including legislators and judges) will have to pay close attention to ensuring that the measures adopted be sufficiently targeted, as well as foresee adequate safeguards in terms of personal data processing. Judicial remedies, security obligations on OCSSPs and the proper information being furnished to data subjects are particularly important in this respect.

Next we examine the application of proportionality and this balancing test in the GDPR context.

⁵³ It is settled case law that any interference with articles 7 and 8 of the Charter must "lay down clear and precise rules governing the scope and application of a measure and imposing minimum safe-guards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data." Derogations apply only insofar as necessary. "Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the Europe-an Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail." Schrems para 91-93.

⁵⁴ Opinion 1/15, ECLI:EU:C:2017:592, (EU-Canada PNR Agreement Opinion), para 150.

⁵⁵ And entail some internal contradictions with regard to not imposing a general monitoring obligation.

⁵⁶ This is also clear from the fact that the previous article 13 specifically called for content recognition technology measures. "The OCSSP is tacitly charged with ingesting or creating a reference file for any content that is the subject of a notice and then screening all subsequent uploads to prevent that content from reappearing. The 'best efforts' requirement is inarguably a de facto technical measures requirement." Birdy, op. cit., p. 23.

⁵⁷ Lenaerts, op. cit., p. 785.

4. Content filtering technologies and the GDPR

This section will address some of the main compliance questions regarding content filtering mechanisms in the context of data protection legislation, with a particular focus on proportionality and balancing. First, the technology is analysed in light of the principle of data minimisation (section 4.1). Second, the potential legal grounds applicable to data processing activities are discussed (see section 4.2). Lastly, the question of compliance with the right to not be subject to a purely automated decision is addressed (section 4.3).

4.1 Assessment of Filtering Technology and Data Minimization

When it comes to assessing the proportionality of the specific filtering mechanisms themselves, this overlaps with the general data protection principle of data minimization. Data minimization is a cross-cutting principle applicable to all data processing activities, under which: processing activities should be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*.⁵⁸ This assessment will very much depend on the nature of the technology, how it functions and how it is designed.

The filtering technologies, a priori, much like the Content ID used by YouTube, *work by monitoring all content from all users all the time*. Such means do pursue a legitimate aim⁵⁹ and are suitable,⁶⁰ meeting the conditions under the first two criteria of the proportionality test. They may, moreover, depending on the state-of-the-art, even be deemed 'necessary' to the extent no other option exists, the option of human assessment of all material posted, not being practically feasible seen the sheer volume of data and too burdensome. This does appear to have been the ECJ's approach in the Facebook 2019 case. Whereas initially under Scarlet and Netlog, filtering is seen as too costly, under Facebook, automated filtering is seen as a means of reducing the burden on the intermediary. This illustrates how the evolution of technology and the state-of-the-art impacts proportionality assessments. As content filtering technologies develop, become cheaper, or otherwise change, so too will proportionality assessments and the concept of data minimization align.

Thus, it could be argued that filtering technologies conform to the principle of data minimisation.⁶¹ In any event, these criteria have to be verified *in concreto* on the basis of how the technology functions and the state-of-the-art.

⁵⁸ Article 5.1 (c).

⁵⁹ Copyright enforcement.

⁶⁰ The means are effective.

⁶¹ Which overlaps with the first three criteria of proportionality (i-iii) (see above section 4.2).

4.2 Legal Grounds and the Balancing of Rights

- i) *Consent*. Consent means an individual's freely given, specific, informed and unambiguous indication of their agreement to processing activities, manifested by a statement or by a clear affirmative action. Users would have to face a veritable choice to either being subject to the filtering technologies or not, for the consent to be valid. This option limits the utility and effectiveness of the measure as many users may opt-out, which entails significant risk for the OCSSP in terms of liability.
- ii) *Necessity for the conclusion or performance of a contract with the user*. It is required that a contract to which the user is a party exists, which can be argued in the case at hand.⁶² Using this legal ground, will require demonstrating that filtering technologies (and the personal data processing it entails) are *objectively necessary* for the performance of the contract.⁶³ First the OCSSP's service offering will have to be analysed⁶⁴ and then, will have to be determined the extent to which no other less invasive measure exists. The outcome is uncertain and will very much depend on the service being offered, the design of the technology, and the state-of-the-art. It is unlikely that the filtering be deemed necessary to the performance of the contract to the extent that the service rendered by the OCSSP can be rendered in absence of such processing. However, this will depend on how services are defined.⁶⁵
- iii) *Legal obligation*. An OCSSP could further try to argue that the filtering technologies and personal data processing they call for are based on a legal obligation, i.e. founded on article 17 of the DSM Directive and any national implementing legislation. This seems, however, like a hard sell to the extent that the DSM Directive and most likely any national texts do not/ will neither explicitly address nor prescribe the use of content filtering technologies and the ensuing data processing. To the contrary the directive was explicitly

⁶² Without getting into too much detail on the abstract concept of a contract, it is important to remember that – at least under civil law – a contract does not require the payment of a price and can be unilateral. This is illustrated – at the European level – in the Directive on certain aspects concerning contracts for the supply of digital content and digital services, article 3.1; Under Belgian law a contract can imply one-sided obligations, Van Ommeslaghe, "Les Obligations", Bruylant, Brussels, 2013, vol. 1 tome II, p. 144; A contract is usually deemed to be concluded when the parties' consents meet. Van Ommeslaghe, op. cit., p. 133, 174, and 513.

⁶³ EDPB Guidelines 2/2019 on the processing of personal data under article 6(1)(b) GDPR in the context of the provision of online services to data subjects, (EDPB Guidelines 2/2019), p. 8.

⁶⁴ "The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. The important issue here is the nexus between the personal data and processing operations concerned, and the performance or non-performance of the service provided under the contract." EDPB Guidelines 2/2019, p. 8.

⁶⁵ One could consider including different obligations incumbent of OCSSPs to encompass content filtering, but this would impose greater contractual liability on OCSSPs, which they are probably unlikely to accept.

amended to exclude any direct mention of such technologies. In all likelihood, national measures will follow in the same vein and also avoid such references. Thus, although article 17 and other legal texts may imply or incite the use of content filtering technologies, they do not/probably will not prescribe the content filtering measures (and thus ensuing data processing) as such. The OCSSP is thus using the filtering technology, essentially, of its own prerogative to avoid copyright liability under article 17 of the DSM Directive. That being said, the OCSSPs are expected to meet 'industry standards' under said regime, which makes it difficult to ignore the reality of these content filtering mechanism and pleads for the recognition of an implicit legal authorization. However, relying on this legal basis would further raise questions with regard to the compatibility with the prohibition of imposing a generalized monitoring obligation and proportionality. From this point of view, relying on a legal obligation as processing grounds is dubious, it will depend mostly on how the national implementation measures are worded, 'the state-of-the-art' of the industry, and the extent to which the OCSSPs can argue that filtering is 'specific' rather than general (discussed next).

- iv) *Legitimate Interest*. Lastly, the OCSSPs could invoke its legitimate interest as grounds for processing personal data under the filtering technologies. However, the OCSSP's legitimate interest cannot be *overridden by the interests or fundamental rights and freedoms of the data subject* (i.e. the user). This calls for a balancing exercise of the OCSSP's interest, in this case at the OCSSP's interest to safeguard third-party's intellectual property rights and preserve its liability, in relation to those of the user, i.e. the users' rights to personal data protection, privacy and freedom of expression.⁶⁶

In this respect, the main concern regarding the use of filtering technologies is with regard to their 'indiscriminate' nature as they apply to all uploaded content, from all users alike. Under the 2019 Facebook case, the ECJ deemed that the measure was acceptable, because the monitoring was with regard to a 'specific case' that had been judged by a national authority as defamatory. The national court's assessment in this respect, is what lends 'specificity' to the measure. The legislators do appear to have wanted tailored monitoring, to the extent that article 17 (4) b⁶⁷ refers to ensuring the unavailability of "*specific works and other subject matter for which the right holders have provided the service providers with the relevant and*

necessary information." However, it is hard to see how this will play out any other way than simply rights holders providing a long list of materials to be filtered for, adding up altogether is a de facto comprehensive monitoring obligation.⁶⁸ Be that as it may, in the end, the directive does suggest, based on this wording, that the content filtering mechanism could be considered as "specific" to the extent, only those works for which the author has provided the requisite information, be covered.

The second hurdle to consider would be whether or not such a 'generalized' content filtering mechanism trespasses on what can be considered the "essence" of (a user's) data protection and privacy rights? In the case of filtering technologies, although the measures would be a type of blanket, indiscriminate 'surveillance' it would apply 'only' to users' uploaded content, which by virtue of this action the user cannot reasonably claim to have a strict, intimate privacy expectation. Moreover, the measures would be 'specific'⁶⁹ to the extent relative to the particular copyrighted works having been communicated about (see above). Indeed, the OCSSPs will have to find a means to tailor filtering as narrowly as possible. Most important is that sufficient procedural safeguards, technical and security standards, and judicial recourse be implemented.

The OCSSPs will likely profile 'at risk users' likely to 'infringe' copyrights. This could lead to user discrimination and engender serious repercussions in terms of the freedom of expression, cultural development, and the public's right to information. The OCSSPs would have to be sure to enact adequate safeguards in this respect, data deletion being one of them.⁷⁰

Any final assessment will very much depend on the factual circumstances of the case and design of the content filtering measures. Technologies that would be designed in a manner to limit the processing of personal data under certain conditions and with multiple safeguards in place (i.e. adequate information, pseudonymisation and immediate deletion) could potentially overcome the balancing tests.⁷¹

⁶⁶ This balancing test is similar to the broader balancing of interests between a copyright owner's property interest and an individual's data protection/privacy interests that the ECJ has conducted when assessing the proportionality of monitoring measures ordered by EU Member States.

⁶⁷ Setting out the new boundaries of the new safe harbour.

⁶⁸ "Adding up all 'specific works and other subject matter' included in right holder notifications, it may become apparent that article 17(4)(b) de facto culminates in a comprehensive filtering obligation that corresponds with the filtering measures which the CJEU prohibited in *Sabam/Netlog*." M. Senftleben, op. cit., p. 7.

⁶⁹ Albeit somewhat artificially.

⁷⁰ It is, again, hard to image that OCSSPs would forego such a treasure trove of data.

⁷¹ Indeed, clearly some lawyers must have found that the generalized filtering mechanisms of Content ID are justified. Though, it is hard to find the trace in the Google privacy policy.

4.3 Automated Decision-Making Under Article 22 of the GDPR

Another salient issue of GDPR compliance which is raised by the filtering technologies is that of the data subject's right under article 22 of the GDPR, *not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*. The filtering technologies are, indeed, a means of automated processing applied to a decision producing legal effects. The Facebook case law discussed above presents a number of questions, not to say, contradictions with this right. This is further explained hereunder.

4.3.1 The Prohibition

Article 22 of the GDPR, in fine, prohibits a controller from making decisions that have a legal or similarly significant effect based solely on automated processing.⁷² To fall under the prohibition, the processing in question has to meet two conditions i) be fully automated, and ii) produce legal effect or similar effect for the data subject.

Looking at the use of filtering technologies these two conditions are met. This is because i) the filtering technologies operate automatically, without human intervention, in order to ii) identify and block user content, which is a decision significant in terms of freedom of expression.⁷³

In the 2019 Facebook case, the ECJ presents the use of automated tools and technologies as a means to ensure 'proportionality'. The Court seems to consider that an injunction, requiring the individual assessment of the legality of particular content would be overly burdensome and disproportionate for an intermediary to handle. Ironically this finding is at arms with the data protection right not to be subject to automated decision making, which requires as a safeguard at least the right to obtain human intervention.⁷⁴

4.3.2 Exceptions to the Prohibition

Like with any legal rule, there are a series of exceptions to the prohibition; solely automated decision making, which implies legal effects for data subject is permitted when:

- necessary for the performance of or entering into a contract;
- authorised by Union or Member State law to which the controller is subject, and which also lays down

suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

- based on the data subject's explicit consent.

An OCSSP could try to invoke the first exception to justify its use of the filtering technologies. As discussed above, relying on this basis will depend primarily on the services being offered.⁷⁵

Regarding the second grounds, it is unlikely that Member States' legislation provides directly for the reliance on purely automated decision making with respect to the implementation of article 17 DSM. Although there are grounds to argue for an implicit or indirect authorization, especially if the content filtering mechanisms are sufficiently tailored.

Lastly, the OCSSPs could resort to explicit consent.⁷⁶ However, this entails granting users the option to not be subject to the automated decision making, and thus, a significant risk for the OCSSP in terms of liability.

As an alternative, the OCSSPs could also implement a step of meaningful human intervention and assessment.⁷⁷ As suggested by the Facebook case law, this may prove burdensome and costly for the OCSSP, but such a step may also be the easiest way to accommodate data protection concerns.

5. Conclusions

As can be seen from the above, the new liability regime under article 17 of the DSM engenders a certain number of data protection implications. In particular, article 17 indirectly prescribes the use of filtering technologies, which de facto calls for the monitoring of users' content by OCSSPs and the subsequent, processing of personal data. This raises question as to the proportionality of such

⁷² Article 29 WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, wp251 rev.01 (Automated Decision-Making Guidelines), p. 19.

⁷³ This is most obvious in the case that the user be denied the opportunity to upload content, in this case the filtering technologies clearly act as a restriction -whether justified or not- to a data subject's freedom of expression.

⁷⁴ Article 22.3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

⁷⁵ It is unlikely that the filtering be deemed necessary to the performance of the contract to the extent that the service rendered by the OCSSP can be (have been) rendered in absence of the such processing.

⁷⁶ This obligation is more accentuated than just 'consent' (described in section X) "The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future." Article 29 Working Party Guidelines on consent under Regulation 2016/679, wp259 rev.01 (Consent Guidelines), p. 18.

⁷⁷ According the article 29 working party "The controller cannot avoid the article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data." Automated Decision Making Guidelines, p. 20-21.

Artikelen

filtering measures, by virtue of the protection of property, in relation to data protection rights and privacy.

It is currently not possible to answer in detail, whether or not, the filtering mechanisms will be deemed proportionate or not, nor the exact legal grounds to be relied upon. This will depend on the national legislative implementations, as well as the concrete characteristics and design of the technology itself, not to mention the state-of-the-art. A priori, however, looking at the ECJ's approach to the essence of data protection and privacy, which is to insist upon the 'necessity' of measures and procedural safeguards on the one hand, and defend a core sphere of intimacy on the other. These aspects do not appear infringed in the content filtering context. The 'infringement' on data protection and privacy is limited to a particular activity, which by virtue of its nature and function (uploading content to such a content sharing platform), the user's privacy expectation is reduced, if not absent.

The main concern will be with regard to ensuring the proportionality of the content filtering measures. That means ensuring that such measures be sufficiently targeted, provide adequate safeguards, and limit risks to data protection, privacy and freedom of expression concerns. Taking these elements into account, the filtering technologies could meet the 'balancing test' that applies when weighing the interests of competing fundamental rights.

It is interesting and representative of the industry and data protection legislation, to see how the approach to content filtering mechanisms is and will continue to evolve. As can be seen in the difference between the Scarlet/Netlog cases and the 2019 Facebook case, the approach to content filtering technologies is vastly different depending on whether or not there is an obligation to keep particular 'infringing content' from re-appearing. When there is no such obligation, under the current notice and take down regime, then content filtering mechanisms are considered too costly. However, when there is an underlying obligation to ensure that particular content does not appear on a platform, as was the case for the 2019 Facebook case and as will be the case under article 17 DSM Directive liability regime -the notice and stay down regime-, then content filtering technologies are a cost savings means and thus, contribute to proportionality. The underlying shift in liability for OCSSPs has changed their cost and risk analysis, as they now have if not a duty, an incentive (to avoid liability) to adopt content filtering measures. In the past content filtering – in particular generalized measures – were treated (and still are considered to a large extent depending on the actor) as too costly and thus disproportionate for intermediaries, thereby infringing their freedom to conduct business. Now, as the liability of the intermediary

changes and the technology market develops, content filtering can be seen as a means of efficiency, risk avoidance, and cost reduction, hence a means of ensuring proportionality.⁷⁸

Lastly, the filtering mechanism appear to be at odds with the prohibition for data subjects not to be subject to automated decision making. It is still to be determined whether OCSSPs may be able to rely on exceptions to the prohibition. The most effective means to manage article 22 may be to foresee an option to opt-in and a step of human intervention (for those who opt-out) of using filtering automated decision making, the users of the latter may experience more delays in their content posting and thus prefer, in the end, to submit to the filtering's automated decision making.⁷⁹ The limitations imposed by data protection do not, thus, appear insurmountable, but inherent to the new world of privacy by design.

⁷⁸ This will impact the assessment of balancing of fundamental rights more broadly in particular with regard to infringing OCSSPs' freedom to conduct business, and thus, compliance under article 15 of the e-commerce directive.

⁷⁹ Although some may argue that this trade-off may undermine the 'free' nature of consent. However "(t)he GDPR does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances." Consent Guidelines p. 11.

Introducing an Ancillary Right for Press Publishers: A European Law-Making Ambition for the Press - but also on Hyperlinking

Computerrecht 2020/83

Shortly after he took office in 2014, Günther Oettinger, the German Commissioner for Digital Economy and Society (2014-2016), first floated the idea for an EU-wide licensing fee to show snippets of news, i.e. the display of short text fragments – thus targeting popular online services such as “Google News”. In its draft Directive on Copyright in the Digital Single Market published in September 2016, the European Commission proposed a new ancillary right building upon the German and Spanish legislative experiences, but also differing from them as the latter did not prove to produce the announced benefits.² The “ancillary” right for press publishers is justified, according to the Commission, by a global digital context where quality journalism is endangered and needs legislative intervention to cope with a situation where press publishers lose revenues because of the widespread reuse of their publications by online news aggregators.³ However, while acknowledging the problem encountered by news publishers to recoup their investments when their publications are widely shared and copied on the Internet, various legal solutions have been brought into the debate.

The Commission opted for a strong legislative intervention: the introduction of an “ancillary” right for the protection of press publications concerning online uses. The introduction of this new right, also known by its critics as the “link tax” or “Google tax” provision, has triggered many reactions, notably in the academic world which rapidly expressed its opposition towards such a new right (see notably the statements from the Max Planck Institute for Innovation and Competition⁴ and from the European Copyright Society).⁵

1. Scope of the Ancillary Right

According to Article 15(1) of Directive 2019/790, Member States shall provide publishers of press publications established in a Member State with the rights provided for in Article 2 – reproduction right – and Article 3(2) – right of making available – of Directive 2001/29/EC (InfoSoc Directive) for the online use of their press publications by information society service providers.

The proposals by the negotiating rapporteur in the Committee on Legal Affairs in the Parliament (also known as the JURI committee), Mr Voss, originally attempted to extend the rights conferred beyond reproduction and making available, to encompass rental, lending and other forms of distribution to the public (Articles 3 and 9 of Directive 2006/115/EEC). Such an approach, which was strongly criticised by academics,⁶ was rejected during the compromise negotiations in JURI.

¹ Anne-Catherine Lorrain is a lawyer with expertise in copyright law. She is Political Advisor (for the Greens-EFA political Group) in the Committee on Legal Affairs in the European Parliament since 2015. She is Associate Fellow of the research centre *Internet & Société* (<https://cis.cnrs.fr>).

² The *Leistungsschutzrecht* introduced in Germany in 2013 was criticised by German academics: see the statement from the Max Planck Institute for Innovation and Competition available at https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/leistungsschutzrecht_fuer_verleger_01.pdf. In Spain, following the entry into force of a law in 2014 (the so-called “Canon Aede” Act), Google closed googlenews.es immediately after the adoption of the Spanish law, in order to avoid what had been widely termed the “Google tax”. In Germany, Google received an exemption from publishers and continued showing snippets in search results. Major German news publishing houses did not join the German collecting society (VG Media) in charge of collecting the related licence fees, thus making the amounts of fees collected quite small. See Barabash, Igor, *Ancillary Copyright for Publishers: The End of Search Engines and News Aggregators in Germany?*, EIPR: European Intellectual Property Review 35.5 (2013): 245. At the end, the German law of 2013 was declared inapplicable by the Court of Justice of the European Union, in the absence of prior notification to the European Commission, in accordance with the requirements of Directive 98/34/EC (CJEU, C-299/17, *VG Media v. Google*, 12 September 2019). See also the Study commissioned by the European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs at the request of the Committee on Legal Affairs: Bently, Kretschmer et al., *Strengthening the Position of Press Publishers and Authors and Performers in the Copyright Directive*, September 2017, esp. pp. 29 (https://www.europarl.europa.eu/thinktank/de/document.html?reference=IPOL_STU%282017%29596810).

³ See Directive 2019/790, Recital 54.

⁴ Statement of the Max Planck Institute for Innovation and Competition of February 2017 https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Position_Statement_PART_E_Publishers_2017_02_21_RM_H_VM-def-1.pdf.

⁵ Statement of the European Copyright Society of April 2018: <https://europeancopyrightsocietydotorg.files.wordpress.com/2018/05/european-copyright-societyopiniononpresspublishersright.pdf>. The ECS had already communicated its criticism to the Commission before the Directive proposal was published, in answering to the Commission’s public consultation on the role of publishers in the copyright value chain (<https://europeancopyrightsocietydotorg.files.wordpress.com/2016/06/ecs-answer-to-ec-consultation-publishers-role-june16.pdf>).

Other academics have also criticised the proposal for an ancillary right, such as Rosati, Eleonora, *Neighbouring Rights for Publishers: Are National and (Possible) EU Initiatives Lawful?*, IIC: International Review of Intellectual Property and Competition Law (2016): 569–594; Ramalho, Ana, *Beyond the Cover Story – An Enquiry into the EU Competence to Introduce a Right for Publishers*, IIC 48.1 (2017): 71–91.

⁶ See the statement of the European Copyright Society (op. cit.).

1.1 *Why “Ancillary”? the new right within the copyright legal framework*

The right newly provided is qualified as “ancillary” as it builds upon the existing exclusive rights of reproduction and of making available to the public, while not being quite similar to the existing “neighbouring” rights (for audiovisual producers, phonogram producers and broadcasting organisations) which similarly aim at guaranteeing financial compensation to their holders, and while depending on certain conditions (which will be detailed below).

Before the Directive of 2019, press publishers already had significant rights in their publications, as they own enforceable rights in large parts of the published material by virtue of assigned copyright (or exclusive licences), through national rules on employer ownership or collective works, and through the EU-wide *sui generis* right on databases (a term broad enough to cover all newspapers).⁷ Therefore, the reproduction or making available of small parts of such material could already be considered as unlawful, in the same way as for any other copyright-protected material. Besides, the *sui generis* right on databases not only gives investors in collections of material the right to prevent copying, but also the right to prevent the systematic extraction of insubstantial parts.

Against this background of pre-existing copyright protection, alternative solutions to a new exclusive right were initially proposed by the original draft report from the Committee on Legal Affairs in the Parliament.

1.2 *How the “Ancillary” Right became the regulatory option favoured by the legislator*

Shortly after the Commission published its long-awaited proposal for a Directive on Copyright in the Digital Single Market in September 2016,⁸ the Parliament started to work on its own amendments to the Commission's proposal, in view of issuing a first-reading resolution before negotiating on a final agreement with the Council and with the Commission, as required by the European Ordinary Legislative Procedure.⁹

The original JURI draft report proposed substantial amendments to the Commission's proposal on the protection of press publications for online uses (provided in Article 11 of the proposal). The position of the original

rapporteur for the Parliament (Ms Comodini Cachia)¹⁰ was not to create a new right, as proposed by the Commission, but to rely on a legal presumption, provided to the publishers of press publications, of representation of authors of literary works contained in press publications, and on a legal capacity to sue in their own name when defending the rights of such authors for the digital use of their press publications.¹¹ The rapporteur justified such an amendment with the importance to enforce the rights upon which press publishers depend to protect their investment made in their publications, by providing them with a reinforced right to taking infringers of the rights held by the authors of the works contained in their press publications to court. However, this wording was rejected in committee, albeit with a very tight majority (by a single vote).¹²

1.3 *Protected subject matter: all publications except academic and scientific publications*

The scope of press publications covered by the ancillary right is particularly broad as it encompasses all kinds of publication, related to “news or other topics.” However, the exclusion of scientific and research publications was proposed by the Parliament and remained in the final trilogue agreement.

Article 2(4) § 2 provides that “*Periodicals that are published for scientific or academic purposes, such as scientific journals, are not press publications for the purposes of this Directive.*”

The ancillary right is not subject to a requirement of investment (by contrast with the existing protection or databases) or to an originality threshold (as applies to copyright). Consequently, the proposed protection would extend to virtually any use, even of the smallest part of a news item or other content, although the Directive attempts to introduce some restrictions to the ancillary right.

⁷ Cf. Statement of the European Copyright Society (Op. Cit, footnote N°6).

⁸ Proposal for a Directive on Copyright in the Digital Single Market, 2016/0280 (COD), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593>.

⁹ The Ordinary Legislative Procedure – formerly known as “Co-Decision” procedure – is enshrined in Article 294 of the Treaty on the Functioning of the European Union.

¹⁰ The original rapporteur for the Parliament, Ms Comodini Cachia (Malta), left the European Parliament in 2018 and was replaced by a Member from the same political group in the Parliament (EPP), Mr Voss (Germany).

¹¹ Original draft report from the Committee on Legal Affairs (JURI) in the Parliament, drafted by Ms Comodini Cachia and published in March 2017 (https://www.europarl.europa.eu/doceo/document/JURI-PR-601094_EN.html?redirect), Amendment N°52: “Member States shall provide publishers of press publications with a presumption of representation of authors of literary works contained in those publications and the legal capacity to sue in their own name when defending the rights of such authors for the digital use of their press publications” (amendment to the Commission's proposal highlighted).

¹² Almost one thousand amendments were tabled on the draft JURI report, with not less than fifty-four amendments on Article 11: https://www.europarl.europa.eu/doceo/document/JURI-AM-604544_EN.html?redirect. The JURI report was adopted on 26 June 2018: https://www.europarl.europa.eu/doceo/document/A-8-2018-0245_EN.html.

1.4 *Scope of beneficiaries: press publishers and news agencies*

The Directive provides that the legal protection for press publications should benefit publishers that are established in a Member State (Article 15(1)) and have their registered office, central administration or principal place of business within the Union (Recital 55). This latter clarification aims at providing a broad understanding of the establishment of publishers in the EU, which was agreed in the final trilogue meeting.

Article 2(4) of the Directive gives a particularly large definition of press publishers:

“Press publication’ means a collection composed mainly of literary works of a journalistic nature, but which can also include other works or other subject matter, and which:

- (a) constitutes an individual item within a periodical or regularly updated publication under a single title, such as a newspaper or a general or special interest magazine;
- (b) has the purpose of providing the general public with information related to news or other topics; and
- (c) is published in any media under the initiative, editorial responsibility and control of a service provider.”

In addition to this broad definition, Recital 55 § 2 provides that the concept of publisher of press publications should be understood as covering service providers, such as news publishers or news agencies, when they publish press publications within the meaning of this Directive. News agencies were added by an amendment from the Parliament’s JURI report.

The inclusion of press agencies raises questions since they do not produce press publications. As highlighted by the European Copyright Society,¹³ if the effect of the proposal is to give rights in any item included within a press publication to both press publishers and news agencies, the result will be yet another layer of licensing. For example, if a press publisher were to permit re-use of a publication, any content within the publication deriving from a news agency would need a distinct licence. In the case where a press publisher re-publishes an item from a news agency – which is a very common practice – would the publisher pay a licence fee to the agency, with the risk of imposing a double payment on the final user?

2. **Attempted Limitations**

Article 15(1) § 4 provides that the rights shall not prevent legitimate private and non-commercial use of press publications by individual users. Such indirect reference

¹³ Op. cit., footnote N° 6.

to copyright exceptions was introduced by the Parliament, which then remained in the final text of the Directive as negotiated between the three institutions.

The Directive provides that Member States shall provide for an exception to the rights provided for in Article 15 for text and data mining (Article 4), for cross-border teaching activities (Article 5), and for the preservation of cultural heritage (notably for the use of out-of-commerce works by cultural heritage institutions, as provided by Article 8 of the Directive).

However, there are no exceptions for services run by small companies or non-profit organisations. The new ancillary right is therefore not limited to search engines and news aggregators, and applies by default to all online services, commercial and non-commercial (except when run by individual users for non-commercial *and* legitimate uses, i.e. covered by copyright exceptions).

The modalities for the restriction in the application of Article 11 triggered vivid discussions inside the Parliament, to such an extent that the mandate to start the trilogue negotiations was challenged.¹⁴ The discussion focused on how to make the new right comply with the use of hyperlinks being inherent to the Internet.

2.1 *Acts of Hyperlinking*

The JURI report amended the Commission’s proposal by specifying that the rights provided in the then Article 11 shall not apply to acts of hyperlinking. The draft Directive did not include such precision within the provisions of the Article but only in one of the related recitals, providing that the protection “*does not extend to acts of hyperlinking which do not constitute communication to the public*” (then Recital 33).

Following the challenge of the decision to enter into inter-institutional negotiations, the Parliament adopted an amendment to its own report on Article 11, providing that the rights shall not extend to “*mere hyperlinks which are accompanied by individual words*.” The inter-institutional negotiations then revealed the difficulty in delineating the authorised acts of hyperlinking based on the criterion of “individual words”: would a link containing – in its title/ formulation and/or in the words next to it? – only a few words but being explicit enough to reveal the content of

¹⁴ Following the adoption of the JURI report in June 2018, the decision to enter into inter-institutional negotiations was rejected by the Parliament in July 2018, following a lack of majority on the most controversial provisions of the Directive, mainly its Article 11 (now Article 15) and Article 13 (now Article 17 on the use of protected content by online content-sharing service providers, also known as the article on “upload filters”). The mandate to enter into trilogue negotiations was then postponed to September 2018, where a few amendments were tabled at plenary level on Article 11. The Parliament’s first reading text was adopted on 12 September 2018, thus giving mandate to enter into inter-institutional negotiations with the Council.

the press publication still be covered by the new right? Such wording left an uncertain margin of interpretation for each act of hyperlinking, which brought the negotiators to abandon the wording proposed by the Parliament.

Therefore, the trilogue agreement came back to the original wording of the JURI report, merely stating that the protection granted under such a right shall not apply to acts of hyperlinking, without further qualifying such acts (Article 15(1) § 3). The qualification of the acts of hyperlinking made by the Commission in its original proposal, restricting their exclusion from the scope of the ancillary right “*when they do not constitute communication to the public*” (Recital 33), was quite rapidly abandoned during the trilogue negotiations. In its original proposal, the Commission attempted to refer to the legal discussion on the conditions under which “clickable links” can be considered as acts of communication to the public and thus fall within the scope of Article 3 of the InfoSoc Directive.¹⁵ Although being relevant, such debate makes the exclusion of hyperlinks dependent on case-by-case interpretations which cannot be addressed with full legal certainty in an ever-changing technological context. Besides, as the institutional negotiators tried to mitigate the strong critics formulated against Article 11 – by academics but also by the public who rapidly used the surname of “link tax” – a wider exclusion of hyperlinks appeared as a more reasonable political solution.

However, is such exclusion of “hyperlinks” as wide as it appears to be? Indeed, “hyperlinks” tend to be more technologically-specific rather than, e.g., the more technologically-neutral term employed by, first, the referring court and, then, the Court of Justice of the European Union in *Svensson*,¹⁶ that is “clickable link” (or “Internet link”).¹⁷ Although the *Svensson* ruling did not make any technological distinctions among the types of “Internet links”,¹⁸ it also acknowledged that the type of link at issue in the background national proceedings was “not clear from the documents before the Court.”¹⁹ If “hyperlinks” are to be interpreted in a restrictive manner, is the use of this term throughout the adoption-process of the Directive intentional from the European legislator?

One could probably extrapolate that such restrictive interpretation could be used by some relevant right holders who could argue that Article 15 only excludes hyperlinks, but that other types of links (e.g., framing, embedding) would fall within the scope of the right.

Furthermore, knowing that, according to Article 15, the ancillary right shall not prevent legitimate private and non-commercial use of press publications by individual users (see above), one incidental question is whether all clickable links, even those published by individual users but not considered to be “non-commercial” or “legitimate”, escape the rule in all circumstances and could thus be regarded *a contrario* as falling into the scope of the ancillary right.

Another open question is whether a hyperlink constitutes an act of communication to the public within the meaning of Article 3(1) of the InfoSoc Directive,²⁰ simultaneously with an act of reproduction, as the case-law can vary according to the technological context at stake.²¹

2.2 The use of (very) short extracts

A new sub-paragraph was added during the trilogue negotiations, providing that the rights shall not apply “*in respect of the use of individual words or very short extracts of a press publication*” (Article 15(1) § 4). Although not directly referring to the acts of hyperlinking as previously attempted in the Parliament’s resolution (see above), which introduced confusion, the Directive still attempts to restrict the scope of the new right. Nevertheless, it remains uncertain what “very short extracts” actually means when applied to a given press publication made accessible through a given hyperlink.

The non-application of the right to “very short extracts” means *a contrario* that what is not deemed as a “very short extract” falls within the scope of the right. Is a short – but still not very short – extract still covered by the rights? How shall this be assessed in practice?²² Although the inter-institutional negotiations showed the weakness and the blurred margin of interpretation of such criteria attempting to delineate the application of the right with respect to the length of the publication extracts, the final trilogue meeting (on 13 February 2019) retained the notion of “very short extracts”, while bringing clarification in the corresponding recital.

15 The treatment of “clickable links” under the InfoSoc Directive was first tackled by the Court of Justice of the European Union (CJEU) in a ruling of 2014 in the landmark *Svensson* case (C-466/12, ruling of the General Court dated of 13 February 2014), followed by its subsequent decisions in the *BestWater* case (C-348/13, 21 October 2014) and *GS Media* case (C-160/15, 8 September 2016).

16 See CJEU ruling in *Svensson* (above-mentioned, footnote N°16).

17 See Rosati, Eleonora, <https://ipkitten.blogspot.com/2019/06/dsm-directive-series-6-hyperlinking-in.html>.

18 See CJEU ruling in *Svensson* (above-mentioned, footnote N°16), para 30: “*That additional circumstance in no way alters the conclusion that the provision on a site of a clickable link to a protected work published and freely accessible on another site has the effect of making that work available to users of the first site and that it therefore constitutes a communication to the public.*”

19 See CJEU ruling in *Svensson* (above-mentioned, footnote N°16), para 29.

20 See CJEU, C-279/13, *C More Entertainment AB*, 26 March 2015, by which the Court clarified that communication to the public and making available are not exactly the same thing (see ruling, para 24).

21 See Rosati, op. cit.

22 On the interrogations pertaining to the concrete implementation of the “ancillary” right, see notably Ihlajarinne, Taina, and Juha Vesala, *Proposed Right of Press Publishers: A Workable Solution?*, Journal of Intellectual Property Law & Practice 13.3 (2018): 220-28; Furgal, Ula, *Ancillary Right for Press Publishers: An Alternative Answer to the Linking Conundrum?*, Journal of Intellectual Property Law & Practice 13.9 (2018): 700-10.

Indeed, Recital 58 provides that, whereas the use of parts of press publications have gained economic relevance, *“the use of individual words or very short extracts of press publications by information society service providers may not undermine the investments made by publishers of press publications in the production of content”*, which justifies an ‘exception’ to the right provided by Article 15(1) for such uses. However, the recital further provides that *“taking into account the massive aggregation and use of press publications by information society service providers, it is important that the exclusion of very short extracts be interpreted in such a way as not to affect the effectiveness of the rights provided for in this Directive.”* This final wording on the interpretation of the exclusion of very short extracts was under discussion until the very end of the last trilogue meeting: a narrow interpretation was abandoned in favour of a more neutral wording.²³

Because readers need to know what a link leads to before clicking, websites almost always include a snippet – or short extract – of the linked-to content as part of a link. Snippets are fundamental for users to find the information they are looking for: without them, users do not have any indication of what is behind a hyperlink. Hence, it is customary to use link descriptors, snippets or thumbnails to assist the user in determining whether the resource linked to is worth consulting. As a consequence, any limitation on snippets is therefore a limitation on hyperlinking.²⁴

2.3 Term of protection

The Directive provides that the ancillary right shall expire two years after the press publication is published. That term shall be calculated from 1 January of the year following the date on which that press publication is published (Article 15(4)). It shall not apply to press publications first published before 6 June 2019. The non-retroactive effect of the right was first introduced by the Parliament.

The Parliament resolution reduced the duration of protection from twenty years, as provided in the original Directive proposal, to five years. The duration was subsequently reduced to two years in the course of the trilogue negotiations.

²³ The wording proposed at the beginning of the final trilogue meeting of 13 February 2019 was the following: *“Taking into account the massive use of press publications by automated computational means (...) it is important that exclusion of very short extracts is interpreted narrowly in order not to affect the economic investments made by publishers of press publications and the effectiveness of the rights provided for in this Directive”* (Recital 34a, now Recital 58).

²⁴ Cf. Statement of the European Copyright Society (op. cit., footnote N° 6).

3. Remuneration

3.1 Remuneration of press publishers

The remuneration of press publishers is not mentioned explicitly in the text of the Directive, even though the first-reading resolution adopted by the Parliament before entering into trilogue negotiations amended the Commission’s proposal by underscoring the justification of the newly created right based on the need for press publishers to be remunerated: *“(...) so that they may obtain fair and proportionate remuneration for the digital use of their press publications by information society service providers.”* (Article 11, § 1).

Such explicit reference to the remuneration of press publishers was lost in the course of the inter-institutional negotiations, although being the main justification underpinning the introduction of the ancillary right.

The “ancillary” (almost “neighbouring”) nature of the right introduced by Article 15 of Directive 2019/790 is actually meant to guarantee financial “compensation”, rather than “remuneration”, to its beneficiaries. Indeed, as the ancillary right is meant to apply to *non-contractual* relationships, so that press publishers can exercise their rights of reproduction and of making available with respect to *all* online uses covered by Article 15, it is more accurate to talk about (general) “compensation”, rather than “remuneration” (related to specific uses). This being said, nothing prevents press publishers from concluding licensing agreements with news aggregators, but such contractual agreements would essentially amount to “blanket licences” meant to target all covered online uses. Could such ad hoc licenses be extended to all potentially concerned online services and give rise, in the future, in some Member States, to a blanket fee implemented under a so-called “mandatory licensing” scheme? How would such a fee be determined?

In addition, the question arises of whether such implicit “fair compensation” would fall under the same legal conditions as other “fair compensation” provisions, especially considering that, according to the Court of Justice of the European Union, such compensation should be justified by an “actual harm.”²⁵ What is the actual harm allegedly suffered by the publishers with respect to each very instance of online use of news snippets?

3.2 Remuneration of journalists

Considering that the press publications protected by the ancillary right contain the copyright protection attached to the content created by authors and journalists (being employed by publishers or being freelance),²⁶ ensuring a

²⁵ See CJEU, C-572/13, *Hewlett-Packard Belgium v. Reprobel*, 12 November 2015.

²⁶ As explained above under 1.1.

fair share of the remuneration granted to press publishers with journalists became a priority for the Parliament.

Although not appearing in the Commission's proposal, the Directive now stipulates that "*Member States shall provide that authors of works incorporated in a press publication receive an appropriate share of the revenues that press publishers receive for the use of their press publications by information society service providers.*" (Article 15(5)).

However, such wording aiming at guaranteeing a fair share of revenues between the press publishers and the authors of works incorporated in press publications is immediately wiped out as the Directive specifies that this "*should be without prejudice to national laws on ownership or exercise of rights in the context of employment contracts*" (Recital 59). The result is that the situation of journalists, whose remuneration will still depend on the working relationship with their employer (the publisher), will remain unchanged. The wording of Recital 59 amounts to saying that journalists who are employed by a press publisher do not receive additional revenues, because their compensation is considered to be covered by their employment contract. The ancillary right for press publishers will at the end strengthen their bargaining position with respect to authors and creators, a relationship which is hardly one of economic equivalence as it stands. This has even led the International Federation of Journalists to withdraw their support for the provision.²⁷

In the same vein, but beyond the remuneration issue, Article 15 provides that the ancillary right shall not be invoked against the authors and other right holders of the works and other subject matter incorporated in a press publication, and shall not deprive them of their right to exploit their works and other subject matter independently from the press publication in which they are incorporated. It further stipulates that when a work is incorporated in a press publication on the basis of a non-exclusive licence, the right shall not be invoked to prohibit the use by other authorised users. In addition, the ancillary right shall not be invoked to prohibit the use of works or other subject matter for which protection has expired.

4. National Implementation

The broad scope of the ancillary right, coupled with an uncertain margin of interpretation left by the Directive to Member States, risks to result in a variety of national implementing solutions, thus hampering legal certainty and the harmonisation objective.

²⁷ IFJ, *New copyright directive makes a mockery of journalists' authors' rights* (<https://www.ifj.org/media-centre/news/detail/category/authors-rights/article/new-copyright-directive-makes-a-mockery-of-journalists-authors-rights.html>).

France is the first Member State to have implemented the neighbouring right for press publishers created by the Directive into national law. The French Parliament proposed a draft law only two years after the Commission published its proposal for a Directive in 2016, which was then discussed while the inter-institutional negotiations on the Directive took place and was finalised only a few months after the Directive was adopted.²⁸

The French law remains faithful to the wording of the Directive, with only a few differences (in particular, the law does not provide for an exception for Text and Data Mining) and leaves the definition of "short extracts", and the implementation of this criterion, to a future implementation Decree.

In reaction to the introduction of the ancillary right in France, Google.fr has stopped using news snippets in order to escape the scope of the exclusive right, which prompted the outcry of press publishers, thus deprived of remuneration. Google then told publishers that they could still grant their authorisation so that news snippets could be copied by the aggregator and incite users to click towards the publishers' sites, but without financial compensation. French press publishers have since then seized the national competition authority for abuse of dominant position.²⁹

5. Conclusion

Despite the inconclusive legislative attempts in Spain and in Germany, the European legislator's ambition to actively protect press publications in the online environment has been enshrined into the European copyright law system.

The nickname of "Google tax" that is sometimes given to the ancillary right, reveals the actual target of the European legislator (Google) while denouncing the incompatibility of the ancillary right (or licensing fee) with the reality of online uses. Google and Facebook have made extensive use of press publications, thus attracting a lot of users and thereby creating a symbiotic relationship between their online services and press publishers' content. Their success, based not only on the access to online uses but also on many other uses and services, has

²⁸ Law n°2019-775 of 24 July 2019 "*tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse*", JORF n° 0172 of 26 July 2019. The law entered into force in France in October 2019.

²⁹ In its decision of 9 April 2020, the *Autorité Nationale de la Concurrence* ruled in favour of the complainants' request for interim measures against Google. The French Competition Authority found that Google's practices were likely to constitute an abuse of a dominant position, and caused serious and immediate damage to the press sector. It therefore enjoined Google, within three months, to conduct negotiations in good faith with publishers and press agencies on the remuneration for the use of their protected content (decision available at: https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2020-04/20mc01.pdf). These interim measures will apply pending a court decision on the merits of the case, to be expected in the following months.

made them so powerful that they do not need to copy press snippets to nurture their ever-growing success... whereas press publishers still need the online platforms to attract readers and make them click on their sites. One can then wonder whether the provisions of the Directive are not counterproductive for a problem that could find solutions in other fields than copyright law (such as the regulation of online advertisement or tax law),³⁰ and perhaps not through regulatory intervention. The target turns out to be stronger than the shooter, the latter depending more on the former than vice versa ...

Is such additional intellectual property right needed to support quality journalism, i.e. independent media and investigative journalism, as claimed by the Directive's explanatory statements and recitals? In spite of the good intention, focused on the need for financial compensation, doubt is allowed as the ancillary right will not change the fundamental problems that news institutions face and will undoubtedly continue to face: they will still have to compete with many other powerful actors for consumer attention, and hence revenue.³¹

Our eyes now turn to the national implementation(s) of the ancillary right by the Member States, but also to the future – and expectable – case law on this new copyright law provision, both at European and national levels.

30 Such alternative paths have been notably explored by the French organisation representing the independent press for online news (SPIIL): “*Not break what makes the strength of the Internet (...) The fight against GAFAs should get organised at other levels (...) The press should not depend on more third players and on more taxes*”, (<https://www.spiil.org/20160616/contribution-spiil-r-flexion-r-diteurs-de-presse-cha-ne-de-droit-dauteur>).

31 Cf. European Copyright Society's Statement (above-mentioned, footnote N° 6).

Nederland

Computerrecht 2020/84

Hoge Raad (Civiele kamer) 27 september 2019,
nr. 18/01667
(Mrs. M.V. Polak, C.E. du Perron, M.J. Kroeze en C.H. Sieburgh)
m.nt. mr. R.J.J. Westerdijk¹

(Art. 3:35, 6:233 en 6:234 lid 4 BW; art. 9 Richtlijn inzake elektronische handel)

RvdW 2019/982
ECLI:NL:PHR:2019:718
ECLI:NL:HR:2019:1445

Browse-wrapping: het aanvaarden van algemene voorwaarden voor gebruik van gegevens gepubliceerd op een website vindt rechte

Arrest in de zaak van:
In de zaak van
RYANAIR LIMITED,
gevestigd te Dublin, Ierland,
EISERES tot cassatie,
hierna: Ryanair,
tegen
PR AVIATION B.V.,
gevestigd te Soest,
VERWEERSTER in cassatie,
hierna: PR Aviation,

1. Procesverloop

Voor het verloop van het geding tot dusver verwijst de Hoge Raad naar:

- zijn arrest in de zaak 12/03167, ECLI:NL:HR:2016:390 van 11 maart 2016;
- het arrest in de zaak 200.189.603/01 van het gerechtshof Den Haag van 23 januari 2018.

Ryanair heeft tegen het arrest van het gerechtshof beroep in cassatie ingesteld. PR Aviation heeft een verweerschrift tot verwerping ingediend.

De zaak is voor partijen toegelicht door hun advocaten, voor PR Aviation door mr. A.P. Groen.

De conclusie van de Advocaat-Generaal G.R.B. van Peursesem strekt tot verwerping van het cassatieberoep. De advocaat van Ryanair heeft schriftelijk op die conclusie gereageerd.

2. Beoordeling van het middel

De in het middel aangevoerde klachten kunnen niet tot cassatie leiden. Dit behoeft, gezien art. 81 lid 1 RO, geen nadere motivering nu de klachten niet nopen tot beantwoording van rechtsvragen in het belang van de rechts-eenheid of de rechtsontwikkeling.

3. Beslissing

De Hoge Raad:
– verwerpt het beroep.

Noot

- De saga rond het gebruik van vluchtgegevens van de website van de Ierse luchtvaartmaatschappij Ryanair gaat door. Van 2008 tot en met 2016 was al tot de Hoge Raad (en het Hof van Justitie van de Europese Unie) geprocedeerd over de IE-aspecten.² Maar Ryanair heeft het niet daarbij gelaten, zodat de zaak in 2019 opnieuw voor de Hoge Raad kwam. Deze keer was de kernvraag of een gebruiker (PR Aviation) de gebruiksvoorwaarden van de site van Ryanair heeft aanvaard door ‘browse-wrapping’, dat wil zeggen het gebruik van de website na een mededeling dat de gebruiksvoorwaarden van toepassing zijn. Helaas doet de Hoge Raad de zaak af op basis van artikel 81 Wet op de rechterlijke organisatie (hierna: ‘RO’), maar de zaak en met name de conclusie van Advocaat-Generaal Van Peursesem³ (hierna: de ‘A-G’) bevat voldoende interessante aspecten voor een annotatie in dit tijdschrift.
- De gebruiksvoorwaarden van Ryanair bevatten in 2008 de volgende mededeling:

“1. Algemeen. De eigenaar van de website is Ryanair Limited (...). Door het gebruik van deze website stemt u ermee in wettelijk gebonden te zijn aan en te handelen in overeenstemming met deze Gebruiksvoorwaarden en alle andere toepasselijke bepalingen; u stemt er in het bijzonder mee in niet de activiteiten uit te voeren die zijn verboden volgens artikel 3 tot en met 5 hierna. Als u niet instemt met deze Gebruiksvoorwaarden en/of met enige andere toepasselijke bepaling, is het u niet toegestaan deze website te gebruiken en gaat u hiermee akkoord.”

PR Aviation maakt gebruik van de informatie op de website van Ryanair om deze vluchtgegevens op prijs te vergelijken met vluchten van andere luchtvaartmaatschappijen. Ryanair is het niet eens met deze gang van zaken en stelt dat er sprake is van een tekortkoming in de nakoming van de overeenkomst door de wijze waarop PR Aviation gebruikmaakt van de gegevens van de website. Ryanair heeft de gebruiksvoorwaarden op haar website

¹ Reinoud Westerdijk is advocaat bij Kennedy Van der Laan te Amsterdam.

² Vgl. Hoge Raad 11 maart 2016, ECLI:NL:HR:2016:390.
³ ECLI:NL:PHR:2019:718.

aangeboden en stelt dat door het gebruik van de website deze voorwaarden zijn aanvaard door de bezoeker van de website. Met dit standpunt is PR Aviation het oneens: zij stelt dat zij de gebruiksvoorwaarden niet heeft willen aanvaarden.

3. Na de hierboven genoemde arresten over de IE-aspecten is bij het Gerechtshof Den Haag (hierna: het 'hof') vooral verder geprocedeerd over de contractuele aspecten en daar concentreer ik mij in deze noot op. Een belangrijke voorvraag die zich in dit kader voordoet is naar welk recht de vraag inzake *browse-wrapping* beantwoord dient te worden. Het hof bepaalt dat lers recht van toepassing is: niet vanwege een geldige rechtskeuze maar vanwege het recht dat ingevolge het EVO⁴ en de Rome I Verordening⁵ van toepassing zou zijn als de overeenkomst geldig zou zijn. Het hof bepaalt vervolgens dat naar lers recht de gebruiksvoorwaarden van Ryanair niet zijn overeengekomen. Overigens geeft het hof in dat kader ook aan dat die vraag naar Nederlands recht niet anders beantwoord zou worden, hetgeen deze procedure ook voor onze rechtspraaklijk van belang maakt.

4. De belangrijkste middelen in cassatie richten zich tegen het oordeel van het hof dat naar lers recht de gebruiksvoorwaarden niet zijn aanvaard. Ryanair stelt in dit kader allereerst dat het oordeel van het hof in strijd is met artikel 9 lid 1 van de E-Commercerichtlijn⁶ (hierna: de 'Richtlijn'). Vanuit processueel oogpunt wijst de A-G er in dit kader terecht op dat tussen private partijen geen direct beroep kan worden gedaan op de Richtlijn; een richtlijn heeft tussen private partijen immers geen directe werking. Ook een beroep op richtlijnconforme uitleg wijst de A-G af: in dit geval zou de Hoge Raad een oordeel moeten geven over de juiste uitleg van lers recht, hetgeen op grond van artikel 79 lid 1 RO niet mogelijk is.

5. Maar ook materieel kan volgens de A-G geen beroep worden gedaan op strijd met artikel 9 lid 1 van de Richtlijn. Dat artikel bepaalt dat het sluiten van overeenkomsten langs elektronische weg mogelijk moet zijn. Dat betekent echter niet dat het nationale recht geen eisen mag stellen aan de totstandkoming van een overeenkomst, zolang die eisen ook online kunnen worden vormgegeven.⁷ Volgens de A-G behandelt het hof ook het lerse recht aldus: via *browse-wrapping* kan een overeenkomst tot stand komen mits sprake is van een op aanvaarding gerichte wil of, als die wil ontbreekt, als een redelijk persoon zal denken dat de gebruiker van de website de voor-

waarden wilde aanvaarden. In de omstandigheden van dit geval achtte het hof dat daarvan geen sprake is.

6. De A-G plaatst dit oordeel in een breder Nederlands kader en stelt, onder verwijzing naar Nederlandse literatuur,⁸ dat het gebruik van een website op zichzelf geen aanvaarding vormt van algemene voorwaarden waarnaar wordt verwezen, en dat dit afhankelijk is van alle omstandigheden van het geval. In deze zaak waren volgens het hof relevante omstandigheden dat de gegevens gratis en vrij toegankelijk waren, en niet beschermd door databank- of auteursrecht, waardoor een redelijk persoon bij bezoek van de website niet zou denken dat PR Aviation gebonden zou zijn aan gebruiksvoorwaarden die juist beperkingen opleggen aan het gebruik van die gegevens.

7. Dat is volgens het hof niet anders doordat PR Aviation (i) van de voorwaarden wist of moest weten, (ii) zelf *browse-wrapping* voorwaarden gebruikte en (iii) naderhand expliciet is gewezen op de voorwaarden. Die eerste en derde overweging is interessant in het licht van een recente Amerikaanse uitspraak:⁹ daarin overwoog de rechter juist dat de gebruiker wel gebonden was door voortgezet gebruik van een website nadat hij op de hoogte was gesteld van de voorwaarden die op dat gebruik van toepassing zijn. Naar Nederlands recht lijkt me dat ook in lijn met het *First Data-KPN Hotspots* arrest van de Hoge Raad.¹⁰ Het hof constateert slechts dat voor aanvaarding meer nodig is dan de drie genoemde omstandigheden (r.o. 81) en geeft vervolgens een voorbeeld dat de gegevens pas na *click-wrap* toegankelijk zouden zijn. Helaas gaat de A-G hier niet nader op in nu het oordeel van het hof in hoge mate is verweven met waarderingen van feitelijke aard die in cassatie niet aan de orde zijn. Ik zou hier van het hof graag meer onderbouwing hebben gezien, dat zou het arrest in het algemeen sterker hebben gemaakt.

8. Met de uitkomst van deze procedure valt uiteindelijk goed te leven. Van de gebruiker van algemene voorwaarden mag meer worden verwacht dan de in de algemene voorwaarden zelf opgenomen bepaling dat gebruik van een website leidt tot aanvaarding van de toepasselijkheid van die voorwaarden. Anders dan Ryanair betoogt geldt ook niet dat *browse-wrapping* een maatschappelijk en commercieel gebruikelijke en algemeen aanvaarde manier is geworden om voorwaarden te stellen aan het gebruik van een website die informatie publiekelijk toegankelijk maakt. Dat heeft Ryanair ook zelf ingezien, nu zij inmiddels ook een *click-wrap* constructie hanteert waarbij de bezoeker van de website de gegevens daarop

4 Verdrag van Rome van 19 juni 1980 inzake het recht dat van toepassing is op verbintenissen uit overeenkomst, *Trb.* 1980/156.

5 Verordening (EG) nr. 593/2008 van het Europees Parlement en de Raad van 17 juni 2008 inzake het recht dat van toepassing is op verbintenissen uit overeenkomst, *PbEU* 2008, L 177/6.

6 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG* 2000, L 178/1.

7 Zie ECLI:NL:PHR:2019:718 par. 2.17 met nuttige verwijzingen naar het verslag over de toepassing van de Richtlijn en de Nederlandse memorie van toelichting bij de implementatiewetgeving.

8 De A-G verwijst naar M.B.M. Loos, *Algemene voorwaarden*, 2018, nr. 66b; R.H.C. Jongeneel, 'Gebondenheid', in: B. Wessels en R.H.C. Jongeneel (red.), *Algemene voorwaarden*, 2017, p. 128; R.E. van Esch, 'Online overeenkomsten', in: S. van der Hof, A.R. Lodder en G.J. Zwenne (red.), *Recht en computer*, 2014, p. 101; en L.A.R. Siemerink, M. van Eijdsen en R.E. van Esch, 'Uitsluiting of beperking van aansprakelijkheid via disclaimers op een website', *Computerrecht* 2006, p. 145-146.

9 *Gutierrez v. FriendFinder Networks Inc.* (3 May 2019), <https://www.leagle.com/decision/infeco20190506976>.

10 Hoge Raad 11 februari 2011, ECLI:NL:HR:2011:B07108.

pas krijgt te zien nadat uitdrukkelijk, via het drukken op een virtuele knop, de toepasselijkheid van de gebruiksvoorwaarden zijn aanvaard. Nu ook het Hof van Justitie van de Europese Unie al in 2015 heeft geoordeeld¹¹ dat *click-wrap* wel een geldige wijze van het aanvaarden van algemene voorwaarden is, lijkt dat in de praktijk de beste optie.

Mr. R.J.J. Westerdijk

Computerrecht 2020/85

Rechtbank Amsterdam 18 december 2019,
nr. C/13/656884 / HA ZA 18-1145
(Mr. C.H. Rombouts)
m.nt. mr. W.F.R. Rinzema¹

(Art. 6:265, 6:271 en 6:272 BW)

ECLI:NL:RBAMS:2019:9635

Als professionele IT-dienstverlener [dient Smart Connection] een CRM-systeem op te leveren dat voldoet aan de verwachtingen die een gemiddelde klant daaraan mag ontlelen. Zelfs als dit dus niet met zoveel woorden in de overeenkomst is opgenomen (die hier overigens slechts een presentatie betreft, waaruit dus sowieso de daadwerkelijke afspraken slecht af te leiden zijn), mag een klant immers van een deskundige ICT-dienstverlener die daarvoor marktconforme prijzen in rekening brengt, verwachten dat deze een systeem levert waarmee door de gemiddelde werknemer kan worden gewerkt. En ook als een ISO-norm niet met zoveel woorden is overeengekomen, mag de klant verwachten dat zijn professionele dienstverlener werkt met inachtneming van de normen die binnen de branche gebruikelijk zijn.

Vonnis in de zaak van:

de besloten vennootschap met beperkte aansprakelijkheid

SMART CONNECTIONS FACTORY B.V.,

gevestigd te Utrecht,

eiseres in conventie,

verweerster in reconventie,

tegen

de besloten vennootschap met beperkte aansprakelijkheid

ALLSAFE MANAGEMENT B.V.,

gevestigd te Amsterdam,

gedaagde in conventie,

eiseres in reconventie,

Partijen zullen hierna Smart Connections en Allsafe genoemd worden.

[...]

2. De feiten

2.1. Smart Connections is een onderneming met als activiteiten (onder meer) dienstverlening en advies op het gebied van informatietechnologie en daarnaast het ontwikkelen en produceren van software. Smart Connections is ontstaan uit de fusie van de twee bedrijven CRM Factory B.V. (hierna: CRM Factory) en [betrokken BV 1] (hierna: [betrokken BV 1]).

2.2. Allsafe voert een onderneming op het gebied van het aanbieden van opslagruimte en aanverwante producten (bijvoorbeeld op het vlak van transport en postbezorging) voor zakelijke gebruikers en particulieren.

2.3. Een Customer Relations Management (CRM) softwaresysteem (hierna: CRM-systeem) is een softwarepakket dat – kort gezegd – voorziet in de contacten tussen bedrijven en hun klanten. Het voorziet in de communicatie met de klant, maar daarnaast ook in de analyse van klantgegevens en het aan de hand daarvan komen tot effectieve marketingactiviteiten (bijvoorbeeld cross selling en upselling).

[...]

2.6. In de periode tussen oktober en december 2015 is tussen partijen kennelijk overeenstemming ontstaan over inschakeling door Allsafe van Smart Connections voor het ontwikkelen van een CRM-systeem. Partijen hebben geen overeenkomst ondertekend die deze afspraken weergeeft. Wel zijn overgelegd een notitie, door Allsafe aangeduid als “de Projectafspraken” van oktober 2015 waarin kennelijk een voorzet is gedaan door Smart Connections en met reactie daarop van Allsafe. Daarnaast is overgelegd een (PowerPoint) presentatie van Smart Connections over het te ontwikkelen systeem met daarin onder meer het onderwerp “Allsafe CRM Projectscope”. Dit onderdeel beschrijft een fase 1 (Datamanagement, Applicatie en Sales) en een fase 2 (Marketing, Customer Service en Dashboard). Ook is in deze presentatie een prijsopgave opgenomen voor de diverse onderdelen van het project en is een planning gemaakt. De planning geeft nog een fase 3 weer die omschreven wordt als “Additionele wensen wijzigingen en ontwikkelingen”. Bij de presentatie zijn bijlagen gevoegd. Eén van die bijlagen betreft een afbeelding met als onderwerp “Indicatie ten behoeve van de gewenste look & Feel”. Beide partijen duiden deze presentatie aan als “de Overeenkomst” en gaan ervan uit dat die op 21 december 2015 tot stand is gekomen. Ook is door Allsafe overgelegd een productie die zij aanduidt als “Plan van Aanpak” met als datum 12 februari 2016. Dit is dezelfde presentatie als de eerdere met een aanpassing van data naar aanleiding van de wens van Allsafe om in een eerder stadium dan voorzien het systeem geschikt te maken voor mailings aan klanten. Tot slot heeft Smart Connections haar algemene

¹¹ Zie Hof van Justitie 21 mei 2015, zaak C-322/14, ECLI:EU:C:2015:334 (*El Majdoub*).

¹ Mr. W.F.R. Rinzema is advocaat bij Ventoux Advocaten en IT-arbiter bij meerdere instituten.

voorwaarden overgelegd waarvan zij stelt dat deze van toepassing zijn verklaard op de overeenkomst tussen partijen.

2.7. Begin 2016 is Smart Connections volgens de planning gestart met het ontwikkelen van een CRM-systeem voor Allsafe. Over de periode 2016-2018 zijn partijen vervolgens in een discussie geraakt over de vraag of dit systeem door Smart Connections werd opgeleverd conform wat Allsafe daarvan mocht verwachten. Van deze discussie hebben partijen een groot aantal e-mails overgelegd waaruit blijkt dat Allsafe over de werking van diverse onderdelen klachten uit en van de reactie daarop van Smart Connections. In 2018 hebben partijen geprobeerd door een mediationtraject overeenstemming te bereiken over de klachten die Allsafe nog had, maar dit heeft niet tot een succesvolle oplossing van het geschil geleid.

[...]

2.9. Bij brief van 17 juli 2018 aan Smart Connections heeft de advocaat van Allsafe de overeenkomst met onmiddellijke ingang ontbonden.

2.10. Allsafe heeft in de procedure een rapport overgelegd van SQMI, Software Quality Measurement & Improvement B.V. (hierna: het rapport van SQMI). In dat rapport zijn de bevindingen neergelegd van onderzoekers naar de kwaliteit van het door Smart Connections voor Allsafe gebouwde CRM-systeem. In het rapport is het systeem getest aan de hand van de (volgens het rapport) internationale standaard ISO/IEC 25010:2011 "Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models" (hierna: de ISO-norm). Het rapport geeft een verantwoording van de methode van onderzoek en de bevindingen van bepaalde onderdelen. Geconcludeerd wordt onder meer:

"[De ISO-norm] definieert hoe de kwaliteit van software systemen en producten benaderd dient te worden. Met deze internationale norm in de hand zijn de kwaliteitsproblemen in het voorhanden systeem in drie groepen onder te verdelen:

1. Performance, compatibiliteit en betrouwbaarheid schieten voorts op sommige vlakken ernstig tekort, en deze goed gedocumenteerde aanhoudende problemen zijn voorts niet opgelost;
2. Door tekortkomingen, fouten en storingen zijn voorts bepaalde noodzakelijke handelingen onmogelijk, hetgeen mogelijk te maken heeft met de mate van onderhoudbaarheid van de software – ook deze goed gedocumenteerde aanhoudende problemen zijn voorts niet opgelost;
3. Verder onderzoek heeft aangetoond dat 41% van de schermen zeer slecht bruikbaar zijn. Vooral op het gebied van 'herkenbaarheid van 'geschiktheid' en 'bescherming tegen gebruikersfouten' schieten veel onderdelen van het voorhanden systeem ernstig tekort. De markt voor CRM systemen is vrij volwassen en dat laat zich onder meer zien in het hoge niveau van bruik-

baarheid van de aangeboden systemen. Vanwege concurrentie worden kwaliteitsproblemen in de markt doorgaans snel verholpen."

Als bijlage A bij het rapport zijn de resultaten van een onderzoek naar de bruikbaarheid van het systeem bijgevoegd. Hieraan wordt het volgende citaat ontleend:

"De onderzoeksopdracht was om de kwaliteit van het door SmartConnections aan ALLSAFE aangeboden CRM systeem te onderzoeken.

Schouw

Op basis van bovenstaande vraagstelling is er eerst een schouw uitgevoerd op het systeem. Tijdens het onderzoek is gebleken dat slechts 4 van de 133 schermen als goed afgewerkt ervaren werden (de "Telesales schermen") en dat er in die schermen rekening gehouden is met ALLSAFE jargon en processen, hetgeen als kritische succesfactor tussen opdrachtgever en opdrachtnemer overeengekomen is. Tevens is gebleken dat 129 van de 133 schermen slecht afgewerkt zijn vanwege onder meer:

- Het gebruik van Engels en Nederlands door elkaar
- Jargon die noch ALLSAFE jargon noch vakjargon is
- Geen enkele aansluiting met ALLSAFE processen
- Het aantal eigenschappen (bijv. kolommen en velden) zo groot is dat de gebruiker geen overzicht kan krijgen
- ALLSAFE 'look and feel' is niet toegepast

74 van deze slecht afgewerkte schermen bleken relatief *eenvoudig* te zijn, maar 55 bleken *niet eenvoudig* te zijn door onder meer:

- tientallen slecht van elkaar te onderscheiden kolommen en velden (veldnamen die bijna identiek zijn en waarbij er geen enkel uitleg op het scherm getoond wordt)
- volstrekt onoverzichtelijke presentatie (gegevens passen noch in de hoogte, noch in de breedte van een beeldscherm waardoor er in twee richtingen gescrold moet worden)
- onduidelijke scherm verloop (geen indicatie van hoe schermen samen gebruikt moeten worden om een ALLSAFE proces uit te voeren)

Bovenstaande heeft ertoe geleid dat de schermen in drie klassen onderverdeeld kunnen worden, namelijk:

- klasse 1: goed afgewerkte schermen
- klasse 2: eenvoudige, slecht afgewerkte schermen
- klasse 3: niet eenvoudige, slecht afgewerkte schermen

Vervolgens is er een uitgebreide analyse uitgevoerd van schermen uit elke klasse, gebruikmakend van het product kwaliteitsmodel die in internationale norm ISO/IEC 25010:2011 uiteen gezet is.

De bruikbaarheid van de verschillende klassen zijn gekwantificeerd door de toepassing van een wegingsfactor, en het geven van een "rapportcijfer" per ISO/IE (sub-karakteristiek (zie Bijlage F).

Hierdoor werd duidelijk dat vooral de zeer slechte bruikbaarheid van 41% van de schermen, het door SmartConnections aangeboden CRM systeem onacceptabel maakt.”

3. Het geschil

In conventie

3.1. Smart Connections vordert, samengevat, dat Allsafe bij uitvoerbaar bij voorraad te verklaren vonnis wordt veroordeeld tot:

1. primair: betaling van € 99.879,46, vermeerderd met de contractuele rente van 1,5% per maand vanaf de vervaldata van de diverse facturen;
subsidiair: betaling van € 99.879,46, vermeerderd met de wettelijke handelsrente vanaf de vervaldata van de diverse facturen;
2. betaling van een bedrag van € 14.981,92 aan buitengerechtelijke incassokosten, vermeerderd met de wettelijke handelsrente vanaf het te wijzen vonnis;
3. betaling van een bedrag van € 17.723,00, onder veroordeling van Allsafe in de proceskosten.

Aan haar vordering onder 1. legt Smart Connections nakoming ten grondslag: Allsafe heeft diverse facturen met dit totaalbedrag onbetaald gelaten. Aan haar vordering onder 3. legt Smart Connections een bepaling uit haar algemene voorwaarden ten grondslag die haar het recht geeft annuleringskosten in rekening te brengen bij de partij die aanleiding heeft gegeven tot beëindiging van een overeenkomst.

3.2. Allsafe voert verweer. Voor het geval de rechtbank zou oordelen dat de overeenkomst niet door haar is ontbonden, voert zij aan dat Smart Connections nog niet mocht factureren zolang diverse fases nog niet waren opgeleverd. Ook voert zij aan dat de gevolgen van de overeenkomst door haar gewijzigd worden op grond van artikel 6:258 BW en beroept zij zich op opschorting.

3.3. Op de stellingen van partijen wordt hierna, voor zover van belang, nader ingegaan.

In reconventie

3.4. Allsafe vordert samengevat – veroordeling van Smart Connections bij uitvoerbaar bij voorraad te verklaren vonnis tot:

Onvoorwaardelijk:

- I. primair: betaling van € 63.721,63,
 - II. subsidiair: betaling van € 60.900,00, en
 - III. schadevergoeding, op te maken bij staat, alles vermeerderd met wettelijke handelsrente en kosten;
- Voorwaardelijk, onder de voorwaarde dat Allsafe in conventie wordt veroordeeld tot betaling van facturen:
- I. nakoming van de overeenkomst door de in het rapport van SQMI genoemde gebreken deugdelijk te herstellen binnen twee maanden na betekening van het vonnis op straffe van een dwangsom, met veroordeling van Smart Connections in de kosten van de procedure.

Allsafe legt aan haar vorderingen ten grondslag dat zij de overeenkomst op grond van een toerekenbare tekortkoming van Smart Connections rechtsgeldig heeft ontbonden. Zij maakt daarom aanspraak op terugbetaling van de door haar betaalde facturen uit hoofde van een ongedaanmakingsverbintenis, dan wel schadevergoeding bestaande uit het negatieve contractsbelang. Daarnaast vordert zij schade die zij heeft geleden doordat zij omzet heeft gemist door minder effectieve marketing als gevolg van het gebrekkige CRM-systeem. Deze schade is nog niet groot, dus daarom vordert ze deze op te maken bij staat. [...]

4. De beoordeling

[...]

4.2. De rechtbank is van oordeel dat Allsafe rechtsgeldig de overeenkomst heeft kunnen ontbinden omdat zij voldoende heeft onderbouwd dat het door Smart Connections ontwikkelde CRM-systeem niet voldeed aan wat van het systeem op grond van de overeenkomst mocht worden verwacht. Hiertoe is als volgt overwogen.

4.3. Allsafe voert aan dat er geen werkend CRM-systeem is opgeleverd. Het klopt weliswaar dat Allsafe met het systeem heeft gewerkt, maar geen van de functionaliteiten konden er behoorlijk mee worden uitgevoerd. Het gebruik van de interface was dusdanig ingewikkeld dat een gemiddelde gebruiker er geen gebruik van kon maken. Het vertoonde bovendien veel storingen en downtime. Bovendien heeft het niet voorzien in waarvoor het bedoeld was, namelijk het genereren van leads en ondersteunen van marketing. Ter comparitie heeft [werknemer], IT manager van Allsafe, hierover het volgende verklaard:

“Daarnaast zijn er maar enkele delen van de applicatie die de manier waarop Allsafe werkt hebben overgenomen waardoor schermen steeds verschillen en knoppen op andere plekken staan als je door de applicatie heen gaat. Het is meer een programmeursinterface dan een gebruikersinterface.”

Voor haar stellingen verwijst Allsafe (voorts) naar het door haar overgelegde deskundigenrapport van SQMI. Ook met de overgelegde producties met afbeeldingen van de gebruikersschermen heeft Allsafe onderbouwd dat er binnen het systeem sprake was van enkele overzichtelijke interfaces, maar ook van vele interfaces met een zeer klein lettertype waarop heel veel moest worden ingevuld.

4.4. Smart Connections brengt daartegen in dat zij een werkend systeem heeft opgeleverd met de tussen partijen afgesproken basale functionaliteit. De klachten van Allsafe over dit systeem komen er alle uit voort dat zij steeds meer functionaliteiten wilde toevoegen waarvan tussen partijen was afgesproken dat deze pas in een later stadium zouden worden toegevoegd. Dat het opgeleverde systeem voldeed, blijkt er uit dat het veelvuldig is ge-

bruikt. Smart Connections heeft data overgelegd waaruit blijkt van volgens haar veel activiteit op het systeem. De deskundige zou voorts niet onpartijdig zijn en deze heeft de afspraken tussen partijen miskend, te weten minder functionaliteit en voorts dat de ISO-norm tussen partijen niet is overeengekomen.

4.5. De rechtbank stelt vast dat Smart Connections hiermee de inhoudelijke stellingen van Allsafe feitelijk niet betwist. Zij vindt alleen het systeem zoals het nu functioneert wel bruikbaar. En, zo begrijpt de rechtbank, meer is niet afgesproken. Dat de deskundige van SQMI in zijn rapport en ter zitting anders beweert, wordt door Smart Connections ongemotiveerd afgedaan als ofwel partijdig ofwel gebrek aan deskundigheid. Zij miskent daarmee dat zij als professionele IT-dienstverlener een CRM-systeem dient op te leveren dat voldoet aan de verwachtingen die een gemiddelde klant daaraan mag ontlelen. Zelfs als dit dus niet met zoveel woorden in de overeenkomst is opgenomen (die hier overigens slechts een presentatie betreft, waaruit dus sowieso de daadwerkelijke afspraken slecht af te leiden zijn), mag een klant immers van een deskundige ICT-dienstverlener die daarvoor marktconforme prijzen in rekening brengt, verwachten dat deze een systeem levert waarmee door de gemiddelde werknemer kan worden gewerkt. En ook als een ISO-norm niet met zoveel woorden is overeengekomen, mag de klant verwachten dat zijn professionele dienstverlener werkt met inachtneming van de normen die binnen de branche gebruikelijk zijn. Uit de feiten vloeit bovendien voort dat Allsafe van meet af aan over deze gebrekkige functionaliteit en de moeilijke interfaces heeft geklaagd en dat Smart Connections daarop vooral heeft gereageerd met een discussie over wat wel of niet zou zijn afgesproken. Tot slot heeft Smart Connections ook niet concreet aangevoerd welke extra functionaliteiten Allsafe eiste die in de weg stonden aan de oplevering van een systeem dat Allsafe zou kunnen gebruiken voor het doel dat het voor haar moest dienen, namelijk het onderhouden van klantcontacten en deze gebruiken voor (al dan niet gerichte) marketing. Dat de marketing pas mogelijk zou zijn in een latere fase, zoals Smart Connections ter comparitie heeft aangevoerd, verhoudt zich niet met de als overeenkomst overgelegde presentatie (die alleen handelt over fases 1 en 2), waarin wordt gesproken over ondersteuning bij “sales[en] marketingprocessen faciliteren”, “event driven marketing” en campagnemanagement als basisfunctionaliteit. Ook is de rechtbank niet duidelijk geworden hoe mogelijke verwachtingen die Allsafe heeft uitgesproken over de “look and feel” van de interfaces kunnen worden beschouwd als “out of scope”. Dit zou pas gevolgd kunnen worden indien er aanleiding was om aan te nemen dat Allsafe niet geklaagd heeft over functionaliteit van de interfaces, maar “slechts” over het uiterlijk. Zoals hiervoor overwogen, is daarvan geen sprake geweest. Uit het rapport van SQMI volgt dat het systeem niet functioneert op een basaal niveau.

[...]

Noot

1. Op IT-vlak treft Allsafe het niet. Door middel van een zogenoemd ‘Customer Relations Management’² softwaresysteem³ wilde zij beter met haar (potentiële) klanten kunnen communiceren. Via een adviseur kwam zij voor zo’n CRM-systeem uit bij Loyalty Lab. Die samenwerking leidde echter niet tot oplevering van een werkend systeem en werd verbroken. Na inschakeling van dezelfde adviseur belandde Allsafe vervolgens bij Smart Connections en ook dat project mislukte. Weliswaar werd het systeem in gebruik genomen en probeerde Allsafe ermee te werken, maar volgens de rechtbank functioneerde het systeem niet “op een basaal niveau” en was de ontbinding van de overeenkomst gegrond.

2. De vraag aan welke eisen (‘specificaties’) een softwaresysteem moet voldoen, is veelvuldig een van de breekpunten in discussies tussen opdrachtgevers en leveranciers. Twee verschillende werelden kunnen dan botsen. Enerzijds de leverancierswereld die de functionaliteit van het product centraal stelt en ervan uitgaat dat de klant daarmee wil, kan en moet werken. Met name de schriftelijke documentatie van de mogelijkheden van de software zijn in die visie bepalend. Anderzijds de wereld van de klant/opdrachtgever die ervan uitgaat dat de software aan zijn bedrijfsseisen en expliciete of impliciete eisen en wensen voldoet. In die wereld wordt verwacht dat de leverancier zich voldoende heeft verdiept in de omstandigheden van zijn klant. Voor beide werelden is wat te zeggen. Het beoordelen van de gevolgen van die botsing wordt verder bemoeilijkt doordat geen enkel IT-project zonder goede samenwerking tussen de betrokken partijen kan worden uitgevoerd. Deugdelijke informatie-uitwisseling over en weer is ook daarbij essentieel.

3. Deze rechtbank lijkt in dit geval het gebruikersperspectief te kiezen. Deels gebruikmakend van gebreken in de stelplicht, oordeelt het dat een *“professionele IT-dienstverlener een CRM-systeem dient op te leveren dat voldoet aan de verwachtingen die een gemiddelde klant daaraan mag ontlelen. Zelfs als dit dus niet met zoveel woorden in de overeenkomst is opgenomen (die hier overigens slechts een presentatie betreft, waaruit dus sowieso de daadwerkelijke afspraken slecht af te leiden zijn), mag een klant immers van een deskundige ICT-dienstverlener die daarvoor marktconforme prijzen in rekening brengt, verwachten dat deze een systeem levert waarmee door de gemiddelde werknemer kan worden gewerkt”*, overweegt deze rechtbank. Zij acht het feit dat er geen duidelijke afspraken zijn gemaakt over de eigenschappen van het CRM-systeem in zoverre dus niet van belang.

² Afgekort als ‘CRM’.

³ In deze annotatie wordt de term ‘softwaresysteem’ gebruikt i.p.v. de term ‘software’ omdat in de praktijk weliswaar de software het onderscheidende kenmerk is van een IT-systeem, maar software niet zonder ondersteunende systemen kan functioneren dan wel via systemen (‘online’) beschikbaar worden gesteld aan gebruikers. Daarom zijn beide nauwkeurig te scheiden.

4. Kijkend naar de uitkomst van vele andere IT-geschillen is dit vonnis bijzonder en betrekkelijk uniek. Doorgaans is juist het feit dat de afspraken tussen partijen niet helder genoeg zijn een breekpunt in het nadeel van de opdrachtgever. Wanneer Eno Zorgverzekeringen in kort geding bijvoorbeeld vordert dat de firma VCD “het gecontracteerde IT-platform oplevert voor de gebruikersacceptatietesten” volgt de voorzieningenrechter⁴ de stelling van VCD dat “de Overeenkomst geen gedetailleerde beschrijving van het platform bevat op grond waarvan voor partijen voldoende duidelijk is aan welke eisen het door VCD op te leveren platform moet voldoen” omdat “in de in gemelde bijlage opgenomen tabel slechts in grote lijnen de bedrijfsprocessen worden beschreven die door [het programma] ondersteund zouden moeten worden en dat elke specificatie van vereiste functionaliteit ontbreekt”.

5. De vraag hoe moet worden vastgesteld of een softwaresysteem juridisch voldoet, is niet eenvoudig te beantwoorden. Tegelijkertijd wordt die vraag door toenemende informatisering van steeds groter belang. Veel IT-projecten verlopen namelijk moeizaam. In *Computerrecht* heeft mr. P.G. van der Putt met regelmaat over de juridische gevolgen hiervan geschreven. Hij stelt dat “falen bijna een gegeven is” en dat de meeste IT-projecten niet binnen budget, planning en/of scope worden geleverd.⁵

6. Nu kunnen niet alle IT-projecten over een kam worden geschoren. Daarom zal ik hierna vanuit twee verschillende perspectieven kijken naar de vraag wat een gebruiker van een softwaresysteem mag verwachten. Bij het eerste perspectief stel ik de aard van het softwaresysteem centraal. Het tweede perspectief baseer ik op de aard van de gebreken in het softwaresysteem. Vervolgens probeer ik die perspectieven te combineren.

De aard van het softwaresysteem

7. Een IT-project kan zijn gebaseerd op het besluit van een opdrachtgever van een standaard softwaresysteem⁶ zonder (maatwerk) aanpassingen gebruik te maken. In dat geval lijken aanpassingen in de software niet nodig te zijn of besluit de klant zijn bedrijfsvoering in te richten op de wijze die het standaardsoftwaresysteem voorschrijft. In de praktijk houdt dit in dat de diensten van de leverancier zich beperken tot het ‘inrichten’ van het softwaresysteem voor de klant en het geven van gebruikerstrainingen. Inrichting kan bestaan uit het maken van voorgeprogrammeerde keuzes in het softwaresysteem of het vullen van tabellen met gegevens van de klant. Eventuele gebruiksbeperkingen van het product kunnen als gevolg hiervan inherent en onvermijdelijk zijn. De

overeenkomst vertoont in dat geval trekken van een leveringsovereenkomst, waarbij de klant dus hoofdzakelijk afnemer is. Ook in die situatie kan het echter fout gaan. Een voorbeeld hiervan is de zaak Exact Software Nederland/Brandmeester’s.⁷ Hierin kwam de vraag aan de orde of Brandmeester’s mocht verwachten dat “in het door Exact geleverde softwarepakket het automatisch afletteren van pintransacties (waar in dit verband creditcardtransacties mede onder begrepen worden) mogelijk zou zijn”. Met haar meent het hof dat Brandmeester’s deze verwachting mocht hebben. Hiervoor verwijst het hof onder meer naar informatie die zij voorafgaand aan het sluiten van de overeenkomst aan Exact had verstrekt, het feit dat het om “een normale boekhoudkundige bewerking van automatisch ingevoerde gegevens” ging en dat Exact Brandmeester’s “er niet op gewezen had dat deze functie in de geleverde software ontbrak”. In deze verhouding moet het softwaresysteem dus geschikt zijn voor het beoogde gebruik. De informatie en mededelingsplicht zijn daarbij voor partijen van belang.⁸

8. De relatie tussen de partijen krijgt sterkere trekken van samenwerking wanneer er in een IT-project sprake is van levering van standaardsoftware in combinatie met het verrichten van aanpassingen daarvan en/of het ontwikkelen van aanvullende software op basis van eisen en wensen van de klant. In dat geval kan niet (alleen) volstaan worden met het kijken naar de geschiktheid van het standaard softwaresysteem maar moet het geheel van activiteiten van partijen worden beoordeeld.⁹ Door regels rond stelplicht en bewijslast kan de vraag welke partij in het gelijk wordt gesteld in dergelijke gevallen moeilijk te beantwoorden zijn. Grondt de rechter zijn oordeel bijvoorbeeld op de geschiktheid van het product dan wel op de invulling van de samenwerking? In laatstgenoemd geval zal de afnemer wellicht moeten bewijzen dat zijn medewerking toereikend was. In de zaak Waterdrinker/SAP koos het Hof Amsterdam een mooie tussenvorm door onderscheid te maken tussen de geschiktheid van de software zelf enerzijds en de nakoming van overige verplichtingen uit hoofde van het IT-project anderzijds. Kern van zijn redenering is dat als de software zelf niet geschikt is voor het beoogde gebruik, de eventuele problemen rond de samenwerking bij de implementatie minder relevant

4 Rb. Overijssel (vzr.) 12 mei 2016, ECLI:NL:RBOVE:2016:1682.

5 Zie P.G. van der Putt, ‘De afdwingbaarheid van contracten bij falende IT-projecten’, *Computerrecht* 2016/44, dat voortbouwt op P.G. van der Putt, ‘De gevolgen van niet-nakoming bij IT-projecten’, *Computerrecht* 2011/33. Verwezen zij ook P.G. van der Putt, ‘Update Nederlandse IT-wanprestatie jurisprudentie’, *Computerrecht* 2019/214.

6 Die zowel lokaal op computers van de klant (‘on premise’) beschikbaar kan worden gesteld als via het internet, bijvoorbeeld als SaaS-dienst (‘Software-as-a-Service’).

7 Hof Den Haag 31 maart 2015, ECLI:NL:GHDHA:2015:1113.

8 Zo oordeelde het Hof ‘s-Hertogenbosch in de zaak Accountantskantoor/IT-bedrijf bijvoorbeeld dat de (gebrekkige) ervaring van het IT-bedrijf met computernetwerken in de accountancybranche voor rekening en risico van het accountantskantoor kwam. “Indien het voor het accountantskantoor zo belangrijk was dit te weten had het op haar weg gelegen hier zelf vragen over te stellen dan wel hier onderzoek naar te verrichten”, aldus Hof ‘s-Hertogenbosch 13 november 2018, ECLI:NL:GHSHE:2018:4670.

9 Deze situatie komt in de rechtspraak veelvuldig voor.

zijn. En andersom.¹⁰ Veel complexe voorbeelden van deze problematiek zijn terug te vinden in de diverse uitspraken rond de mislukte invoering van Alert®PFH bij een aantal Nederlandse ziekenhuizen. In die zaken wordt gestreden over de vraag of een buitenlandse IT-leverancier verantwoordelijk is voor het leveren van software die geschikt is voor gebruik in Nederlandse ziekenhuizen en de verantwoordelijkheden die ziekenhuizen zelf hebben bij het geschikt maken van die software en het invoeren daarvan. Opvallend is dat de verschillende zaken ongelijke uitkomsten kennen en dat de geraadpleegde rechters verschillende redeneringen kiezen. Zo achtte het Hof 's-Hertogenbosch¹¹ in de zaak Tweesteden/Alert het “*van groot belang tot uitgangspunt te nemen dat Alert c.s. degene zijn die zich hebben verbonden tot levering, ontwikkeling en implementatie van door hen vervaardigde complexe software*”. Als gevolg daarvan legde het hof de verantwoordelijkheid voor het leveren van deugdelijke software “*geheel bij Alert*” neer waardoor “*van een samenwerking ten aanzien van deze (ICT-)kerntaak van Alert c.s. dan ook geen sprake was geweest*”. Hetzelfde hof oordeelde echter in de zaak JBZ/Alert¹² dat er een “*complexe en grootschalige relatie*” tussen partijen bestond, nu zij “*met de Raamovereenkomst immers beoogden te bereiken dat binnen een groot ziekenhuis met meerdere locaties een nieuw innovatief Elektronisch Patiëntendossier en een Zorg Logistiek Systeem in gebruik zouden worden genomen*”. Naar het oordeel van het hof was het daardoor “*evident dat de Raamovereenkomst en het op basis daarvan tot stand te brengen project samenwerking tussen JBZ en Alert c.s. veronderstelde*”.

9. Een derde situatie is die, waarin een leverancier geen standaardsoftware levert maar enkel maatwerksoftware ontwikkelt. Dit doet zich in de IT-praktijk overigens steeds minder voor. In dergelijke gevallen is er sprake van een overeenkomst van opdracht en hebben beide partijen verplichtingen, waarbij de zorgplicht van de leverancier een grote rol speelt. In de zaak tussen stichting ITV Hogeschool voor tolken & vertalen en Avetica B.V.¹³ hield de voorzieningenrechter hier bijvoorbeeld rekening mee door bij het toekennen van een dwangsom op de verplichting tot levering, de stelling van Avetica relevant te achten dat invoering van de onderhavige software (een maatwerkproduct) een kwestie van passen en meten is, in die zin dat onvolkomenheden in het systeem ('bugs') steeds door de opdrachtgever gerapporteerd moesten worden en dat die bugs dan verholpen moesten worden, “*zodat het*

systeem steeds verder vervolmaakt kan worden voordat het definitief in gebruik kan worden genomen”.

Aard van de gebreken

10. Een andere insteek voor het beoordelen van (beveerde) gebreken in IT-systemen is het beschouwen van de aard van de geconstateerde gebreken. Eerder¹⁴ onderscheidde ik ‘technische’, ‘functionele’ en ‘belevings-’gebreken. *Technische* gebreken betreffen het niet of niet goed functioneren van software zonder dat aan het gebrek een gebruikershandeling ten grondslag ligt. Een voorbeeld hiervan is het vastlopen van de computer door een softwarefout. Van *functionele* gebreken is sprake wanneer de software technisch wel functioneert, maar functioneel niet doet wat de gebruiker daarvan verwachtte. De uitkomsten van het systeem zijn voor de gebruiker bijvoorbeeld niet bruikbaar (genoeg) c.q. voldoen niet aan wettelijke vereisten. Er is tenslotte sprake van *belevingsgebreken* wanneer de software technisch en functioneel goed functioneert maar de gebruiker daar andere verwachtingen van had. Deze belevingsgebreken zijn soms terug te voeren op interpretatieverschillen ten aanzien van de overeengekomen specificaties. Een afnemer kan de software bijvoorbeeld niet gebruiksvriendelijk vinden. De beleving kan ook de uitleg van het afgesloten contract betreffen, bijvoorbeeld als de leverancier de wel werkende software niet verder doorontwikkelt zodat onderhoud op termijn onmogelijk is.

De perspectieven gecombineerd

11. De twee door mij onderkende perspectieven kunnen helpen om ‘guidance’ te hebben bij het beoordelen van de vraag of softwaresystemen voldoen. Zo zullen technische gebreken juridisch snel tot een tekortkoming leiden en is de vraag over welke onderwerpen partijen bij de totstandkoming van de overeenkomst hebben gecommuniceerd minder van belang. Bij functionele gebreken is het wel van belang of de leverancier op de hoogte was of moest zijn van de toepassing die de gebruiker aan het softwaresysteem wilde geven. Het eerdergenoemde geval Exact Software Nederland/Brandmeester's laat zien dat de leverancier in dat geval verantwoordelijk is voor de geschiktheid van het product voor de toepassing die de klant voor ogen heeft. Maar als de klant standaard softwaresystemen *off-the-shelf* aanschaft¹⁵ dan is de betrokkenheid van de leverancier beperkt en zullen functionele gebreken eerder voor rekening van die klant blijven. Deze had zich in dat geval beter moeten informeren over de eigenschappen van het standaardproduct. Is het de bedoeling het standaardstelsel aan te passen en met maatwerk uit te breiden, dan vind ik de redenering van het Hof Amsterdam in de geciteerde zaak Waterdrinker/SAP overtuigend.

10 Hof Amsterdam 14 februari 2012, IT 688, randnummer 3.13. “Daarbij dient te worden bedacht dat de overeenkomst tussen partijen tot meer verplicht dan alleen de oplevering van een computersysteem dat aan de overeengekomen eisen voldoet, maar tevens (aan beide zijden) inspanningsverbintenissen meebrengt om de ontwikkeling en implementatie van het systeem zo goed mogelijk te laten verlopen en (aan de zijde van SAP) de verplichting om de afspraken over de (maximale) financiële vergoeding na te komen”.

11 Hof 's-Hertogenbosch 3 november 2015, ECLI:NL:GHSHE:2015:4428.

12 Hof 's-Hertogenbosch 17 februari 2015, ECLI:NL:GHSHE:2015:480.

13 Rb. Rotterdam 14 augustus 2017, ECLI:NL:RBROT:2017:6180.

14 Mr. W.F.R. Rinzema, ‘Kwaliteit en software: een goede zaak’, *Computerrecht* 2012/40. Zie ook mr. W.F.R. Rinzema & F.B. Melis, ‘Hoe kan de kwaliteit van ICT systemen juridisch meetbaar worden gemaakt?’, *Computerrecht* 2014/150.

15 Zoals de aanschaf van het Microsoft Office-pakket.

Belevingsproblemen zullen bij standaardsoftware niet snel tot juridische tekortkomingen leiden omdat de functionaliteit van de software simpelweg een gegeven is. Dit kan ook gelden bij standaardsoftware met maatwerk aanpassingen, omdat de keuze van het standaardpakket doorgaans aan de basis ligt van het IT-project. Die basisfunctionaliteit is leidend voor de betrokken partijen en een van de doelen van het project is geen of weinig aanpassingen aan de software. Ook de minder aantrekkelijke kanten van het product zijn daardoor vaak een gegeven. Bij maatwerksoftware zal een belevingsprobleem moeten worden beoordeeld op basis van de redelijke verwachtingen die de opdrachtgever van de software mocht hebben. In dat kader zijn zowel de kennis die de leverancier heeft of moet hebben van de eisen en wensen van zijn opdrachtgever van belang als de informatie-uitwisseling tussen de partijen.¹⁶

12. Terugkerend naar de constatering van Van der Putt over het veelvuldig falen van IT-projecten rijst de vraag of normering gewenst is. Met 'normering' bedoel ik dat de vraag of een IT-prestatie van voldoende kwaliteit is, niet alleen wordt beoordeeld op basis van de omstandigheden van het geval, maar met name op grond van algemeen geldende normen en criteria. Door middel van diverse publicaties heb ik daarvoor gepleit en heb ik verwezen naar de ISO 25010 norm die op dit vlak grote relevantie kan hebben. De kern van mijn betoog is dat gezien de eminente rol die softwaresystemen in de huidige maatschappij hebben, de kwaliteit daarvan voorspelbaar moet zijn. De ISO 25010 norm stelt immers duidelijke criteria die zowel vanuit het perspectief van de gebruiker als vanuit het perspectief van IT-systemen zijn opgesteld om 'kwaliteit' meetbaar te maken. Hierbij moet wel worden opgemerkt dat ISO 25010 de relevante kaders noemt en dat het aan de partijen is die kaders (contractueel) in te vullen.¹⁷ Enkel verwijzing naar die norm is dus niet voldoende.

Mr. W.F.R. Rinzema

Computerrecht 2020/86

Afdeling bestuursrechtspraak van de Raad van State
22 januari 2020, nr. 201901989/1/A3
(Mr. H.G. Sevenster)
m.nt. mr. dr. A. Drahmman¹

(Art. 6:11 Awb; art. 20 Wet elektronische publicaties)

Gst. 2020/58
ECLI:NL:RVS:2020:175

Verschoonbare termijnoverschrijding. E-mailservice van www.overheid.nl.

Uitspraak op het hoger beroep van:
[appellant A] en [appellant B], wonend te Amsterdam, tegen de uitspraak van de rechtbank Amsterdam van 29 januari 2019 in zaak nr. 18/4116 in het geding tussen: [appellanten] en het college van burgemeester en wethouders van Amsterdam.

Procesverloop

Bij besluit van 14 december 2017 heeft het college een vergunning verleend aan [vergunninghouder] voor het wijzigen van de samenstelling van de woonruimtevoorraad door het vormen van vijf woningen op de tweede, derde en vierde verdieping van het pand aan de [locatie 1] (hierna: de vergunning). Bij besluit van 15 mei 2018 heeft het college het door [appellanten] daartegen gemaakte bezwaar niet-ontvankelijk verklaard. Bij uitspraak van 29 januari 2019 heeft de rechtbank het door [appellanten] daartegen ingestelde beroep ongegrond verklaard. Deze uitspraak is aangehecht. Tegen deze uitspraak hebben [appellanten] hoger beroep ingesteld. [vergunninghouder] heeft een schriftelijke uiteenzetting gegeven. De Afdeling heeft de zaak ter zitting behandeld op 12 november 2019, waar [appellanten], vertegenwoordigd door mr. D. op de Hoek, advocaat te Amsterdam, zijn verschenen. Voorts is ter zitting [vergunninghouder] gehoord.

Overwegingen

Inleiding

1. [appellanten] zijn eigenaar van de woning aan de [locatie 2] te Amsterdam. Voor de woningen op de tweede, derde en vierde verdieping boven de woning van [appellanten] is vergunning verleend voor het vormen van

¹⁶ Zie in dit kader bijvoorbeeld P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', *Computerrecht* 2018/4.

¹⁷ Zo noemt de norm 'Maintainability' als één van de kwaliteitscriteria en vermeldt de norm subcriteria om duidelijk te maken wat deze term inhoudt, namelijk 'Modularity', 'Reusability', 'Analysability', 'Modifiability' en 'Testability'. Hoewel deze subcriteria worden toegelicht dient de concrete invulling door partijen plaats te vinden.

¹ Annemarie Drahmman is universitair hoofddocent aan de afdeling staats- en bestuursrecht van de Universiteit Leiden.

vijf woningen. [appellanten] hebben niet binnen de bezwaartermijn bezwaar aangetekend tegen de verlening van deze vergunning.
[...]

Hoger beroep

3. [appellanten] betogen dat de termijnoverschrijding in bezwaar verschoonbaar is. Zij hebben erop vertrouwd dat zij door aanmelding bij de berichtenservice van www.overheid.nl bericht zouden krijgen van de verlening van de vergunning. Zij stellen dat niet is gebleken dat zij zich niet juist hebben aangemeld voor de berichtenservice van www.overheid.nl. Daarnaast is ten onrechte geoordeeld dat de berichtenservice enkel een serviceproduct is waaraan geen rechten kunnen worden ontleend. [appellanten] hebben er gerechtvaardigd op mogen vertrouwen dat zij met de aanmelding voor de berichtenservice op de hoogte zouden worden gehouden van de vergunningverlening. Het betreft een van overheidswege beheerde website, waarbij de gemeente Amsterdam is aangesloten. De website wekt de indruk dat deze bij aanmelding een volledig beeld geeft van de besluiten van de daarbij aangesloten overheidslichamen. Het college gaat daar zelf ook van uit zo blijkt uit de e-mail van het college van 22 maart 2018. Daarin stelt het college dat je niet meer zelf hoeft te gaan zoeken naar publicaties als je je aanmeldt voor de berichtenservice. Het oordeel van de rechtbank dat de toezegging in de e-mail van 22 maart 2018 niet onvoorwaardelijk is omdat in de e-mail wordt gezegd dat op de website de opties moeten worden aangevinkt waarvan men op de hoogte wil worden gehouden, gaat hier niet op omdat [appellanten] alle opties voor vergunningen hebben aangevinkt. [appellanten] hebben e-mails van de berichtenservice overgelegd waaruit blijkt dat zij wel notificaties kregen van de berichtenservice over andere vergunningen en besluiten. Het college heeft ter zitting bij de rechtbank gezegd dat als wel alle opties waren aangevinkt de termijnoverschrijding verschoonbaar zou zijn. Desondanks is niet nagegaan of dat het geval was, aldus [appellanten]. Het college heeft hen daarnaast ten onrechte niet gehoord, zodat zij hun standpunt omtrent de verschoonbaarheid niet hebben kunnen toelichten.

3.1. De bezwaartermijn liep tot en met 26 januari 2018. Het bezwaarschrift van [appellanten] is door het college op 13 februari 2018 ontvangen. [appellanten] betwisten niet dat dit buiten de bezwaartermijn is. Het besluit van 14 december 2017 is op 20 december 2017 in de Staatscourant gepubliceerd en bekendgemaakt op www.overheid.nl en geplaatst op www.redactie-bekendmakingen.amsterdam.nl. Bij de berichtenservice op www.overheid.nl kun je je aanmelden voor de service "berichten over uw buurt". De berichten zijn verdeeld over vier hoofdcategorieën: Rondom een adres, Voorlichting, Bestemmingsplannen en Voorschriften en beleid. Onder de categorie Rondom een adres vallen onder andere de subcategorieën onttrek-

kingsvergunning, splitsingsvergunning en gebruiksvergunning. Onder de categorie Voorlichting vallen volgens de website berichten over voorlichting voor de hele gemeente over bijvoorbeeld openingstijden, huisafval, inspraak en verkiezingen.

In het advies van de bezwaarschriftencommissie dat in het besluit op bezwaar is overgenomen, staat dat de bekendmaking van de vergunning onder de subcategorie "overig" in de hoofdcategorie "Voorlichting" is gepubliceerd.

3.2. Zoals de Afdeling eerder heeft overwogen in haar uitspraak van 13 december 2017, ECLI:NL:RVS:2017:3419 brengt de enkele omstandigheid dat [appellanten] zich hebben aangemeld bij de e-mailservice van www.overheid.nl niet mee dat zij er gerechtvaardigd op mochten vertrouwen dat zij op de hoogte zouden worden gehouden van alle voor hen mogelijk relevante besluiten, zoals in dit geval het verlenen van een woningvormingsvergunning in de omgeving van hun perceel. Bedoelde e-mailservice laat onverlet dat het tot de eigen verantwoordelijkheid van [appellanten] behoort om er zorg voor te dragen dat zij op de hoogte geraken van verlening van vergunningen. Er kan echter sprake zijn van bijzondere omstandigheden op grond waarvan [appellanten] er rechtens op mochten vertrouwen dat zolang geen daartoe strekkend e-mailbericht van www.overheid.nl is ontvangen nog geen vergunning is verleend.

[appellanten] hebben stukken overgelegd waarmee aanmerkelijk is gemaakt dat alle opties voor kennisgeving van vergunningen rondom hun adres in de berichtenservice zijn aangevinkt. Het college heeft het tegendeel niet aangevoerd, terwijl het ter zitting bij de rechtbank heeft gesteld dat als alles aangevinkt was, de termijnoverschrijding verschoonbaar is. Dit strookt met de mededeling van het college aan [appellanten] dat je niet meer zelf hoeft te gaan zoeken naar publicaties als je je aanmeldt voor de berichtenservice. Dat de bekendmaking van de vergunning is geplaatst in de categorie "overig" onder de hoofdcategorie "Voorlichting" past niet in de systematiek van de categorieën van de berichtenservice nu de bekendmakingen van vergunningen op grond van de Huisvestingsverordening onder de hoofdcategorie "Rondom een adres" staan vermeld. Het kan [appellanten] daarom niet worden aangerekend dat zij de categorie "overig" onder "Voorlichting" niet hebben aangevinkt. Gelet op het voorgaande is de termijnoverschrijding verschoonbaar en heeft het college het bezwaar van [appellanten] ten onrechte niet-ontvankelijk verklaard..

Het betoog van [appellanten] slaagt.

4. Het hoger beroep is gegrond. De aangevallen uitspraak dient te worden vernietigd. Doende hetgeen de rechtbank zou behoren te doen, zal de Afdeling het beroep tegen het besluit van 15 mei 2018 van het college alsnog gegrond verklaren. Dat besluit komt voor vernietiging in aanmerking. Het college dient opnieuw te beslissen op het bezwaar met inachtneming van deze uitspraak.

5. Het college dient op na te melden wijze tot vergoeding van de proceskosten te worden veroordeeld.

Beslissing

De Afdeling bestuursrechtspraak van de Raad van State:

- I. verklaart het hoger beroep gegrond;
- II. vernietigt de uitspraak van de rechtbank Amsterdam van 29 januari 2019 in zaak nr. 18/4116;
- III. verklaart het bij de rechtbank ingestelde beroep gegrond;
- IV. vernietigt het besluit van het college van burgemeester en wethouders van Amsterdam van 15 mei 2018, kenmerk Z-17-31237-uit-18-63642;
- V. veroordeelt het college van burgemeester en wethouders van Amsterdam tot vergoeding van bij [appellant A] en [appellant B] in verband met de behandeling van het beroep en hoger beroep opgekomen proceskosten tot een bedrag van € 2100,00 (zegge: tweeduizend honderd euro), geheel toe te rekenen aan door een derde beroepsmatig verleende rechtsbijstand;
- VI. gelast dat het college van burgemeester en wethouders van Amsterdam aan [appellant A] en [appellant B] het door hen betaalde griffierecht ten bedrage van € 429,00 (zegge: vierhonderdnegenentwintig euro) voor de behandeling van het beroep en hoger beroep vergoedt.

[...]

Noot

1. De appellanten in deze procedure wonen in een appartement in Amsterdam. Het college van burgemeester en wethouders (hierna: 'college') verleent een vergunning om de drie verdiepingen boven de woning van appellanten te wijzigen in vijf woningen. Tegen een dergelijk besluit kan op grond van de Algemene wet bestuursrecht (hierna: 'Awb') binnen zes weken een bezwaarschrift worden ingediend. Appellanten hebben niet binnen deze bezwaartermijn bezwaar aangetekend. Dat betekent dat het bezwaarschrift niet-ontvankelijk is, tenzij de termijnoverschrijding verschoonbaar is (art. 6:11 Awb). Volgens appellanten is dit het geval omdat zij erop vertrouwden dat zij door aanmelding bij de e-mailservice van www.overheid.nl bericht zouden krijgen van de verlening van de vergunning. Deze uitspraak is een annotatie waard, omdat de Afdeling bestuursrechtspraak van de Raad van State (hierna: de 'Afdeling') tot het oordeel komt dat sprake is van bijzondere omstandigheden die de termijnoverschrijding verschoonbaar maakt.

2. Op grond van art. 3:41 Awb wordt een vergunning bekendgemaakt door toezending aan de aanvrager van de vergunning. Belanghebbenden kunnen binnen zes weken vanaf de dag na deze bekendmaking bezwaar maken. Zij moeten dan uiteraard wel kennis kunnen nemen van het verlenen van de vergunning. Daarom zijn steeds meer bestuursorganen er in de loop der jaren toe overge-

gaan om dergelijke vergunningen ook mede te delen op de gemeentelijke websites en de website www.overheid.nl. Deze aanvullende publicatie is echter geen wettelijke verplichting en niet alle gemeenten maken hun besluiten bekend via www.overheid.nl.² Zowel gemeentelijke websites als www.overheid.nl bieden vaak daarnaast nog de mogelijkheid een e-mailattendering aan te maken: een burger kan aangeven een e-mail te willen krijgen als een vergunning wordt verleend binnen een bepaalde afstand van de woning van die burger.³ Deze e-mailservice wordt niet door de Awb gereguleerd. In deze uitspraak staat deze berichtenservice van www.overheid.nl centraal. Bij deze berichtenservice kan men zich aanmelden voor de service "berichten over uw buurt". De berichten zijn verdeeld over vier hoofdcategorieën: "Rondom een adres", "Voorlichting", "Bestemmingsplannen" en "Voorschriften en beleid". Onder de categorie "Rondom een adres" vallen onder andere de subcategorieën "onttrekkingsvergunning", "splitsingsvergunning" en "gebruiksvergunning". Onder de categorie "Voorlichting" vallen volgens de website berichten over voorlichting voor de hele gemeente over bijvoorbeeld openingstijden, huisafval, inspraak en verkiezingen.

3. In deze uitspraak was aan de wettelijke bekendmakingseis van art. 3:41 Awb voldaan. Het besluit was bovendien niet alleen bekendgemaakt aan de aanvrager, maar ook nog in de Staatscourant gepubliceerd en op www.overheid.nl en www.redactie-bekendmakingen.amsterdam.nl geplaatst. Door deze bekendmakingen hadden appellanten kennis kunnen nemen van de vergunningverlening. Waarom is de termijnoverschrijding dan toch verschoonbaar? Dit komt doordat het college de vergunning via de verkeerde (sub)categorie van de berichtenservice bekend heeft gemaakt. De vergunning is namelijk bekendgemaakt onder de subcategorie "overig" in de hoofdcategorie "Voorlichting". Appellanten hebben stukken overgelegd waarmee aannemelijk is gemaakt dat zij alle opties voor kennisgeving van vergunningen rondom hun adres in de berichtenservice hebben aangevinkt. Dat de bekendmaking van de vergunning is geplaatst in de categorie "overig" onder de hoofdcategorie "Voorlichting" past volgens de Afdeling niet in de systematiek van de categorieën van de berichtenservice nu de bekendmakingen van vergunningen op grond van de Huisvestingsverordening onder de hoofdcategorie "Rondom een adres" staan vermeld. Het kan appellanten daarom niet worden aangerekend dat zij de categorie "overig" onder "Voorlichting" niet hebben

² Op dit moment ligt het wetsvoorstel Wet elektronische publicaties bij de Eerste Kamer (*Kamerstukken I* 2019/20, 35218, nr. A). Met dit wetsvoorstel wordt de ontwikkeling om algemene bekendmakingen, mededelingen en kennisgevingen te publiceren in de officiële elektronische publicatiebladen geformaliseerd en gestructureerd. Zie hierna onder punt 7 van deze annotatie.

³ Deze e-mailservice is daarmee een ander instrument dan de Berichtenbox van MijnOverheid.nl waarover Van Kaam heeft geschreven in de vorige aflevering van *Computerrecht* (S. van Kaam, 'Berichtenbox van MijnOverheid: burger voldoende bereikbaar voor bekendmaking besluiten via de elektronische weg?', *Computerrecht* 2020/44).

aangevinkt. Daarom is de termijnoverschrijding verschoonbaar en heeft het college het bezwaar van appellanten ten onrechte niet-ontvankelijk verklaard.

4. Als ik het goed zie dan is de omstandigheid dat het bestuursorgaan de vergunning via de verkeerde categorie bekend heeft gemaakt doorslaggevend om de termijnoverschrijding verschoonbaar te achten: als een burger zich attendeert op e-mails over vergunningverlening dan moet die burger erop kunnen vertrouwen dat vergunningen ook via die categorie bekend worden gemaakt en niet via de categorie "Voorlichting". Met deze redenering kan ik mij geheel verenigen. Ik vind het een redelijke bewijslastverdeling dat als een bestuursorgaan beslist om gebruik te maken van de e-mailservice en de burger kan aantonen dat hij zich heeft aangemeld voor die e-mailservice, dat dan van het bestuursorgaan mag worden verwacht dat het op juiste wijze van die e-mailservice gebruikmaakt en dat bij een onjuist gebruik ervan dit niet aan de burger wordt tegengeworpen.

5. Opvallend is echter dat de Afdeling in deze uitspraak expliciet verwijst naar een eerdere uitspraak uit 2017 en herhaalt dat de e-mailservice onverlet laat dat het tot de eigen verantwoordelijkheid van appellanten behoort om er zorg voor te dragen dat zij op de hoogte geraken van verlening van vergunningen. Kennelijk hadden appellanten in dit geval aan deze eis voldaan door zich aan te melden voor de e-mailservice en was het niet nodig om in aanvulling daarop de gemeentelijke website te controleren. Ik vraag mij af of de hier gepubliceerde uitspraak daarmee een andere, burgervriendelijkere lijn inzet dan in de uitspraak uit 2017. In die uitspraak uit 2017 oordeelde de Afdeling dat: *"de enkele omstandigheid dat [appellant] zich heeft aangemeld bij de e-mailservice van www.overheid.nl niet mee [brengt] dat hij er gerechtvaardigd op mocht vertrouwen dat hij op de hoogte zou worden gehouden van alle voor hem mogelijk relevante besluiten [...] in de omgeving van zijn perceel [...]. Bedoelde e-mailservice laat onverlet dat het tot de eigen verantwoordelijkheid van [appellant] behoort om er zorg voor te dragen dat hij op de hoogte geraakt van de voortgang van de aanvraag om vergunning. De gevolgen van zijn keuze om daarbij te vertrouwen op de e-mailservice van www.overheid.nl komen voor zijn risico. De omstandigheid dat er problemen waren met de technische koppeling tussen de gemeentelijke website en www.overheid.nl met als gevolg dat in 2015, onder meer in de periode waarin de door [appellant] bestreden omgevingsvergunning is verleend, gedurende lange tijd besluiten van de deelgemeente niet zijn doorgezet naar www.overheid.nl, maakt dat niet anders. Dat het bij Vorm, een medewerker van de afdeling bouw- woningtoezicht, bekend was dat hij bezwaar had tegen het bouwwerk waarop de verleende omgevingsvergunning ziet, ontsloeg [appellant] niet van de verplichting om er zelf voor zorg te dragen zich op de hoogte te houden van het verloop van de vergunning door het raadplegen van de gemeentelijke website www.amsterdam.nl."* De Afdeling legde hiermee de lat

voor de burger erg hoog en Wertheim schreef dan ook destijds al een kritische annotatie bij deze uitspraak.⁴

6. Mijns inziens had het in lijn met deze uitspraak uit 2017 gelegen als de Afdeling in de hier gepubliceerde uitspraak had geoordeeld dat het aanmelden voor een e-mailservice de burger niet ontslaat van de verplichting om zelf nog de gemeentelijke website te raadplegen. In ieder geval zie ik niet waarom een technische storing (waardoor de e-mailservice in het geheel niet functioneert) in 2017 wel aan de burger kon worden tegengeworpen en een verkeerde categorie aanduiding (waardoor de e-mailservice ook niet goed functioneert) in 2020 niet. Nu de Afdeling in de hier geannoteerde uitspraak niet aangeeft thans anders van oordeel te zijn, kan niet met zekerheid worden geconcludeerd dat de Afdeling een andere lijn heeft ingezet. De hier gepubliceerde uitspraak past echter in een bredere tendens waarbij in de jurisprudentie van de Afdeling een verschuiving plaatsvindt van het bestuurlijke naar het burgerperspectief. Zo heeft de Afdeling in 2019 een nieuwe jurisprudentielijn ontwikkeld bij de beoordeling van een beroep op het vertrouwensbeginsel. In het kader van de vraag of een toezegging aan het bevoegde bestuursorgaan kan worden toegerekend, wordt nu meer waarde gehecht aan het burgerperspectief: de Afdeling legt minder de nadruk op de precieze juridische bevoegdheidsverdeling, maar beoordeelt of de betrokkene op goede gronden mocht veronderstellen dat degene die de toezegging heeft gedaan de opvatting van het bevoegde orgaan vertolkte. De hier gepubliceerde uitspraak sluit hier goed op aan, omdat met de mogelijkheid van een e-mailservice bij redelijk denkende burgers redelijkerwijs de indruk wordt gewekt dat zij geattendeerd zullen worden op vergunningverlening rondom hun woning. Deze uitspraak zie ik dan ook als een stap in de goede richting.

7. Zoals ik onder punt 2 van deze annotatie stelde, wordt de e-mailservice niet door de Awb gereguleerd. Daarom wijs ik ten slotte nog op het wetsvoorstel voor de Wet elektronische publicaties (Wep). Dit wetsvoorstel ligt nu bij de Eerste Kamer en zou op 1 januari 2021 in werking moeten treden. Kort samengevat bepaalt dit wetsvoorstel dat alle overheden hun algemene bekendmakingen en kennisgevingen moeten doen in een officieel elektronisch publicatieblad dat op www.overheid.nl wordt gepubliceerd en dat iedereen met een account op MijnOverheid per e-mail geattendeerd zal worden op kennisgevingen met betrekking tot de directe woonomgeving. In de memorie van toelichting bij dit wetsvoorstel wordt, onder verwijzing naar de Afdelingsuitspraak uit 2017, benadrukt dat er geen opschorting van de bezwaartermijn plaatsvindt als een mededeling of kennisgeving ten onrechte niet heeft geleid tot een attenderings-e-mail, omdat de attendering een service blijft die de burger niet ontslaat van zijn eigen verantwoordelijkheid.⁵ Gelet op de hier gepubliceerde uit-

⁴ ABRvS 13 december 2017, ECLI:NL:RVS:2017:3419, AB 2018/133, m.nt. R.S. Wertheim.

⁵ Kamerstukken II 2018/19, 35218, nr. 3, p. 47-48.

spraak waarin de Afdeling de termijnoverschrijding wel verschoonbaar acht, zou de wetgever er verstandig aan doen om de in het wetsvoorstel gemaakte keuze nog eens te heroverwegen.⁶

Mr. dr. A. Drahmman

Computerrecht 2020/87

Rechtbank Den Haag 5 februari 2020

nr. C-09-550982-HA ZA 18-388

(Mrs. M.C. Ritsema van Eck-van Drempt, J.S. Honée en H.J. van Harten)

m.nt. mr. S. van Schendel¹

(Art. 8 EVRM; art. 64 en 65 Wet SUWI)

RAV 2020/35

TRA 2020/49

ECLI:NL:RBDHA:2020:865

De rechtbank komt tot het oordeel dat de SyRI-wetgeving in haar huidige vorm de toets van artikel 8 lid 2 EVRM niet doorstaat. De rechtbank heeft de doelen van de SyRI-wetgeving, namelijk het voorkomen en bestrijden van fraude in het belang van het economisch welzijn, afgezet tegen de inbreuk op het privéleven die de wetgeving maakt. Volgens de rechtbank voldoet de wetgeving niet aan de 'fair balance' die het EVRM vereist om te kunnen spreken over een voldoende gerechtvaardigde inbreuk op het privéleven. De wetgeving is wat betreft de inzet van SyRI onvoldoende inzichtelijk en controleerbaar.

Vonnis in de zaak van:

in de zaak van

1. **NEDERLANDS JURISTEN COMITÉ VOOR DE MENSENRECHTEN** te Leiden,
 2. **STICHTING PLATFORM BESCHERMING BURGERRECHTEN** te Amsterdam,
 3. **STICHTING PRIVACY FIRST** te Amsterdam,
 4. **STICHTING KOEPEL VAN DBC-VRIJE PRAKTIJKEN** te Amsterdam,
 5. **LANDELIJKE CLIËNTENRAAD** te Den Haag,
 6. **[eisende partij sub 6]** te [plaats 1],
 7. **[eisende partij sub 7]** te [plaats 2],
- eisers,
- en
- FEDERATIE NEDERLANDSE VAKBEWEGING** te Utrecht,

⁶ Vgl. ook het voorgestelde art. 2:22 in het wetsvoorstel Wet modernisering elektronisch bestuurlijk verkeer (*Kamerstukken II* 2018/19, 35261, nr. 2) waarin wordt bepaald dat een termijnoverschrijding niet wordt tegengehouden als de e-mailattendering van de plaatsing van een elektronisch bericht in een berichtenbox niet is verzonden.

¹ Sascha van Schendel is werkzaam als promovenda bij het 'Tilburg Institute for Law, Technology and Society' (TILT) van Tilburg University.

interveniente aan de zijde van eisers, advocaat mr. A.H. Ekker te Amsterdam, tegen

STAAT DER NEDERLANDEN zetelende te Den Haag, gedaagde,

Eisers worden hierna gezamenlijk ook NJCM c.s. genoemd en afzonderlijk respectievelijk het NJCM, het Platform Bescherming Burgerrechten, Privacy First, de Koepel van DBC-Vrije Praktijken, de Landelijke Cliëntenraad, [eisende partij sub 6], [eisende partij sub 7]. Interveniente wordt FNV genoemd. Gedaagde wordt de Staat genoemd.

[...]

3. De feiten

3.1. Het Systeem Risicoindicatie (hierna: SyRI) is een wettelijk instrument dat de overheid gebruikt ter voorkoming en bestrijding van fraude op het terrein van de sociale zekerheid en inkomensafhankelijke regelingen, de belasting- en premieheffing en de arbeidswetten. Het gaat volgens de wetgever om technische infrastructuur en de bijbehorende procedures waarmee in een beveiligde omgeving anoniem data kunnen worden gekoppeld en geanalyseerd, zodat risicomeldingen kunnen worden genereerd.

[...]

3.3. Het instrument wordt ingezet door de Minister op verzoek van bepaalde overheidsinstanties of andere instanties met een publieke taak. Dit zijn op dit moment de colleges van burgemeester en wethouders (hierna: de gemeenten), het UWV, de SVB, de rijksbelastingdienst (hierna: de Belastingdienst), de Immigratie- en Naturalisatiedienst (hierna: de IND) en toezichthouders, zoals de Inspectie SZW. Die instanties kunnen een samenwerkingsverband aangaan waarin zij gegevens uitwisselen. Met de inzet van SyRI worden bestanden waarover die (overheids)instanties beschikken gestructureerd gekoppeld om samenhangende misstanden op de genoemde terreinen te kunnen onderkennen en om de pakkans te verhogen.

4. De SyRI-wetgeving

4.1. De Wet SUWI is met ingang van 1 januari 2014 gewijzigd om de inzet van SyRI wettelijk te verankeren. De voorwaarden voor die inzet zijn nader bepaald in het Besluit Wet SUWI. SyRI heeft nu een wettelijke basis in de artikel 65 Wet SUWI in samenhang gezien met artikel 64 Wet SUWI en hoofdstuk 5a van het Besluit SUWI.

[...]

4.8. Artikel 65 Wet SUWI biedt vervolgens de wettelijke grondslag voor de verwerking van de genoemde noodzakelijke gegevens in SyRI door de Minister voor het uitvoeren van risicoanalyses. Dit artikel bevat ook bepalingen over het doen van een risicomelding, geheimhouding, bewaring van het gegeven dat een risicomelding heeft plaatsgevonden, gebruikmaking van een risi-

comelding, terugkoppeling en verwijdering. Ten slotte is bepaald welke nadere regels bij algemene maatregel van bestuur in ieder geval worden gesteld. Aan dit laatste is uitvoering gegeven met het Besluit SUWI, in het bijzonder met hoofdstuk 5a van dat besluit.

[...]

4.14. Er is een register risicomeldingen met het oog op deze informatieverstrekking aan de deelnemende (overheids)instanties en het OM en de politie en om degene op wie een risicomelding betrekking heeft op aanvraag te informeren. Betrokkenen worden niet na afloop van een onderzoek afzonderlijk geïnformeerd over de risicomeldingen die in het register worden verwerkt (artikel 5a.5 Besluit SUWI).

[...]

4.23. Volgens de nota van toelichting bij het Besluit SUWI dienen de indicatoren en het te hanteren risicomodel helder benoemd te zijn en zou zonder deze bepaling het koppelen van de gegevensbestanden kunnen leiden tot een "fishing expedition" en zelfs tot willekeur. Volgens de Minister wordt op deze manier recht gedaan aan het principe "select before you collect". Volgens het Besluit SUWI is een indicator een gegeven dat de aanwezigheid van een bepaalde omstandigheid aannemelijk maakt. Onder risicomodel wordt een model verstaan dat bestaat uit vooraf bepaalde indicatoren en dat aangeeft of sprake is van een verhoogd risico op onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, belasting- en premiefraude of het niet naleven van arbeidswetten (artikel 1.1. sub y, respectievelijk artikel 1.1. sub aa Besluit SUWI).

5. Het geschil

5.1. NJCM c.s. vordert bij voor zover mogelijk uitvoerbaar bij voorraad te verklaren vonnis:

- I. te verklaren voor recht dat toepassing van de artikelen 64 en 65 Wet SUWI en hoofdstuk 5a van het Besluit SUWI onverenigbaar is met hoger recht, in het bijzonder met artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden (hierna: EVRM), artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest) en/of artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke Rechten (hierna: IVBPR); en/of artikel 6 en/of artikel 13 van het EVRM; en/of artikel 5, 6, 13, 14, 22 en/of 28 van de AVG, althans met de daarmee corresponderende artikelen uit de Wbp, althans, [...]
- III. te verklaren voor recht dat de verwerking van persoonsgegevens die plaatsvindt in het kader van, door middel van en/of ten behoeve van de inzet van, SyRI, in het bijzonder de onderlinge uitwisseling van persoonsgegevens door bestuursorganen (waaronder de Belastingdienst), de verstrekking van persoonsgegevens aan de Minister (waaronder door de Belastingdienst), de verstrekking

van persoonsgegevens aan het IB, de verwerking van persoonsgegevens door het IB, waaronder profilering, de verstrekking van persoonsgegevens door het IB aan de Minister, het doen van risicomeldingen en/of het opnemen van (informatie over) meldingen in het meldingenregister, onrechtmatig is wegens strijd met artikel 8 EVRM, artikel 7 en 8 Handvest en/of artikel 17 IVBPR; en/of artikel 6 en/of artikel 13 EVRM; en/of artikel 5, 6, 13, 14, 22 en/of 28 AVG en/of de daar mee corresponderende artikelen uit de Wbp;

- IV. de artikelen 64 en 65 Wet SUWI en hoofdstuk 5a Besluit SUWI, althans de onderdelen daarvan zoals door de rechtbank onverenigbaar geacht met hoger recht op grond van vordering I en/of II, althans de onderdelen zoals door de rechtbank in goede justitie onverenigbaar geacht met hoger recht, buiten werking te stellen althans onverbindend te verklaren, althans te bepalen dat deze buiten toepassing dienen te worden gelaten, eventueel onder oplegging van een voorwaarde;

5.2. NJCM c.s. legt aan haar vorderingen onrechtmatig handelen van de Staat ten grondslag. [...]

6. De beoordeling: inleidend

6.1. NJCM c.s. beoogt met deze procedure een 'halt' toe te roepen aan het gebruik van SyRI. Zij meent dat met SyRI inbreuk wordt gemaakt op mensenrechten. NJCM c.s. heeft ter zitting toegelicht dat zij vooral voor ogen heeft dat de SyRI-wetgeving onverbindend wordt verklaard. De SyRI-wetgeving maakt volgens NJCM c.s. een ongeoorloofde inbreuk op de persoonlijke levenssfeer, in het bijzonder het recht op respect voor het privéleven. Zij acht de SyRI-wetgeving niet met voldoende waarborgen omgeven. [...]

6.6. Op grond van artikel 8 EVRM rust op Nederland als lidstaat bij de toepassing van nieuwe technologieën een bijzondere verantwoordelijkheid om de juiste balans te vinden in de weging van enerzijds de voordelen die aan het gebruik van die technologieën verbonden zijn in het kader van de voorkoming en bestrijding van fraude en anderzijds de inmenging die dat in de uitoefening van het recht op respect voor het privéleven kan opleveren. De wetgeving moet uit het oogpunt van bescherming van het recht op respect voor het privéleven, waaronder het recht op bescherming van persoonsgegevens valt, een voldoende effectief kader bieden waarmee alle in het geding zijnde belangen inzichtelijk en controleerbaar tegen elkaar kunnen worden afgewogen. Eenieder moet op grond van de wetgeving de redelijke verwachting kunnen hebben dat in het geval van de inzet van SyRI zijn privéleven voldoende wordt gerespecteerd. Hieraan voldoet de SyRI-wetgeving naar het oordeel van de rechtbank niet.

6.7. De SyRI-wetgeving voldoet niet aan de in artikel 8 lid 2 EVRM gestelde eis dat de inmenging in de uitoefening van het recht op respect voor het privéleven noodzakelijk is in een democratische samenleving, dat wil zeggen noodzakelijk, evenredig (proportioneel) en subsidiair in

relatie tot het beoogde doel. De rechtbank zet de inhoud van de SyRI-wetgeving in het licht van de doelen die deze wetgeving dient af tegen de inbreuk op het privéleven die de SyRI-wetgeving maakt. Zij is van oordeel dat de wetgeving niet voldoet aan de 'fair balance' (de redelijke verhouding) die op grond van het EVRM moet bestaan tussen het maatschappelijke belang dat de wetgeving dient en de inbreuk op het privéleven die de wetgeving oplevert om te kunnen spreken over een voldoende gerechtvaardigde inbreuk op het privéleven. Daarbij neemt de rechtbank de fundamentele beginselen die ten grondslag liggen aan de bescherming van gegevens op grond van het Unierecht (het Handvest en de AVG) in aanmerking, in het bijzonder de beginselen van transparantie, het doelbindingsbeginsel en het beginsel van dataminimalisatie. Zij oordeelt dat de wetgeving wat betreft de inzet van SyRI onvoldoende inzichtelijk en controleerbaar is. Het is om die reden dat de rechtbank artikel 65 Wet SUWI en hoofdstuk 5a Besluit SUWI bij dit vonnis wegens strijdigheid met artikel 8 lid 2 EVRM onverbindend zal verklaren.

[...]

6.41. De rechtbank zal bij haar beoordeling of de SyRI-wetgeving voldoet aan artikel 8 EVRM de genoemde algemene beginselen van gegevensbescherming uit het Handvest en de AVG betrekken. Oftewel: de rechtbank legt artikel 8 lid 2 EVRM mede uit aan de hand van die beginselen. Er zijn geen aanknopingspunten dat de minimumbescherming van het recht op respect voor het privéleven, waaronder de bescherming van persoonsgegevens valt, op grond van het EVRM minder ver gaat dan de gegevensbescherming die het Handvest en de AVG bieden op grond van de algemene beginselen die daarin zijn bepaald.

6.54. Ten slotte geldt dat de SyRI-wetgeving niet voorziet in een informatieverplichting van degenen van wie de gegevens in SyRI worden verwerkt opdat die betrokkenen in redelijkheid kunnen worden geacht te weten dat zijn of haar gegevens voor die verwerking worden of zijn gebruikt. De SyRI-wetgeving voorziet ook niet in een verplichting om betrokkenen in voorkomend geval afzonderlijk te informeren over het feit dat een risicomelding is gedaan. Er is slechts vooraf een wettelijke verplichting tot bekendmaking van de aanvang van een SyRI-project door publicatie in de Staatscourant en achteraf op aanvraag toegang tot het register van risicomeldingen. [...]

6.70. In hoeverre de wettelijke waarborgen toereikend zijn, hangt volgens het EHRM dus af van de concrete omstandigheden en komt neer op een weging van het geheel van wettelijke waarborgen. De mate waarin en de gedetailleerdheid waarmee waarborgen in de wet moeten zijn vastgelegd, hangt af van de ingrijpendheid van de inmenging.

[...]

6.72. De rechtbank laat – net als het EHRM in die zaak – bij haar beoordeling in het midden of de SyRI-wetgeving voldoende toegankelijk en voorzienbaar is en aldus een voldoende rechtsbasis biedt zoals artikel 8 lid 2

EVRM vereist voor een gerechtvaardigde beperking van het recht op bescherming van de persoonlijke levenssfeer. De rechtbank is van oordeel dat de SyRI-wetgeving in ieder geval onvoldoende waarborgen bevat voor de conclusie dat zij noodzakelijk is in een democratische samenleving in het licht van de doelen die de wetgeving dient, zoals artikel 8 lid 2 EVRM ook vereist. Daarmee doorstaat die wetgeving in haar huidige vorm de toets van artikel 8 lid 2 EVRM niet en is zij derhalve onrechtmatig. De rechtbank acht daartoe het volgende redengevend. [...]

6.75. Partijen twisten erover of sprake is van een 'pressing social need', oftewel of de inmenging voldoet aan een dwingende maatschappelijke behoefte. NJCM c.s. stelt dat dit niet het geval is, waartoe zij van belang acht dat sprake is van een zeer ernstige inmenging in het privéleven van burgers. De Staat heeft daarnaast volgens NJCM c.s. niet aangetoond dat het noodzakelijk is om een zodanig zwaar instrument als SyRI in te zetten voor het in stand houden van het socialezekerheidsstelsel. Zij wijst erop dat de bredere maatschappelijke opvattingen over SyRI negatief, althans op zijn minst terughoudend zijn en dat de SyRI-projecten niets opleveren dus geen effectief middel zijn om fraude te bestrijden.

6.76. De rechtbank verwierpt deze stelling van NJCM c.s. De SyRI-wetgeving streeft op zichzelf een voldoende zwaarwegende doelstelling na om inmenging in het privéleven te rechtvaardigen. Daarbij neemt de rechtbank de hiervoor verwoorde uitgangspunten over wat SyRI is en het effect op het privéleven in het geval de gegevensverwerking in SyRI leidt tot een risicomelding, die de mate en ernst van de inmenging bepalen, in aanmerking (zie hiervoor 6.44 - 6.60). De fraude op het gebied van de sociale zekerheid en de bijstand is omvangrijk: de Staat heeft onweersproken bedragen van 153 miljoen euro aan sociale zekerheidsfraude, respectievelijk een half tot één miljard euro per jaar aan bijstandsfraude genoemd en 135 miljoen euro aan maatschappelijke schade ten gevolge van sociale zekerheidsfraude. Fraudebestrijding heeft daarnaast indirecte effecten, onder meer op de integriteit van het economisch stelsel en het vertrouwen in de financiële instellingen. Mede gelet op de beoordelingsmarge die de nationale autoriteiten hebben, rechtvaardigt de directe en indirecte schade die gemoeid is met fraude op dit terrein de conclusie van de wetgever dat sprake is van een dwingende maatschappelijke behoefte om in het belang van het economisch welzijn van Nederland maatregelen te treffen waarin de SyRI-wetgeving voorziet.

[...]

6.90. Het vorenstaande leidt ertoe dat niet kan worden gecontroleerd hoe de eenvoudige beslisboom, waarover de Staat spreekt, tot stand komt en uit welke stappen deze bestaat. Aldus valt moeilijk in te zien hoe een betrokkene zich kan verweren tegen het gegeven dat ten aanzien van hem of haar een risicomelding is gedaan. Evenzeer valt moeilijk in te zien hoe een betrokkene van wie de gegevens wel in SyRI zijn verwerkt, maar die niet hebben geleid tot een risicomelding, ervan op de hoogte kan zijn dat

zijn of haar gegevens op juiste gronden zijn verwerkt. Dat in deze laatste situatie de gegevens niet hebben geleid tot een risicomelding en bovendien uiterlijk vier weken na analyse moeten zijn vernietigd, doet niet af aan de vereiste transparantie ten aanzien van die verwerking. Het recht op respect voor het privéleven houdt ook in dat een betrokkene in redelijke mate in staat moet worden gesteld zijn of haar gegevens te volgen.

6.91. Het belang van transparantie, met het oog op controleerbaarheid, is mede zwaarwegend omdat aan het gebruik van het risicomodel en de analyse die dat verband wordt verricht het risico verbonden is dat (onbedoeld) discriminerende effecten optreden. De Afdeling advisering wijst in haar hiervoor in 6.46 genoemde advies erop dat het analyseren van grote verzamelingen data, al dan niet met deep learning/zelflerende systemen ontegenzeggelijk nut heeft, maar ook ongewenste resultaten kan hebben, waaronder onterechte uitsluiting of discriminatie. [...]

6.93. Het is juist dat SyRI, tot nu toe alleen is ingezet in zogenoemde 'probleemwijken', zoals de Staat ter zitting ook heeft bevestigd. Dat op zichzelf hoeft niet te impliceren dat die inzet in alle gevallen disproportioneel of anderszins in strijd is met artikel 8 lid 2 EVRM. Gegeven echter de grote hoeveelheden gegevens die in aanmerking komen voor verwerking in SyRI, waaronder ook bijzondere persoonsgegevens, en de omstandigheid dat gebruik wordt gemaakt van risicoprofielen, bestaat wel het risico dat met de inzet van SyRI onbedoeld verbanden worden gelegd op basis van bias, zoals een lagere sociaal economische status of een immigratieachtergrond, zoals NJCM c.s. betoogt.

6.94. Op basis van de SyRI-wetgeving kan niet worden beoordeeld of dit risico voldoende is ondervangen, bij gebrek aan controleerbaar inzicht in de risico-indicatoren en de (werking van) het risicomodel, daaronder begrepen de methode van analyse door de Inspectie SZW. De omstandigheid dat het proces van gegevensverwerking bestaat uit twee fasen en de analyse-eenheid van de Inspectie SZW na de koppeling van de bestanden door het IB de ontsleutelde gegevens toetst op onderzoekswaardigheid, waarbij voorzien is in menselijke controle op *false positives* en *false negatives*, acht de rechtbank daarvoor onvoldoende. De wijze van totstandkoming van de definitieve risicoselectie is immers niet openbaar. Evenmin worden betrokkenen geïnformeerd over de wijze van totstandkoming van de definitieve risicoselectie en de daaraan verbonden conclusie of al dan niet een risicomelding wordt gedaan, terwijl de SyRI-wetgeving uitsluitend voorziet in algemeen toezicht achteraf van de AP.

6.96. De rechtbank is ook van oordeel dat in de SyRI-wetgeving, getoetst aan artikel 8 lid 2 EVRM, onvoldoende acht is geslagen op het doelbindingsbeginsel en het beginsel van dataminimalisatie. De rechtbank stelt voorop dat de doelomschrijving van artikel 64 leden 1 en 2 Wet SUWI op zichzelf voldoende is bepaald. Vooraf is duidelijk in verband met welke doelen gegevens ten behoeve van een

samenwerkingsverband moeten worden verstrekt. De keuze van de wetgever voor een groot aantal terreinen waarop kan worden samengewerkt en gegevens moeten worden verstrekt kan ook als gerechtvaardigd, in de zin van noodzakelijk, evenredig en subsidiair, worden beschouwd. Daarbij betreft de rechtbank mede het belang van de bestrijding van misbruik en fraude en de beoordelingsmarge die de Staat als nationale autoriteit heeft. De rechtbank verwerpt de stelling van NJCM c.s. en volgt het verweer van de Staat op dit punt. De SyRI-wetgeving acht de rechtbank in zoverre niet in strijd met het doelbindingsbeginsel.

6.97. Dit wordt anders indien en voor zover die doelen in samenhang worden gezien met de grote hoeveelheid gegevens die op grond van artikel 65 Wet SUWI en het Besluit SUWI in aanmerking komen voor verwerking in SyRI, de omstandigheid dat de noodzakelijkheidstoets zoals vereist door de aangewezen (overheids)instanties afzonderlijk wordt verricht en geen sprake is van een integrale toets vooraf door een onafhankelijke derde. De noodzakelijkheidstoets die de aangewezen (overheids)instanties moeten uitvoeren raakt zowel het doelbindingsbeginsel als het dataminimalisatiebeginsel. [...]

Noot

1. In deze zaak kwamen verschillende problematische punten naar voren met betrekking tot de omschakeling van overheidsdiensten naar meer datagedreven processen. Het is een vonnis dat verschijnt op een cruciaal moment en door rechters zowel in Nederland als daarbuiten zal worden bestudeerd, alsmede door academici. Niet voor niets werd het vonnis ook in het Engels gepubliceerd.²

2. Beginnend bij de partijen. Het is een belangrijke zaak voor belangenverenigingen, zoals partijen die opkomen voor de bescherming van mensenrechten, of specifiek, de bescherming van privacy en persoonsgegevens. Dit soort zaken, waarbij veel burgers geraakt worden maar het niet duidelijk is hoe dit zich vertaalt naar schade, zijn moeilijk te starten en voeren door burgers alleen.³ Toch is het niet altijd zo dat belangenverenigingen in dit soort grootschalige zaken ontvankelijk verklaard worden op grond van artikel 3:305a Burgerlijk Wetboek (hierna: 'BW'). Nu het in deze zaak gaat om het algemeen belang, omdat het gaat over het systeem en de wetgeving van het Systeem Risico Indicatie (hierna: 'SyRI') op zich en niet over specifieke besluiten, zijn de belangenverenigingen, die opkomen voor de privacybelangen van hun achterban of privacy in het algemeen, ontvankelijk in hun vorderingen. De twee individuen die zich bij de publieke campagne tegen SyRI en bij de eisers hadden aangesloten, zijn

² Zie ECLI:NL:RBDHA:2020:1878 voor de Engelstalige versie van dit vonnis.

³ B. van der Sloot & S. van Schendel, 'Tien voorstellen voor aanpassingen aan het Nederlands procesrecht in het licht van Big Data', *Computerrecht* 2020/2.

juist niet ontvankelijk in dit geval, nu er geen “concrete aanknopingspunten zijn waaruit kan volgen dat gegevens die op hen betrekking hebben onderdeel zijn van de verwerking in SyRI”.⁴ Zij hebben geen voldoende concreet en eigen belang in de zin van artikel 3:303 BW.

3. Dan over de grondslag. NJCM c.s. dragen verschillende bepalingen aan die door de SyRI-wetgeving zouden worden geschonden waardoor de SyRI-wetgeving en het gebruik van SyRI onrechtmatig zouden zijn. Daarbij wordt een beroep gedaan op verschillende bepalingen uit verdragen en bepalingen van de AVG. De nadruk wordt door NJCM c.s. in hun stellingen gelegd op artikel 8 Europees Verdrag voor de Rechten van de Mens (hierna: ‘EVRM’), de rechtbank gaat daarin mee. Echter er zijn een aantal stappen die de rechtbank neemt om te constateren of artikel 8 EVRM van toepassing is en hoe het artikel 8 EVRM dan zal toepassen. De rechtbank volgt de uitleg die door het Europees Hof voor de Rechten van de Mens (hierna: ‘EHRM’) aan artikel 8 is gegeven en benadrukt dat het recht op persoonlijke identiteit en ontwikkeling deel uitmaakt van het respect voor het privéleven, en dat het recht op persoonlijke identiteit nauw samenhangt met het recht op bescherming van persoonsgegevens. Vervolgens ziet het recht op het respect voor het privéleven ook deels op het recht op bescherming tegen discriminatie, ongelijke behandeling en stigmatisering, wanneer het gegevensverwerking betreft.⁵ Hiermee plaatst de rechtbank alle door NJCM c.s. aangevoerde fundamentele rechten binnen de bescherming geboden door artikel 8 EVRM. Nadat is vastgesteld dat artikel 8 EVRM inderdaad van toepassing is bespreekt de rechtbank de verhouding tussen het EVRM en Unierecht, zoals de Algemene Verordening Gegevensbescherming (hierna: de ‘AVG’). De rechtbank benadrukt dat het EVRM voorziet in minimumbescherming van het recht op eerbiediging van de persoonlijke levenssfeer, de inhoud en de reikwijdte van de EU-grondrechten in het Handvest zijn hetzelfde. Daarnaast maken de rechten uit het EVRM deel uit van het Unierecht door algemene beginselen. Het Unierecht biedt daarmee tenminste evenveel bescherming als het EVRM, de AVG bouwt daarop verder en biedt meer gedetailleerde bepalingen.⁶ NJCM c.s. en de Staat nemen in hun stellingen en verweer ook aan dat de rechten uit het EU-Handvest hetzelfde minimumniveau kennen als artikel 8 EVRM, en omgekeerd dat de bescherming van artikel 8 EVRM mede inhoudt dat moet zijn voldaan aan de Unierechtelijke bepalingen.⁷ Omdat er geen aanwijzingen zijn dat de bescherming van artikel 8 EVRM minder ver gaat dan die van Unierecht toetst de rechtbank ook aan algemene beginselen van de AVG, zoals het transparantiebeginsel, het doelbindingsbeginsel en het gegevensminimalisatiebeginsel.

4. Vervolgens waagt de rechtbank zich aan een conceptuele oefening, er wordt geprobeerd SyRI te classificeren:

hebben we het over Big Data? Profileren? Geautomatiseerde besluitvorming? De rechtbank stelt terecht dat het voor gegevensbeschermingsrecht er bijvoorbeeld niet zozeer toe doet of iets als Big Data kan worden gezien, maar het neemt de technische kenmerken van SyRI die door deze oefening naar voren worden gehaald wel mee in de bepaling van de zwaarte van de inmenging. De rechtbank stelt vast dat de SyRI-wetgeving geen basis biedt voor ongestructureerde gegevensverzameling, de categorieën gegevens die verzameld kunnen worden staan opgesomd. Er kan wel sprake zijn van grote hoeveelheden gestructureerde gegevensverzamelingen die afkomstig zijn uit verschillende bronnen. Het staat vast dat bij inzet van SyRI naar verbanden tussen gegevens wordt gezocht en de wetgeving laat de mogelijkheid open dat deep learning en data mining worden gebruikt, echter de rechtbank kan niet vaststellen of dit daadwerkelijk het geval is door de ondoorzichtigheid van SyRI. Wat betreft profilering kan de rechtbank niet vaststellen of er geen risicoprofielen worden ontwikkeld met behulp van bestandskoppeling. Wel acht de rechtbank het inherent aan SyRI, de doelen waarvoor gegevens in SyRI worden verwerkt en aan het gebruik van een risicomodel en risico-indicator, “dat bij de inzet van SyRI gebruik wordt gemaakt van risicoprofielen op basis van bestaande feitelijke gegevens”.⁸ Wat de rechtbank ook nog van belang acht bij het gebruik van SyRI is dat er geen wettelijke informatieverplichting is naar degenen van wie de gegevens in SyRI worden verwerkt noch een verplichting om betrokkenen afzonderlijk te informeren over het feit dat een risicomelding is gedaan.⁹ Tot slot stelt de rechtbank met betrekking tot geautomatiseerde besluitvorming nog vast dat een “risicomelding wel een aanmerkelijk effect op het privéleven van degene op wie de melding betrekking heeft”.¹⁰ De rechtbank laat in het midden of wordt voldaan aan de precieze definitie in de AVG van geautomatiseerde individuele besluitvorming. Het aanmerkelijk effect van de risicomelding en opname in het register zijn wel factoren van betekenis bij de beoordeling of de SyRI-wetgeving voldoet aan artikel 8 lid 2 EVRM.¹¹

5. Voor de invulling van de toets van artikel 8 lid 2 EVRM haakt de rechtbank aan bij de uitspraak van het EHRM in de zaak van S. en Marper tegen het Verenigd Koninkrijk:¹² “Uit het arrest van het EHRM in die zaak blijkt dat de nationale wet, om aan de eisen van toegankelijkheid en voorzienbaarheid te voldoen, voldoende bescherming moet bieden tegen willekeur en met voldoende duidelijkheid de discretionaire ruimte die aan de bevoegde autoriteiten wordt toegekend en de wijze waarop daarvan gebruik mag worden gemaakt moet bepalen”.¹³ Aan de hand hiervan toetst de rechtbank aan het geheel van wettelijke waarborgen om te bepalen of deze toereikend zijn en het ver-

4 Zie r.o. 6.15.

5 Zie r.o. 6.23 en 6.24.

6 Zie r.o. 6.37.

7 Zie r.o. 6.39 en 6.40.

8 Zie r.o. 6.53.

9 Zie r.o. 6.54.

10 Zie r.o. 6.59.

11 Zie r.o. 6.60.

12 EHRM 4 december 2008, nr. 30562/04 en 30566/04 (S. en Marper/Verenigd Koninkrijk).

13 Zie r.o. 6.69.

eiste niveau van de waarborgen hangt af van de ingrijpendheid van de inmenging.¹⁴ Het EHRM heeft in bovengenoemde zaak ook bepaald dat de vraag of de inmenging bij de wet is voorzien sterk samenhangt met de vraag of die inmenging noodzakelijk is in een democratische samenleving.¹⁵ De rechtbank volgt deze lijn van het EHRM en toetst niet of de SyRI-wetgeving voldoende toegankelijk en voorzienbaar is.¹⁶ De rechtbank focust op de vraag of de inmenging noodzakelijk is in een democratische samenleving, meer specifiek of deze voldoet aan de eisen van proportionaliteit en subsidiariteit.

6. Een groot struikelblok voor de SyRI-wetgeving om te voldoen aan bovenstaande eisen is transparantie. De SyRI-wetgeving voorziet niet in informatie die ziet op het risicomodel of informatie naar betrokkenen toe. Doordat deze informatie niet geboden wordt bestaan er volgens de rechtbank verschillende risico's en problemen. Ten eerste kunnen betrokkenen zelf niet nagaan of gegevens die betrekking hebben op hen worden verwerkt en of er een risicomelding is gedaan, dit hindert betrokkenen in de uitoefening van hun rechten. Daarnaast zijn er risico's in de controleerbaarheid. Door deze ondoorzichtigheid is het lastig vast te stellen of er sprake is van discriminatie, bijvoorbeeld doordat er onbedoelde discriminerende effecten optreden. NJCM c.s. refereren in die context ook aan een rapport van de Speciaal Rapporteur van de Verenigde Naties op het gebied van extreme armoede en mensenrechten waar al problemen rondom SyRI met discriminatie en stigmatisatie werden geconstateerd: *"Zij wijst erop dat met SyRI wijken die al als probleemwijk bekend staan aan een nader onderzoek worden onderworpen. Daardoor is de kans dat onregelmatigheden worden gevonden hoger dan in andere wijken, hetgeen weer het beeld bevestigt van probleemwijk, stereotypering in de hand werkt en een negatief beeld over de bewoners die in de wijk wonen wordt versterkt, ook al is ten aanzien van hen geen risicomelding gedaan"*.¹⁷ Een laatste probleem met transparantie is dat van transparantie naar derden of actoren buiten de SyRI samenwerking. De noodzakelijkheidstoets voor gegevensverstrekking is overgelaten aan verschillende actoren binnen de SyRI-samenwerking, waarbij de rechtbank een integrale toets vooraf of een onafhankelijke toets van derden op het gebied van noodzakelijkheid mist. Doordat er sprake is van zoveel data en deze toets ontbreekt kan de SyRI-wetgeving ook niet voldoen aan eisen van doelbinding en dataminimalisatie. De SyRI-wetgeving zal dan ook een concrete toets op dit punt moeten introduceren.

7. SyRI kan gecategoriseerd worden als risicoprofilering. De rechtbank gaat hier niet op in tijdens haar beoordeling of er sprake is van bijvoorbeeld Big Data of geautomatiseerde besluitvorming, er zitten ook geen juridische gevolgen vast aan deze classificering, maar het

helpt wel SyRI te plaatsen in de maatschappelijke context. Binnen overheidssystemen, maar ook binnen de private sector zoals in kredietverstrekking of het afsluiten van verzekeringen, worden individuen in toenemende mate gecategoriseerd naar, of gerangschikt op, risico. Met dit soort systemen wordt steeds meer de focus verlegd van reactief naar proactief beleid en wordt meer gezocht naar patronen en correlaties ter ondersteuning van beleid.¹⁸ Deze ontwikkeling gaat vaak gepaard met ondoorzichtige processen, uit overwegingen van nationale veiligheid, bescherming van intellectuele eigendomsrechten, of bescherming van de werkwijze van de politie. Daarnaast zijn risicoprofileringsinstrumenten datagedreven systemen waarbij data het uitgangspunt vormen en veel processen worden geautomatiseerd. Al deze elementen creëren uitdagingen en dat zijn precies de problematische punten waarop de SyRI-wetgeving niet was voorzien. De rechtbank concludeert niet dat het gebruik van risicoprofileringsinstrumenten zoals SyRI niet is toegestaan, alleen dat dit gebruik gepaard moet gaan met voldoende waarborgen. De rechtbank kent een bijzondere verantwoordelijkheid toe aan de wetgever in de tijd van snel ontwikkelende technologie, aangezien instrumenten zoals SyRI diep ingrijpen op het privéleven van burgers: *"(...) voor een betrokkene is moeilijk te overzien wat het effect van het instrument op zijn of haar privéleven precies is en het EVRM vereist dat de wetgeving die daarvoor een grondslag biedt voldoende waarborgen bevat om misbruik en willekeur tegen te gaan"*.¹⁹ Dit roept de vraag op of het gemakkelijk is bijvoorbeeld in het geval van SyRI om enkele aanpassingen aan de wetgeving te maken waardoor wel wordt voldaan op papier aan de vereisten van de AVG en EVRM, maar de maatschappelijke problemen zoals discriminatie, stigmatisatie, obstakels in het uitoefenen van rechten door betrokkenen in verband met transparantieproblemen, blijven voortbestaan. Gezien de aard van risicoprofileringsystemen, zoals SyRI, zullen deze problemen niet gemakkelijk te ondervangen zijn door simpele veranderingen aan te brengen in de wetgeving. Verdere rechtspraak zal moeten uitwijzen welke waarborgen wel voldoende zijn om fundamentele rechten te beschermen in een samenleving waar dit soort technologieën een steeds grotere rol zullen spelen.

Mr. S. van Schendel

¹⁴ Zie r.o. 6.70.

¹⁵ Zie r.o. 6.71.

¹⁶ Zie r.o. 6.72.

¹⁷ Zie r.o. 6.92.

¹⁸ Voor meer hierover zie: S. van Schendel, 'The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI' in: L. Reins (ed.), *Regulating New Technologies in Uncertain Times (Information Technology and Law Series vol. 32)*, The Hague 2019, T.M.C. Asser Press.

¹⁹ Zie r.o. 6.85.

Computerrecht 2020/88

Rechtbank Rotterdam 19 maart 2020
nr. 10/961510-19

(Mrs. I.M.A. Hinfelaar, J.J. Bade en R.J.A.M. Cooijmans)
m.nt. prof. mr. dr. J.J. Oerlemans¹

(Art. 139d lid 2 sub a jo. art. 138ab Sr)

ECLI:NL:RBROT:2020:2395

In deze zaak ontwikkelde de verdachte een programma (Rubella Macro Builder), waarmee aan Office-documenten zoals Word en Excel een stuk verborgen code wordt toegevoegd. Bij het openen van een geïnfecteerd document wordt de code uitgevoerd. Daarmee maakt de verdachte het bijvoorbeeld mogelijk andere malware te downloaden op de computers van slachtoffers. De verdachte heeft zich schuldig gemaakt aan het vervaardigen, verkopen, verspreiden en voorhanden hebben van malware met het oogmerk computervredesbreuk te plegen.

(...)

raadvrouw mr. F.E. den Hertog, advocaat te Amersfoort.

(...)

3. Eis officier van justitie

De officier van justitie mr. W.S. Koorn heeft gevorderd:

- bewezenverklaring van het onder 1 en 2 ten laste gelegde;
- veroordeling van de verdachte tot een gevangenisstraf voor de duur van 18 maanden met aftrek van voorarrest, waarvan 6 maanden voorwaardelijk, met een proeftijd van 2 jaar.

4. Waardering van het bewijs

4.1 Bewezenverklaring feit 2 zonder nadere motivering

Het onder 2 ten laste gelegde voorhanden hebben van creditcardgegevens is door de verdachte bekend. Dit feit zal zonder nadere bespreking bewezen worden verklaard.

4.2 Bewijswaardering feit 1

4.2.1 Standpunt officier van justitie

Aangevoerd is dat de verdachte drie typen malware heeft vervaardigd, te weten Rubella, Dryad en Cetan. Deze typen malware zijn hoofdzakelijk geschikt voor het voorbereiden van het plaatsen van af luister- en/of hackapparatuur. Dit is strafbaar op grond van artikel 139d lid 2 sub a van

het Wetboek van Strafrecht (hierna: WvSr) voor wat betreft het faciliteren van hacken ex artikel 138ab WvSr. Voor wat betreft het kunnen aftappen van toetsaanslagen is dit strafbaar op grond van artikel 350d sub a WvSr. De verdachte heeft deze malware vervolgens verkocht, verspreid, anderszins ter beschikking gesteld en voorhanden gehad. Gelet op het type malware dat de verdachte ontwikkelde en de professionele manier waarop hij zijn handel inrichtte, had hij daarmee ook het oogmerk in de zin van artikel 139d lid 3 WvSr. Het was de persoonlijke bedoeling van de verdachte dat zijn malware zou worden gebruikt voor onder andere hacken.

4.2.2 Standpunt verdediging

De verdediging heeft aangevoerd dat Rubella, Dryad en Cetan in feite één programma zijn. Rubella is door de verdachte vervaardigd en daarna door hem op kleine punten gewijzigd en doorontwikkeld, hetgeen heeft geleid tot de andere programma's. De verdachte heeft deze software weliswaar vervaardigd en daarna op de markt gebracht, echter heeft de verdachte hierbij nooit de bedoeling gehad dat er met deze software strafbare feiten zouden worden gepleegd. Dat de verdachte handelde met het oogmerk op computervredesbreuk en/of computersabotage kan niet worden vastgesteld. Voorwaardelijk opzet is daarvoor onvoldoende. De verdachte dient daarom te worden vrijgesproken van het onder 1 ten laste gelegde.

4.2.3 Beoordeling

Onder feit 1 is de verdachte ten laste gelegd dat hij drie programma's heeft vervaardigd die hoofdzakelijk geschikt gemaakt en/of ontworpen zijn tot het kortgezegd plegen van '(eenvoudige) computervredesbreuk' en (als cumulatief/alternatief) 'computersabotage', en dat hij deze programma's met het oogmerk op deze misdrijven heeft vervaardigd, verkocht, verspreid, anderszins ter beschikking gesteld of voorhanden gehad.

De rechtbank stelt het volgende voorop. Ter zitting heeft de verdachte verklaard dat hij zich in de periode van 15 februari 2018 tot en met 11 maart 2019 bezig hield met het vervaardigen en verkopen van Rubella, Dryad en Cetan. De verdachte heeft verklaard dat hij zich al jaren eerder uit interesse in de beveiliging van geautomatiseerde werken en de werking van malware is gaan verdiepen in dit onderwerp. Toen hij hier veel kennis over had opgedaan heeft hij bij wijze van intellectuele uitdaging Rubella vervaardigd. De verdachte heeft verklaard dat Rubella gezien moet worden als een 'lege huls', die ongedetecteerd door anti-virussoftware toegang kan verkrijgen tot andermans computer. Het is mogelijk dat met gebruik van deze 'lege huls' andere (kwaadwillende) malware op een computer geplaatst wordt. De verdachte heeft ook verklaard dat hij Rubella is gaan verkopen toen hij merkte dat er interesse was voor dergelijke programma's. Dryad en Cetan zijn iets later door hem (door)ontwikkeld en op de markt gebracht. Deze laatste twee programma's dienen hetzelfde doel als Rubella. De verdachte heeft verklaard dat zijn oogmerk,

¹ Jan-Jaap Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht en verbonden aan het Montaigne Centrum voor Rechtsstaat en Rechtspleging en het Willem Pompe Instituut voor Strafrechtwetenschappen.

zowel bij het vervaardigen als bij het verkopen van de software, niet gericht was op het faciliteren van computercriminaliteit en dat hij zijn programma's ook niet als zodanig aanbood.

Hoofdzakelijk geschikt

De rechtbank is van oordeel dat Rubella, Dryad en Cetan hoofdzakelijk geschikt gemaakt of ontworpen zijn om computercriminaliteit mogelijk te maken. De rechtbank komt tot deze conclusie op basis van de volgende omstandigheden.

In het proces-verbaal van bevindingen 'onderzoek aan Rubella Macro Builder' relateert de politie dat (een programma als) Rubella Macro Builder een onmisbare functie vervult in het proces van cybercriminaliteit met behulp van malware. Rubella zorgt namelijk voor de eerste stap van 'infectie'; het ongedetecteerd bezorgen van malware op een computersysteem. In het proces-verbaal van bevindingen 'onderzoek aan Cetan' en het proces-verbaal van bevindingen 'onderzoek aan Dryad' is door de politie gerelateerd dat het ook met deze programma's mogelijk is om ongedetecteerd een geautomatiseerd werk binnen te komen. Cetan en Dryad werken op dezelfde manier als Rubella: met behulp van deze programma's lukt het om een macro te genereren in een Worddocument. Zodra dit document wordt geopend, downloadt de macro een bestand van een externe server en voert deze uit. Cetan Macro Builder is een meer geavanceerde, dan wel verbeterde, macro builder ten opzichte van Rubella. Zo is het in Cetan mogelijk om een document door middel van een tekst en een foto een betrouwbaar uiterlijk te geven, zodat een slachtoffer eerder geneigd is om de macrofunctionaliteit in te schakelen. Met Dryad kan een Word-document worden geprepareerd met een macro die vervolgens een programma vanaf een externe locatie downloadt en uitvoert.

De rechtbank is van oordeel dat voor zover de software ook geschikt is voor legale activiteiten (bijvoorbeeld het testen van de eigen beveiliging) dit er niet aan af doet dat de software van de verdachte hoofdzakelijk geschikt gemaakt en ontworpen is om de delicten van eenvoudige computervredesbreuk (artikel 138ab eerste lid WvSr), en vervolgens/tevens de delicten van 138b WvSr (belemmering van een geautomatiseerd werk) en/of 139c WvSr (het aftappen of opnemen van gegevens) mogelijk te maken. Uit berichtenverkeer van de telefoon van de verdachte kan worden afgeleid dat de verdachte zelf het verband tussen het maken en verkopen van deze software en de strafbaarstelling op grond van artikel 139d lid 2 WvSr onder a heeft gelegd.

Dat dit programma in hoofdzaak geschikt of ontworpen is om het wissen/onbruikbaar maken dan wel vernielen van een geautomatiseerd werk te plegen (artikel 350a en/of 350c WvSr) acht de rechtbank gelet op de dossierinformatie onvoldoende vaststaan. De verdachte wordt dan ook – partieel – vrijgesproken van overtreding van artikel 350d WvSr.

Oogmerk in artikel 139d lid 2 sub a WvSr

De rechtbank is van oordeel dat met 'oogmerk' in artikel 139d lid 2 WvSr wordt bedoeld 'met de (persoonlijke) bedoeling'. Artikel 139d lid 2 WvSr is aan de Nederlandse strafwetgeving toegevoegd en op 1 september 2006 in werking getreden, om aan de verplichtingen die voortvloeien uit het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (hierna: Cybercrimeverdrag) te voldoen. Artikel 6 van het Cybercrimeverdrag verplicht de verdragspartijen om in hun nationale wetgeving als strafbaar aan te merken:

- a. *het opzettelijk en wederrechtelijk vervaardigen, verkopen, verkrijgen voor gebruik invoeren, verspreiden of anderszins beschikbaar stellen van:*
 - i. *een technisch hulpmiddel, waaronder begrepen een computerprogramma, dat hoofdzakelijk is ontworpen of geschikt gemaakt voor het plegen van een van de strafbare feiten, bedoeld in de artikel 2 tot en met 5 (van hetzelfde verdrag).*

In artikel 6 lid 2 van het Cybercrimeverdrag is bepaald dat dit artikel niet als zodanig mag worden uitgelegd dat sprake is van strafrechtelijke aansprakelijkheid wanneer de in het eerste lid van dit artikel bedoelde vervaardiging, verkoop, verkrijging voor gebruik, invoer, verspreiding of andere vorm van beschikbaarstelling of het bedoelde bezit niet bedoeld is voor het plegen van een overeenkomstig de artikelen 2 tot en met 5 van dit Verdrag strafbaar gesteld feit, zoals ten behoeve van het geautoriseerd testen of het beschermen van een computersysteem.

In de Nederlandse wetgeving is blijkens de tweede nota van wijziging (*Kamerstukken II* 2005/06, 26671, 7) uiting gegeven aan het voorgaande door het begrip 'oogmerk' op te nemen in artikel 139d lid 2 (en 3) WvSr. Indien iemand een technisch hulpmiddel voorhanden heeft dat hoofdzakelijk ontworpen is tot het plegen van computervredesbreuk, maar hij dit middel alleen gebruikt om de beveiliging van z'n eigen computer te testen, heeft hij niet het oogmerk om het misdrijf computervredesbreuk te plegen. Hij valt dan niet in de termen van de strafbepaling.

De persoonlijke bedoeling van de verdachte

De rechtbank is van oordeel dat de verdachte bij zowel het vervaardigen van de software, als het verkopen en voorhanden hebben de bedoeling had dat hiermee tenminste computervredesbreuk en daarmee samenhangende computercriminaliteit wordt gepleegd. De rechtbank leidt dit af uit de volgende omstandigheden.

De technische mogelijkheden van de door de verdachte vervaardigde malware zijn volledig gericht op het omzeilen van anti-virussoftware. De verdachte heeft de producten zelf gemaakt en had dan ook als geen ander de wetenschap van alle functionaliteiten en mogelijkheden, waaronder met name ook de illegale mogelijkheden, die zijn software de gebruikers ervan daardoor biedt. De verdachte heeft ter terechtzitting verklaard dat hij zich 'niet zo bezighield met waar zijn klanten zijn software voor gebruikten', maar de rechtbank acht dat niet aannemelijk.

Dat de verdachte zijn producten aan de man bracht op hackersfora acht de rechtbank daarbij een relevant gegeven, evenals de wijze waarop hij zijn producten aanpreept. Zo is te lezen in een digitale advertentie van Rubella dat het mogelijk is om aan deze malware een powershell payload toe te voegen. Met 'payload' wordt malware bedoeld die een kwaadwillende wil uitvoeren bij zijn slachtoffer.² In de advertentietekst wordt verder benadrukt dat het mogelijk is om met deze malware anti-virusdetectie te omzeilen. Tevens wordt benadrukt in de advertentietekst dat de malware al vier weken FUD zou zijn. Wanneer een bestand FUD is, wordt bedoeld dat het niet door anti-virus software wordt herkend als zijnde een virus.³

De rechtbank leidt het oogmerk in het bijzonder ook af uit de volgende door de verdachte gevoerde gesprekken. Op 30 augustus 2018 is vanuit het toestel van de verdachte een screenshot gestuurd naar een nummer dat is opgeslagen onder de naam [naam]. Het screenshot bevat een afbeelding van een e-mail afkomstig van Google waarin wordt aangegeven dat de FBI informatie met betrekking tot een Google-account heeft gevorderd. Dit screenshot werd direct gevolgd door berichten van de verdachte die er op neerkwamen dat de verdachte enorm geschrokken was van deze e-mail. Zo stuurde de verdachte: *"Ik stop nu per direct"*. De verdachte verdiepte zich vervolgens in de strafbaarheid van computervredebreuk en stuurde tevens: *"het maken, vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van dergelijke software is een strafbaar feit (art. 139d lid 2 onder a). Hierop staat een jaar cel (of een boete van 16.750 euro)." Zijn gesprekspartner zegt daarop: "Dan betaal je je boete en je zit goed". De verdachte zegt dan: "Ik denk niet dat ik met dat geld die boete kan betalen". Zijn gesprekspartner zegt dan: "En dan mag je nog 2 jaar zitten" en "Want illegaal geld". De verdachte stuurde vervolgens: "Dat is kk lang" en "Een jaar in de cel".*

Een dag later is de verdachte er kennelijk achter gekomen dat de aanleiding voor de FBI om zijn accountgegevens op te vragen betrekking heeft op iets uit het verleden en niet ziet op waar hij op dat moment mee bezig is. De verdachte voert dan een gesprek met de gebruiker van het telefoonnummer [telefoonnummer] en zegt deze persoon die e-mail van Google te negeren: *"Ja negeer die mail"* en *"Is oude case"*, en iets verderop in het gesprek: *"Er staat 2017 in de case nummer"*. Daarna werd er vanuit de telefoon van de verdachte het volgende bericht verstuurd: *"Maar ik zit nog diep er in"*. Op de vraag verstuurd vanaf de telefoon met het nummer [telefoonnummer]: *"Hoe bedoel je"* werd volgend antwoord gestuurd: *"Dat ik nog malware doe"* en *"Ik code het nu"*. Enige tijd later in het gesprek wordt vanuit het toestel van de verdachte verstuurd: *"Ik dacht zeg,*

maar dat dat mailtje over mijn shit van nu ging" en *"Ik dacht ze hebben me gevonden"*.

De rechtbank leidt uit voorgaande gesprekken af dat de verdachte wel degelijk wist dat het product dat hij verkocht door anderen gebruikt werd voor kwalijke en niet legale activiteiten. Het stadium van 'klieren' op internet, zoals de verdachte zelf verklaard heeft begonnen te zijn, was de verdachte toen al lang voorbij en dat wist hij ook. Desondanks ging de verdachte direct nadat hij van de schrik was bekomen door met het vervaardigen en verkopen van zijn malware op hackersfora.

De verdachte wist als geen ander dat zijn producten in feite alleen betekenis hadden voor illegale toepassingen – al lemaal te begrijpen onder de noemer van computercriminaliteit als hiervoor bedoeld – en dat de kopers van zijn producten geen ander doel (kunnen) hebben gehad dan gebruikmaking daarvan voor dergelijke illegale toepassingen. In die volle wetenschap heeft de verdachte, tegen betaling van aanzienlijke bedragen, een groot aantal verkooptransacties uitgevoerd. Deze hebben gedurende lange tijd plaatsgevonden, zoals ten laste gelegd in de periode van 15 februari 2018 tot en met 11 maart 2019. Het handelen van de verdachte moet daarom worden aangemerkt als met de bedoeling dat hiermee computercriminaliteit zou worden gepleegd. Aan deze gevolgtrekking doet niet af dat het verdachte uiteindelijk te doen zal zijn geweest om zijn financieel voordeel. De conclusie is dat sprake is van het in artikel 139d lid 2 sub a WvSr vereiste oogmerk.

Oogmerk artikel 193d lid 3 WvSr

De rechtbank zal niet ingaan op het betoog van de officier van justitie om overtreding van artikel 139d lid 3 WvSr bewezen te verklaren, nu die strafbare gedraging niet ten laste is gelegd.

4.2.4 Conclusie

Het eerste onderdeel onder 1 ten laste gelegde is wettig en overtuigend bewezen. De rechtbank spreekt de verdachte partieel vrij voor het tweede onderdeel van het onder 1 ten laste gelegde.

4.3 Bewezenverklaring

(...)

De verdachte heeft de bewezen verklaarde feiten op die wijze begaan dat:

Feit 1:

hij in de periode van 15 februari 2018 tot en met 11 maart 2019 te Utrecht, meermalen, een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt en/of ontworpen is tot het plegen van een misdrijf als bedoeld in artikel 138ab eerste lid, 138b en/of 139c Wetboek van strafrecht, heeft vervaardigd, verkocht of voorhanden heeft gehad, met het oogmerk dat daarmee een van die misdrijven werd gepleegd,

² Bron vermeld in het proces-verbaal van verdenking (LERDA18011-13) (vul geboortedatum in): <https://nl.wikipedia.org/wiki/Payload>, bezocht op 21-11-2018.

³ Bron vermeld in het proces-verbaal van verdenking (LERDA18011-13) (vul geboortedatum in): https://en.wikipedia.org/wiki/Fully_undetected, bezocht op 21-11-2018.

immers heeft verdachte malware (Rubella Macro Builder, Dryad en Cetan) vervaardigd en op hackfora verkocht, welke malware hoofdzakelijk was ontworpen om voornoemde misdrijven te plegen door het mogelijk te maken om op met deze malware geïnfecteerde computers:

- .xls en/of.doc bestanden te genereren die macros bevatten
- bestanden te downloaden en/of uit te voeren
- opdrachten uit te voeren.
- toetsaanslagen te loggen

Feit 2:

hij in de periode van 20 mei 2017 tot en met 11 maart 2019 te Utrecht, creditcardgegevens (42) voorhanden heeft gehad, waarvan verdachte wist dat die bestemd waren tot het plegen van het in artikel 231b Wetboek van Strafrecht omschreven misdrijf. Hetgeen meer of anders is ten laste gelegd is niet bewezen. De verdachte moet daarvan worden vrijgesproken.

5. Strafbbaarheid feiten

De bewezen feiten leveren op:

Ten aanzien van feit 1:

met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b en/of 139c van het Wetboek van Strafrecht wordt gepleegd, een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigen, verkopen en voorhanden hebben, meermalen gepleegd;

Ten aanzien van feit 2:

gegevens voorhanden hebben waarvan hij weet dat zij bestemd zijn tot het plegen van een in artikel 231b van het Wetboek van Strafrecht omschreven misdrijf.

Er zijn geen feiten of omstandigheden aannemelijk geworden die de strafbaarheid van de feiten uitsluiten. De feiten zijn dus strafbaar.

6. Strafbbaarheid verdachte

Er is geen omstandigheid aannemelijk geworden die de strafbaarheid van de verdachte uitsluit. De verdachte is dus strafbaar.

7. Motivering straf

(...)

7.3 Persoonlijke omstandigheden van de verdachte

7.3.1 Strafbblad

De rechtbank heeft acht geslagen op een uittreksel uit de justitiële documentatie van 14 maart 2019, waaruit blijkt dat de verdachte niet eerder is veroordeeld voor strafbare feiten.

7.3.2 Rapportages

Reclassering Nederland heeft een rapport over de verdachte opgemaakt, gedateerd 18 februari 2020. Dit rapport houdt het volgende in.

De reclassering schat de kans op recidive op korte termijn in als laag, echter is het onduidelijk hoe deze kans op langere termijn zal zijn als de interesse in informatietechnologie toeneemt en de verdachte in contact komt met nieuwe vrienden met dezelfde interesse en (mogelijk andere) vaardigheden. Om de kans op recidive te verkleinen en de vaardigheden van de verdachte een positieve draai te geven, wil de reclassering hem, in het kader van een verplicht reclasseringscontact, aanmelden bij het programma Hack_Right, voor jonge hackers. In het toezicht kan verder worden gecontroleerd of betrokkene zich daadwerkelijk niet meer bezighoudt met criminele zaken.

De rechtbank heeft acht geslagen op dit rapport.

7.4 Conclusies van de rechtbank

Gelet op hetgeen de rechtbank hierboven heeft overwogen, komt zij tot de volgende conclusies.

Gezien de ernst van de feiten zou in beginsel niet anders kunnen worden gereageerd dan met het opleggen van een onvoorwaardelijke gevangenisstraf. De rechtbank zal echter afzien van het opleggen van een onvoorwaardelijke gevangenisstraf die langer is dan het voorarrest van 12 dagen in maart 2019, gezien de persoon van de verdachte. In plaats daarvan wordt de maximale taakstraf opgelegd van 240 uren en een voorwaardelijke gevangenisstraf van 180 dagen met een proeftijd van 3 jaren.

De verdachte was nog heel jong ten tijde van de bewezen verklaarde feiten (te weten 19 en net 20 jaar) en was voorafgaand aan deze zaak niet eerder veroordeeld voor strafbare feiten. De verdachte studeert Informatiekunde en heeft zijn leven verder op orde. De rechtbank heeft, mede op basis van de zitting, de indruk verkregen dat de verdachte inmiddels van de ernst van de feiten en alle mogelijke consequenties daarvan, ook in strafrechtelijke zin, doordrongen is. Dit geeft voor de rechtbank in dit specifieke geval de doorslag om als strafmodaliteit niet te kiezen voor een onvoorwaardelijke gevangenisstraf die langer is dan de voorlopige hechtenis destijds heeft geduurd.

Het voorwaardelijke strafdeel dient er tevens toe de verdachte ervan te weerhouden in de toekomst opnieuw strafbare feiten te plegen. Vanwege de voorwaardelijke gevangenisstraf gedurende een proeftijd van drie jaren en vanwege het leereffect dat van deze strafzaak zal uitgaan voor de verdachte, vindt de rechtbank het niet nodig of wenselijk daarbij ook nog bijzondere voorwaarden op te leggen, ook niet voor het volgen van het programma Hack_Right.

Alles afwegend acht de rechtbank de voorgenoemde straffen, tesamen met de hieronder besproken verbeurdverklaringen, passend en geboden.

Dit is een andere en minder zware bestraffing dan door de officier van justitie is geëist. Deels komt dit door voor-

noemde overwegingen over de persoon van de verdachte, deels doordat de rechtbank minder bewezen acht dan dan de officier van justitie.

(...)

9. Toepasselijke wettelijke voorschriften

(...)

Noot

1. De verdachte in deze zaak ontwikkelde het programma 'Rubella Marco Builder'. Het is zogenoemde 'macromalware', omdat het aan Office-documenten zoals Word en Excel een stuk verborgen code toevoegt die iets uitvoert. De verdachte had het programma zo geprogrammeerd dat het heimelijk verbinding legde met een externe server waardoor cybercriminelen hun eigen malware konden plaatsen op de computers van de slachtoffers. De zaak is interessant, omdat het een van de weinige veroordelingen is voor de vervaardiging van malware door een Nederlander en het misbruik maken van de macrofunctionaliteit in Office-documenten een veelgebruikte aanvalstechniek is van cybercriminelen.

2. De zaak begon niet met een opsporingsonderzoek door de politie, maar met een onderzoek van cybersecuritybedrijf McAfee.⁴ De onderzoekers bij McAfee viel een advertentie van het programma op een hackersforum op het oog. Het screenshot van een geprepareerd Word-document had Nederlandse taalinstellingen. Dat is ongebruikelijk in de hackerswereld, waar de voertaal volgens McAfee doorgaans Engels is. Ook was een chataccount (van Jabber) van ene 'Rubella' te vinden. De onderzoekers namen contact op via Jabber met de aanbieder en toonden interesse in de software. Nader onderzoek van de malware – 'Dryad' genaamd – toonde verschillende functionaliteiten aan van het programma, zoals (1) de mogelijkheid een uitvoeringsbestand te downloaden van een aangegeven URL, (2) de mogelijkheid (o.a.) een.exe-bestand op een computer te starten, (3) de bestandsnaam van de download te wijzigen, (4) verschillende functionaliteiten om antivirusprogramma's te omzeilen, en (5) de functionaliteit een Word of Excel-document te genereren.

3. De verdachte wordt ten laste gelegd het vervaardigen van malware, te weten 'Rubella', 'Dryad' en 'Cetan'. Deze typen malware zijn hoofdzakelijk geschikt voor het voorbereiden van het plaatsen van af luister- en/of hackapparatuur (strafbaar gesteld in art. 139d lid 2 sub a jo. art. 138ab Sr). De verdachte heeft deze malware vervolgens verkocht, verspreid, anderszins ter beschikking gesteld en voorhanden gehad. Het fungeert als 'tool' voor cybercriminelen.⁵ In 2017 berichtte Europol dat misbruik

van de macrofunctionaliteit in Office-documenten een veelgebruikte aanvalstechniek is van cybercriminelen.⁶

4. De verdediging voert aan dat de verdachte geen oogmerk had dat met de software computervredebreuk wordt gepleegd. Het benodigde oogmerk voor de strafbaarstelling zou dus ontbreken, waardoor de verdachte moet worden vrijgesproken. De rechtbank gaat daar niet in mee. Er is veel bewijs voorhanden dat tot bewezenverklaring van het benodigde oogmerk leidt. De verdachte zegt in zijn verklaring bijvoorbeeld dat de software is ontwikkeld om antivirusprogramma's te omzeilen en toegang te krijgen tot andermans computer. Ook verklaart hij ter zetting dat hij de Rubella software is gaan verkopen.⁷ Dat is mijns inziens in feite een bekentenis.

5. De rechtbank overweegt dat verdachte de producten op hackersfora verkocht en daarop zijn producten aanpreekt. Zo is te lezen in een digitale advertentie van Rubella dat het mogelijk is om aan deze malware een 'powershell payload' toe te voegen. Met 'payload' wordt malware bedoeld die een kwaadwillende wil uitvoeren bij zijn slachtoffer. In de advertentietekst wordt verder benadrukt dat het mogelijk is om met deze malware antivirusdetectie te omzeilen. Tevens wordt benadrukt in de advertentietekst dat de malware al vier weken FUD zou zijn. Wanneer een bestand FUD is, wordt bedoeld dat het niet door antivirussoftware wordt herkend als zijnde een virus, aldus de rechtbank in zijn uitleg van deze zaak met een hoog technisch karakter.⁸

6. De rechtbank leidt het oogmerk onder andere af uit het geanalyseerde berichtenverkeer op de telefoon van de verdachte. Hieruit blijkt dat de verdachte zelf het verband al heeft gelegd tussen het maken en verkopen van deze software en de strafbaarstelling op grond van art. 139d lid 2 sub a Sr.⁹ De verdachte wordt ook veroordeeld voor het voorhanden hebben van creditcardgegevens van 42 personen, terwijl hij wist dat het mogelijk was om met deze gegevens creditcardfraude te plegen. De rechtbank acht het ontoegankelijk maken van gegevens met de programma's *niet* bewezen, omdat uit de beschikbare dossierinformatie onvoldoende is gebleken dat de door de verdachte vervaardigde en verkochte malware hoofdzakelijk geschikt of ontworpen was om gegevens te wissen of onbruikbaar te maken, dan wel vernieling van een geautomatiseerd werk te plegen (zoals bij ransomware).¹⁰

⁴ Zie voor onderstaande beschrijving: J. Fokker & T. Rocca, 'McAfee ATR Aids Police in Arrest of the Rubella and Dryad Office Macro Builder Suspect', *McAfee Blog*, 16 juli 2019.

⁵ Zie r.o. 4.2.1.

⁶ Europol, *Internet organised threat assessment report 2017*, p. 57: "A common approach is to attach a malicious attachment to an email, often a Microsoft Office document containing malicious macro code – a tactic that Dridex is notorious for resurrecting. Alternatively the message may include a link to a malicious URL which will then attempt to infect the target computer when they visit the site."

⁷ R.o. 4.2.3.

⁸ Zie r.o. 4.2.3.

⁹ R.o. 4.2.3.

¹⁰ Zie ook Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153, *Computerrecht* 2018/210, m.nt. J.J. Oerlemans over de strafbaarstelling van het vervaardigen en voorhanden hebben van ransomware.

7. De verdachte wordt veroordeeld tot twaalf dagen gevangenisstraf (de tijd dat hij in voorarrest heeft gezeten) en een taakstraf van 240 uur, met daarbij een voorwaardelijke gevangenisstraf van 180 dagen met een proeftijd van drie jaren. Opvallend is dat de reclassering adviseerde de verdachte aan te melden bij het programma 'Hack_Right' om een positieve draai te geven aan de vaardigheden van de verdachte. Binnen het programma lopen jonge hackers bijvoorbeeld stage bij een cybersecuritybedrijf. De rechtbank vindt het niet nodig dat de verdachte het programma Hack_Right volgt, vanwege 'de voorwaardelijke gevangenisstraf gedurende een proeftijd van drie jaren en vanwege het leereffect dat van deze strafzaak zal uitgaan voor de verdachte'.¹¹ De strafoplegging valt lager uit dan de officier van justitie heeft geëist. Dat is volgens de rechtbank te verklaren vanwege de overwegingen van de persoon van de verdachte en deels omdat minder wordt bewezen dan de officier van justitie ten laste had gelegd.

8. Juridisch gezien is er weinig op te merken aan de uitspraak. De rechtbank voert de juiste overwegingen in deze technische zaak en het oordeel van de rechtbank is begrijpelijk. De straf kan als laag worden gezien, omdat de software het mogelijk maakt voor cybercriminelen om op grote schaal computervrederebreuk te plegen. De veroorzaakte schade door de software is mogelijk aanzienlijk. Echter, op het delict staat maximaal twee jaar gevangenisstraf en de rechtbank legt een flinke voorwaardelijke gevangenisstraf met proeftijd op. Met deze straf kan de verdachte verder gaan met zijn studie en verder werken aan zijn toekomst. Het was wel interessant geweest meer te lezen over de bewijsgaring van de politie onder leiding van het Openbaar Ministerie. Vermoedelijk is een netwerkzoeking ex art. 125j Sv toegepast toen de politie in de collegezaal de verdachte arresteerde en de laptop van de verdachte doorzocht. In de media is te lezen dat de laptop nog aan stond en de politie het bewijs direct heeft verzameld.¹² Het zou goed zijn daar meer over te lezen, omdat er nauwelijks jurisprudentie is over de bevoegdheid van de netwerkzoeking. De advocaat heeft hier echter geen verweer op gevoerd, waardoor de rechtbank er ook geen overwegingen aan hoeft te wijden. De (technische) details van de zaak en het geringe aantal veroordelingen voor het vervaardigen van software die als 'tool' wordt gebruikt door cybercriminelen, maakt de uitspraak vooral lezenswaardig.

Prof. mr. dr. J.J. Oerlemans

11 Ook worden 6,76 Bitcoin verbeurdverklaard, omdat deze vermoedelijk met de strafbare feiten zijn verkregen.

12 Zie o.a. R. Wassens, 'Celstraf voor 21-jarige malware-ontwikkelaar', *NRC.nl*, 19 maart 2020 en Redactie, 'Utrechtse student krijgt 192 dagen cel voor verkoop malware', *Security.nl*, 20 maart 2020.

Europa

Hof van Justitie geeft ViaSat ongelijk in geschil met Inmarsat over mobiele satellietdiensten

Computerrecht 2020/89

Bij arrest van 5 maart 2020 heeft het Hof van Justitie geantwoord op een prejudiciële vraag van het Hof van beroep Brussel (afdeling Marktenhof) in verband met de interpretatie van Beschikking nr. 626/2008/EG van het Europees Parlement en de Raad van 30 juni 2008 inzake de selectie en machtiging van systemen die mobiele satellietdiensten (MSS) leveren (MSS-beschikking).

De prejudiciële vraag werd gesteld in het kader van het beroep tot nietigverklaring dat ViaSat bij het Marktenhof heeft ingesteld tegen de beslissing van het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT) waarbij Inmarsat gemachtigd wordt om op het Belgische grondgebied “complementaire grondcomponenten” (CGC, terrestrische basisstations) te exploiteren ten behoeve van haar *European Aviation Network* (EAN). Met het EAN beoogt Inmarsat om door middel van een combinatie van een satelliet en een netwerk van terrestrische basisstations (de CGC) internettoegangsdiensten te verstrekken aan boord van vliegtuigen die het Europese luchtruim doorkruisen (“*in-flight connectivity*”). ViaSat is een concurrerende aanbieder van dergelijke diensten, net als Eutelsat dat in de zaak geïntervenieerd is aan de zijde van ViaSat.

De vragen die het Marktenhof aan het Hof van Justitie gesteld heeft, komen in wezen neer op de vraag of het feit dat Inmarsat zijn dekkingsverplichtingen conform artikel 4, lid 1, onder c), ii) van de MSS-beschikking niet (tijdig) heeft nageleefd, voor het BIPT een dwingende of facultatieve grond vormt om de betwiste machtiging te weigeren. De MSS-beschikking voorziet in de organisatie door de Europese Commissie van een pan-Europese selectieprocedure voor het toekennen van gebruiksrechten in de 2 GHz-frequentieband voor de exploitatie van MSS. Artikel 4, lid 1, onder c), ii) van de MSS-beschikking bepaalt dat één van de selectievoorwaarden is dat de kandidaten zich ertoe moeten verbinden dat het mobiele satellietstelsel in alle lidstaten en voor ten minste 50% van de bevolking beschikbaar is en ten minste 60% van het totale landoppervlak van elke lidstaat bestrijkt op een door de aanvrager aan te geven tijdstip doch niet later dan zeven jaar na de datum van bekendmaking van het selectiebesluit van de Commissie. Inmarsat heeft zich kandidaat gesteld en heeft er zich als dusdanig toe verbonden deze dekkingsverplichting na te leven.

Samen met nog een ander bedrijf werd de kandidatuur van Inmarsat weerhouden. Het selectiebesluit van de Commissie werd op 12 juni 2009 in het *Publicatieblad* van de EU gepubliceerd. Bijgevolg was Inmarsat verplicht om

tegen 12 juni 2016 aan de dekkingsverplichting te voldoen. Dit is echter niet gebeurd aangezien de EAN-satelliet van Inmarsat pas op 28 juni 2017 is gelanceerd en pas op 29 augustus 2017 in gebruik is genomen.

Het Hof wijst erop dat krachtens artikel 8, lid 1 van de MSS-beschikking de lidstaten ervoor moeten zorgen dat de bevoegde instanties de geselecteerde aanvragers de nodige machtigingen moeten verlenen voor de exploitatie van CGC op hun grondgebied. Het is niet betwist dat Inmarsat een geselecteerde aanvrager is. Bovendien laat geen enkel element van het dossier toe om vast te stellen dat het door de selectiebeschikking toegekende recht om radiofrequenties te gebruiken inmiddels aan Inmarsat is ontnomen.

Er moet ook een onderscheid gemaakt worden tussen enerzijds de gemeenschappelijke voorwaarden voor de toekenning van een machtiging om CGC te exploiteren op het grondgebied van een lidstaat (artikel 8, lid 3 van de MSS-beschikking), en anderzijds de gemeenschappelijke voorwaarden voor de toekenning van gebruiksrechten voor radiofrequenties aan de geselecteerde aanvragers (artikel 7, lid 2 van de MSS-beschikking). In tegenstelling tot artikel 7, lid 2 verwijst artikel 8, lid 3 niet naar de nakoming van toezeggingen die de geselecteerde aanvrager bij zijn aanvraag heeft gedaan, waaronder de dekkingsverplichtingen van artikel 4, lid 1, onder c), ii) van de MSS-beschikking.

Het Hof wijst er voorts op dat artikel 9 van de MSS-beschikking specifieke handhavingsregels vaststelt in geval een geselecteerde operator de bij zijn aanvraag aangegane verbintenissen niet nakomt. Deze zijn verder uitgewerkt in het handhavingsbesluit nr. 2011/667/EU van de Commissie van 10 oktober 2011. Dit besluit voorziet in een gecoördineerde toepassing van de handhavingsregels bedoeld in artikel 9, lid 3 van de MSS-beschikking door de lidstaten en de Commissie via overleg in de schoot van het Comité voor Communicatie ingesteld door artikel 22 van de Kaderrichtlijn (Richtlijn 2002/21/EG). Deze procedure heeft tot doel inconsistenties in de toepassing van nationale handhavingsmaatregelen te voorkomen die zouden leiden tot een lappendeken van handhavingsmaatregelen, hetgeen in strijd zou zijn met de pan-Europese aard van MSS.

Een inbreuk op de in artikel 7, lid 2 van het MSS-besluit vermelde gemeenschappelijke voorwaarden, waaronder de naleving van de dekkingsverplichtingen van artikel 4, lid 1, onder c), ii) van de MSS-beschikking, kan enkel mits toepassing van dit gecoördineerde handhavingsmechanisme leiden tot een intrekking van de machtiging om MSS te exploiteren in de 2 GHz-frequentieband. Zolang deze procedure niet heeft geleid tot een intrekkingbesluit, blijft de geselecteerde exploitant gemachtigd om het radiospectrum te gebruiken voor de exploitatie van MSS en kunnen de lidstaten dan ook niet om die reden weigeren om een vergunning te verlenen voor de exploitatie van CGC op hun grondgebied.

<https://curia.europa.eu>

Karl Stas

Nederland

Advocaat-Generaal Campos Sánchez-Bordona over netneutraliteit en zero rating

Computerrecht 2020/90

Advocaat-generaal Manuel Campos Sánchez-Bordona heeft zich in de zaak *Telenor Magyarország Zrt. t. NMHH* (C-807/18 en C-39/19) uitgesproken over de verenigbaarheid van een zogenaamd “zero rated” aanbod met de bepalingen inzake netneutraliteit van Verordening (EU) 2015/2120 van het Europees Parlement en de Raad van 25 november 2015 tot vaststelling van maatregelen betreffende open-internettoegang.

De zaak gaat over bepaalde pakketten aangeboden door Telenor Magyarország (“Telenor”), waarbij het dataverbruik van de abonnee voor bepaalde sociale netwerk- of messagingtoepassingen c.q. toepassingen voor het streamen van muziek niet meegeteld worden bij de berekening van de datalimiet. Dit wordt ook wel een “zero rated” aanbod genoemd omdat voor het dataverbruik van de “bevoorrechte” toepassingen een “nultarief” wordt toegepast. Wanneer de gebruiker de overeengekomen datalimiet overschrijdt, wordt het dataverkeer beperkt of vertraagd, behalve voor deze “bevoorrechte” toepassingen. De Hongaarse telecomregulator NMHH besliste dat dergelijke aanbiedingen in strijd waren met Verordening (EU) 2015/2120, en in het bijzonder met artikel 3, lid 3 van de verordening, dat bepaalt dat aanbieders van internettoegangsdiensten bij het aanbieden van internettoegangsdiensten alle verkeer op gelijke wijze moeten behandelen, zonder discriminatie, beperking of interferentie, en ongeacht de verzender en de ontvanger, de inhoud waartoe toegang wordt verleend of die wordt verspreid, de gebruikte of aangeboden toepassingen of diensten, of de gebruikte eindapparatuur (beginsel van “netneutraliteit”). Telenor ging tegen deze beslissing in beroep bij het gerechtshof van Budapest-Hoofdstad (Fővárosi Törvényszék). Die besloot het Hof van Justitie een prejudiciële vraag te stellen over de interpretatie van de verordening.

Artikel 3, lid 1 van de verordening waarborgt het recht van eindgebruikers om op niet-discriminatoire wijze toegang te krijgen tot informatie en inhoud en deze te delen en om toepassingen en diensten te gebruiken en aan te bieden via een internettoegangsdienst. De advocaat-generaal wijst erop dat, waar artikel 3, lid 1 van de verordening het heeft over “eindgebruikers”, daaronder niet alleen de consumenten moeten worden verstaan die internettoegangsdiensten gebruiken om gebruik te maken van inhoud, toepassingen en diensten op het internet, maar ook elke persoon die internettoegangsdiensten gebruikt om inhoud, toepassingen en diensten voor het

publiek toegankelijk te maken. Artikel 3 waarborgt aldus het recht op een “open internet” niet alleen voor consumenten, maar ook voor o.a. ontwikkelaars van apps.

Volgens de advocaat-generaal zijn alinea's 2 en 3 van artikel 3 van de verordening te begrijpen als verschillende vormen van bescherming van het recht dat door het eerste lid wordt gewaarborgd. Het tweede lid van artikel 3 ziet op contractuele beperkingen terwijl het derde lid van artikel 3 op technische beperkingen ziet.

De advocaat-generaal stelt verder dat, waar artikel 3, lid 2 bepaalt dat overeenkomsten tussen aanbieders van internettoegangsdiensten en eindgebruikers en commerciële praktijken van aanbieders van internettoegangsdiensten (isp's) het recht op een “open internet” niet mogen beperken, het verschil tussen een “overeenkomst” en een “commerciële praktijk” erin bestaat dat in het eerste geval de consument uitdrukkelijk met de voorwaarden instemt wanneer hij deze met de aanbieder overeenkomt, terwijl in het tweede geval de instemming voortvloeit uit de impliciete aanvaarding door de wederpartij van de eenzijdig door de aanbieders vastgestelde voorwaarden.

Wat artikel 3, lid 3 betreft, stelt de advocaat-generaal dat het recht op gelijke behandeling van alle verkeer niet absoluut is, in die zin dat het de isp's niet belet om “redelijke verkeersbeheersmaatregelen te treffen”, op voorwaarde dat deze transparant, niet-discriminerend en evenredig zijn. Een gedifferentieerde (maar niet-discriminerende) behandeling van verkeer is dus toegestaan voor zover dit noodzakelijk is met het oog op een technisch doeltreffend verkeersbeheer.

De advocaat-generaal beschouwt dat een analyse op grond van zowel lid 2 als lid 3 van artikel 3 van de verordening tot de conclusie leidt dat een maatregel die ertoe strekt om de toegang tot niet-bevoorrechte toepassingen te vertragen onrechtmatig is. De vertraging van de toegang tot niet-bevoorrechte toepassingen is immers een technische verkeersbeheersmaatregel die uitvoering geeft aan een contractuele beperking. Toch stelt de advocaat-generaal dat het derde lid voorrang moet krijgen, omdat pas indien de vrije toegang tot het internet technisch gegarandeerd is, de vraag aan de orde komt of er contractuele beperkingen zijn die deze toegang belemmeren (bijvoorbeeld door de gebruiker ertoe aan te zetten voornamelijk of exclusief bepaalde diensten te gebruiken).

De advocaat-generaal besluit aldus dat een commerciële overeenkomst tussen een aanbieder van internettoegangsdiensten en een abonnee waarbij voor bepaalde toepassingen een nultarief wordt gehanteerd en de snelheid van de toegang tot andere toepassingen afneemt zodra het overeengekomen datavolume is verbruikt, een verkeersbeheersmaatregel inhoudt die in strijd is met de in artikel 3, lid 3, van Verordening (EU) 2015/2120 vastgestelde verplichting tot gelijke en niet-discriminerende behandeling, tenzij die maatregel onder de in dat lid opgenomen uitzonderingen valt, hetgeen ter beoordeling van de verwijzende rechter staat. Zodra een schending van artikel 3, lid 3 vaststaat, hoeft niet meer nagegaan te

worden of ook artikel 3, lid 2 van de verordening geschon- den is en hoeft evenmin een uitvoerige beoordeling van de markt en de gevolgen van de maatregel te worden ver- richt.

Conclusie van advocaat-generaal Manuel Campos Sánchez-Bordona van 4 maart 2020 in gevoegde zaken C-807/18 en C-39/19, *Telenor Magyarország Zrt. t. Nemzeti Média- és Hírközlési Hatóság Elnöke*

Karl Stas

Hoogste rechter vernietigt besluit ACM over openstellen netwerken KPN en VodafoneZiggo

Computerrecht 2020/91

Het College van Beroep voor het bedrijfsleven (CBB) heeft op 17 maart 2020 uitspraak gedaan in de beroepsproce- dures van onder meer VodafoneZiggo en KPN tegen het marktanalysebesluit Wholesale Fixed Access (WFA-be- sluit) van 27 september 2018.

In het besluit had de ACM KPN en VodafoneZiggo geza- menlijk aangewezen als partijen met aanmerkelijke markt- macht op de brede wholesalemarkt voor wholesale fixed access bestaande uit (i) (virtueel) ontbundelde toegang tot het koper- en glasvezelnetwerk (SDF-, MDF-, OLT- en ODF- access); en (ii) wholesalebreedbandtoegang (WBT) tot ko- per-, glas- en kabelnetwerken. Volgens de ACM zouden KPN en VodafoneZiggo zonder regulering beschikken over gezamenlijke marktmacht (in mededingingsrechtjargon joint dominance), omdat ze beschikken over vergelijkbare marktaandeelen en mogelijkheden en daarnaast bovendien de prikkel en de mogelijkheid zouden hebben om stilzwij- gend tot onderling afgestemd gedrag te komen. Dit zou hen in staat stellen om alternatieve aanbieders gezamenlijk van de markt te weren en daardoor te hoge retailprijzen voor eindgebruikers te hanteren. De ACM heeft beide partijen daarom verplicht om hun netwerken open te stellen onder non-discriminatoire voorwaarden en tegen gereguleerde tarieven.

Het CBB is evenwel van oordeel dat de ACM niet voldoen- de aannemelijk heeft gemaakt dat KPN en VodafoneZiggo zonder regulering de prikkel en de mogelijkheid hebben om stilzweigend tot onderling afgestemd gedrag te ko- men, gericht op het weigeren van toegang tot het eigen netwerk aan toetreders. Volgens het CBB is ACM's analyse aan de hand van de zogenoemde *Airtours*-criteria zoals deze door het Gerecht van eerste aanleg van de Europese Gemeenschappen in de uitspraak *Airtours/Commissie*

(T-342/99; ECLI:EU:T:2002:146) zijn geformuleerd, on- toereikend. Dat geldt volgens het CBB in elk geval voor de speltheoretische analyse die de ACM ten grondslag had gelegd om aannemelijk te maken dat disciplinerende via toegangsverlening een geloofwaardige disciplinerings- strategie is (derde *Airtours*-criterium). Maar ook voor de andere criteria geldt volgens het CBB dat de analyse van de ACM gebreken vertoont. Hiermee ontvalt de grondslag aan het betoog van de ACM dat KPN en VodafoneZiggo op de wholesalemarkt de prikkel en mogelijkheid zouden hebben tot het niet verlenen van toegang.

Het CBB verklaart dan ook de beroepen van onder meer VodafoneZiggo en KPN gegrond en vernietigt het WFA-be- sluit. T-Mobile had nog verzocht om de ACM de gelegen- heid te geven de gebreken te herstellen, dan wel de rechts- gevolgen van het besluit (deels) in stand te laten of een voorlopige voorziening te treffen, maar het CBB ziet daar- toe gelet op de aard van de geconstateerde gebreken geen aanleiding.

Het gevolg van de uitspraak is dat de WFA-regulering vol- ledig vervalt en dat zowel KPN als VodafoneZiggo dus niet meer gehouden zijn om toegang tot hun netwerken te ver- lenen onder non-discriminatoire voorwaarden en kosten- georiënteerde tarieven. Beide partijen hebben inmiddels hun wholesale-aanbod aangepast of volledig ingetrokken.

CBB 17 maart 2020, ECLI:NL:CBB:2020:177

Wetsvoorstel toestemmings- vereiste (opt-in) telemarketing ingediend bij Kamer

Computerrecht 2020/92

Op 25 maart 2020 heeft de Staatssecretaris van Econo- mische Zaken en Klimaat (EZK) het wetsvoorstel tot wijzi- ging van de Telecommunicatiewet (Tw) in verband met het invoeren van een opt-insysteem voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan natuurlijke personen (*Kamerstukken II* 2019/20, 35421) bij de Tweede Kamer in- gediend. Een voorontwerp was al in de zomer van 2019 via internet geconsulteerd (zie *Computerrecht* 2019/185). Het wetsvoorstel strekt tot wijziging van het Nederlandse systeem voor het telefonisch overbrengen van communi- catie voor commerciële, ideële of charitatieve doeleinden (hierna: telemarketing). Voor telemarketing geldt op dit moment nog op grond van artikel 11.7 Tw een zogenaamd opt-outsysteem: abonnees die natuurlijke personen zijn mogen ongevraagd telefonisch worden benaderd, tenzij zij zich hebben ingeschreven in het bel-me-nietregister (BMNR) of aan de verzender anderszins te kennen hebben gegeven niet te willen worden benaderd.

Dit systeem werkt in de praktijk niet goed en leidt tot veel irritatie en overlast. Het kabinet heeft daarom besloten om vooruitlopend op de inwerkingtreding van de e-Privacyverordening ook voor telemarketing een opt-insysteem te hanteren zoals thans ook al voor e-mail, fax en automatische oproepsystemen geldt.

Het uitgangspunt van dit nieuwe systeem is dat telemarketing aan natuurlijke personen niet mag plaatsvinden, tenzij de verzender kan aantonen dat deze hiervoor vooraf toestemming hebben gegeven. Op grond hiervan kunnen nieuwe klanten niet langer telefonisch worden benaderd als ze niet eerst toestemming hebben gegeven. Deze toestemming moet voldoen aan de eisen van de Algemene verordening gegevensbescherming (AVG). Voor bestaande klanten blijft gelden dat deze ongevraagd kunnen worden benaderd voor eigen gelijksoortige producten of diensten, mits de verzender kan aantonen dat hij gebruikmaakt van elektronische contactgegevens die hij heeft verkregen in het kader van de verkoop van een product of dienst, bij de verkrijging van de contactgegevens de mogelijkheid tot verzet is geboden en deze mogelijkheid ook bij elke communicatie wordt geboden.

Nieuw is voorts in het wetsvoorstel dat het gebruik van nummerblokkering niet meer is toegestaan en dat in het achtste en negende lid kapstokbepalingen zijn opgenomen voor het stellen van nadere regels voor het gebruik van contactgegevens, het recht van verzet en de termijn die kan worden gesteld voor direct marketing op basis van een klantrelatie. Opdrachtgevers en opdrachtnemers van telemarketing hebben aangegeven dit door middel van zelfregulering vorm te willen geven. Het BMNR zal komen te vervallen.

Kamerstukken II 2019/20, 35421, nr. 2

Aanpassing Nummerplan telefoon en ISDN-diensten ten behoefte van gebruik voor 113 voor zelfmoordpreventie

Computerrecht 2020/93

Bij besluit van 22 maart 2020 heeft de Staatssecretaris van Economische Zaken en Klimaat (EZK) het Nummerplan telefoon- en ISDN-diensten gewijzigd om het nummer 113 onder bepaalde voorwaarden beschikbaar te maken voor hulpverlening in het kader van suïcidepreventie. Voorheen was het nummer 113 alleen bestemd voor zogenoemde geharmoniseerde Europese korte nummers en was het niet beschikbaar voor toekenning. Met dit wijzigingsbesluit is gevolg gegeven aan kabinetsbeleid (zie Kamerbrief voortgang nummer 113 suïcidepreventie van 16 december 2019, *Kamerstukken II 2019/20, 32793, nr. 468*).

Besluit van de Staatssecretaris van Economische Zaken en Klimaat van 22 maart 2020 nr. DGBI-DE/20068537, tot wijziging van het Nummerplan Telefoon- en ISDN-diensten in verband met gebruik van het nummer 113 voor hulp in het kader van suïcidepreventie, *Stcrt.* 2020, 19241

Uitvoerbaarheidstoets ACM wijziging Tw toegangsregulering bij replicatiebelemmeringen

Computerrecht 2020/94

Op 26 maart 2020 heeft de ACM de uitvoerbaarheidstoets gepubliceerd die zij op 7 juni 2019 heeft uitgevoerd ten aanzien van de voorgenomen wijziging van de Telecommunicatiewet (hierna: Tw) in verband met toegangsregulering bij replicatiebelemmeringen. Een voorontwerp van dit wetsvoorstel is in de zomer van 2019 via internet geconsulteerd. Het wetsvoorstel zelf is in gewijzigde vorm in december 2019 naar de Tweede Kamer gestuurd (zie *Kamerstukken II 2019/20, 35368*).

Het wetsvoorstel voorziet (onder meer) in de implementatie van artikel 61 lid 3 van Richtlijn (EU) 2018/1972 van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (kortweg Telecomcode) door middel van een nieuw artikel 6.3 Tw. Deze bepaling geeft de ACM de mogelijkheid om verplichtingen op te leggen aan aanbieders van elektronische communicatienetwerken of bijbehorende faciliteiten of aan een rechthebbende van de kabels of de bijbehorende faciliteiten om de mededinging te bevorderen indien er economische of fysieke belemmeringen zijn voor de replicatie van kabels of bijbehorende faciliteiten. Indien sprake is van verschillende netwerken, kunnen dezelfde verplichtingen in beginsel aan alle aanbieders en aan andere rechthebbenden worden opgelegd. Deze mogelijkheid bestaat ongeacht of een aanbieder beschikt over aanmerkelijke marktmacht (AMM). Om deze reden wordt internationaal wel gesproken over symmetrische regulering in tegenstelling tot de asymmetrische AMM-regulering.

In de uitvoerbaarheidstoets verwelkomt de ACM de aanvullende mogelijkheden die de bepaling geeft om de doelen van de Tw te realiseren. De ACM acht deze wijzigingen van de Tw uitvoerbaar en handhaafbaar, maar vraagt de Staatssecretaris van Economische Zaken en Klimaat wel om de punten in de Annex bij de uitvoerbaarheidstoets in het wetsvoorstel of de memorie van toelichting te verwerken. Tevens geeft de ACM aan dat de uitvoering van de bepaling waarschijnlijk extra inzet van mensen en middelen zal vergen.

Nieuwsbericht ACM, 'Uitvoeringstoets Toegangsregulering replicatiebelemmeringen', 26 maart 2020

Uitvoerbaarheidstoets ACM wijziging Tw verlagen drempels overstappen en geografisch onderzoek

Computerrecht 2020/95

Op 30 maart 2020 heeft de ACM de uitvoerbaarheidstoets gepubliceerd die zij op 17 mei 2019 heeft uitgevoerd in verband met de voorgenomen wijziging van de Telecommunicatiewet (Tw) inzake het verder verlagen van drempels bij het overstappen van telecomaandbieder, en het voorzien in een bevoegdheid tot het vorderen van inlichtingen ten behoeve van een geografisch onderzoek naar het bereik van elektronische communicatienetwerken.

Een voorontwerp was al eind 2018 via internet geconsulteerd. Uiteindelijk is de regeling evenwel gezamenlijk met de regeling voor toegangsverplichtingen bij replicatiebelemmeringen in een wetsvoorstel opgenomen en in december 2019 naar de Tweede Kamer gestuurd (zie *Kamerstukken II 2019/20, 35368*).

De ACM geeft aan dat zij de wijzigingen van de Tw uitvoerbaar en handhaafbaar acht en het toezicht met de bestaande mensen en middelen uitvoert. Wel geeft de ACM aan dat het de voorkeur heeft indien de Staatssecretaris van Economische Zaken en Klimaat nadere regels stelt zoals het formaliseren van de werkprocessen van de Vereniging COIN en het uitwerken van hoe de wilsuiking van de abonnee aan de nieuwe telecomaandbieder opgevraagd kan worden door de oude dienstverlener.

Nieuwsbericht ACM, 'Uitvoeringstoets verlagen drempels overstappen en geografisch onderzoek', 30 maart 2020

AMC neemt besluit op bezwaar over glasvezels TenneT

Computerrecht 2020/96

Op 31 januari 2020 heeft de ACM een besluit op bezwaar genomen van de Federatie Particulier Grondbezit (FPG). De ACM had eerder besloten een handhavingsverzoek van de FPG niet in behandeling te nemen omdat er onvoldoende informatie was verstrekt. Aangezien de FPG in de bezwaarprocedure nieuwe informatie had verstrekt, kon de ACM het handhavingsverzoek nu toch in behandeling nemen. In het handhavingsverzoek had de FPG de ACM verzocht om onderzoek te doen naar het vermeende gebruik van glasvezels van TenneT voor een openbaar elektronisch communicatienetwerk. Glasvezels van TenneT die onder

de grond van een van de leden van de FPG liggen, zouden volgens de FPG gebruikt worden om een openbaar elektronisch communicatienetwerk aan te bieden omdat onbenutte overcapaciteit door TenneT tegen betaling beschikbaar werd gesteld, onder andere aan Relined, een 100% dochteronderneming van TenneT. Het was de ACM echter niet gebleken dat TenneT haar netwerk zelf als openbaar elektronisch communicatienetwerk exploiteert. TenneT heeft een elektronisch communicatienetwerk, bestaande uit glasvezels, aangelegd voor het functioneren van een hoogspanningsverbinding. Dit functioneren ziet volgens TenneT op de bediening, bewaking en besturing van het hoogspanningsnet. Bovendien legt TenneT extra capaciteit en lege mantelbuizen aan om de integriteit van het netwerk te beschermen bij storingen. Dit netwerk kwalificeert derhalve naar het oordeel van de ACM niet als een openbaar elektronisch communicatienetwerk.

Nieuwsbericht ACM, 'Beslissing op bezwaar FPG over glasvezels van TenneT', 23 maart 2020

Raoul Grifoni Waterman

AMC adviseert EZK over frequentievergunningen

Computerrecht 2020/97

De ACM heeft op 14 februari 2019 een advies gegeven aan het Ministerie van Economische Zaken en Klimaat (EZK) over mogelijke beperkingen op het gebruik van radiofrequenties. EZK had de ACM gevraagd om advies in het kader van een voorgenomen wijziging van de Telecommunicatiewet. EZK vroeg de ACM onder meer of de gebruiksbeperking van radiofrequenties moest worden aangepast. Momenteel mogen commerciële radiozenders namelijk over maximaal vier landelijke frequentievergunningen beschikken. Daarmee kunnen vier radiozenders worden uitgezonden. In het advies heeft de ACM haar visie gegeven op de markten voor radio (de radioluistermarkt en de radioadvertentiemarkt) en de concurrentiesituatie op die markten. De ACM heeft op basis van die visie geadviseerd om het toegestane maximumbezit van vier landelijke frequentievergunningen niet verder uit te breiden.

De besluiten die door de Nederlandse regering zijn genomen met betrekking tot frequenties voor (digitale) radio zijn hieronder beschreven.

Nieuwsbericht ACM, 'Advies gebruiksbeperking radiofrequenties', 31 maart 2020

Raoul Grifoni Waterman

Tijdelijke verdeling frequenties lokale digitale radio

Computerrecht 2020/98

In februari en maart 2020 is een vijftal besluiten en regelingen in de *Staatscourant* gepubliceerd die van belang zijn voor de tijdelijke verdeling van frequenties voor digitale radio-omroep die door de Staatssecretaris van Economische Zaken en Klimaat (EZK) bij brief van 1 april 2019 is aangekondigd (zie *Kamerstukken II* 2018/19, 24095, nr. 463). Deze tijdelijke verdeling vindt plaats in afwachting van de definitieve uitkomsten van de lopende internationale coördinatie van frequentieruimte die naar verwachting voor de voor lokale digitale radio gereserveerde laag 6 in 2022 gereed zijn. De huidige verdeling is een tijdelijke uitgifte onder lichte voorwaarden tot en met uiterlijk 31 augustus 2022. Na deze termijn zal de beschikbare frequentieruimte opnieuw worden uitgegeven onder nieuwe voorwaarden. De volgende besluiten en regelingen zijn gepubliceerd:

- 1) Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 19 februari 2020, nr. WJZ/20004712, tot wijziging van de Regeling aanvraagprocedure bij verlening op volgorde van binnenkomst en de Regeling extra vergunningen publieke mediadienst, in verband met een tijdelijke verdeling van frequentieruimte in laag 6 voor lokale digitale radio-omroep.
- 2) Besluit van de Staatssecretaris van Economische Zaken en Klimaat van 19 februari 2020, nr. DE/20028289, houdende wijziging van het Nationaal Frequentieplan 2014 (digitale radio-omroep, laag 6).
- 3) Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 13 februari 2020, nr. WJZ/19242023, tot vaststelling van tijdelijke regels met betrekking tot de maximale hoeveelheid frequentieruimte bestemd voor commerciële FM-radio-omroep die één rechtspersoon kan gebruiken of verwerven (Tijdelijke regeling gebruiksbeperking commerciële FM-radio-omroep).
- 4) Besluit van 21 februari 2020 tot vaststellen aanvang aanvraagprocedure vergunningen voor lokale digitale radio-omroep.
- 5) Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 24 maart 2020, nr. WJZ/19185916, tot instelling van het Adviescollege verdeling frequentieruimte commerciële radio (Regeling instelling Adviescollege verdeling frequentieruimte commerciële radio).

De besluiten en regelingen hebben de volgende gevolgen.

- 1) De wijzigingsregeling voegt een nieuwe paragraaf 3a toe aan hoofdstuk 3 Regeling aanvraagprocedure bij verlening op volgorde van binnenkomst waardoor bepaalde voorschriften voor de verdeling van vergun-

ningen voor laagvermogen middengolf grotendeels van overeenkomstige toepassing zijn verklaard op de verdeling van vergunningen voor commerciële digitale radio-omroep in laag 6. Tevens wordt bepaald dat aanvragen pas kunnen worden ingediend vanaf een door de minister te bepalen tijdstip en dat voor aanvragen die binnen vier weken na dit tijdstip worden ingediend ten hoogste één vergunning per allotment wordt verleend per rechtspersoon. Daarnaast creëert de wijzigingsregeling ook een grondslag voor de verlening van extra vergunningen aan lokale publieke media-instellingen voor een bepaalde hoeveelheid frequentieruimte in laag 6.

- 2) Het Besluit van 19 februari 2020 strekt ertoe het Nationaal Frequentieplan 2014 te wijzigen om de genoemde frequentieruimte in laag 6 voor lokale digitale radio-omroep beschikbaar te stellen.
- 3) De Tijdelijke regeling gebruiksbeperking commerciële FM-radio-omroep strekt ertoe tijdelijke regels vast te stellen met betrekking tot de maximale hoeveelheid frequentieruimte bestemd voor commerciële FM-radio-omroep die één rechtspersoon kan gebruiken of verwerven. Deze regels beogen vooral de al onder de Mediawet 2008 bestaande voorschriften beter aan te laten sluiten op de terminologie van de Telecommunicatiewet.
- 4) Het Besluit van 21 februari 2020 tot vaststellen aanvang aanvraagprocedure vergunningen voor lokale digitale radio-omroep bepaalt dat aanvragen voor de tijdelijke verdeling van frequentieruimte in laag 6 voor lokale digitale radio-omroep kunnen worden ingediend vanaf 10 maart 2020 om 09:00 uur.
- 5) De Regeling instelling Adviescollege verdeling frequentieruimte commerciële radio regelt de instelling van het Adviescollege verdeling frequentieruimte commerciële radio, dat advies uit zal brengen over de wijze waarop en de voorwaarden waaronder de vergunningen bestemd voor commerciële radio-omroep kunnen worden uitgegeven voor de periode na 2022, alsmede over het beëindigen van het gebruik van frequentieruimte voor commerciële analoge radio-omroep.

Bronnen:

- Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 19 februari 2020, nr. WJZ/20004712, tot wijziging van de Regeling aanvraagprocedure bij verlening op volgorde van binnenkomst en de Regeling extra vergunningen publieke mediadienst, in verband met een tijdelijke verdeling van frequentieruimte in laag 6 voor lokale digitale radio-omroep, *Stcrt.* 2020, 8766
- Besluit van de Staatssecretaris van Economische Zaken en Klimaat van 19 februari 2020, nr. DE/20028289, houdende wijziging van het Nationaal Frequentieplan 2014 (digitale radio-omroep, laag 6), *Stcrt.* 2020, 9370
- Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 13 februari 2020, nr. WJZ/

19242023, tot vaststelling van tijdelijke regels met betrekking tot de maximale hoeveelheid frequentieruimte bestemd voor commerciële FM-radio-omroep die één rechtspersoon kan gebruiken of verwerven (Tijdelijke regeling gebruiksbeperking commerciële FM-radio-omroep), *Stcrt.* 2020, 10066

- Besluit van 21 februari 2020 tot vaststellen aanvang aanvraagprocedure vergunningen voor lokale digitale radio-omroep, *Stcrt.* 2020, 11907
- Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 24 maart 2020, nr. WJZ/19185916, tot instelling van het Adviescollege verdeling frequentieruimte commerciële radio (Regeling instelling Adviescollege verdeling frequentieruimte commerciële radio), *Stcrt.* 2020, 19074

Raoul Grifoni Waterman

Besluiten frequenties mobiele communicatie 700, 1400 en 2100 MHz-band

Computerrecht 2020/99

Op 6 maart 2020 zijn door het Ministerie van Economische Zaken en Klimaat ook drie besluiten en regelingen met betrekking tot de veiling van frequentievergunningen voor mobiele communicatie in de 700, 1400 en 2100 MHz-band in de *Staatscourant* gepubliceerd. Het gaat om:

- 1) Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 6 maart 2020, nr. WJZ/20063207, tot vaststelling van de maximale hoeveelheid frequentieruimte voor mobiele communicatie (Capregeling frequenties mobiele communicatie 2020).
- 2) Besluit van de Staatssecretaris van Economische Zaken en Klimaat van 6 maart 2020, nr. WJZ/20062913, inzake de keuze voor het instrument veiling van vergunningen voor mobiele communicatie in de 700, 1400 en 2100 MHz-band en de vaststelling van de te veilen vergunningen.
- 3) Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 6 maart 2020 nr. WJZ/20062897, tot vaststelling van de aanvraag- en veilingprocedure voor vergunningen voor frequentieruimte in de 700, 1400 en 2100 MHz-band ten behoeve van mobiele communicatietoepassingen en wijziging van de Regeling vergoedingen Agentschap Telecom 2020 (Regeling aanvraag- en veilingprocedure vergunningen 700, 1400 en 2100 MHz) *Stb.* 2020, 13725.

De besluiten en regelingen hebben de volgende gevolgen:

- 1) De Capregeling frequenties mobiele communicatie 2020 stelt vast hoeveel frequentieruimte door een enkele partij kan worden verworven. Uit de regeling

blijkt dat er twee 'caps' zijn. Het gaat allereerst om een globale spectrumcap waardoor partijen niet meer dan 40% van de totale frequenties voor mobiele communicatie kunnen hebben. In aanvulling daarop wordt er een cap ingevoerd op lage frequenties voor mobiele communicatie van 40% van de frequenties onder de 1 GHz.

- 2) Het Besluit van 6 maart 2020 bevat de keuze voor het instrument veiling van vergunningen voor mobiele communicatie in de 700, 1400 en 2100 MHz-band en de vaststelling van de te veilen vergunningen.
- 3) De Regeling aanvraag- en veilingprocedure vergunningen 700, 1400 en 2100 MHz bevat de voorwaarden waaraan aanvragen moeten voldoen en bevat de regels voor de veiling.

Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 6 maart 2020, nr. WJZ/20063207, tot vaststelling van de maximale hoeveelheid frequentieruimte voor mobiele communicatie (Capregeling frequenties mobiele communicatie 2020), *Stcrt.* 2020, 13724

Besluit van de Staatssecretaris van Economische Zaken en Klimaat van 6 maart 2020, nr. WJZ/20062913, inzake de keuze voor het instrument veiling van vergunningen voor mobiele communicatie in de 700, 1400 en 2100 MHz-band en de vaststelling van de te veilen vergunningen, *Stcrt.* 2020, 13729

Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 6 maart 2020 nr. WJZ/20062897, tot vaststelling van de aanvraag- en veilingprocedure voor vergunningen voor frequentieruimte in de 700, 1400 en 2100 MHz-band ten behoeve van mobiele communicatietoepassingen en wijziging van de Regeling vergoedingen Agentschap Telecom 2020 (Regeling aanvraag- en veilingprocedure vergunningen 700, 1400 en 2100 MHz), *Stcrt.* 2020, 13725

Raoul Grifoni Waterman

Belgie

BMA verlengt de voorlopige maatregel met betrekking tot de samenwerking tussen Proximus en Orange niet

Computerrecht 2020/100

Zoals wij in "BMA schort samenwerking tussen Proximus en Orange tijdelijk op", *Computerrecht* 2020/21 berichtten, heeft het College van de Belgische Mededingingsautoriteit

op 8 januari 2020 beslist om een voorlopige maatregel op te leggen aan Proximus en Orange, die ertoe strekte hun samenwerking op het vlak van het delen van mobiele netwerkinfrastructuur op te schorten tot 16 maart 2020. De partijen dienden het College en het Auditoraat van de BMA ten laatste op 9 maart 2020 te informeren over hun besprekingen met het BIPT over deze samenwerking. De BMA heeft ervan afgezien om de maatregel nog te verlengen of andere maatregelen op te leggen. Blijkbaar heeft het Auditoraat, na kennis te hebben genomen van het verslag van de partijen en het standpunt van het BIPT, het niet nodig geacht om het College nog om maatregelen te vragen. Proximus en Orange kunnen dus de uitvoering van hun samenwerkingsakkoord hervatten. Het onderzoek ten gronde over de klacht van Telenet loopt nog.

Persbericht Proximus van 18 maart 2020

BIPT neemt 5 operatoren in aanmerking voor voorlopige gebruiksrechten 5G, verlengt termijn voor kandidaturen voor bijkomend 4G spectrum

Computerrecht 2020/101

Het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT) heeft de lijst gepubliceerd van in aanmerking genomen kandidaten voor de toekenning van voorlopige gebruiksrechten in de radiofrequentieband 3600-3800 MHz, bestemd voor het aanbieden van 5G-diensten. De weerhouden kandidaten zijn, naast de bestaande mobiele netwerkopérateurs Proximus, Orange en Telenet, het Limburgse IT-bedrijf Cegeka en het West-Vlaamse bedrijf Entropia, dat zich toelegt op missie-kritische telecommunicatienetwerken voor spraak- en datacommunicatie (inclusief IoT).

In totaal is er 200 MHz beschikbaar in de frequentieband 3600-3800 MHz. Er is dus voldoende spectrum beschikbaar om elke kandidaat 40 MHz toe te kennen. Deze voorlopige gebruiksrechten zijn geldig tot de toekenning van de definitieve gebruiksrechten via een klassieke veiling die wellicht pas in de loop van 2021 zal kunnen doorgaan. De besluitvorming over de veiling zit in een impasse wegens onenigheid tussen de federale regering en de deelstaten over de verdeling van de opbrengst ervan.

Zoals we hier eerder berichtten (*Computerrecht 2020/61*), heeft het BIPT daarom een voorlopige oplossing uitgewerkt. Op 30 januari 2020 publiceerde het Instituut een oproep tot kandidaten die een voorlopige vergunning

wensen te bekomen voor een initiële ontplooiing van 5G in België. De kandidaten konden tot 28 februari 2020 een aanvraag indienen.

Over de toekenning van de voorlopige gebruiksrechten organiseert het BIPT nu een openbare raadpleging die tot 21 april 2020 loopt. Nadien zal het BIPT vijf individuele besluiten nemen over de toekenning van de voorlopige gebruiksrechten aan de kandidaten.

Daarnaast heeft het BIPT ook de termijn verlengd voor het indienen van de kandidaturen voor het verkrijgen van bijkomend spectrum voor 4G. Het betreft een nog niet toegewezen blok van 15 MHz duplex in de frequentieband 2,6 GHz. Het Brugse bedrijf Citymesh, dat al private netwerken exploiteert in de 3,6 GHz-frequentieband, had daar interesse voor getoond. De bestaande mobiele netwerkopérateurs, die al over spectrum in deze band beschikken, komen niet in aanmerking.

De oorspronkelijke deadline om zich kandidaat te stellen, 23 maart 2020, wordt nu uitgesteld tot 15 mei 2020. Het BIPT rechtvaardigt dit door te verwijzen naar de strenge maatregelen om de verspreiding van het coronavirus tegen te gaan, waardoor “de kandidaten de nodige hinder ondervinden om hun dossier tijdig in te dienen”.

Publicaties BIPT van 24 maart 2020 en 19 maart 2020

CRC meldt groothandels-tarieven voor kabeltoegang aan bij de Europese Commissie

Computerrecht 2020/102

De Belgische regulatoren voor telecommunicatie- en audiovisuele mediadiensten, verenigd in de Conferentie van Regulatoren voor de elektronische communicatiesector (CRC), hebben op 6 april 2020 hun ontwerpbesluit over de (definitieve) groothandelstarieven voor de gereguleerde toegang tot de kabel aangemeld bij de Europese Commissie. In haar besluit betreffende de analyse van de markten voor breedband en televisieomroep van 29 juni 2018 had de CRC de operatoren met aanmerkelijke marktmacht onder meer een verplichting tot prijscontrole opgelegd. Wat betreft de toegang tot de kabel betrof het een verplichting om “billijke” prijzen toe te passen. Deze “billijke” prijzen zouden vastgesteld worden op basis van een kostenmodel. In afwachting dat zo een kostenmodel kon worden uitgewerkt, stelde de CRC “voorlopige” tarieven vast.

In juli 2019 legde de CRC een ontwerpbesluit tot vaststelling van de “definitieve” groothandelstarieven ter openbare consultatie voor. Op dat ontwerpbesluit kwam heel wat kritiek van de kabeloperatoren, die vonden dat een aantal kosten ten onrechte niet mee in rekening was genomen.

Op basis van de reacties op de raadpleging heeft de CRC nu haar ontwerpbesluit herzien, wat geleid heeft tot een verhoging van de groothandelstarieven. Orange, op dit ogenblik de enige afnemer van de groothandelstoegang tot de kabelnetten, heeft onmiddellijk gereageerd dat de nieuwe tarieven tot “*een aanzienlijke overcompensatie van de werkelijke kosten van de kabelnetten*” zouden leiden. Orange vreest vooral dat de toegekende investeringstoeslag de kabeloperatoren een “*monopolie-meeropbrengst*” zal opleveren.

De Commissie heeft nu 30 dagen (dus tot begin mei) om haar standpunt te bepalen. Indien de Commissie geen fundamentele opmerkingen heeft, zullen de Belgische reguleratoren het ontwerpbesluit definitief aannemen.

CIRCABC databank van de Europese Commissie en persbericht van Orange van 7 april 2020

geselecteerde operator niet aan de dekkingseisen heeft voldaan tegen de vastgestelde datum (*in casu* 12 juni 2012), dit een automatisch verval van zijn gebruiksrechten voor frequenties in de 2 GHz-band tot gevolg heeft.

In het licht van de hiervoor besproken uitspraak van het Hof van Justitie over de andere prejudiciële vraag, laat het antwoord zich raden.

Publicatie BIPT van 14 februari 2020

Rechtbank van eerste aanleg stelt prejudiciële vraag aan Hof van Justitie over regelgevend kader voor mobiele satellietdiensten

Computerrecht 2020/103

In een zaak van ViaSat tegen het BIPT en de Belgische Staat heeft de Franstalige rechtbank van eerste aanleg van Brussel een prejudiciële vraag gesteld aan het Hof van Justitie over de interpretatie van Beschikking nr. 626/2008/EG van het Europees Parlement en de Raad van 30 juni 2008 inzake de selectie en machtiging van systemen die mobiele satellietdiensten (MSS) leveren (MSS-beschikking).

Deze zaak is te situeren in de context van de pogingen van ViaSat om via diverse gerechtelijke procedures in verschillende lidstaten te verhinderen dat Inmarsat haar *European Aviation Network* (EAN) zou kunnen ontplooiën. Dit netwerk zou moeten toelaten om breedband internettoegang te verschaffen aan boord van vliegtuigen die het Europese luchtruim doorkruisen. Elders in dit nummer berichtten wij al over een recente uitspraak van het Hof van Justitie over een andere prejudiciële vraag die in dezelfde context werd gesteld door het Hof van beroep Brussel (afdeling Marktenhof).

De vordering van ViaSat voor de nationale rechter strekt ertoe te horen zeggen voor recht dat het recht van Inmarsat om in België gebruik te maken van de frequentieband 2 GHz voor het leveren van mobiele satellietdiensten vervallen is, omdat Inmarsat niet tijdig aan haar dekkingseisen heeft voldaan.

Met haar prejudiciële vraag aan het Hof van Justitie wil de rechtbank in wezen vernemen of de MSS-beschikking zo moet worden geïnterpreteerd dat, indien vaststaat dat een

Europa

Persoonsgegevens als betaalmiddel voor digitale diensten

Computerrecht 2020/104

Op 27 november 2019 keurden het Europees Parlement en de Raad een nieuwe richtlijn goed die wijzigingen aanbrengt aan het Europese consumentenrecht (met name aan Richtlijn 93/13/EEG (oneerlijke bedingen in consumentenovereenkomsten), Richtlijn 98/6/EG (prijsaanduiding), Richtlijn 2005/29/EG (oneerlijke handelspraktijken van ondernemingen jegens consumenten) en Richtlijn 2011/83/EU (consumentenrechten), samen aangeduid als het consumentenbeschermingsrecht). Deze nieuwe Richtlijn (EU) 2019/2161 beoogt de modernisering van het consumentenbeschermingsrecht gelet op de ontwikkelingen in de online handel met consumenten.

De nieuwe richtlijn wijzigt het toepassingsgebied van Richtlijn 2011/83/EU inzake consumentenrechten. Voorheen kon een consument zijn rechten enkel afdwingen indien hij een prijs betaalde voor de levering van een digitale dienst. Deze nieuwe richtlijn maakt dit expliciet ook mogelijk wanneer de consument de digitale diensten ontvangt zonder betaling van een geldsom maar in ruil voor zijn persoonsgegevens. Waar de handelaar uitsluitend persoonsgegevens verwerkt die noodzakelijk zijn voor het leveren van de digitale diensten of om aan een wettelijke verplichting te voldoen en de persoonsgegevens niet voor andere doeleinden verwerkt, zal er geen sprake zijn van enige "betaling" met persoonsgegevens.

Richtlijn (EU) 2019/2161 roept verder nieuwe regels in het leven of wijzigt bestaande regels inzake onder andere de prijsaanduiding van producten, het herroepingsrecht, het aanbieden van een online marktplaats en het weergeven van (valse) consumentenbeoordelingen en -aanbevelingen.

Ten slotte worden ook de sanctiemechanismen in het consumentenbeschermingsrecht aangepast om meer geharmoniseerde en verstrengde sanctieregels in te voeren voor wijdverbreide inbreuken of wijdverbreide inbreuken met een Uniedimensie (in de zin van Verordening (EU) 2017/2394). Het betreft inbreuken waarbij schade wordt veroorzaakt of waarschijnlijk wordt veroorzaakt aan de collectieve belangen van consumenten in ten minste drie lidstaten of in ten minste twee derde van de lidstaten waarvan de bevolking ten minste twee derde uitmaakt van de bevolking van de Unie. Als gevolg van een gecoördineerde actie op grond van Verordening (EU) 2017/2394, kan een nationale bevoegde autoriteit aan de verantwoordelijke handelaar een geldboete opleggen van ten minste 4% van de jaar-

omzet van de handelaar in alle lidstaten die betrokken zijn bij de gecoördineerde handhavingsactie.

België heeft tot 28 november 2021 de tijd om de bepalingen van Richtlijn (EU) 2019/2161 om te zetten naar Belgisch recht. De nieuwe bepalingen zullen van toepassing zijn op de ondernemingen vanaf 28 mei 2022.

Richtlijn (EU) 2019/2161 van het Europees Parlement en de Raad van 27 november 2019 tot wijziging van Richtlijn 93/13/EEG van de Raad en Richtlijnen 98/6/EG, 2005/29/EG en 2011/83/EU van het Europees Parlement en de Raad wat betreft betere handhaving en modernisering van de regels voor consumentenbescherming in de Unie.

Dorien Taeymans

Schending art. 8 EVRM omwille van onbeperkte bewaring persoonsgegevens

Computerrecht 2020/105

Het Europees Hof voor de Rechten van de Mens ("EHRM") oordeelde op 13 februari 2020 dat artikel 8 van het Europees Verdrag voor de Rechten van de Mens ("EVRM") werd geschonden omwille van onbeperkte bewaring van persoonsgegevens.

In 2008 werd de heer Gaughran tegengehouden tijdens een politiecontrole. De politie meende dat de heer Gaughran reed onder invloed en nam hem mee naar het politiebureau voor verder onderzoek. Bij dit onderzoek werden vingerafdrukken, een foto en een DNA-speekseltest afgenomen bij de heer Gaughran. Op basis van deze DNA-speekseltest werd een DNA-profiel opgesteld. De heer Gaughran werd door de rechtbank schuldig bevonden aan rijden onder invloed. Hij kreeg een boete van 50 Britse pond en een rijverbod van twaalf maanden.

In 2015 werd het resultaat van de DNA-speekseltest verwijderd door de politiediensten. Het DNA-profiel, de foto en de vingerafdrukken werden bijgehouden ondanks verscheidene verzoeken van de heer Gaughran om deze biometrische gegevens te vernietigen of terug te geven. Na een verwoede poging om via de nationale gerechtelijke weg de vernietiging of teruggave van zijn persoonsgegevens te bekomen bracht de heer Gaughran de zaak voor het EHRM. Volgens de heer Gaughran werd met het bijhouden van zijn biometrische gegevens voor een onbepaalde termijn zijn recht op privé-, familie- en gezinsleven onder artikel 8 EVRM geschonden.

Het werd door het Verenigd Koninkrijk niet betwist dat het bijhouden van deze persoonsgegevens een inmenging betreft van het recht op privéleven van de heer Gaughran. De vraag waar het EHRM zich dan ook over moest buigen betrof de (beweerde) rechtvaardiging van deze inmenging op grond van het tweede lid van artikel 8 EVRM.

Het EHRM oordeelde dat de inmenging in overeenstemming was met de nationale wetgeving (er was immers een wettelijke basis voorhanden voor de politiediensten om de vingerafdrukken, de foto en het DNA te verzamelen) en dat het een legitiem doel nastreefde, namelijk de opsporing en voorkoming van misdaad. De grote hamvraag was de noodzakelijkheid in een democratische samenleving. De persoonsgegevens werden bijgehouden zonder enig onderscheid in of verwijzing naar de aard en de ernst van de overtreding en zonder enige verwijzing naar de noodzaak voor het bijhouden van deze persoonsgegevens voor onbepaalde tijd. Meer zelfs, de politiediensten werden bij wet enkel toegestaan om deze gegevens te verwijderen in uiterst uitzonderlijke omstandigheden. Er bestond geen bepaling die de betrokkene het recht gaf om de verwijdering van zijn biometrische gegevens en foto's te vragen indien blijkt dat zij niet langer noodzakelijk zijn gelet op onder andere de aard van de overtreding, de leeftijd van de betrokkene of de tijd die is verstreken. Het EHRM stelt dan ook vast dat de ongedifferentieerde bevoegdheid om het DNA-profiel, de vingerafdrukken en de foto van de heer Gaughran te bewaren, zelfs nadat zijn straf reeds werd volbracht, zonder verwijzing naar de ernst van het strafbaar feit of de noodzaak van de bewaring voor onbepaalde tijd en bij gebrek aan een reële controlemogelijkheid voor de betrokkene, geen billijk evenwicht creëert tussen de concurrerende openbare en particuliere belangen. Artikel 8 EVRM werd geschonden door het Verenigd Koninkrijk.

EHRM nr. 45245/15, 13 februari 2020, *Gaughran t. Verenigd Koninkrijk*.

Dorien Taeymans

Nederland

Standpunten AP in het kader van Corona & Privacy

Computerrecht 2020/106

In navolging van de verklaringen van de European Data Protection Board (EDPB) heeft de Autoriteit Persoonsgegevens (AP) standpunten ingenomen over privacy in relatie tot (de bestrijding van) corona.

Thuiswerken en passende maatregelen

Op 18 maart 2020 publiceert de AP een nieuwsbericht op haar website met adviezen over veilig thuiswerken.

Coulance

Op 20 maart 2020 publiceert de AP een nieuwsbericht dat overheden en bedrijven tijdens de coronacrisis meer ruimte krijgen. De AP benoemt dat partijen langer de tijd krijgen om te reageren op vragen en dat initiatieven om de volksgezondheid te beschermen ruim baan krijgen. Wat de coulanceregeling precies inhoudt wordt niet nader ingevuld.

Corona op de werkvloer

De AP benadrukt op de speciale webpagina 'Corona op de werkvloer' dat verwerking van medische gegevens door werkgevers niet is toegestaan en zoals gebruikelijk via de bedrijfsarts moet verlopen. Wel mag de werkgever onder de bijzondere omstandigheid van het coronavirus werknemers naar huis sturen bij verkoudheid of koorts. Ten aanzien van het testen van werknemers op corona heeft de AP de informatie een aantal keer gewijzigd en aangevuld. Dat wijst mogelijk op voortschrijdend inzicht. Op 23 maart 2020 publiceerde de AP een bericht dat het voor werkgevers in de zorgsector is toegestaan om hun werknemers te testen op corona. Later is deze opmerking verwijderd en is slechts nog opgenomen dat werkgevers niet zelf mogen testen op corona. Vervolgens is gepubliceerd dat werknemers wel gevraagd mag worden om zichzelf te testen. Het ontbreekt op dit punt echter aan duidelijke richtsnoeren voor de praktijk.

Gebruik corona-app

De AP publiceert op 8 april 2020 een nieuwsbericht waaruit volgt dat de inzet van corona-apps waarbij data van telecomproviders worden gedeeld zonder toestemming van betrokkenen een wetswijziging vereist.

www.autoriteitpersoonsgegevens.nl

Eliëtte Vaal

Kabinet versoepelt privacy-regels voor delen persoonsgegevens huisartsen

Computerrecht 2020/107

Vanwege het coronavirus stemt het kabinet in met een tijdelijke maatregel die vanaf 15 april 2020 inzage in medische gegevens mogelijk maakt door artsen op de huisartsenpost of spoedeisende hulp van patiënten die daar

geen expliciete toestemming voor hebben gegeven. Normaliter zijn via het Landelijk Schakel Punt (LSP) medische gegevens van ongeveer acht miljoen Nederlanders met toestemming van betrokkenen beschikbaar op de huisartsenpost (HAP). Een klein deel van de Nederlanders heeft toestemming geweigerd, maar een veel groter deel heeft nog geen keuze gemaakt. Voor deze laatste groep maakt de tijdelijke maatregel het mogelijk dat inzage wordt verkregen zonder opt-in. Dat zorgt ervoor dat artsen minder tijd kwijt zijn en vaker beschikken over een medisch dossier zodat ze beter kunnen afwegen of patiënten naar het ziekenhuis worden doorgestuurd of thuis moet uitzielen. Deze 'corona opt-in' is alleen van kracht tijdens de duur van de coronacrisis. Volgens de AP mogen artsen op de huisartsenpost of spoedeisende hulp alleen met toestemming van coronapatiënten het medisch dossier bij hun huisarts inzien via een elektronisch uitwisselingssysteem.

Artsenfederatie KNMG

Eliëtte Vaal

Kentekenparkeersysteem gemeente Amsterdam niet in strijd met art. 8 EVRM

Computerrecht 2020/108

De gemeente Amsterdam hanteert sinds 2013 een systeem van kentekenparkeren waarbij de persoon die parkeert via de parkeerautomaat of mobiele telefoon verplicht is het kenteken van zijn auto in te voeren om parkeerbelasting te betalen. Controle vindt plaats met gebruik van scanauto's. De resultaten worden in versleutelde vorm bewaard. Als blijkt dat de parkeerbelasting niet is voldaan, wordt de versleuteling ongedaan gemaakt en vraagt de heffingsambtenaar bij de Rijksdienst voor het Wegverkeer de persoonsgegevens van de kentekenhouder op. Vervolgens wordt een naheffingsaanslag parkeerbelasting opgelegd aan de kentekenhouder.

Het Hof Amsterdam oordeelde dat het parkeersysteem van de gemeente geen ongeoorloofde inbreuk op de privacy inhield en dat aan artikel 8 EVRM geen recht op betaling van parkeerbelasting door middel van contant geld kan worden ontleend.

Onder verwijzing naar jurisprudentie van het EHRM oordeelt de Hoge Raad (HR) – anders dan het Hof – dat het gebruik van het kentekenparkeersysteem wel degelijk een inmenging oplevert door de gemeente in het recht van de parkeerder op respect voor zijn privéleven ex artikel 8

EVRM. Daarbij is van belang dat het kenteken door de heffingsambtenaar kan worden gekoppeld aan de gedragingen van de persoon en dat het kenteken op een systematische wijze wordt verzameld, vastgelegd, bewerkt, gedurende enige tijd wordt bewaard en gebruikt. Het feit dat de controle van de parkeerbelasting met registratie van het kenteken verwacht kon worden door de parkeerder, doet daar niets aan af. De redelijke privacyverwachting is volgens de HR niet doorslaggevend bij de beoordeling van de vraag of het privéleven wordt geraakt als het gaat om waarnemingen in de openbare ruimte. De HR acht de inmenging door het hanteren van het kentekenparkeersysteem door de gemeente echter wel gerechtvaardigd op grond van artikel 8 lid 2 EVRM. De inmenging is voorzien bij wet (de eis van opgave van het kenteken volgt uit de Gemeentelijke Parkeerverordening in combinatie met de Gemeentewet) en dient een legitiem doel (te weten het waarborgen dat gemeentelijke belasting zoals de parkeerbelasting wordt betaald voor het economisch welzijn van het land). Het kentekenparkeersysteem is dus niet in strijd met artikel 8 EVRM.

HR 10 april 2020, ECLI:NL:HR:2020:639

Eliëtte Vaal

De bestuursrechter bevoegd inzake schadevergoeding op grond van de AVG

Computerrecht 2020/109

Op 1 april 2020 verklaart de Afdeling bestuursrechtspraak van de Raad van State zich in een viertal zaken bevoegd te oordelen over verzoeken van schadevergoeding op grond van de AVG die zijn veroorzaakt door privacyschendingen van bestuursorganen. De grondslag voor bevoegdheid wordt aangenomen op grond van artikel 8:88 Awb in combinatie met artikel 34 Uitvoeringswet AVG. Vereist is dat de schadevergoedingsclaim in verband staat met een besluit van een bestuursorgaan op een verzoek ex artikel 15-22 AVG (zoals een verzoek tot inzage, rectificatie en/of wissing van persoonsgegevens). Niet vereist is dat het besluit van het bestuursorgaan op het verzoek tot inzage, rectificatie zelf onrechtmatig is. Voor de beoordeling van vergoeding van immateriële schade sluit de Afdeling volgens vaste jurisprudentie aan bij het civiele schadevergoedingsrecht. Daarnaast is de bestuursrechter onbevoegd te oordelen over schadevergoedingen van meer dan EUR 25.000.

In slechts één van de vier zaken is schadevergoeding toegewezen. Dit betreft de ongeoorloofde verstrekking van medische gegevens aan een tuchtcollege door de directeur

van het Pieter Baan Centrum bij de afwikkeling van een klacht die tegen hem was ingesteld. Het betrof concept-versies van psychologische en psychiatrische onderdelen van Pro Justitia rapportages waarin strikt vertrouwelijke persoonsgegevens waren opgenomen. De Afdeling komt tot het oordeel dat de inbreuk op de persoonlijke levenssfeer van de betrokkene een 'aantasting in de persoon' betreft in de zin van artikel 6:106 lid 1 sub b BW. De Afdeling meent dat de nadelige gevolgen van de verstrekking van de gevoelige persoonsgegevens 'voor de hand liggen' en wijst een schadevergoeding toe ten bedrage van EUR 500. Bij de hoogte van dat bedrag is rekening gehouden met het feit dat de persoonsgegevens verstrekt zijn aan een kleine groep professionals (het tuchtcollege) met een beroepsgeheim.

De andere drie zaken gingen over schending van inzageverzoeken en informatieplicht door (het college van B&W van) gemeenten in relatie tot het plaatsen van gegevens op het internetforum van de Vereniging van Nederlandse Gemeenten (VNG). De Afdeling overweegt in deze zaken dat een inbreuk op de AVG niet zonder meer tot aantasting van de integriteit van een persoon en daarmee tot vergoedbare schade leidt. Onvolledige inzage en het niet tijdig verstrekken van alle verwerkte persoonsgegevens is geen situatie waarbij de nadelige gevolgen van de normschending voor de hand liggen. De Afdeling concludeert dat geen sprake is van een "aantasting in de persoon" als bedoeld in artikel 6:106 lid 1 sub b BW en wijst de verzoeken tot schadevergoeding af.

ABRvS 1 april 2020, ECLI:NL:RVS:2020:898

ABRvS 1 april 2020, ECLI:NL:RVS:2020:899

ABRvS 1 april 2020, ECLI:NL:RVS:2020:900

ABRvS 1 april 2020, ECLI:NL:RVS:2020:901

Medisch specialist heeft geen recht op afgifte patiëntendossiers

Computerrecht 2020/110

De Rechtbank Midden-Nederland oordeelt op 26 maart 2020 dat een medisch specialist na faillissement van het ziekenhuis geen recht heeft op afgifte van dossiers van behandelde patiënten. Bij haar beoordeling past de rechtbank de rechtsregel uit Hoge Raad van 25 mei 2012 (ECLI:NL:HR:2012:BV8508) toe: De beroepsbeoefenaar die zelfstandig de praktijk in het ziekenhuis uitoefent heeft in beginsel recht op kopieën van de patiëntendossiers op grond van de op hem rustende bewaarplicht inzake de Wet op de geneeskundige behandelingsovereenkomst (WGBO).

In deze zaak was de medisch specialist echter het grootste deel van zijn werkzame periode bij het ziekenhuis in loondienst. De rechtbank komt tot het oordeel dat voor wat betreft de dossiers die de specialist als werknemer behandelde geen zelfstandige bewaarplicht rust bij de specialist. Hetzelfde geldt voor de dossiers van patiënten die de specialist eerst als vrijgevestigde arts behandelde en later in loondienst. Voor wat betreft de dossiers van patiënten van wie de behandeling definitief was geëindigd ten tijde van de overgang van de vrijgevestigde periode van de specialist naar de periode van loondienst, neemt de rechtbank een gezamenlijke bewaarplicht aan. Deze gezamenlijke bewaarplicht leidt volgens de rechtbank in de bijzondere omstandigheden van het geval echter niet tot een verplichting van de curatoren om de specialist kopieën te verstrekken van deze dossiers. De rechtbank overweegt in dit kader dat het aantal dossiers met wettelijke bewaarplicht van de medisch specialist beperkt zal zijn en dat het maken van onderscheid tussen de dossiers 'tamelijk ingewikkeld en bovendien arbitrair' is. Daarnaast meent de rechtbank dat met het uitzoekwerk hoge kosten gemoeid zijn als alle 120 medisch specialisten de ca. 500.000 dossiers van patiënten die bij hen in behandeling waren willen inzien. De vordering tot afgifte wordt afgewezen.

Rb. Midden-Nederland 26 maart 2020,

ECLI:NL:RBMNE:2020:1107

Eliëtte Vaal

Artsenfederatie KNMG publiceert geactualiseerde richtlijnen omgang met medische gegevens

Computerrecht 2020/111

Artsenfederatie KNMG heeft haar Richtlijn 'Omgaan met medische gegevens' geactualiseerd. De vorige versie dateert uit 2018. In 2020 zijn onder andere de Wet zorg en dwang (Wzd), de Wet verplichte ggz (Wvvggz) en een aantal wijzigingen in de WGBO in werking getreden. Omdat die ook van toepassing zijn op het omgaan met medische gegevens, is de richtlijn daaraan (voor wat betreft de Wvvggz en de Wzd vooralsnog alleen globaal) aangepast. Tevens zijn de inhoudelijke bepalingen uit de KNMG-richtlijn Online arts-patiënt contact opgenomen.

Artsenfederatie KNMG

Eliëtte Vaal

Nationaal Cyber Security Centrum publiceert whitepaper over security-testen

Computerrecht 2020/112

Het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid (NCSC) publiceert in samenwerking met verschillende partners in het bedrijfsleven en overheden een white paper over securitytesten. Het betreft een handleiding voor het uitvoeren van securitytesten door opdrachtgevers inclusief stappenplan en checklist standaardelementen securitytestovereenkomsten.

Eliëtte Vaal

Focus AP op connected cars

Computerrecht 2020/113

Op 2 maart 2020 heeft de AP een handleiding gepubliceerd met tips voor gebruikers van "connected vehicles". Connected vehicles zijn rijdende computers die zijn verbonden met het internet. Denk aan moderne auto's, maar ook motoren, scooters en fietsen. De AP benadrukt in haar handleiding dat met behulp van "connected vehicles" bijzondere persoonsgegevens worden verkregen en dat privacyrisico's verbonden zijn aan het (toelaten van het) gebruik hiervan. De AP wijst onder andere op bovenmatige verwerking, slechte beveiliging en doorverkoop van persoonsgegevens. De AP is daarnaast gestart met een onderzoek naar de wijze waarop autofabrikanten omgaan met data verzameld door voertuigen. De toezichthouder heeft een aantal autofabrikanten hiervoor aangeschreven. Dit past in het toezichtkader 2020-2023 van de AP waar zij aangeeft te focussen op onder meer 'the internet of things'.

Eliëtte Vaal

SyRI-wetgeving in strijd met het Europees Verdrag voor de Rechten voor de Mens

Computerrecht 2020/114

De rechtbank oordeelt op 5 februari 2020 dat de wetgeving voor het instellen van de Systeem Risico Indicatie (SyRI) in strijd is met artikel 8 EVRM. SyRI is een wettelijk instrument

dat overheidsinstanties gebruiken voor de bestrijding van fraude op het terrein van uitkeringen, toeslagen en belastingen. Het stelt overheden in staat om gegevens te delen met andere instanties zoals de Belastingdienst en het UWV en om een analyse te maken van personen met een verhoogd risicoprofiel. De rechtbank komt tot het oordeel dat de SyRI-wetgeving in haar huidige vorm de toets van artikel 8 lid 2 EVRM niet doorstaat. De doelen van SyRI-wetgeving, namelijk het voorkomen en bestrijden van fraude in het belang van het economisch welzijn, rechtvaardigen volgens de rechter niet de inbreuk op het privéleven die de wetgeving maakt. Volgens de rechtbank voldoet de wetgeving niet aan de 'fair balance' die het EVRM vereist om te kunnen spreken over een voldoende gerechtvaardigde inbreuk op het privéleven. Dat komt onder meer door het gebrek aan transparantie en controleerbaarheid van de SyRI-wetgeving. Zo bleven het risicomodel, de risico-indicatoren en de in elk project gebruikte gegevens geheim en werden betrokkenen niet geïnformeerd. Ook bevat de wetgeving geen andere waarborgen die dit gebrek aan transparantie compenseren. De wetgeving is onrechtmatig want in strijd met hoger recht en dus onverbindend.

De rechtbank maakt in deze principiële uitspraak duidelijk dat de overheid een bijzondere verantwoordelijkheid heeft als het gaat om het koppelen van bestanden en het analyseren van bestanden met toepassing van algoritmen. De kern van de uitspraak is dat de overheid in wetgeving voldoende waarborgen moet opnemen om misbruik en willekeur tegen te gaan. Wat die waarborgen precies moeten inhouden wordt niet duidelijk gemaakt.

Eliëtte Vaal

AP publiceert rapport over toezicht op AI & Algoritmes

Computerrecht 2020/115

In haar toezichtkader 2020-2023 kondigde de AP al aan dat zij haar toezicht de komende jaren focust op artificiële intelligentie (AI) en algoritmes. Extra nadruk op deze thema's is volgens de AP nodig om misbruik of onverantwoordelijk gebruik van persoonsgegevens dat kan leiden tot foutieve beslissingen, uitsluiting van mensen en discriminatie, tegen te gaan. In het verlengde daarvan publiceerde de AP op 17 februari 2020 het toetsingskader op AI en algoritmes. De AP biedt concrete richtlijnen. Daarin wordt uitgelegd hoe de AVG-verplichtingen moeten worden toegepast bij AI-toepassingen. De AP wijst onder andere op de verantwoordingsplicht door middel van een bij het gebruik van algoritmes (veelal) verplichte data protection impact assessment (DPIA). Daarin moet onder andere onderbouwd worden waarom het nodig is te werken met het betreffende algoritme. De AP stelt in haar rapport dat

zij voor toezicht op AI-toepassingen ook samenwerkt met andere toezichthouders als de inzet van algoritmes ook gevolgen heeft voor andere rechtsgebieden zoals consumentenrecht, mededingingsrecht en antidiscriminatie.

Eliëtte Vaal

Stemopname is persoonsgegevens

Computerrecht 2020/116

Op 9 januari 2020 oordeelt de Rechtbank Midden-Nederland over de rechtmatigheid van het gebruik van een opname van een stem. De aanleiding van deze procedure is het gebruik van een geluidsfragment in een theatershow door rapper Ali B van een vrouw die zegt dat haar overvaller 'praatte met een Ali B accent'. Het geluidsfragment was eerder door het tv-programma "Opsporing verzocht" uitgezonden. De vrouw stelt zich op het standpunt dat het gebruik van de stemopname in de theatershow heeft te gelden als een onrechtmatige verwerking van haar persoonsgegevens en wenst dat haar gegevens worden verwijderd. De rechtbank oordeelt dat de stem een biometrisch persoonsgegeven is. De identiteit van de vrouw kan zonder onevenredige inspanning worden vastgesteld door de combinatie van het stemfragment en overige informatie tijdens de show. Er is volgens de rechtbank echter geen sprake van een onrechtmatige verwerking omdat Ali B's gebruik van de stemopname valt onder de vrijheid van de artistieke uitdrukkingsvorm. Dat feit brengt met zich mee dat op grond van artikel 43 Uitvoeringswet AVG ook geen recht op vergetelheid bestaat zodat het verwijderingsverzoek wordt afgewezen.

Rb. Midden-Nederland 9 januari 2020,
ECLI:NL:RBMNE:2020:24

Eliëtte Vaal

België

Marktenhof vernietigt beslissing van de Gegevensbeschermingsautoriteit en draait boete van 10.000 EUR terug (Arrest 19 februari 2020)

Computerrecht 2020/117

Het Hof van beroep Brussel, sectie Marktenhof, heeft op 19 februari 2020 een arrest geveld (rolnummer 2019/AR/1600)

waarbij zij de beslissing 06/2019 van de Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) van 17 september 2019 vernietigd heeft.

Met deze beslissing 06/2019 had de Geschillenkamer een administratieve boete van EUR 10.000 opgelegd aan een drankenhandelaar die de elektronische identiteitskaart gebruikte bij de aanmaak van klantenkaarten. De betrokken handelaar zou namelijk geweigerd hebben een klantenkaart te verstrekken aan een klant die zijn gegevens enkel schriftelijk wilde verstrekken. De Geschillenkamer achtte deze praktijk niet in overeenstemming met de Algemene Verordening Gegevensbescherming, vermits het gebruik van alle gegevens van de eID-kaart (inclusief foto, geslacht, geboortedatum en rijksregisternummer) disproportioneel zou zijn, de informatieplichten niet correct nageleefd zouden zijn en er bovendien geen geldige rechtsgrond voorhanden zou zijn (zie *Computerrecht* 2019/6).

De handelaar ging vervolgens bij het Marktenhof in beroep tegen deze beslissing van de Geschillenkamer.

Het Marktenhof bevestigt ten eerste zijn bevoegdheid om niet enkel beslissingen van de GBA te vernietigen, maar om ook zijn eigen beslissing in de plaats te stellen van de vernietigde beslissing (mits het hof geen betwistingen oproept die niet aan tegenspraak zijn onderworpen geweest en voor zover geen beslissing wordt getroffen waaromtrent de procespartijen zich niet hebben kunnen verdedigen).

Ten tweede oordeelt het Marktenhof dat er ten tijde van de feiten geen wettelijke verplichting bestond om een alternatief aan te bieden naast het gebruik van de elektronische identiteitskaart, vermits de regelgeving ter zake slechts in werking trad enkele maanden na de feiten en een 'aanbeveling' ter zake niet voldoende is.

Ten derde stelt het Marktenhof dat er *in casu* geen eID-kaart aangeboden werd door de klager, die dit namelijk weigerde, en er aldus geen verwerking van diens persoonsgegevens plaatsgevonden heeft. Bijgevolg, zo oordeelt het hof, toont de GBA geen daadwerkelijke inbreuk in verband met persoonsgegevens aan.

Vervolgens stelt het Marktenhof dat de beslissing van de GBA onvoldoende gemotiveerd werd, vermits bepaalde motieven uit haar beslissing onverenigbaar zijn met de stukken alsook met de toepasselijke wettelijke bepalingen en de aangehaalde motieven het bewezen verklaren van de inbreuken niet kunnen schragen. Het Marktenhof besluit dan ook dat de beslissing op onwettelijke wijze genomen werd en nietig verklaard dient te worden.

Ook wat de opgelegde administratieve boete van EUR 10.000 betreft oordeelt het Marktenhof dat deze onvoldoende gemotiveerd werd en dat de boete niet voldoet

aan de criteria van doeltreffendheid en evenredigheid. Sterker nog, zij stelt zelfs dat de sanctie op zich onwettig is vermits *in casu* de klager geen identiteitsgegevens ter beschikking heeft gesteld en zij persoonlijk geen nadeel kan hebben ondergaan, en de omstandigheid dat geen alternatief voorhanden was geen geldige rechtsgrond was op het moment van de klacht. Bijgevolg beveelt het Marktenhof de GBA om de reeds betaalde administratieve boete terug te betalen.

Hof van beroep Brussel, sectie Marktenhof, 19 februari 2020, 2019/AR/1600

Carolien Michiels

GBA: Beslissing 03/2020 van 21 februari 2020

Computerrecht 2020/118

Op 21 februari 2020 heeft de Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) een beslissing genomen (Beslissing 03/2020) naar aanleiding van een klacht van een betrokkene tegen twee voormalige werkgevers.

De klager was op 24 augustus 2016 aangenomen als communicatiemedewerker bij een groep van verschillende huisartsen. Op 2 oktober 2017 werd de klager per aangetekende brief ontslagen, mits uitvoering van een opzegtermijn van twee maanden. De groep van huisartsen was echter van mening dat de klager zijn verplichtingen niet nakwam tijdens deze opzegtermijn en verklaarde hem voor de maand december 2017 met onbetaald verlof zonder bezoldiging. Hierop schakelde de klager zijn vakbond in, die de redenen voor het ontslag betwistte en de groep van huisartsen in gebreke stelde.

In het kader van dit geschil verliep er heel wat briefwisseling tussen de verschillende partijen, waaronder een brief van de groep huisartsen aan de vakbond daterend van 14 juni 2018. In die brief verwees de groep huisartsen naar contacten met de nieuwe werkgever van de klager, door wie hij ook ontslagen werd, en naar een procedure waarbij de klager door de rechtbank veroordeeld geweest zou zijn in het kader van het terugvorderen van bepaalde documenten aan het einde van de arbeidsovereenkomst.

De klager diende een klacht in (i) ten aanzien van de tweede werkgever, die informatie verstrekt had aan de eerdere werkgever over de uitvoering van zijn werkzaamheden en informatie over de gerechtelijke procedure alsook (ii) ten aanzien van de eerste werkgever, die informatie verza-

melde bij de tweede werkgever en deze informatie via een brief meedeelde aan zijn vakbond.

De Geschillenkamer oordeelt dat de klacht ten aanzien van de tweede werkgever ongegrond is, vermits de mondelinge mededeling van deze informatie geen geautomatiseerde verwerking uitmaakt, noch een manuele verwerking van persoonsgegevens die bestemd zijn om deel uit te maken van een bestand zoals bedoeld in artikel 2 van de Algemene Verordening Gegevensbescherming (AVG).

Wat de eerste werkgever betreft, stelt de Geschillenkamer dat het verzamelen van informatie bij de nieuwe werkgever en de mededeling van die informatie per brief aan de vakbond wel verwerkingen van persoonsgegevens zijn die onder het toepassingsgebied van de AVG vallen. Verder stelt de Geschillenkamer dat informatie betreffende burgerrechtelijke veroordelingen niet onder de striktere bescherming voor gegevens in verband met strafrechtelijke veroordelingen en strafbare feiten zoals voorzien door artikel 10 AVG valt, maar dat dergelijke informatie niettemin zeer gevoelig van aard is.

De Geschillenkamer oordeelt dat de eerste werkgever zich niet rechtmatig kon beroepen op de rechtsgrond van noodzakelijkheid voor de verwezenlijking van haar gerechtvaardigde belang (artikel 6, § 1, f) AVG), namelijk het belang van haar verdediging in rechte met betrekking tot de klachten en dreigementen van de vakbondsorganisatie. Hoewel de Geschillenkamer erkent dat de verdediging in rechte een gerechtvaardigd belang uitmaakt, is ze van oordeel dat de verwerking van de gegevens, die plaatsvond ná het ontslag, niet noodzakelijk noch proportioneel was voor de uitoefening van dit juridisch verweer ten aanzien van de vakbond. De Geschillenkamer stelt: *“Het zou buitensporig zijn en in strijd met deze vereisten van noodzakelijkheid en proportionaliteit om toe te geven dat alle vorige werkgevers van een werknemer op grond van deze hoedanigheid alle informatie met betrekking tot een werknemer kunnen uitwisselen, zelfs met het oog op een verdediging in rechte.”*

De Geschillenkamer concludeert dat de artikelen 5 en 6 AVG geschonden werden door het gebrek aan een rechtmatige grondslag en door disproportionele en irrelevante informatie te verwerken die geen verband hielden met de gronden waarop het ontslag van de klager gebaseerd werd, die afkomstig was van derden zonder medeweten van de klager.

De Geschillenkamer legt enkel een berisping op, rekening houdend met het ad hoc-karakter van de verwerking en het ontbreken van een relevante eerdere overtreding.

www.gegevensbeschermingsautoriteit.be

Carolien Michiels

Nederland

Kamerbrief over de aanpak van cybercrime door regionale eenheden van de politie

Computerrecht 2020/119

In opdracht van het Ministerie van Justitie en Veiligheid heeft een onderzoeksbureau in februari 2020 een ontvankelijk rapport afgeleverd over de 'de aanpak van cybercrime door regionale eenheden van de politie'.

Naast het Team High Tech Crime (THTC) is sinds 2016 ook op regionaal niveau binnen de politie-eenheden aandacht gekomen in de vorm van acht gespecialiseerde 'cybercrime teams'. Maar in de eenheid Den Haag en Oost-Nederland bestaat dat nog niet uit 10 FTE, waardoor het formeel niet voldoende capaciteit heeft voor een 'cyberteam'. In het rapport worden nogal wat problemen bij de cyberteams signaleerd. Ook gaat het bij de intake van cybercrime nog steeds niet goed, omdat misdrijven te vaak niet herkend en geregistreerd worden als cybercrime.

Het gaat überhaupt niet goed met de kennis en kunde over cybercrime bij de politie volgens de onderzoekers. In het rapport staat: 'voor de cyberteams in de onderzochte eenheden geldt dat er een grote behoefte is om de specialistische digitale kennis binnen de generieke opsporing te versterken. De dieptekennis op digitaal vlak is met name voorhanden bij de Landelijke Eenheid (THTC) en bij de teams digitale opsporing. De cyberteams werken regionaal en pakken landelijk nauwelijks zaken op, terwijl cybercrime uiteraard niet regionaal van aard is'.

Door de cyberteams worden nu wel meer cybercrimezaken vervolgd. Het accent ligt daarbij op 'veel voorkomen de cybercriminaliteit', zoals phishing. Maar in deze zaken komt men weinig succesvol tot een veroordeling van een verdachte. Het blijkt dat bij de vervolging van cybercriminelen verdachten vaak buiten beeld blijven. Mede hierom wordt ingezet op 'barrières tegen digitale criminaliteit'. Door de aanpak van cybercrime met specifieke cyberteams blijft de expertise binnen de reguliere opsporing achter en is er bij andere teams weinig aandacht voor de digitalisering van criminaliteit, volgens de onderzoekers. De regering komt later dit jaar met een meer uitgebreide reactie over de aanpak van cybercrime.

Onderzoeksrapport over aanpak cybercrime door regionale eenheden van politie

Kamerbrief over aanpak van 'pedohandboek'

Computerrecht 2020/120

In de Kamerbrief van 10 februari 2020 geeft de Minister van Justitie en Veiligheid aan dat vervolging voor het verspreiden van teksten uit een pedohandboek reeds mogelijk is. Het vervaardigen, bezit of verspreiden van het handboek valt volgens de minister onder het delict opruiing (artikel 131 Sr e.v.). Op dit moment brengt volgens het OM een zelfstandige strafbaarstelling van het pedohandboek geen extra mogelijkheden voor opsporing en vervolging mee. Toch laat de minister verkennen wat de (wettelijke) mogelijkheden zijn om de verspreiding van het 'pedohandboek' als zelfstandig strafbaar feit aan te pakken. Hierover wordt de Tweede Kamer nog voor de zomer geïnformeerd.

~~Onderzoeksrapport over aanpak cybercrime over aanpak van pedohandboek~~

Kamerbrief over 'Citrix-problematiek' en WRR-rapport over digitale ontworping

Computerrecht 2020/121

Op 20 maart 2020 heeft de Minister van Justitie en Veiligheid de kabinetsreactie gestuurd op het rapport 'Voorbereiden op digitale ontworping' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en een overzicht van de geleerde lessen van de Citrix-problematiek.

Het valt daarbij op dat de minister veel aanbevelingen van de WRR niet overneemt of er slechts indirect op ingaat. De WRR beval bijvoorbeeld aan een 'helder afgebakende wettelijke bevoegdheid voor digitale hulpdiensten te creëren en de noodzaak van een aparte regeling voor overheidsdiensten gericht op tegengaan van escalatie te onderzoeken'. Vervolgens wijst de minister op de al bestaande 'nationale crisisstructuur' en het 'Nationaal Crisisplan Digitaal' dat in februari 2020 is gepubliceerd, waar we waarschijnlijk uit moeten afleiden dat dit voldoende wordt geacht.

De WRR wees er ook op dat private dienstverleners vaak geen belang hebben in opsporing of attributie van aanvallen. De minister reageert daar indirect op door aan te geven dat 'onder bestaande wettelijke kaders kan worden

ingegrepen wanneer dit toch nodig is. Vakdepartementen hebben hierin bevoegdheden om in te grijpen op basis van sectorale wetgeving'. Wel zegt de minister toe deze bevoegdheden in kaart te brengen zodat het gehele instrumentarium voor ingrijpen bij crises met digitale elementen inzichtelijk wordt en zodat kan worden gezien waar eventuele aanvullingen nodig zijn. Hierbij worden onder meer de Coördinatiewet uitzonderingstoestanden en de Wet buitengewone bevoegdheden burgerlijk gezag betrokken. Verder is interessant dat de minister in de Kamerbrief melding maakt van een nieuw samenwerkingsplatform op het gebied van cybersecurity, waar op dezelfde fysieke locatie samengewerkt wordt door politie, OM, NCSC, de AIVD en de MIVD met als doel informatie over cyberdreigingen en -incidenten bijeen te brengen en gezamenlijke analyses te verrichten.

De minister benadrukt een aantal keer in de Kamerbrief dat alle organisaties primair zelf verantwoordelijk zijn voor digitale weerbaarheid. Tijdens de Citrix-problematiek werd duidelijk dat er nog veel sectoren zijn die niet over een eigen computercrisisteam of samenwerkingsverband beschikken. Uiteindelijk moet elk bedrijf en elke organisatie ergens terecht kunnen voor informatie en advies. Deze moeten in beginsel worden opgericht door de sectoren zelf, aldus de minister. Om de betrouwbaarheid van cybersecuritydiensten te borgen is een subsidie verstrekt 'om te komen tot een risicomodel en een kwaliteitsregeling voor leveranciers van cybersecuritydiensten'.

Kamerbrief van 20 maart 2020 over rapport 'Voorbereiden op digitale ontwrichting'

Veroordelingen voor criminele kinderporno-organisatie op het dark web

Computerrecht 2020/122

Enkele verdachten zijn in februari en maart 2020 veroordeeld voor het bezit en de verspreiding van kinderporno via chatwebsites op het darkweb.

De Rechtbank Rotterdam veroordeelt op 27 januari 2020 (ECLI:NL:RBROT:2020:501) een verdachte voor de deelname aan een criminele organisatie waarvoor hij beheerstaken heeft uitgevoerd en zodoende mede kinderporno heeft verspreid en aangeboden. Ook had de verdachte 11.354 afbeeldingen en 1560 kinderpornovideo's in zijn bezit. De overwegingen van de rechtbank over de deelname aan een criminele organisatie zijn interessant.

De Rechtbank Rotterdam overweegt dat drie "chatsites" 'als één organisatie kunnen en moeten worden beschouwd, omdat zij alle 'chatsites op het Darkweb' waren, dezelfde modus operandi hadden, een gemeenschappelijk uitgangspunt hadden (onderling contact hebben met 'liefhebbers van minderjarigen') en dezelfde mogelijkheden boden (afbeeldingen aanbieden en beschikbaar stellen via een link), op hetzelfde script en dezelfde architectuur waren gebaseerd en de structuur en werkwijze op de sites overeen kwam. Daar komt nog bij dat de beheersmatige handelingen op deze sites werden verricht door vrijwel dezelfde personen'. De verdachte was ten minste twee jaar lang samen met andere personen actief als oprichter/beheerder, hoofdadministrator, moderator of administrator van de websites. Ook konden zij andere personen voordragen voor genoemde functies en konden leden worden gemonitord.

Uit de bewijsmiddelen blijkt dat er sprake was van een hiërarchie en structuur, omdat de moderators en administrators meer rechten en privileges hadden dan de geregistreerde gebruikers en de gasten en zij alleen toegang hadden tot bepaalde afgeschermdede gedeeltes van de sites. Ook uit de hiervoor genoemde functies en rol-en taakverdeling blijkt van een georganiseerd verband. Daarom was er sprake van een criminele organisatie als bedoeld in artikel 140 Sr, waar de verdachte deel van uitmaakte. De verdachte wordt veroordeeld tot drie jaar gevangenisstraf (waarvan één voorwaardelijk) en een proeftijd van drie jaar met bijzondere voorwaarden.

Rb. Rotterdam 27 januari 2020, ECLI:NL:RBROT:2020:501

De Rechtbank Overijssel veroordeelt op 3 maart 2020 (ECLI:NL:ROVE:2020:913) een verdachte voor het gewoonte maken van het verspreiden van kinderporno via chatrooms, het bezit van kinderporno en de deelname aan een criminele organisatie. De verdachte kwam volgens de uitspraak in beeld 'nadat de Britse opsporingsautoriteiten berichtten dat voornoemd webadres werd gehost op het IP-adres van verdachte'. In de uitspraak van de Rechtbank Overijssel zijn meer details over het onderzoek '26Somerville' te lezen. De verdachte in deze zaak was 'hoofdadministrator en hoster' van twee chatrooms. Hij 'promoveerde' bezoekers bijvoorbeeld tot moderator als deze 'langere tijd positief' opvielen.

De 'staff' van de chatsites had verschillende rangen met eigen chatkanalen. Op die kanalen kon men makkelijker en vrijer praten, omdat buitenstaanders minder makkelijk konden meelezen. De leden hielden aantekeningen van vergaderingen; hetgeen achteraf bijdroeg aan het bewijs tegen de kinderpornogebruikers. De database van een chatroom met 185 gebruikersnamen met hun rang is tevens in beslag genomen. De chatroom werd door de verdachte gehost via een virtuele machine op zijn PC.

De rechtbank ging niet mee in het verweer dat het delen van tekst en links naar kinderporno geen verspreiding van kinderporno is. Ook de waarschuwing op de chatsites dat geen kinderporno mocht worden verspreid, overtuigde de rechters niet omdat uit ander bewijs was af te leiden dat daadwerkelijk kinderporno is verspreid. Uit de uitspraak wordt niet duidelijk op welke wijze het bewijs verzameld is, maar de politie kon blijkbaar vaststellen dat in één van de chatrooms bijvoorbeeld 2410 afbeeldingen tussen 26 januari 2018 en 14 juni 2018 zijn gedeeld, waarvan er 298 kinderpornografisch waren. Feitelijk was dus sprake van de verspreiding van kinderporno. Door slechts te volstaan met de enkele vermelding van het verbod op de pagina na het inlogschermpje op [chatroom 3] en het handmatig – door moderators – laten controleren van afbeeldingen, heeft verdachte bewust de aanmerkelijke kans aanvaard dat toch kinderporno zou worden gedeeld op [chatroom 3], aldus de rechtbank.

De rechtbank acht daarom bewezen dat verdachte voorwaardelijk opzet had op het verspreiden, aanbieden, openlijk tentoonstellen, verwerven en in bezit hebben van kinderpornografische afbeeldingen, alsook op het toegang verschaffen tot kinderpornografische afbeeldingen. Ook op andere gegevensdragers werd bij de verdachte kinderporno gevonden. Interessant is bijvoorbeeld dat in een virtuele machine via de browser 'Internet Explorer' of 'Edge' bestanden geopend waren met kinderpornografische namen. Door de politie werden verder werden veertien bestandsnamen op kinderpornografische fora aangetroffen. De verdachte kreeg een gevangenisstraf opgelegd van drie jaar met bijzondere voorwaarden.

Rb. Overijssel 3 maart 2020, ECLI:NL:RBOVE:2020:913

Veroordeling voor webcamseks met Filipijns meisje

Computerrecht 2020/123

Op 24 maart 2020 heeft de Rechtbank Overijssel een verdachte veroordeeld (ECLI:NL:RBOVE:2020:1249) voor ontucht en het bezit van kinderporno. De verdachte is veroordeeld tot een voorwaardelijke gevangenisstraf van achttien maanden, een proeftijd van drie jaar met voorwaarden en een taakstraf van 240 uur.

Deze zaak met ernstige feiten kwam aan het licht door een Belgische onderzoeksjournalist. De verdachte zou één van de mannen zijn die achter een webcam naar een seksshow keek van een minderjarige. De politie heeft daarop een doorzoeking gedaan en gegevensdragers in beslag genomen. Daarop is kinderporno aangetroffen, maar geen informatie waaruit bleek dat de verdachte zich bezighield

met 'livestreaming' seksshows. Wel is een betaling via Western Union aan een slachtoffer gevonden. Later bleek dat de verdachte maandenlang chatgesprekken van seksuele aard heeft gevoerd met dit minderjarige slachtoffer.

De rechtbank overweegt dat de verdachte met zijn gedragingen ervoor heeft gezorgd dat meisjes als het slachtoffer gedwongen blijven om deel uit te maken van een enorm winstgevend verdienmodel, waarbij jonge kinderen voor een webcam worden gezet om seksshows te doen voor volwassenen die daarvoor slechts een wiferverbinding en een laptop, en soms een paar euro, nodig hebben. De kinderen die deel uitmaken van dit soort internationale netwerken worden vanaf jonge leeftijd geseksualiseerd en krijgen niet waar elk kind ter wereld recht op heeft, namelijk een normale seksuele ontwikkeling. Dat verdachte zijn eigen dochter, van toen negen jaar jong, heeft betrokken in zijn seksueel getinte chatgesprekken met het slachtoffer, vindt de rechtbank zorgelijk.

In artikel 245 Sr is ontucht met een minderjarige strafbaar gesteld, waarbij sprake is van seksueel binnendringen in het lichaam. Van deze gedraging was volgens de rechtbank geen sprake, omdat niet de verdachte maar twee meisjes in opdracht van de verdachte dat elders met zichzelf en/of elkaar deden. De motivatie waarom het artikel niet van toepassing is met een verwijzing naar het 'Pollepel-arrest' (ECLI:HR:2004:AQ0950) en literatuur is lastig te volgen en wellicht nog voor discussie vatbaar. Wel wordt aldus het plegen van ontuchtige handelingen via een 'livestream' en bezit van kinderporno bewezen geacht.

Rb. Overijssel 24 maart 2020, ECLI:NL:RBOVE:2020:1249

Phishing van creditcardgegevens

Computerrecht 2020/124

De Rechtbank Amsterdam heeft op 25 maart 2020 een bijzondere uitspraak gedaan over phishing van creditcardgegevens. Twee verdachten zijn veroordeeld tot een taakstraf vanwege oplichting. De uitspraak bevat interessante details over het opsporingsproces, maar ook enkele slordigheden.

Het onderzoek ving aan met een melding van de onderzoeksafdeling fraudedetectie van International Card Services B.V. van mogelijk frauduleuze transacties. Kort daarop werden met de creditcard bestellingen via Mediamarkt gedaan. Na contact met het Openbaar Ministerie werd besloten om het pakket gecontroleerd te laten afleveren op het aangegeven adres. Geobserveerd wordt dat de verdachte het pakketje in ontvangst neemt en meeneemt naar haar woning. De politie treedt een half

uur later binnen en treft verdachte en medeverdachte aan in haar slaapkamer samen met een geopende doos van de Mediamarkt. De doos met daarin een MacBook Pro is uit eerdergenoemde doos gehaald en op de pakbon staan de door Mediamarkt opgegeven bestelgegevens.

De verdediging voert aan dat niet voldoende bewezen is dat de verdachte het product heeft besteld en eist dat bijvoorbeeld DNA-onderzoek op de laptop wordt gedaan. De rechtbank gaat daarin niet mee. De rechtbank stelt op basis van het bewijs vast dat de persoonlijke gegevens van de creditcardhouder via phishing zijn verkregen. Vervolgens is op de webportal van de creditcardmaatschappij ingelogd, het telefoonnummer gewijzigd en zijn met de creditcard bestellingen geplaatst. Op de in beslag genomen laptops stonden e-mailaccounts open met diverse bestellingen op naam en rekening van creditcardhouders.

De rechtbank acht het voorhanden hebben van technische hulpmiddelen met het oogmerk om computervredebreuk te plegen bewezen, maar verwijst daarbij naar een verkeerd artikelnummer (artikel 138d Sr in plaats van artikel 139d lid 2 sub a Sr). Daarbij wordt uitgelegd: 'op beide laptops stonden diverse softwareprogramma's, waaronder Sendblaster, waarmee bulk-e-mailberichten kunnen worden verstuurd. Hierin trof men lijsten aan met duizenden e-mailadressen, verzonden phishing-e-mailberichten naar onder meer banken en meerdere (templates) voor phishingberichten. Ook de op de laptops aanwezige programma's Havij en Filezilla hebben bijgedragen aan de gepleegde computervredebreuk, te weten het binnendringen van webportals. Ook zijn gegevens van cardhouders gewijzigd door frauduleus in te loggen op hun webportals'. Het is technisch gezien natuurlijk lariekoek dat je kan binnendringen in een "webportal"; dat doe je namelijk in de geautomatiseerde werken (de servers) van ICS. Het ligt voor de hand dat dan sprake is van binnendringen via een valse hoedanigheid (namelijk met het account van het slachtoffer), maar dat acht de rechtbank (met een minimale motivering) niet bewezen.

Rb. Amsterdam 25 maart 2020, ECLI:NL:RBAMS:2020:1960 en ECLI:NL:RBAMS:2020:1961.

Grootschalige oplichting via Marktplaats

Computerrecht 2020/125

De Rechtbank Midden-Nederland heeft op 6 maart 2020 een verdachte veroordeeld tot een flinke gevangenisstraf van twintig maanden, waarvan acht voorwaardelijk en een proeftijd van drie jaar, voor phishing (oplichting), be-

dreiging en diefstal. In de uitspraak wordt uitvoerig de modus operandi van de criminelen besproken.

De rechtbank overweegt dat de verdachte samen met andere verdachten steeds dezelfde modus operandi (gebruikte werkwijze) aanhield. Een koper benaderde de aangever via Marktplaats of via het telefoonnummer van de aangever dat de koper via Marktplaats had verkregen. De koper liet de aangever, meestal via WhatsApp, weten dat hij het door de aangever aangeboden goed op Marktplaats wilde kopen. De koper vroeg de aangever vervolgens om € 0,01 over te maken via een door hem toegestuurd betaallink en zei daarbij dat hij er op die manier zeker van kon zijn dat de aangever te vertrouwen was en hij niet opgelicht zou worden. Wanneer de aangevers de betaallink openden, zagen zij een website die qua uiterlijk overeenkwam met de website van hun eigen bank. De aangever vulde vervolgens enkele persoonlijke gegevens in om deze € 0,01 over te maken. Deze gegevens konden bestaan uit de gebruikersnaam en het wachtwoord van hun bankrekening, het bankpasnummer en de vervaldatum van de bankpas.

Deze website sloeg vervolgens de gegevens op, waarna de koper of een derde kon inloggen op de bankrekening van de aangever en transacties kon uitvoeren. In enkele gevallen werd een geldbedrag overgemaakt naar de bankrekening van een derde (een *money mule*) en in diverse andere gevallen verplaatste de koper een geldbedrag van de spaarrekening van de aangever naar diens betaalrekening. Hierbij werd gedaan alsof de koper een geldbedrag van zijn eigen rekening had overgemaakt naar de rekening van de aangever. In dit geval vertelde de koper de aangever dat hij per ongeluk een te groot geldbedrag had overgemaakt, waarna hij de aangever vroeg om het teveel overgemaakte geld terug te storten. Als de aangever voldeed aan dit verzoek, maakte de aangever in werkelijkheid zijn of haar eigen spaargeld over naar de koper.

Bij een deel van de aangevers is de voornoemde methode niet voltooid. Deze aangevers kregen op verschillende momenten in dit proces argwaan, werden door hun bank benaderd en gewaarschuwd voor verdachte transacties of wilden om andere redenen niet meer meewerken met de koper. Zodra de koper dit beseftte, werd zijn communicatie vaak agressief jegens deze aangevers en probeerde hij ze onder bedreiging van geweld te dwingen mee te werken of een geldbedrag af te staan. De bedreigingen stonden in whatsappjes op de in beslag genomen telefoons opgeslagen, zoals: [slachtoffer 4]: "Ik steek je huis in de fik en ik steek jou kapot en ik kom van het kamp en ik steek jouw hond kapot en ik steek je vrouw neer, ik maak heel jouw familie kapot" en daarbij het adres van die [slachtoffer 4] te noemen. Dit leverde natuurlijk het benodigde bewijs op voor het delict bedreiging.

De zaak kent ook een interessante overweging over de bewijsvoering. Het bewijs wordt zeer uitvoerig besproken, zoals verkeersgegevens van telefonie, betaalgegevens en wifigegevens ter lokalisering van de verdachte. De verdachte voert aan dat de naam van een verdachte bekend moet zijn om historische verkeersgegevens van telefonie onder artikel 126nd Sv te vorderen. De rechtbank overweegt dat dit sinds het arrest van HR 22 maart 2005, ECLI:NL:HR:2005:AS4689 niet meer noodzakelijk is. Wel opmerkelijk is de overweging dat 'phishingwebsites' als technisch hulpmiddel worden gekwalificeerd met het oogmerk om computervrederebreuk te plegen, terwijl later wordt gesproken over de ontwikkeling van phishingsoftware.

De verdachten zijn in dit traject op verschillende manieren betrokken geweest bij de phishing, terwijl deze elementen van oplichting door middel van computervrederebreuk, na phishingactiviteiten met gebruik van specifiek ontwikkelde software in essentiële zin met elkaar samenhangen om tot oplichting via phishingsoftware te komen. Hieruit blijkt volgens de rechtbank dat beide verdachten voldoende hebben bijgedragen aan dit proces om als medeplegers te worden beschouwd.

Rb. Midden-Nederland 6 maart 2020,
ECLI:NL:RBMNE:2020:853

De Rechtbank Den Haag heeft op 6 maart 2020 eveneens een verdachte veroordeeld tot 36 maanden waarvan zes maanden voorwaardelijk met een proeftijd van twee jaren voor het op grote schaal medeplegen van identiteitsfraude, (marktplaats)oplichtingen, gewoontewitwassen en deelnemen aan een criminele organisatie. Ook zijn er meer dan 150 vorderingen van benadeelde partijen (gedeeltelijk) toegewezen. De zeer uitgebreide uitspraak is eveneens interessant vanwege de besproken modus operandi van de criminelen en de bewijsvoering.

De rechtbank overweegt dat de oplichter (verkoper) via WhatsApp contact zocht met de koper via in advertentie opgegeven mobiele nummer. In eerste instantie was ophalen en opsturen van het apparaat mogelijk. Echter als de koper koos voor ophalen werd het door de verkoper zo gedraaid dat het wel heel ver weg was en/of dat een afspraak niet mogelijk was. Vervolgens werd het vertrouwen van de koper gewonnen door het sturen van een (selfie met een) identiteitsbewijs en door het gebruik van een gelijkende profielfoto op WhatsApp. Na ontvangst van de betaling bleef de verkoper enige tijd bereikbaar voor de koper en kreeg de koper een valse track-en-tracecode. Vervolgens was de verkoper niet meer bereikbaar. Geen van de kopers ontving het gekochte product. In bijna alle gevallen maakte de verkoper gebruik van de identiteit van kopers die bij een aankoop zelf waren opgelicht en hun identiteitsbewijs naar de verkoper hadden verstuurd. Dit alles leverde het delict identiteitsfraude op.

Het geld werd overgemaakt naar rekeningen die kort daarvoor waren geopend door personen uit Oostbloklanden (waarvan 41 rekeningen bij de ING). Deze rekeningnummers werden korte tijd gebruikt en de daarop gestorte gelden werden gedurende de dagen dat de rekeningen actief waren, op een enkele uitzondering na, contant opgenomen bij geldautomaten en casino's in Amsterdam. De verdachten wisselden vaak van simkaart in hun mobiele telefoon. De geschreven aantekeningen – om bij te houden met excuses waarom het pakket niet was geleverd – leverden in de zaak een deel van het bewijs voor oplichting. De rechtbank overweegt dat de verdachte ervoor kiest om te zwijgen, maar het bovenstaande schreeuwt om een verklaring, zeker toen de verdachte bewijsmateriaal probeerde te vernietigen tijdens de inval van de politie.

Ten slotte is de bewijsvoering nog interessant over de netwerken waarmee verbinding is gemaakt (een wifinetwerk). Het netwerk had blijkbaar 'twee unieke MAC-adressen', waarbij onderzoek in openbare bronnen vervolgens uitwees dat 'deze MAC-adressen behoorden bij twee Blackberry telefoons. De historische locatiegegevens van deze MAC-adressen gaven GPS locatiecoördinaten [GPS locatie 1], [GPS locatie 2] die, met een nauwkeurigheid van 150 meter, de [adres 1] – de straat waar de verdachte woont – aanwijzen als de plek waar deze netwerken zijn gebruikt'.

Hoewel de oplichtingen per persoon slechts bedragen tussen € 300 en € 600 bedroegen, wordt bewezen geacht dat de verdachte – samen met anderen – in totaal voor een bedrag van € 105.261,41 heeft opgelicht.

Rb. Den Haag 6 maart 2020, ECLI:NL:RBDHA:2020:2595

België

Publicatie: Strafrechtelijk beslag. Digiproof en (multi)functioneel

Computerrecht 2020/126

In april 2020 verscheen het boek "Strafrechtelijk beslag. Digiproof en (multi)functioneel" van de hand van Sofie Royer. Het boek vormt de geüpdatete versie van het doctoraal proefschrift dat de auteur in januari 2020 aan de KU Leuven verdedigde. Centraal in dit boek staat de vraag naar een coherent wettelijk kader voor de inbeslagneming van goederen en gegevens dat de verschillende functies van het strafrechtelijk beslag kan vervullen en de mensenrechten respecteert.

Het eerste deel beschrijft de bredere context waarin de beslagbevoegdheid moet worden gekaderd. Niet alleen de

internationale vermogensaanpak heeft een directe weerslag op de nationale beslagregels. Ook de digitalisering beïnvloedt de manier waarop criminaliteit wordt bestreden en de rol die daarin aan de beslagbevoegdheid wordt toebedeeld (denk aan de inbeslagname van cryptomunten, de blokkering van websites...).

Het tweede deel bestaat uit een grondige analyse van het huidige recht, opgebouwd volgens de verschillende functies van het strafrechtelijk beslag, namelijk bewijsvergaring, verzekering van de uitvoering van een latere veroordeling, waarborging van de vergoeding van slachtoffers en stopzetting van misdrijven. Daarnaast bevat dit deel een analyse van de rechtspraak van het Europees Hof voor de Rechten van de Mens. Niet alleen de bescherming van eigendom en het recht op een eerlijk proces, maar ook het recht op privacy en de vrije meningsuiting passeren de revue. De bescherming van informatie die onder het beroepsgeheim van advocaten en artsen valt, neemt daarbij een belangrijke plaats in.

In het derde deel volgt tot slot een aanzet voor nieuwe beslagregels die multifunctioneel en *digiproof* zijn, waarbij ook enkele rechtsvergelijkende inzichten (Nederland, Verenigde Staten) aan bod komen.

S. Royer, *Strafrechtelijk beslag. Digiproof en (multi)functionaliteit*, Brugge: die Keure 2020, 480 p.

Charlotte Conings

COVID-19: uitbreiding onderzoeksmaatregelen en strijd tegen criminele webshops en fake news

Computerrecht 2020/127

Naar aanleiding van de coronacrisis voerde de Belgische regering enkele aanpassingen door in het strafprocesrecht. Zo worden de termijnen in de artikelen 46bis en 88bis Sv. verlengd. Op basis van die artikelen kunnen respectievelijk de procureur des Konings en de onderzoeksrechter metadata van communicatie opvragen bij operatoren en dienstenaanbieders (zie o.a. *Computerrecht* 2019/138). De periode waarin de speurders kunnen teruggaan, varieert en is afhankelijk van de ernst van de misdrijven (zie *Computerrecht* 2016/70 en *Computerrecht* 2016/161). Volgens de regering was het nodig om die termijnen te verlengen omdat veel strafonderzoeken door de crisis vertraging oplopen. Bovendien is het mogelijk dat sommige misdrijven pas na de crisis aan het licht komen

of dat slachtoffers dan pas een klacht indienen. Alleen de termijn om verkeers- en locatiegegevens op te vragen voor terroristische misdrijven, wordt niet verlengd omdat die overlapt met de maximale bewaarperiode van metadata, namelijk twaalf maanden. De regering kijkt wel of die bewaartermijn ook kan worden verlengd in de huidige omstandigheden.

Daarnaast lanceerde het College van procureurs-generaal ook een omzendbrief met maatregelen om de webshops te bestrijden die valse medicijnen of waardeloos beschermingsmateriaal verkopen. Dit kan strafbaar zijn als (poging tot) oplichting (artikel 496 Sw.) en misbruik van elektronische communicatienetwerken of -diensten om overlast of schade te veroorzaken (artikel 145, § 3bis Wet Elektronische Communicatie). De federale politie zal actieve internetpatrouilles voeren om de bewuste webshops te identificeren. Als de Dienst Internetrecherche op zo'n webshop stuit, moet een proces-verbaal worden opgesteld, ongeacht waar de website wordt gehost. Het federaal parket zal vervolgens een vordering tot blokkering van de website op grond van artikel 39bis Sv. instellen (zie hierover ook *Computerrecht* 2016/163 en *Computerrecht* 2018/204). Opmerkelijk stelt de omzendbrief dat het offline halen van de website het hoofddoel is en dat er geen verder strafonderzoek wordt ingesteld.

Daarnaast zijn er ook websites die *fake news* verspreiden over het virus. In de omzendbrief geeft het College van procureurs-generaal aan dat dit op zich niet strafbaar is. Het federaal parket zal dus in principe geen vorderingen tot blokkeringen instellen om censuur te vermijden. Uitzonderlijk kan dit wel, namelijk wanneer de valse informatie de publieke volksgezondheid in gevaar kan brengen.

KB nr. 3 houdende diverse bepalingen inzake strafprocedure en uitvoering van straffen en maatregelen in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19, BS 9 april 2020;

Omzendbrief nr. 10/2020, Richtlijnen van het College van procureurs-generaal inzake de strijd tegen de fake webshops en de fake news sites, 2 april 2020, www.om-mp.be/nl/meer-weten/omzendbrieven.

Sofie Royer

Ook Grondwettelijk Hof keurt ontsleutelplicht voor verdachte goed

Computerrecht 2020/128

Het Hof van Cassatie heeft op 4 februari 2020 het licht op groen gezet voor het bevel aan een verdachte tot ontgrendeling van zijn smartphone. Het Hof achtte het zwijgrecht en verbod op zelfincriminatie niet geschonden door genoemd bevel. Op 11 december 2018 is ook een prejudiciële vraag gesteld aan het Grondwettelijk Hof (rolnummer 7075 (NL)), waarbij we het antwoord van dat Hof met veel belangstelling tegemoetzagen.

Op 20 februari 2020 sprak het Grondwettelijk Hof zich over de materie uit. Het Hof trad daarbij het Hof van Cassatie bij, in die zin dat het ook oordeelde dat de ontsleutelplicht uit artikel 88^{quater} § 1 Sv. het zwijgrecht en verbod op zelfincriminatie niet schendt. Meer bepaald oordeelde het Grondwettelijk Hof dat het recht om niet mee te werken aan zijn eigen beschuldiging simpelweg niet van toepassing is, aangezien aan de verdachte enkel informatie wordt gevraagd die onafhankelijk van zijn wil bestaat. Het Hof onderschrijft daarmee de stelling dat een toegangscode onafhankelijk van de wil van de verdachte bestaat. Het 'verschil in behandeling' met de actieve medewerkingsplicht uit artikel 88^{quater} § 2 Sv., op grond waarvan men onder meer kan worden verplicht actief naar gegevens te zoeken maar waarbij de verdachte wél is uitgesloten van het toepassingsgebied, acht het Hof bovendien verantwoord. Die plicht zou de verdachte er immers wel toe kunnen brengen mee te werken aan zijn eigen beschuldiging.

De noodzaak om de gepaste middelen ter beschikking te stellen van de gerechtelijke overheden om misdrijven te vervolgen en te bestraffen, verantwoordt volgens het Hof dat aan een persoon het bevel kan worden gegeven informatie te verstrekken waarover hij beschikt met betrekking tot de werking van of de toegang tot een informatiesysteem. Het recht op eerbiediging van het privéleven, zoals gewaarborgd door artikel 22 Grondwet en artikel 8 EVRM, doen het Grondwettelijk Hof om die reden evenmin besluiten tot een schending.

GwH 20 februari 2020, nr. 28/2020

Charlotte [Coninx](#)

- 86 ABRvS 22 januari 2020, ECLI:NL:RVS:2020:175, m.nt. mr. dr. A. Drahmman / p. 179

Verschoonbare termijnoverschrijding. E-mailservice van www.overheid.nl.

- 87 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, m.nt. mr. S van Schendel / p. 183

De rechtbank komt tot het oordeel dat de SyRI-wetgeving in haar huidige vorm de toets van artikel 8 lid 2 EVRM niet doorstaat. De rechtbank heeft de doelen van de SyRI-wetgeving, namelijk het voorkomen en bestrijden van fraude in het belang van het economisch welzijn, afgezet tegen de inbreuk op het privéleven die de wetgeving maakt. Volgens de rechtbank voldoet de wetgeving niet aan de 'fair balance' die het EVRM vereist om te kunnen spreken over een voldoende gerechtvaardigde inbreuk op het privéleven. De wetgeving is wat betreft de inzet van SyRI onvoldoende inzichtelijk en controleerbaar.

- 88 Rb. Rotterdam 19 maart 2020, ECLI:NL:RBROT:2020:2395, m.nt. prof. mr. dr. J.J. Oerlemans / p. 189

In deze zaak ontwikkelde de verdachte een programma (Rubella Macro Builder), waarmee aan Office-documenten zoals Word en Excel een stuk verborgen code wordt toegevoegd. Bij het openen van een geïnfecteerd document wordt de code uitgevoerd. Daarmee maakt de verdachte het bijvoorbeeld mogelijk andere malware te downloaden op de computers van slachtoffers. De verdachte heeft zich schuldig gemaakt aan het vervaardigen, verkopen, verspreiden en voorhanden hebben van malware met het oogmerk computervredereuk te plegen.

89-103 TELECOMMUNICATIE / P. 195

104-118 PRIVACYBESCHERMING / P. 204

119-128 STRAFRECHT / P. 211

