Online privacybescherming is bepaald géén kinderspel - Over de nieuwe Europese regels voor de persoonsgegevensbescherming van minderjarigen

Hof, S. van der

Gaat de Telecomwet straks spammers en botnets beschermen?

Gerrit-Jan Zwenne

Op 1 januari 2013 treedt art. 7.6a van de Telecommunicatiewet in werking. Vanaf die datum kan een internetaanbieder de levering van zijn internettoegangsdiensten alleen nog beëindigen of opschorten als er sprake is een van de in het artikel uitputtend opgesomde omstandigheden. De diensten kunnen alleen worden beëindigd of opgeschort als de abonnee daarom vraagt, of als hij zijn betalingsverplichting niet nakomt, of als er sprake is van bedrog,[1] overmacht[2] of onvoorziene omstandigheden,[3] of als dat nodig ter uitvoering van een wettelijk voorschrift of rechterlijk bevel. Ook als het gaat om een abonnement dat voor een of twee jaar is aangegaan mag de dienstverlening, als de abonnementstermijn is verstreken, alleen worden beëindigd met instemming van de abonnee.

Het artikel is bij amendement ingevoegd om internetgebruikers te beschermen tegen lichtvaardig afsluiten van internettoegang. Gelet op het belang van internettoegang in Nederland, zo staat het in de toelichting bij het amendement, is het nodig om de omstandigheden waaronder internettoegang kan worden beëindigd of opgeschort, uitputtend te omschrijven.[4]

Het nieuwe artikel roept veel lastig te beantwoorden vragen op. Wat als een internetaanbieder af wil van een abonnee die zijn abonnement misbruikt om te spammen of om botnets te verspreiden? Wat is straks de betekenis van algemene voorwaarden op grond waarvan in zo een geval het abonnement kan worden beëindigd? In de parlementaire behandeling zei de bewindspersoon dat een dergelijke ontbindende voorwaarde wel kan leiden tot ontbinding van de overeenkomst, maar dat de aanbieder niettemin verplicht blijft de internettoegangsdienst te leveren.[5]

Zoals we wel vaker zien bij amendementen[6] zijn de implicaties ervan niet doordacht. Want wat als de abonnee verhuist naar plaats buiten het verzorgingsgebied van zijn aanbieder? Kan deze abonnee dan aanspraak blijven maken op voortzetting van de dienstverlening? Of moet dat dan maar worden gezien als overmacht? Onduidelijk is ook wat er gebeurt bij vernietiging van een overeenkomst, bijvoorbeeld op grond van handelingsonbekwaamheid of een wilsgebrek. Wat wordt dan de rechtsgrondslag van voortgezette dienstverlening? De wet?

U als internetjurist mag wellicht volgend jaar de antwoorden gaan bedenken.

1. Art. 3:44 BW.
2. Art. 6:75 BW
3. Art. 6:258 BW.
4. *Kamerstukken II* 2010/11, 32 549, nr. 40.
5. *Kamerstukken I* 2011/12, 32 549, E, p. 20.
6. Vgl. *Kamerstukken II* 2010/11, 32 549, nr. 29; *Kamerstukken II* 2010/11, 32 549, nr. 39.

Online privacybescherming is bepaald géén kinderspel

Over de nieuwe Europese regels voor de persoonsgegevensbescherming van minderjarigen

*Simone van der Hof**

Introductie

Bescherming van de online privacy van kinderen en – meer het bijzonder – die van hun persoonsgegevens wordt als steeds belangrijker beschouwd. Dat heeft onder meer te maken met het hoge Internetgebruik onder kinderen en jongeren. De Europese wetgever beoogt om die reden bij de aanpassing van het regelgevend kader voor dataprotectie in het bijzonder aandacht te besteden aan de belangen van kinderen in het licht van technologische ontwikkelingen. De vragen die in deze bijdrage worden beantwoord zijn welke veranderingen de door de Europese Commissie recentelijk voorgestelde nieuwe regels brengen voor de bescherming van kinderen en hoe kunnen deze veranderingen worden gewaardeerd vanuit het oogpunt van het belang van het kind? Om deze vragen te kunnen beantwoorden zal worden geschetst hoe privacy- en gegevensbescherming voor kinderen momenteel worden geregeld en welke zorgen er zijn in dat verband, alvorens wordt ingegaan op de veranderingen die de voorgestelde algemene dataprotectie-verordening zou moeten brengen. De bijdrage wordt afgesloten met een waardering van deze veranderingen in het licht van de problemen en de belangen van kinderen en enkele slotopmerkingen.

Privacy- en gegevensbescherming voor kinderen in Europa

Het vigerende Europeesrechtelijke regime voor de bescherming van persoonsgegevens[1] bevat geen bepalingen die specifiek gericht zijn op kinderen. Kinderen vallen dus onder de regels die voor alle natuurlijke personen – in dataprotectie-jargon: betrokkenen – gelden. Tot hun zestiende levensjaar oefenen wettelijke vertegenwoordigers – in de regel de ouders – namens hen de rechten uit die zij onder deze regelgeving hebben. Daarna kunnen zij dat zelf doen. Sinds enige jaren groeit de aandacht voor bijzondere bescherming van persoonsgegevens van kinderen echter sterk. De twee belangrijkste redenen daarvoor zijn: (1) de aandacht voor kinderrechten en (2) de zorgen over online risico's voor kinderen. Beiden worden hier achtereenvolgens toegelicht. Aansluitend besteedt deze paragraaf meer specifiek aandacht aan enkele initiatieven op het terrein van zelfregulering van online privacy van kinderen. Zelfregulering wordt op dit moment door de Europese Commissie als een belangrijk sturingsinstrument beschouwd voor het realiseren van online veiligheid voor kinderen.

Groeiend belang van kinderrechten en de bescherming van persoonsgegevens van kinderen

Het belang van de in het uit 1989 stammende VN-Kinderrechtenverdrag neergelegde rechten voor kinderen wordt steeds nadrukkelijker onderkend. Kinderen zijn volgens het verdrag personen die de leeftijd van achttien jaar nog niet hebben bereikt, tenzij meerderjarigheid volgens hun nationale recht eerder wordt bereikt.[2] Zij hebben een bijzondere positie in het recht, omdat ze gelet op hun leeftijd en in het bijzonder hun fysieke en psychische rijpheid in de regel meer zorg en bescherming nodig hebben dan volwassenen.[3] Art. 16 lid 1 van het Verdrag[4] bepaalt dat ook kinderen een recht op privacy hebben.[5] Het recht op privacy omvat mede een recht op bescherming van hun persoonsgegevens.[6] De twintigste verjaardag van het VN-Kinderrech-

---

* Prof. dr. mr. Simone van der Hof is hoogleraar recht en informatiemaatschappij aan eLaw – Centrum voor recht en informatiemaatschappij, Universiteit Leiden, s.van.der.hof@law.leidenuniv.nl.

1. Dat wil zeggen de richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens *PbEG* L 281, 23/11/1995, p. 31 en richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEG* L 201, 31/07/2002, p. 37.
2. Art. 1, VN Kinderrechtenverdrag 1989.
3. Zie Preambule van de 'Declaration of the Rights of the Child': *[T]he child, by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection, before as well as after birth*. Ook in deze zin: art. 24, lid 1, EU Handvest van de grondrechten.
4. De originele Engelse tekst luidt: *No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.*
5. Zie ook art. 8, EVRM en art. 7, EU Handvest van de grondrechten dat van toepassing is ongeacht iemands leeftijd.
6. Ingevolge art. 8, EU Handvest van de grondrechten hebben burgers het recht op bescherming van hun persoonsgege-

tenverdrag 1989 was voor de Europese Commissie aanleiding om kinderrechten als beleidsprioriteit te herbevestigen in haar Mededeling 'Towards an EU Strategy on the Rights of the Child'.[7] De artikel 29-werkgroep[8] heeft in een opinie uitwerking gegeven aan de speciale status van kinderen bij de bescherming van persoonsgegevens door het geven van richtlijnen in de context van het onderwijs die echter ook in meer algemene zin relevantie hebben.[9] Zo moeten verwerkers van persoonsgegevens in het licht van de privacybeginselen extra zorgvuldigheid betrachten wanneer de verwerkingen gegevens van kinderen betreft.[10] Een eerste voorbeeld is het verstrekken van informatie over gegevensverwerkingen in Jip en Janneke-taal, zodat deze begrijpelijk is voor kinderen.[11] Een ander voorbeeld is het op een afgesloten website publiceren van persoonsgegevens van scholieren, waardoor niet deze niet door iedereen kunnen worden gezien. Een derde voorbeeld is de proportionaliteit die dient te worden betracht bij de invoering van, in het licht van de privacy ingrijpende, beveiligingstechnologieën op scholen, zoals biometrie en camerabewaking. Kinderen kunnen wel met het ouder (en mondiger) worden steeds meer eigen inbreng krijgen in de vorm van het al dan niet (mede) toestemming geven voor het gebruik van zijn of haar persoonsgegevens (bijv. in weerwil van de wensen van zijn of haar ouders) of het zelf uitoefenen van hun rechten.[12] Dit is lijn met de gedachte achter het VN Kinderrechtenverdrag 1989.[13]

Complexe door technologie gemedieerde leefomgeving

Voorts zijn technologische ontwikkelingen aanleiding om uitdrukkelijker dan voorheen het vizier te richten op de rechtspositie van kinderen. Kinderen maken steeds meer gebruik van Internet en mobiele diensten en lopen daarbij risico's die samenhangen met het gebruik of misbruik van hun persoonsgegevens. Het online publiceren of verstrekken van persoonsgegevens kan bijvoorbeeld (identiteits)fraude, seksueel misbruik, pestgedrag of reputatieschade in de hand werken. Adequate bescherming van je persoonsgegevens draagt met andere woorden bij aan de veiligheid op Internet. Meer algemeen rijzen er vragen over de legitimiteit en wenselijkheid van online surveillancepraktijken van bedrijven en overheden waarin online activiteiten en communicatie van kinderen en volwassenen minutieus (soms letterlijk) in kaart worden gebracht en zij vervolgens worden gesorteerd in economisch of sociaal relevante (risico)categorieën.[14] We hebben het dan meer specifiek over profilering, wat inhoudt het creëren van een persoonlijk of groepsprofiel in de vorm van een set aan elkaar gecorreleerde persoonsgegevens die individuele personen kunnen representeren. Profielen kunnen bijvoorbeeld worden gebruikt om personen op hun wensen en behoeften afgestemde aanbiedingen toe te sturen of om te bepalen of iemand tot een bepaalde risicocategorie (bijvoorbeeld wanbetaler) zou kunnen behoren (zogeheten risicoprofiel). Voor zover ze zich er bewust van zijn, is het voor ouders, laat staan voor kinderen, lastig om te doorgronden wat er van hun surfgedrag door wie en hoe wordt vastgelegd, hoe de op basis van deze data geconstrueerde profielen worden toegepast en op welke manier het online observeren kan worden gestopt of op zijn minst teruggedrongen.[15] De artikel 29-werkgroep heeft benadrukt dat bij het vastleggen van surfgedrag van kinderen door commerciële partijen deugdelijke informatie moet worden verstrekt aan ouders alvorens hen om toestemming te vragen.[16] Nu is het realiseren van daadwerkelijke transparantie op dit zowel juridisch als technisch complexe en van grote commerciële belangen doordrongen terrein een lastig onderwerp gebleken, waarover het laatste woord nog niet is gesproken. Bedrijven lopen hier namelijk aan tegen de moeilijkheid dat er een gebrek is aan adequate mogelijkheden om iemand's leeftijd online te verifiëren en vast te stellen of men te maken heeft met kinderen.[17] Een verdere complicerende factor is dat de bestaande regelgeving door de technische ontwikkelingen voorbij is gestreefd en onvoldoende bescherming biedt tegen de steeds slimmere omgeving, waarin het individu continu online wordt gevolgd en geprofileerd door de technologie.[18] Het is derhalve interessant of de – verderop te bespreken – ontwerpverordening verbetering brengt.

Zelfregulering

De Europese Commissie spoort intussen bedrijven aan om zelfregulering te ontwikkelen die de online veiligheid van kinderen moet garanderen en vaak ook ziet op de bescherming van de online privacy van kinderen.[19] Zelfregulering

---

vens, waarbij o.g.v. art. 24 van het EU Handvest rekening moet worden gehouden met de bijzondere belangen van kinderen. Zie ook art. 3, VN-Kinderrechtenverdrag 1989.

7. COM (2006) 367 final.
8. De artikel 29-werkgroep is het onafhankelijke orgaan van Europese privacytoezichthouders dat de Europese Commissie adviseert over bescherming van persoonsgegevens.
9. Working Document 1/2008 on the protection of children's personal data, WP 147, February 2008. In eerdere opinies besteedde de Artikel 29-werkgroep mede aandacht aan de rechtspositie van kinderen op welbepaalde onderwerpen; zie o.a. Opinion 2/2010 on online behavioural advertising en Opinion 5/2009 on online social networking.
10. Working Document 1/2008, *supra* noot 9, p. 7 e.v.
11. Working Document 1/2008, *supra* noot 9, p.10.
12. Working Document 1/2008, *supra* noot 9, p. 5-6 en 9.
13. Vergelijk art. 5, VN-Kinderrechtenverdrag 1989.
14. David Lyon heeft deze ontwikkelingen als 'social sorting' aangeduid, zie D Lyon, *Surveillance as social sorting, Privacy risk and digital discrimination*, London/New York: Routledge, 2003.
15. Niet meer vol te houden is in dit verband de opmerking van de Artikel 29-werkgroep dat marketing geen probleem van gegevens- maar van consumentenbescherming is, Working Document 1/2008, *supra* noot 9, p. 12.
16. Advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising'), *WP* 171, 22 juni 2010.
17. In een eerder advies drong de werkgroep al aan op onderzoek naar en implementatie van leeftijdsverificatie, alsmede bewijs van toestemming, Advies 5/2009 over online sociale netwerken, *WP* 163, p. 13.
18. Zie o.m. A Roßnagel, J Müller, 'Ubiquitous Compunting – neue Herausforderungen für den Datenschutz, Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze', *Computer und recht*, 20 98), 2004, p. 625-632; M Hildebrandt, 'A Vision of Ambient Law', in: R Brownsword, K Yeung (eds), Oxford: Hart, 2008, p. 175-191.
19. Overigens heeft ook de Raad van Europa zich nadrukkelijk voor zelfregulering van online kindveiligheid en

is soms te verkiezen boven overheidsreguliering, bijvoorbeeld wanneer flexibiliteit, technische expertise en (kosten) efficiency gevraagd zijn. Zelfregulering kan ook leiden tot een groter 'commitment' van de industrie en daarmee – mogelijk – grotere effectiviteit van regelgeving. Echter, bedrijven kunnen het ook als marketinginstrument zien zonder dat regelnaleving (volledig) wordt gerealiseerd.[20] Een tweetal zelfreguleringsinitiatieven is hier noemenswaard. Ten eerste de 'Safer Social Networking Principles for the EU' (verder: SSNP) en ten tweede de zogeheten 'Coalition to make the Internet a better place for kids'.[21]
De SSNP zijn begin 2009 door de de belangrijkste sociale netwerkaanbieders[22] aangenomen.[23] Het doel van de SSNP is:

> To provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services.

Beginsel 6 van de SSNP ziet direct op privacy en gegevensbescherming en luidt:

> Enable and encourage users to employ a safe approach to personal information and privacy

Maar andere beginselen zijn eveneens relevant voor een veilig gebruik en bescherming van persoonsgegevens.[24]
Op basis van de SSNP moeten bedrijven zorgen voor online veiligheidsstrategieën voor kinderen,[25] waaronder standaardinstellingen die de privacy van kinderen maximaal beschermen, systemen voor leeftijdsverificatie, mogelijkheden voor ouders om toezicht uit te oefenen en begrijpelijke informatie over de gebruiksvoorwaarden en online kindveiligheid. De vraag is vervolgens of de SSNP werken? Het antwoord is dat we dat niet weten. Zelfrapportage door bedrijven laat zien dat bedrijven inderdaad maatregelen nemen, maar zeker niet alle beginselen waren in 2011 naar tevredenheid geïmplementeerd.[26] Implementatie van de beginselen betekent bovendien niet per definitie dat de gekozen maatregelen effectief zijn. Om dat te achterhalen is meer onderzoek nodig.[27]
Een ander recent initiatief is wat de '*Coalition to make the Internet a better place for kids*' (hierna: de Safer Internetcoalitie) wordt genoemd.[28] De coalitie bestaat uit telecom- en ICT-bedrijven, waaronder wederom de grootste sociale netwerkaanbieders. De coalitie beoogt om in samenwerking met de Europese Commissie en belangenorganisaties een veilige online omgeving voor kinderen te realiseren door het delen van expertise en ontwikkelen van concrete veiligheidstools. Er is dus zowel wat betreft deelnemende partijen als inhoudelijk een overduidelijke overlap met de SSNP, maar of er afstemming is tussen beide initiatieven en, zo ja, welke, is niet duidelijk. Een van de speerpunten van de coalitie is het uitwerken van 'age-appropriate privacy settings'; dat wil zeggen voor kinderen toegankelijke en begrijpelijke instellingen waarmee ze kunnen bepalen wie online informatie over hen (waaronder contactgegevens, berichtjes en foto's) kan zien en – ook belangrijk – wie niet. Uitgangspunt is dat de standaardinstellingen – ofwel de instellingen zoals deze zijn gedefinieerd op het moment dat het kind zich als nieuwe gebruiker aanmeldt bij een online dienst – zo veilig voor kinderen zijn als redelijkerwijs mogelijk is. Zo zet de Nederlandse sociale netwerksite Hyves de profielen van kinderen jonger dan 16 jaar standaard op besloten. Bij het veranderen van de privacyinstellingen zouden kinderen vervolgens duidelijk moeten worden gewezen op de consequenties, met name de potentiële risico's, daarvan.
In de loop van 2012 worden de resultaten van het initiatief door de Europese Commissie tegen het licht gehouden en wordt er hopelijk meer duidelijk over de status van de activiteiten binnen de Coalitie. Dat neemt niet weg dat het proces nauwgezet wordt gevolgd door o.a. de Europese digitale burgerrechtenorganisatie EDRi die kritische kanttekeningen plaatst bij de ontwikkelingen omtrent de 'age-appropriate privacy settings'. Ten eerste gaat het slechts over informatie die gebruikers van sociale netwerken onderling uitwisselen en niet over de persoonsgegevens van kinderen die door deze bedrijven zelf of door derden bijeen worden gesprokkeld op basis van hun online activiteiten om gericht te kunnen adverteren.[29] Ten tweede zouden sommige partijen verder gaan – verder dan bijvoorbeeld Facebook –

---

waarborgen van kinderrechten uitgesproken, zie Recommendation Rec(2001)8 of the Committee of Ministers to member states on selfregulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), Draft Recommendation on measures to protect and promote respect for human rights with regard to social networking services. Committe of Experts on New Media, March 2010. Zie ook Artikel 29-werkgroep, Advies 5/2009 over online sociale netwerken, p. 13.

20. J de Haan, S van der Hof, W Bekkers, R Pijpers, 'Self-regulating online child safety in Europe', in: B O'Neill et al (eds), *Promoting a Safer Internet for Children. European Policy Debates and Challenges, Nordicom* (forthcoming).
21. Zie ook een derde zelfreguleringsinitiatief: European Framework for Safer Mobile Use by Young Teenagers and Children, http://ec.europa.eu/information_society/activities/sip/self_reg/phones/index_en.htm. Meer hierover: J de Haan, S van der Hof, W Bekkers, R Pijpers, *supra* noot 20.
22. Voor een lijst van de 20 ondertekenaars, zie: <http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm>. Onder de ondertekenaars bevinden zich zowel internationale (zoals Facebook, MSN en Youtube) als lokale sociale netwerkaanbieders.
23. Zie uitgebreider over de SSNP: J de Haan, S van der Hof, W Bekkers, R Pijpers, *supra* noot 20.
24. Zo o.a. Beginsel 3 dat luidt: '*Empower users through tools and technology*'.
25. Zie ook over veiligheidsstrategieën voor online sociale netwerken: Werkgroep artikel 29, Advies 5/2009 over online sociale netwerken, p. 13 (voorlichting, eerlijke en rechtmatige verwerking, beschermingstechnologieën, zelfregulering en bijzondere regels voor oneerlijk of misleidende praktijken).
26. J de Haan, S van der Hof, W Bekkers, R Pijpers, *supra* noot 20.
27. J de Haan, S van der Hof, W Bekkers, R Pijpers, *supra* noot 20.
28. Coaltition to make the Internet a better place for kids, Statement of purpose, Brussels, December 2011, http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm.
29. Iets waarvan kinderen naar mening van de Artikel

in de bescherming van kinderen door toestemming van ouders te vragen alvorens kinderen toe te laten op hun sociale netwerksites. Recentelijk is echter gesuggereerd dat Facebook eveneens instrumenten ontwikkelt om kinderen jonger dan 13 jaar onder ouderlijk toezicht gebruik te laten maken van hun sociale netwerkdiensten, bijvoorbeeld door het profiel van kinderen te koppelen aan dat van hun ouders.[30] Bovendien is er m.i. veel voor te zeggen om kinderen zelf te leren omgaan met hun privacyinstellingen en hen in relatie tot hun ouders – een steeds grotere mate van – privacy te geven, passend binnen de geest van het VN-Kinderrechtenverdrag 1989. Ten slotte zijn toegankelijke privacyinstellingen ook relevant voor andere kwetsbare groepen, zoals mensen met een verstandelijke bespreking of mensen die onder curatele gesteld zijn, maar daar wordt in de Coalitie dan weer geen aandacht besteed.[31]

Gelet op de toegenomen aandacht voor kinderrechten, de zorgen om ineffectieve bescherming van persoonsgegevens ingevolge technologische ontwikkelingen en de kanttekeningen bij zelfregulering is het interessant om te bezien welke veranderingen de ontwerpverordening beoogt te brengen en hoe deze kunnen worden gewaardeerd.

Het voorstel voor een algemene dataprotectieverordening

In januari 2012 heeft de Europese Commissie een voorstel voor een verordening gepubliceerd die de dataprotectierichtlijn 95/46/EG moet vervangen.[32] Met dit nieuwe instrument[33] beoogt de Commissie de bescherming van persoonsgegevens in de Europese Unie meer op één lijn te brengen en te moderniseren in licht van nieuwe technologieën die het gebruik en publiceren van persoonsgegevens ingrijpend hebben veranderd en – zoals de voorgaande paragraaf reeds aangaf – nieuwe risico's met zich brengen.[34] De verordening geeft uitvoering aan art. 16 Verdrag betreffende de werking van de EU dat sinds de invoering van het Verdrag van Lissabon een nieuwe rechtsgrondslag biedt voor regelgeving betreffende de bescherming van persoonsgegevens en het waarborgen van het vrije verkeer van gegevens. Deze grondslag omvat nadrukkelijk de opdracht tot effectieve bescherming van burgers, en daarmee ook kinderen, wat onder meer inhoudt dat *de burger zoveel mogelijk zelf moeten kunnen bepalen wat er met zijn gegevens gebeurt*.[35] Eerder had de Europese Commissie al laten weten dat kinderen extra bescherming verdienen, omdat onderzoek[36] heeft aangetoond dat:

> zij zich allicht minder bewust zijn van de risico's, gevolgen, beschermingsmaatregelen en rechten in verband met de verwerking van persoonsgegevens.[37]

Bovendien vraagt het Handvest van de grondrechten van de Europese Unie[38] naast het recht van burgers op bescherming van hun persoonsgegevens afzonderlijk aandacht voor de bijzondere bescherming en belangen van kinderen.[39]

De voorgestelde verordening heeft voor de definitie van kinderen aansluiting gezocht bij het VN-Kinderrechtenverdrag 1989 en verstaat daaronder personen die jonger zijn dan achttien jaar. De bijzondere bescherming die het voorstel voor kinderen op het oog heeft, bestaat uit verschillende elementen. Het meest in het oog springend is art. 8 dat met zoveel woorden ziet op de verwerking van persoonsgegevens van kinderen, maar andere bepalingen wijden zich eveneens aan kinderen.[40] Zorgen over de gegevensbescherming voor kinderen die in vorige paragraaf werden beschreven beoogt de verordening daarmee aan te pakken. Hier worden regels onder de voorgestelde verordening voor enkele relevante thema's nader toegelicht.

26-werkgroep verschoond moeten blijven, zie Opinion 2/2010 on online behavioural advertising, 22 June 2010, p. 17.

30. 'Facebook Explores Giving Kids Access', *Wall Street Journal*, 4 June 2012, http://online.wsj.com/article/SB10001424052702303506404577444711741019238.html?mod=WSJ_hpp_LEFTTopStories.
31. 'Ceo Coalition To Make The Internet A Better Place For Kids', *EDRi-gram newsletter*, nr. 10.5, 14 March 2012.
32. Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), COM(2012) 11 def, Brussel, 25 januari 2012. Naast de verordening is er een voorstel voor een richtlijn voor bescherming van persoonsgegevens in het kader van rechtshandhaving in strafzaken: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012)10 final.
33. Een verordening heeft rechtstreekse werking in de lidstaten en hoeft – anders dan een richtlijn – dus niet door de nationale wetgevers te worden geïmplementeerd, waardoor een grote diversiteit aan regels in beginsel wordt voorkomen. Overigens blijven lidstaten bevoegd om in bepaalde gevallen afwijkende regels te stellen, zie H Hijmans, 'Nieuwe Europese regels voor privacy: commissie stelt pakket voor om gegevens ook in het informatietijdperk te beschermen', *NtEr* mei 2012, nr. 4.
34. Overigens heeft Tweede Kamer al een motie *tegen* de verordening aangenomen, omdat deze lager niveau van bescherming zou bieden dan de huidige regelgeving; zie http://www.nl-prov.eu/nl-prov/hnpewcm.nsf/_/68413B7B936DF39BC12579D4002FD99A?OpenDocument.
35. H Hijmans, *supra* noot 34. Zie bijvoorbeeld het voorgestelde recht van gegevensoverdraagbaarheid in art. 18 dat hier verder buiten beschouwing blijft.
36. Zie Eurobarometer 2007, Safer Internet for Children – a children's perspectives, beschikbaar via http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm.
37. Zie: Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie, COM(2010) 609 def, Brussel 4 november 2010, p. 7.
38. Het Handvest is een opsomming van grondrechten die de EU-instellingen, alsmede de lidstaten bij de uitvoering van het Europese recht, ter harte moeten nemen, zie art. 51, EU-Handvest, en sinds de inwerkingtreding van het Verdrag van Lissabon juridisch bindend is voor EU-instellingen en EU-lidstaten (vergelijk art. 6, eerste lid, EU-Verdrag).
39. Zie art. 8 respectievelijk art. 24, EU-Handvest.
40. Voor bepalingen waaraan in het bijzonder aandacht voor

Toestemming en leeftijdsverificatie

Ingevolge het voorgestelde art. 8 van de verordening is de verwerking van persoonsgegevens van kinderen die jonger dan 13 jaar zijn bij het aanbieden van online diensten[41] alleen rechtmatig wanneer ouders toestemming hebben gegeven en deze toestemming verifieerbaar is. Hier valt op dat de leeftijdsgrens van 18 jaar in dit geval is ingeperkt tot kinderen jonger dan 13 jaar. Dat is een goede zaak in het licht van de vrijheid van informatie zoals neergelegd in het VN-Kinderrechtenverdrag 1989.[42] Bovendien past het in het idee dat jongeren tijdens het opgroeien steeds meer rechten en vrijheden moeten krijgen die ze zelfstandig – lees: los van hun ouders of andere volwassenen – kunnen uitoefenen. Ten aanzien van kinderen onder de 13 jaar sluit de verordening aan bij de wens om een grotere betrokkenheid van ouders bij jongere gebruikers van online diensten te realiseren. Ook in dat opzicht valt deze bepaling toe te juichen, maar dat neemt niet weg dat er tegelijkertijd wel wat haken en ogen aan zitten. Het begrip 'toestemming' krijgt mede door de nieuwe verordening steeds verdere verduidelijking en er lijkt een onderscheid te worden voorzien tussen toestemming door een kind en een volwassene, aangezien de eerste groep wellicht minder goed de risico's van het geven van toestemming overziet.[43] Dat wordt vervolgens echter gekoppeld aan het recht om te worden vergeten en dus het bieden van een *ex post* waarborg, waarvan we nu al denken dat die niet zal uitmunten in effectiviteit.[44] Weliswaar wordt er voorzien in een mogelijkheid om de voorwaarden voor toestemming nader te regelen in lagere regelgeving,[45] maar het is belangrijk om vanuit oogpunt van adequate bescherming en rechtszekerheid in de verordening zelf reeds helderheid te verschaffen over het verschil ligt tussen de voorwaarden voor 'consent' door volwassenen en door kinderen van dertien jaar en ouder. Voorts is het de vraag wat er in het geval van 'verifiable consent' wordt verstaan onder verifieerbaarheid. Het gaat dan om de verifieerbaarheid van de leeftijd van de gever van de toestemming. Met andere woorden met hoeveel zekerheid kan worden vastgesteld dat iemand jonger (of ouder) is dan dertien jaar en dat de gegeven toestemming inderdaad afkomstig is van een ouder. Is het voldoende dat er, zoals nu vaak gebeurt, een geboortedatum moet worden ingevuld en ouders in het registratieproces aanvinken dat ze toestemming geven? Of dient er een (meer) geavanceerd systeem voor verificatie van leeftijd en ouderlijke toestemming te worden geïmplementeerd? En welke online dienstverleners dienen een dergelijk systeem te implementeren? Zijn dat alleen de dienstverleners die specifiek op kinderen gerichte websites aanbieden of ook zij die meer algemene diensten bieden die mede door kinderen zou kunnen worden gebruikt?[46] De verordening zou ook hierover meer duidelijkheid moeten verschaffen om rechtszekerheid te waarborgen. Niet in de laatste plaats omdat het aanzienlijke bedrijfsmatige en financiële consequenties[47] kan hebben voor online dienstverleners als het betekent dat bedrijven geavanceerde en kostbare technieken voor leeftijdsverificatie moeten implementeren die bij voorkeur over landsgrenzen heen kunnen worden toegepast.[48] Vooralsnog zijn deze technieken niet beschikbaar en bovendien is de ontwikkeling ervan mede afhankelijk van door de Europese Commissie nader te bepalen technische specificaties.[49] Daarnaast is het van belang om bij de implementatie van dergelijke technieken voor ogen te houden dat het niet de bedoeling is om gebruikers te verplichten tot het verstrekken van (nog) meer persoonsinformatie.[50] Tot slot dient er voor te worden gewaakt dat 'parental consent' niet wordt verward met – al te vergaande – 'parental control' en de gekozen technische oplossingen de rechten en vrijheden van kinderen onnodig beperken.

Verwijderen van informatie

In de ontwerpverordening wordt een – overigens niet geheel nieuw[51] – gecombineerd recht om te worden vergeten en recht om gegevens te wissen geïntroduceerd in art. 17. Hiermee moeten betrokkenen in staat worden gesteld om bijvoorbeeld jeugdzonden en andere – al dan niet onwelgevallige – gegevens te verwijderen van het Internet en verder verspreiding te voorkomen. Zoals de bepaling terecht constateert, is het recht met name relevant voor kinderen die de – lange termijn – consequenties van hun acties niet – altijd – goed overzien en online wellicht gedrag vertonen waar ze als volwassenen liever niet meer aan worden herinnerd.[52] Het Internet heeft echter een ijzeren geheugen en het kan

---

de belangen van kinderen ten grondslag ligt maar die hier verder buiten beschouwing blijven, zie bijv. art. 6 (rechtmatige verwerking) en art. 33 (privacyeffectbeoordeling).

41. De verordening sluit aan bij het inmiddels bekende concept 'diensten van de informatiemaatschappij', zoals omschreven in art. 1, lid 2, van Richtlijn 98/34/EG, zoals gewijzigd bij Richtlijn 98/48/EG.
42. Art. 17, VN-Kinderrechtenverdrag 1989.
43. Zie overweging 53.
44. Zie hierna, onder Verwijderen van informatie.
45. Zie overweging 129 en art. 8, lid 3, ontwerpverordening.
46. Vergelijk Center for Democracy & Technology, Analysis of the proposed data protection regulation, 28 March 2012, https://www.cdt.org/files/pdfs/CDT-DPR-analysis.pdf, die pleiten voor beperking tot websites voor kinderen, zoals onder de Amerikaanse Children's Online Privacy Protection Act (hierna: COPPA) het geval is, tenzij een algemene online dienstverlener 'actual knowledge' heeft dat hij met een kind te maken. Het 'actual knowledge'-vereiste betekent niet dat algemene online dienstverleners verplicht zijn om de leeftijd van klanten of gebruikers te verifiëren. Verder wordt onder COPPA thans een 'sliding scale'-benadering gehanteerd. Dat houdt in dat wanneer persoonsgegevens slechts voor intern gebruik worden verzameld er een minder zware methode voor het verkrijgen van ouderlijke toestemming is vereist dan wanneer de persoonsgegevens ook worden gepubliceerd of gedeeld met derden, zie uitgebreider Notice of Proposed Rulemaking seeking comment on proposed changes to the Commission's COPPA Rule, September 2011, p. 59817.
47. Op het niet voldoen aan de voorwaarden voor toestemming *ex* art. 8 van de ontwerpverordening staat bovendien een boete van maximaal €1.000.000, zie art. 79, lid 6, onder a, ontwerpverordening.
48. Zie overigens de voorgestelde verordening betreffende elektronische identiteiten die beoogt om interoperabiliteit tussen nationale e-identificatiesystemen te bewerkstelligen, zie: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm.
49. Zie art. 86, ontwerpverordening.
50. Zie art. 10, ontwerpverordening.
51. Zie bijv. art. 12, onder c, dataprotectierichtlijn 95/46/EG.
52. Preventie blijft derhalve erg belangrijk naast meetregelen achteraf – hier ligt een bijzondere taak voor privacytoezichthouders bij de voorlichting aan kinderen over risico's,

lastig, zo niet onmogelijk zijn, om eenmaal geplaatste informatie, in welke vorm dan ook, weer te verwijderen. De bepaling heeft daar overigens iets op gevonden door aan de verantwoordelijke voor de verwerking een plicht op te leggen om

> redelijke maatregelen, waaronder technische maatregelen, [te nemen] ten aanzien van de gegevens die onder zijn verantwoordelijkheid zijn openbaar gemaakt, teneinde derden die deze gegevens verwerken ervan op de hoogte te stellen dat een betrokkene hun verzoekt ieder koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

Op die manier wordt beoogd om het vergeet- c.q. wisrecht te laten doorwerken naar derden. Een voorbeeld is het automatisch doorgeven van persoonlijke informatie tussen sociale netwerken, zoals Hyves, Twitter, LinkedIn en Facebook, waarbij de informatie weer automatisch zou kunnen verwijderd, als de betrokkene zich tegenover de aanbieder waar de informatie oorspronkelijk werd geplaatst op zijn vergeet-c..q. wisrecht beroept. In beginsel is het weliswaar voldoende dat de verantwoordelijke een *verzoek tot wissen* doet aan derden, maar het is goed voorstelbaar dat de Europese wetgever dat verder specificeert tot een geautomatiseerd – uitvoerbaar – verzoek tot wissen van gegevens. Dat neemt niet weg dat de uitvoerbaarheid van het – als zodanig – sympathieke vergeetrecht gelet op de architectuur van het Internet zeer lastig is en het effect vermoedelijk gering zal zijn, een onderwerp waarop in de literatuur reeds uitvoerig is ingegaan.[53]

Omdat de ontwerpverordening niet van toepassing is op privé-gebruik van gegevens, zoals gegevensuitwisseling tussen vrienden en bekenden op sociale netwerksites, is de groep van derden waartegen een kind zich kan richten op basis van het vergeet- en wisrecht evenwel beperkt tot partijen die, eventueel met commercieel doel, gegevens publiceren buiten de persoonlijke sfeer. Hijmans stelt hier terecht de vraag of de grens van de persoonlijke sfeer niet wordt overschreden in geval van bijvoorbeeld een dusdanig grote vriendengroep op een sociale netwerksite dat informatie ver buiten de directe familie- en vriendenkring wordt verspreid.[54]

Profilering

Het lijkt erop dat kinderen ingevolge de overwegingen van de ontwerp-verordening niet onderworpen mogen worden aan geautomatiseerde profilering. Op basis van art. 20, lid 1, ontwerpverordening zouden personen het recht krijgen om niet te worden onderworpen aan geautomatiseerde profilering, tenzij dat bijvoorbeeld gebeurt in het kader van een contractuele relatie of wordt gesanctioneerd door een wettelijke bepaling, en is omgeven met adequate waarborgen. De Europese Commissie lijkt hier vervolgens een uitzondering voor kinderen te hebben willen maken op de tenzij-clausule, maar geheel eenduidig is dat niet. De kind-exceptie wordt namelijk genoemd in de overwegingen,[55] echter deze is niet met zoveel woorden terug te vinden in de bepalingen van de regeling. Art. 20 over profilering zwijgt erover. Wel bepaalt art. 6, lid 1, onder f, ontwerpverordening in meer algemene zin dat het verwerken van persoonsgegevens op basis van legitieme belangen van de verwerker is toegestaan, tenzij dat o.m. in strijd is met de bescherming van kinderen. Dan zou de redenering zijn dat geautomatiseerde profilering een verwerking van persoonsgegevens behelst waarvoor op zich legitieme belangen kunnen bestaan, tenzij in een specifiek geval of bij een specifieke groep personen – met name kinderen – beschermingsbelangen zwaarder wegen.[56] Aan die uitleg kleeft een tweetal bezwaren. Ten eerst gaat deze in tegen de geest van art. 20 (geen profilering, tenzij…). Ten tweede is niet direct duidelijk dat en op basis waarvan de bepaling zich verzet tegen profilering van kinderen en daarmee wordt op zijn minst de rechtszekerheid niet gediend. Als het de Europese Commissie ernst is met de kind-exceptie voor profilering dan is aan te raden om deze nadrukkelijk in de tekst van de verordening zelf op te nemen. Overigens ontstaat er dan wel weer een ander probleem dat aanhaakt bij de eerder behandelde leeftijdsverificatie. Het zal voor bedrijven welhaast ondoenlijk zijn om met zekerheid vast te stellen of iemand een kind is of niet, zolang er geen adequate en betrouwbare methoden voor leeftijdsverificatie zijn.[57]

Transparantie

Informatie over de wijzen waarop hun gegevens worden verwerkt – denk aan een privacyverklaring – in zulke heldere en eenvoudige taal te worden geschreven dat kinderen die ook daadwerkelijk kunnen begrijpen (art. 11, ontwerpverordening). Dit is ook een meer algemeen aandachtspunt van de verordening aangezien het voor veel mensen – jong en oud – vaak niet meer te overzien is hoe en door wie hun gegevens online worden geoogst en vervolgens gebruikt en het dus sowieso een goed idee is om de informatie daarover aanzienlijk te verbeteren. Gegeven de complexiteit van dataprotectieregelgeving alsmede van de technologie is dat evenwel geen sinecure.[58] De privacyverklaring van Facebook beschrijft bijvoorbeeld in toegankelijk taal en voorzien van concrete voorbeelden beschrijven hoe zij persoonsgegevens verwerken, maar de achterliggende technologie is dermate ondoorzichtig dat zelfs goed ingevoerde Facebook-gebrui-

---

regels en rechten ten aanzien van de verwerking van persoonsgegevens, zie ook art. 52, ontwerpverordening.

53. Uitgebreider hierover: G J Zwenne, 'Nog veel onzekerheden over het recht om te worden vergeten', *IR* 2012, nr. 3, p. 68 e.v., met verdere verwijzingen.
54. H Hijmans, *supra* noot 34.
55. Te weten: *Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child* (Overweging 58).
56. Een andere uitleg zou kunnen zijn dat de kind-exceptie wel nadrukkelijk was opgenomen in een eerdere versie van het ontwerp, maar later is geschrapt uit de bepalingen en abusievelijk vermeld bleef in de overwegingen.
57. Dat is temeer zorgelijk daar voor overtreding van art. 20, ontwerpverordening flinke boetes worden voorgesteld (zie art. 79, lid 6, onder d, ontwerpverordening).
58. Zie in dit verband: B van den berg, S van der Hof, 'What happens to my data? A novel approach to informing users of data processing practices', *First Monday*, Volume 17, Number 7 - 2 July 2012, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/4010/3274.

kers onbewust en ongewild data kunnen 'lekken'. Het systeem is er namelijk op gericht om gebruikers te verlokken tot het delen van zoveel mogelijk persoonlijke informatie, omdat op basis daarvan gericht advertenties kunnen worden voorgeschoteld aan gebruikers. Dat online aanbieders op die manier geld beogen te verdienen, is niet per definitie verkeerd, maar bij de weinig transparante en oncontroleerbare manier waarop dat gebeurt kunnen wel degelijk vraagtekens worden geplaatst. Voor Facebook geldt dit in buitengewone mate, maar ook op andere websites zijn de achterliggende processen niet altijd even transparant.[59] Transparantie in de vorm van begrijpelijke en toegankelijke informatie is derhalve onvoldoende om kinderen (en anderen) adequaat te beschermen. Dat probleem onderkent de Europese wetgever met de introductie van een tweetal nieuwe beginselen: 'privacy by default' en 'privacy by design'.

'Privacy by default' en 'privacy by design'

Bedrijven en overheden krijgen onder de verordening meer verantwoordelijkheid voor de naleving van dataprotectievoorschriften,[60] onder meer met verplichtingen gebaseerd op de beginselen 'privacy by default' en 'privacy by design'.[61] Het eerste beginsel heeft tot doel om te garanderen dat persoonlijke informatie in principe niet voor een ongelimiteerde groep mensen toegankelijk is. Dat staat haaks op het business model van veel sociale netwerksites, zoals Twitter en Facebook, waar de gebruiker eerst zijn privacy settings moet aanpassen om de bedoelde beslotenheid te creëren. Een eerdergenoemde uitzondering zijn Hyves-profielen van jongeren onder de 16 jaar die alleen voor vrienden toegankelijk zijn, tenzij de minderjarige Hyver deze zelf voor een groter publiek 'open zet'. Het tweede beginsel bedoelt de verantwoordelijke verwerker er toe te verplichten om de voorschriften uit de verordening technisch-organisatorisch in te bouwen in het ontwerp van haar diensten. [voorbeeld] Hoe beide beginselen in de praktijk zullen uitwerken is nog een vraagteken en afhankelijk van de verdere specificaties die de Europese Commissie naar alle waarschijnlijkheid zal vaststellen. Zeker lijkt echter wel dat het een grote impact zal hebben op het bedrijfsleven. Overigens zagen we eerder al dat bedrijven in het kader van o.a. de SSNP en de Safer Internet-coalitie al doende zijn om voor kinderen geschikte privacyinstellingen te definiëren en implementeren, maar het wettelijk verankeren van deze beginselen betekent een stevige stok achter de deur voor een integrale en effectieve, technische en organisatorische naleving van privacyvoorschriften. Daarmee kan bijvoorbeeld ook tegemoet worden gekomen aan een grotere transparantie van dataverwerkingspraktijken – en hoe daaraan als Internetgebruiker te ontsnappen.

Waardering van de veranderingen

Met de enorme vlucht die het Internetgebruik onder kinderen heeft genomen, is het bijzonder heuglijk dat de ontwerpverordening nadrukkelijk aandacht besteedt aan de bescherming van persoonsgegevens van kinderen door speciale regels voor te stellen. Inmiddels is ook voldoende duidelijk geworden dat kinderen risico's lopen als gevolg van Internetgebruik en – het in uiteenlopende vormen gemanifesteerde – misbruik van hun persoonsgegevens daarbij een een rol kan spelen. Dat misbruik kan echter in belangrijke mate plaatsvinden binnen de privé-sfeer, waarop de verordening dan weer niet van toepassing zou zijn, zodat bescherming in het licht van de in onderzoek geconstateerde online risico's voor kinderen (denk aan digitaal pesten) tamelijk beperkt is. Terecht is het dataprotectierecht echter niet in alle gevallen (denk bijvoorbeeld aan misleidende online diensten) het aangewezen juridisch kader om problemen te adresseren. Daarnaast kunnen andere beschermingsinstrumenten, zoals het stimuleren van mediawijsheid door onderwijs en voorlichting, in bepaalde gevallen verstandiger en effectiever zijn dan een juridische aanpak.[62] Dat neemt niet weg dat de ontwerpverordening zou moeten uitleggen wat in een online omgeving wordt verstaan onder persoonlijke en huishoudelijke activiteiten[63] om onduidelijke situaties over de afbakening van de privé-sfeer zoveel mogelijk te voorkomen. Belangrijke verbeteringen zijn evenwel de bijzondere regels voor transparante informatie aan kinderen en meer algemeen de implementatie van de beginselen van 'privacy by default' en 'privacy by design', ofschoon moet blijken hoe effectief deze in de praktijk uitwerken.

De ontwerpverordening houdt – mede in de geest van het VN Kinderrechtenverdrag 1989 – terecht rekening met de behoefte van jongeren om steeds zelfstandiger te worden en zelf beslissingen te nemen door het vereiste van ouderlijke toestemming voor de verwerking van persoonsgegevens van hun kinderen te koppelen aan de leeftijd jonger dan dertien jaar. Verduidelijking is echter noodzakelijk ten aanzien van het verschil in toestemming door volwassenen en kinderen van dertien jaar en ouder. Ofschoon het wenselijk is om jongeren meer eigen verantwoordelijk te geven, betekent dit niet automatisch dat zij de gevolgen van hun beslissingen in dezelfde mate overzien als volwassenen. Op welke wijze en in hoeverre daar rekening mee moet worden gehouden, is nu volstrekt onbepaald. Met recht wordt weliswaar aangehaakt bij het recht om te worden vergeten, maar in de literatuur is in dat verband reeds uitvoerig ingegaan op problemen van praktische onuitvoerbaarheid en verwachte geringe effectiviteit. Voorts geeft de verordening ten onrechte geen uitleg aan het begrip '*verifiable* consent', wat op zijn minst in twee opzichten problematisch is. Ten eerste geeft het veel rechtsonzekerheid voor bedrijven en andere online aanbieders als zij niet weten of zij 'parental consent' moeten vragen en, zo ja, op welke manier. Afhankelijk van de precieze inkleuring van deze voorwaarde kan het in meer of mindere mate bedrijfsmatige en financiële consequenties hebben. Bovendien zal die inkleuring van invloed zijn op de ontwikkeling van leeftijdsverificatie, waarvoor op dit moment een grensoverschrijdend en waterdicht systeem ontbreekt. Ten tweede moet worden voorkomen dat 'parental consent' zich ontwikkeld tot onwenselijke vormen van 'parental control' die de vrijheden van kinderen teveel inperken. Ook hierbij zal het van belang zijn hoe 'verifiable consent' en leeftijdsverifi-

59. Op basis van de recente Cookiewet moeten transparantie en controle voor Internet gebruikers worden verbeterd, maar vooralsnog lijkt de naleving nog gaten te vertonen, zie: Cookiewet genegeerd door grote Nederlandse sites, Webwereld 3 augustus 2012, http://webwereld.nl/nieuws/111372/cookiewet-genegeerd-door-grote-nederlandse-sites.html.
60. Zie art. 22, ontwerpverordening.
61. Zie art. 23, ontwerpverordening.
62. Vergelijk S van der Hof, E J Koops, 'Adolescents and Cybercrime: Navigating between Freedom and Control', *Policy & Internet*: Vol. 3: Iss. 2, Article 4.
63. Zie art. 2, lid, onder d, ontwerpverordening.

catie worden geïnterpreteerd en vervolgens praktisch vormgegeven.
Het uitdrukkelijk reguleren van profilering van individuele personen is een belangrijke stap voorwaarts in hun bescherming tegen ondoorgrondelijke profileringspraktijken. Eerder werd al duidelijk dat de zelfreguleringsinitiatieven voor een veiliger Internet voor kinderen zich vooral richten op de persoonlijke informatie die Internetgebruikers onderling uitwisselen en niet zozeer op de profileringspraktijken van overheid en bedrijfsleven, waarbij enorme hoeveelheden data – waar niet voor niets vaak aan wordt gerefereerd met de term 'big data' – worden geoogst van Internetgebruikers, inclusief kinderen. Ook de huidige regelgeving is niet ingericht op deze tamelijk recente ontwikkelingen door de focus te hebben op data *an sich* en niet de daaruit op vaak ingenieuze wijze geconstrueerde persoonlijke en risicoprofielen. Helaas is in de huidige versie van de ontwerpverordening evenwel volstrekt onduidelijk of kinderen een bijzondere positie hebben in dat verband en zo ja, welke. De overwegingen van de verordening wijzen wel in die richting, maar in de tekst van de overordening is er vervolgens niet met zoveel woorden iets over terug te vinden. Hierover moet om reden van rechtszekerheid dus meer helderheid komen. Gegeven het feit dat een kind-exceptie vergaande consequenties heeft voor het bedrijfsleven en de leeftijd van kinderen momenteel slechts met een beperkte mate van zekerheid kan worden vastgesteld, zal de verordening dan wel goed moeten aangeven wat er van bedrijven wordt verlangd.
Al met al is de ontwerpverordening een verbetering ten opzichte van het huidige dataprotectiekader als het gaat om de bescherming van kinderen tegen de verwerking van hun persoonsgegevens buiten de privé-sfeer. Tegelijkertijd zijn er nog teveel onduidelijkheden van een werkelijk geslaagde voorstel te kunnen spreken. Er is dus nog veel werk aan de winkel voor de Europese wetgever.

Tot besluit

Tot slot nog een tweetal opmerkingen. Ten eerste heb ik me in deze bijdrage gericht op de bescherming van kinderen. Dat laat onverlet dat er – zoals eerder ook reeds kort werd aangegeven – andere groepen zijn die wellicht vergelijkbare bescherming in het kader van dataprotectieregelgeving behoeven. Denk bijvoorbeeld aan mensen met een verstandelijke beperking, die – evenals kinderen – risico's en problemen kunnen ondervinden op het Internet. Het zou overweging verdienen om te bezien in hoeverre de ontwerpverordening niet moet worden uitgebreid naar andere kwetsbare groepen, voor zover ze niet reeds onder de kinderen vallen.
Ten tweede wil ik nog even kort terugkeren naar zelfregulering door bedrijven die is bedoeld om de online veiligheid voor kinderen te vergroten. Ondanks eerdergenoemde kanttekeningen die daarbij te plaatsen zijn, denk ik dat het belangrijk blijft om het bedrijfsleven (en andere belanghebbenden) proactief te betrekken bij het realiseren van bescherming en vergroting van de weerbaarheid van kinderen op Internet.[64] Essentieel is wel om daarbij meer dan nu het geval is oog te hebben voor aandachtspunten, zoals het profileren van klanten, die voor bedrijven wellicht gevoelig liggen, maar niettemin ook onderdeel van het beleid zouden moeten zijn. De ontwerpverordening biedt daartoe – ondanks eerder gemaakte voorbehouden over noodzaak tot meer helderheid en effectiviteit van regels – goede uitgangspunten. Ook in dat verband is het hoogst belangrijk dat er een stevige basis komt met de ontwerpverordening (lees: effectieve en heldere regels), waarop verder voort kan worden gebouwd met zelfregulering door het bedrijfsleven.

64. Zie ook art. 38, ontwerpverordening.

Boekbespreking

De wet op internet

Franke van der Klaauw[*]

De wet op internet, editie 2010
Arnoud Engelfriet
Uitgeverij Ius Mentis BV Eindhoven, 300 p.

Een leuk boek

Ter bespreking ligt het boek 'De wet op internet' van Arnout Engelfriet voor. Ik heb het boek niet alleen gelezen voor het maken van deze boekbespreking, maar ik heb het ook, naast ander juridisch onderwijsmateriaal, voorgeschreven toen ik onderwijs gaf aan niet juridisch geschoolde (ICT in Business) masterstudenten. Ik had die keuze voor het gebruik van het boek van Engelfriet gemaakt omdat de studenten behoorden tot de doelgroep waarvoor Engelfriet zijn boek heeft geschreven, te weten 'internetters' die willen weten wat wettelijk mag en wat niet. En daarnaast uiteraard omdat zijn boek veel onderwerpen bevat die ik in het onderwijs wilde behandelen en het een breed aanbod van voorbeelden bevat. Bij de evaluatie van een en ander betreffende dat onderwijs, waaronder ook het onderwijsmateriaal, bleken de studenten unaniem in hun oordeel over het boek: het boek is goed leesbaar en leuk. Een dat vonden ze echt niet van al het voorgeschreven onderwijsmateriaal. Om te beginnen en om die reden durf ik daarom over *De wet op internet* van Engelfriet te beweren dat het voor techneuten/niet-juristen een leuk boek is.

Waar gaat het boek over?

Als gezegd geeft Engelfriet aan dat hij zijn boek heeft geschreven voor Internetters die zich bij internetgebruik geconfronteerd zien met vragen van juridisch mogen en moeten. Hij benadert deze vragen vanuit de praktijk van de internetgebruiker om er aan de hand van mogelijke juridische kwalificaties antwoorden op te geven.
In zijn *leeswijzer op onderwerp* (p. 21) wordt duidelijk welke vier groepen van internetgebruikers hij voor ogen heeft en welke onderwerpen hij voor hen relevant vindt. De vier groepen gebruikers zijn:

Bloggers en forumdeelnemers

De volgende hoofdstukken (onderwerpen) zijn voor bloggers en forumdeelnemers van belang: 2 (over weblogs); 3 (over forums); 5 (over hyperlinks); 8 (over Creative Commons); en 11 (over internetproviders).

Websitebouwers

De volgende hoofdstukken (onderwerpen) zijn voor websitebouwers van belang: 5 (over hyperlinks); 6 (over auteursrecht); 4 (over privacyregels); en 10 (over hergebruik van andermans site).

Online verkopers

De volgende hoofdstukken (onderwerpen) zijn voor online verkopers van belang: 13 (over webwinkels); 12 (over merkenrecht); en 4 (over privacyregels).

Distributeurs en hosters van informatie

De volgende hoofdstukken (onderwerpen) zijn voor de distributeurs en hosters van belang: 6 (over auteursrecht); 10 (over licenties); 7 (over filesharing); 8 (over Creative Commons); 9 (over open source software); en 11 (over internetproviders).

De hoofdstukken die in deze leeswijzer niet genoemd worden zijn, behalve het inleidende hoofdstuk 1, de twee laatste hoofdstukken: hoofdstuk 14 (Misdaad per PC) over computer- en internetcriminaliteit en hoofdstuk 15 (Virtuele wereld, echte wet) over rechtsregels die van toepassing kunnen zijn ingeval van diverse online-omgevingen als Second Life, World of Warcraft en dergelijke.
Ik denk dat het behandelde niet alleen voor de genoemde groepen internetters nuttig is, maar zeker ook voor de, laten we maar zeggen, gewone huis-, tuin- en keukeninternetgebruiker.

Concluderend

Weer lezend door de goed en toegankelijk geschreven hoofdstukken, kan ik me heel wel voorstellen dat mijn studenten het boek leuk vonden. De aangehaalde casus zijn voorstelbaar en aansprekend. Maar stel ik mij de bedoelde lezer van het boek voor, waarschijnlijk een niet-juridisch onderlegde internetter, dan vraag ik mij af of deze in staat is om de door Engelfriet beoogde heldere omgang met de bestaande wettelijke regels met behulp van dit boek goed op te pikken. 'In dit boek leg ik uit hoe de wet (volgens mij) in elkaar zit. Niet hoe de wet zou moeten zijn', aldus Engelfriet op p. 208 in zijn nawoord. Ik ben namelijk bang dat lezers er niet goed achter komen hoe de wet in elkaar zit. Daarvoor wordt *de wet* naar mijn mening niet of te weinig en daarnaast te losjes uitgelegd. Ik heb daarom voor de volgende druk een advies. Wat mij namelijk op een soms ergerlijke wijze dwars zit is een voor de lezer informatief gemis. Ik kom zelf niet los van een behoefte om bij bijna ieder hoofdstuk de lezer te voorzien van wat meer rechtssystematisch accurate achtergrondinformatie, een juridisch preciezere formulering en daarnaast meer samenhangend. De niet-jurist heeft doorgaans weinig benul van wat een overeenkomst is, wat een wanprestatie, wat een onrechtmatige daad, en kent nauwelijks het verschil is tussen burgerlijk recht en straf- en

* Mr. F.A.M. van der Klaauw-Koops is verbonden aan eLaw@Leiden, Centrum voor recht in de informatiemaatschappij, Universiteit Leiden.

administratief. In het boek waarschuwt Engelfriet nauwelijks voor de soort reacties, rechtsgevolgen en al dan niet financiële risico's die het gevolg kunnen zijn van divers (on) rechtmatig handelen 'op het internet'. Het ontbreekt de lezer aan een informatief overzicht van de reikwijdte van de rechten en plichten, en zeker aan de consequenties van de diverse rechtsfeiten.

Het zal mijn professie als internetrechtdocent zijn die maakt dat ik de tekorten op genoemde punten constateer en eigenlijk heel vervelend vind, ook, of misschien juist, voor niet juridische lezers. Een toegankelijke juridische inleiding en context bij de diverse onderwerpen die best beknopt mogen zijn, zou veel van de behandelde onderwerpen in een juister begrip en perspectief kunnen plaatsen, en de risico's van bepaald internetgebruik duidelijker maken. Weliswaar bevat het boek als laatste een uitgebreid eindnotenapparaat (p. 209 – 300), dat voornamelijk verwijst naar rechterlijke uitspraken en naar wetsartikelen, maar dat de tekst daarmee niet verduidelijkt. Zonder noodzakelijke juridische basiskennis vormen de eindnoten weliswaar een verantwoording van de schrijver, maar de spreekwoordelijke paarlen voor de zwijnen voor de lezers.

Onduidelijkheid blijft voor hosters

Joran Spauwen[*]

Annotatie bij Rechtbank Den Haag 21 augustus 2012 (Altushost)

Sinds Lycos/Pessers[1] weten we dat internet tussenpersonen onder bepaalde omstandigheden een verantwoordelijkheid dragen voor het handelen van hun klanten op grond van 6:162 BW.[2] De laatste tijd ontdekken rechthebbenden steeds vaker de tegen tussenpersonen gerichte streng geformuleerde verbodsrechten in de specifieke I.E.-wetten die zijn gebaseerd op de Handhavingsrichtlijn uit 2004.[3] Deze ontwikkeling begon bij het auteursrecht[4] en lijkt nu ook in het merkenrecht navolging te krijgen. In de hier gepubliceerde uitspraak volgt de rechtbank Den Haag namelijk niet het toetsingskader van de onrechtmatige daad, maar verbiedt de tussenpersoon in kwestie meerdere websites van gedaagde te hosten op grond van art. 2.22 lid 6 BVIE. Het is niet de eerste keer dat dit verbodsrecht tegen internet tussenpersonen wordt aangewend.[5] Het is echter wel één van de eerste keren dat een beroep op art. 2.22 lid 6 BVIE in kort geding succesvol is.

De internet tussenpersoon die in de onderhavige uitspraak onder vuur ligt is AltusHost, althans een Zweedse en een Belizaanse vennootschap varend onder deze naam. AltusHost is door een groep van 11 luxe horlogemakers aangesproken op het feit dat op haar servers websites worden gehost waar nephorloge's c.q. replica's worden verkocht.

De horlogemakers vorderen een verbod op het hosten van deze websites en doen hiervoor een beroep op art. 2.22 lid 6 BVIE. De rechtbank wijst dit verbod toe. Hoewel de uitspraak op zichzelf niet verbazingwekkend is, bevat deze wel een aantal opmerkelijke overwegingen.

Toepassinsgebied BVIE

Gedaagde is een hostingbedrijf dat kennelijk gevestigd is in Zweden en Belize. Zonder veel omwegen concludeert de rechtbank dat het BVIE van toepassing is omdat de websites leveren aan Nederland, er met euro's kan worden betaald en de websites zijn opgesteld in de door Nederlanders begrepen Engelse taal.

In het algemeen zou men zich kunnen afvragen of op deze wijze niet tè lage drempels worden gesteld aan het toepassen van Nederlands recht op online activiteiten. De rechtbank lijkt hier impliciet aansluiting te zoeken bij de Ladbrokesuitspraak van de Hoge Raad, waarin werd bepaald dat een online kansspel gericht is op Nederland als dit kan worden geselecteerd in een lijst met landen van waaruit men deel kan nemen.[6] De situatie ligt bij een webshop mogelijk enigszins genuanceerder. Het betreft immers niet het leveren van een dienst, zoals een kansspel. Vaak hanteren websites een ongelimiteerde lijst met alle landen van wereld, terwijl zij niet daadwerkelijk van plan zijn daarmee handel te drijven. Voor de bevoegdheid van de rechter (en het toepasselijk recht) moet een dergelijk 'plan' volgens het Hof van Justitie echter wel aanwezig zijn.[7] De rechtbank noemt tevens de betaalmogelijkheid in euro en de Engelse taal als relevante omstandigheden. Deze omstandigheden zullen echter voor veel websites binnen de Eurozone gelijk zijn, omdat er nu eenmaal een gezamenlijke munt bestaat en het vrij gebruikelijk is een website (ook) in het Engels aan te bieden. Interessant is dat de uitspraak deels haaks staat op de conclusie van het Hof Den Haag, wat betreft 'gebruik' in de Benelux door een internationale website waar bloemen verkocht werden.[8] Het Hof overwoog: '*Weliswaar behoeft het gebruik van de Engelse taal geen belemmering te zijn voor een deel van de consumenten in de Benelux - dit geldt overigens niet voor alle consumenten -, maar het kan geen reden zijn om aan te nemen dat de website (specifiek) mede gericht is op de Benelux, waar het Engels immers niet een van de officiële talen is*.' Overigens kon op de website alleen in dollars betaald worden, maar kon men wel door middel van een Nederlands vlaggetje doorklikken naar een pagina waar voorbeelden werden getoond van bloemen die in Nederland bezorgd konden worden.

In het bijzonder kun je je afvragen of de website - en dus het handelen - van een derde voldoende grondslag biedt om het BVIE van toepassing te verklaren op een buitenlandse host. Zijn eigen handelen, het hosten van inbreukmakende websites, is immers niet gericht op Nederland. De host heeft geen invloed op de gebieden waar zijn klanten zich op richten. Als deze uitspraak strikt gevolgd wordt dient de host rekening te houden met het feit dat hij gebonden is aan alle landen die zijn aangesloten op het internet, omdat het goed

---

* Mr. J. Spauwen is advocaat bij Kennedy Van der Laan te Amsterdam.

1. HR 25 november 2005 (Lycos/Pessers), *NJ* 2009, 550.
2. Zie noot Hugenholtz, *NJ* 2009, p. 5482.
3. Art. 2.22 lid 6 BVIE bevat geen uitzondering of toepassingsdrempels: 'De rechter kan op vordering van de merkhouder een bevel uitvaardigen tot staking van diensten van tussenpersonen wier diensten door derden worden gebruikt om inbreuk op zijn merkrecht te maken.'
4. Toepassing van art. 26d Auteurswet in de Pirate Bay en FTD zaken. Zie bijvoorbeeld: Vzr.Rb. Amsterdam 30 juli 2009, *LJN* BJ4298 (BREIN/TPB) en Hof Den Haag 15 november 2010, *LJN* BO3980 (EYEWORKS/FTD).
5. Hof Leeuwarden 22 mei 2012, *LJN* BW6296 (Stokke/Markplaats); Vzr.Rb. Amsterdam 18 augustus 2011, *LJN* BR5357 (Heineken/Olm) en Vzr.Rb. Rotterdam 12 december 2008, IEPT 20081212 (KvK).
6. HR 18 februari 2005, *NJ* 2005, 404, m.nt. Mok.
7. HvJEU 7 december 2010, C-585/08 (Pammer en Alpenhof); vgl. ook HvJEU 6 september 2012, C190/11 (Mühlleitner/Yusufi).
8. Hof Den Haag 27 april 2010, *LJN* BM5134 (1-800-FLOWERS.COM).

mogelijk is dat een van zijn klanten een website heeft gericht op één van deze jurisdicties.
Alhoewel er goede redenen kunnen zijn het BVIE van toepassing te verklaren, rijst de vraag waarom de horlogemakers hun eisen niet baseerden op het Zweedse recht en een rechtbank in Zweden als competent forum verkozen. Niet vergeten mag worden dat in principe de gedaagde in zijn woonplaats gedagvaard moet worden (art. 2 EEX-Vo) en de internet tussenpersoon in principe niet verantwoordelijk is voor het aanbod van haar klanten (art. 6:196c BW). Niet voor niets biedt art. 3 van de eCommerce-richtlijn tussenpersonen de waarborg dat zij in andere lidstaten niet onderworpen worden aan een strenger regime dan in hun land van vestiging, zoals eind 2011 is bevestigd door het Hof van Justitie.[9]

Subsidiariteit en proportionaliteit

Ondanks de onvoorwaardelijke formulering van art. 2.22 lid 6 BVIE overweegt de rechtbank wel of de subsidiariteit en proportionaliteit niet in de weg staan aan toepassing van het verbod. Dit lijkt ook gepast nu het verbod een beperking op de vrijheid van meningsuiting en ondernemerschap met zich meebrengt.[10] AltusHost voerde in dit kader aan dat de horlogemakers ook een minder verstrekkende maatregel voor handen hadden, te weten het initiëren van domeinarbitrage. De rechtbank merkt hierover terecht op dat domeinarbitrage enkel ziet op de domeinnaam en geen betrekking heeft op de gehoste inbreukmakende content. Daarnaast stelde AltusHost zich op het standpunt dat de horlogemakers te weinig hadden ondernomen tegen de websitehouders zelf. Het ligt immers voor de hand dat eerst de daadwerkelijke inbreukmaker wordt aangesproken, voordat een (tussen)persoon betrokken wordt die niet zelf in strijd heeft gehandeld met de wet.[11] De rechtbank meent dat de horlogemakers voldoende actie hebben ondernomen door de websitehouders aan te schrijven. Opmerkelijk genoeg is door de horlogemakers vervolgens geen procedure tegen de websitehouders geïnitieerd. Volgens de horlogemakers waren de websitehouders veelal afkomstig uit landen waarvan bekend is dat deze niet met grote voortvarendheid tegen merkinbreukmakers optreden. Deze uitleg wordt door rechtbank gevolgd. Niet duidelijk is waarom de horlogmakers enkel in het land van afkomst een procedure kunnen aanspannen. Het stond hen immers vrij een procedure in Nederland te beginnen. Bovendien lijkt mij dat 'voortvarendheid' een betrekkelijk vaag criterium is om een procedure tegen de tussenpersoon voorrang te verlenen. Men zou zich ook de vraag kunnen stellen hoe het met de I.E.-handhaving in Belize gesteld is, waar één van de gedaagden gevestigd is. Als het niveau van I.E.-handhaving voor de subsidiariteittoets van belang is, ligt het immers voor de hand dit niveau te vergelijken met het land waar handhaving volgens de horlogemakers kennelijk wel adequaat is.
Wat betreft de proportionaliteit doet AltusHost een beroep op het argument dat een blokkade zinloos is, omdat de houders hun websites binnen de kortste keren bij een andere host kunnen onderbrengen. Dit verweer veegt de rechtbank van tafel, omdat de horlogemakers ter zitting onbetwist hebben gesteld dat zij ook optreden tegen andere hostingproviders. Evenals in de zaak over de Pirate Bayfilters wil de rechtbank dus niet meegaan in dit effectiviteitsverweer.[12] De rechtbank neemt het gebrek aan effectiviteit desalniettemin mee in zijn beoordeling van de vereiste proportionaliteit en concludeert dat dit, afgezet tegen het '*niet al te ingrijpende karakter'* en de lage kosten, voldoet. De rechtbank legt helaas niet uit waarom een verbod op het hosten van een gehele website niet al te ingrijpend is. Het lijkt mij dat de hostingfaciliteiten voor een webwinkel cruciaal zijn. Ervan uitgaande dat de rechtbank vasthoudt aan zijn vaststelling dat de horlogemakers ook tegen andere hostingpartijen optreden, betekent dit effectief dat de webwinkel zijn deuren kan sluiten; of beter gezegd: dat zijn deuren gesloten worden. Dit is naar mijn mening tamelijk ingrijpend voor de webwinkel in kwestie; inbreukmaker of niet.

Conclusie

Al met al resten na het lezen van deze uitspraak de nodige vragen en lijkt het alsof de rechtbank iets te eenvoudig tot haar conclusies komt. Daarbij is niet gezegd dat nadere uitleg noodzakelijk tot een ander resultaat moet leiden. Het was echter waardevol geweest voor de rechtspraktijk als de rechtbank, net als in de zaak over de Pirate Bay-filter,[13] zijn motivatie uitgebreider uiteen had gezet. Op die manier kunnen de voorwaarden die gesteld worden door het Hof van Justitie[14] en de eCommercerichtlijn[15] gewaarborgd worden, ondanks dat zij niet expliciet in de onderhavige verbodsbepaling genoemd worden.[16]

9. HvJEU 25 oktober 2011, C-509/09; C-161/10 (eDate; Martinez v. MGM), r.o. 68.
10. HvJ EU 24 november 2011, C-70/10, (Sabam /Scarlet), zie ook Rb. Den Haag 11 januari 2012, *LJN* BV0549 (BREIN/ Ziggo en XS4All).
11. Zie ook T. Cohen Jehoram, *Industriële Eigendom, Deel 2*, Kluwer 2009, p. 435.
12. Rb. Den Haag 11 januari 2012, *LJN* BV0549 (BREIN/ Ziggo en XS4All), r.o. 4.34.
13. Rb. Den Haag 11 januari 2012, *LJN* BV0549 (BREIN/ Ziggo en XS4All).
14. HvJ EU 24 november 2011, C-70/10, (Sabam /Scarlet) en HvJEU 16 februari 2012, C-360/10 (SABAM/Netlog),
15. Richtlijn 2000/31/EG, zie ook 6:196c.
16. Art. 2.22 lid 6 BVIE (dit geldt eveneens voor art. 26d Auteurswet).

Duurzame drager: achterhaald concept?

Arno Lodder

Annotatie bij Hof van Justitie EU, 5 juli 2012, zaak C-49/11, (Content Services Ltd/Bundesarbeitskammer)

1. Op 5 juli 2012 heeft het Hof van Justitie het concept 'duurzame drager' afkomstig uit de 15 jaar daarvoor tot stand gekomen Richtlijn 97/7/EG inzake overeenkomsten op afstand toegelicht.
2. De reden hiervoor is mij niet bekend, maar veel zaken over elektronisch contracteren bij het Hof van Justitie betreffen een Duitse prejudiciële vraag.[1] In deze zaak is de vraag afkomstig van de Oostenrijkse rechter. Content services is een Engelse BV met een filiaal in Mannheim en biedt via een website in het Duits software aan, vooral gratis en proefversies, uiteraard ook op de Oostenrijkse markt. Het wordt uit de zaak niet geheel duidelijk, maar de verleende dienst lijkt eruit te bestaan dat gedurende een bepaalde periode toegang wordt verkregen tot de genoemde 'gratis' software alsmede proefversies.
3. Gebruikers vullen een online aanmeldingsformulier in en worden verzocht aan te vinken dat ze de voorwaarden accepteren *en* afstand doen van hun herroepingsrecht.
4. Er wordt in deze zaak niet ingegaan op het afstand doen van het herroepingsrecht. Dit zou geen consequenties moeten hebben. Achtergrond van dit wettelijk recht is immers consumenten te beschermen. Als het mogelijk zou zijn daar afstand van te doen, vervalt de betekenis van dit recht. Alleen bij bepaalde overeenkomsten op afstand bestaat geen wettelijk retourrecht, zoals bij levering van bederfelijke waar of producten die aan prijsschommelingen onderhevig zijn. In die gevallen kan overigens desgewenst een herroepingtermijn worden overeengekomen (art. 7 lid 3 Richtlijn 97/7/EG), maar gezien de aard van de overeenkomsten bestaat hier geen wettelijk herroepingsrecht.
5. Na invulling van het aanmeldingsformulier ontvangen gebruikers een e-mail met naam en wachtwoord die toegang bieden tot de aangevraagde dienst. Informatie over het herroepingsrecht (r.o. 19) staat niet in de mail, maar is via een link benaderbaar. Onduidelijk is overigens *waarom* er informatie over het herroepingsrecht wordt verstrekt als gebruikers hebben aangevinkt er afstand van te doen.
6. De vraag wordt niet behandeld, maar algemeen aanvaard is dat het niet mogelijk is om een overeenkomst met betrekking tot een dienst te herroepen als met de uitvoering van de dienst begonnen is. Men kan betogen dat hier zo lang naam en wachtwoord nog niet gebruikt zijn herroepen mogelijk is.
7. Na toezending van de mail met naam en wachtwoord krijgt de gebruiker een factuur van Euro 96 voor 12 maanden toegang tot de website. Deze praktijk roept herinneringen op aan de notoire oplichters achter LIS/BER bv.[2] Over de handelswijze gaat het in deze zaak overigens niet. De vraag betreft de wijze waarop informatie over het herroepingsrecht is verstrekt.
8. Zoals de AG in zijn advies[3] al terecht opmerkte wordt de duurzame drager niet gedefinieerd in Richtlijn 97/7/EG. De strekking is echter van begin af aan duidelijk geweest, namelijk de mogelijkheid om bij op afstand gesloten overeenkomsten de beschikking te hebben over essentiële informatie op papier of middels een ander duurzaam medium. Al vrij snel was men het erover eens dat een e-mail, althans de in de mailbox van de consument gearriveerde boodschap, ook gezien kon worden als een duurzame drager. In 2002 schreven Hörnle e.a[4] dat ook de Britse wetgever daarvan uitging en vervolgde: 'However, it is questionable whether a distinction can be made between an email, which is sent to the consumer by the supplier, from a web site, which requires the consumer to initiate the process of obtaining the information. (…) However ultimately this issue has not been decided yet.' In deze zaak ging het precies over deze kwestie, of via een website ter beschikking gestelde informatie kan vallen onder het begrip duurzame drager.

---

1. Onder andere HvJ EU 16 oktober 2008 (Verbraucherzentrale Bundesverband/deutsche internet versicherung), C-298/07 (over noodzaak e-mail adres op website) AG,HvJ EU 3 september 2009 (Messner/Kruger), C-489/07 (over retourneren kapotte laptop), HvJ EU 15 april 2010 (Handelsgesellschaft Heinrich Heine/Verbraucherzentrale), C-511/08 (leveringskosten bij retourzending).
2. Zie o.a. A.R. Lodder (2007). Noot bij: Rb. Den Bosch. (30-11-2006), *Computerrecht* 2007-2, (DVD box). p.104-108.
3. Conclusie van Advocaat-Generaal P. Mengozzi van 6 maart 2012, Zaak C-49/11, onder 5.
4. J. Hörnle, G. Sutter & I. Walden (2002), Chapter 2 - Directive 97/7/EC on the protection of consumers in respect of distance contracts, in: A.R. Lodder & H.W.K. Kaspersen (eds.), *eDirectives: guide to European Union law on e-commerce. Commentary on the directives on distance selling, electronic signatures, electronic commerce, copyright in the information society, and data protection*, Kluwer Law International, p. 16.

9. De uitspraak geeft om te beginnen een mooi overzicht van de wijze waarop 'duurzame drager' in de verschillende richtlijnen is gedefinieerd. Het heeft iets weg van het bekende kinderspel 'Zoek de verschillen', want geen van onderstaande vier omschrijvingen is hetzelfde. In het voordeel van de EU wetgever kan worden toegevoegd dat sommige, maar lang niet alle, verschillen door schijnbaar verschillende visies van vertalers zijn ontstaan. Het blijft niettemin merkwaardig dat er zo slordig door de richtlijnen heen met eenzelfde begrip wordt omgegaan.
10. Art. 2, sub f Richtlijn 2002/65/EG inzake financiële dienstverlening op afstand: 'ieder hulpmiddel dat de consument in staat stelt om persoonlijk aan hem gerichte informatie op te slaan op een wijze die deze informatie toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de informatie kan dienen, en die een ongewijzigde reproductie van de opgeslagen informatie mogelijk maakt'.
11. Art. 2 onder 10 Richtlijn 2002/92/EG betreffende verzekeringsbemiddeling: 'elk hulpmiddel dat de klant in staat stelt aan hem persoonlijk gerichte informatie op zodanige wijze op te slaan dat hij deze gedurende een voor het doel van de informatie toereikende periode kan raadplegen en waarmee de opgeslagen informatie ongewijzigd kan worden gereproduceerd'.
12. Art. 3, sub m Richtlijn 2008/48/EG inzake kredietovereenkomsten: 'ieder hulpmiddel dat de consument in staat stelt persoonlijk aan hem gerichte informatie op te slaan op een wijze die deze informatie toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de informatie kan dienen, en die een ongewijzigde reproductie van de opgeslagen informatie mogelijk maakt'.
13. Art. 2 onder 10 Richtlijn 2011/83/EU inzake consumentenrechten: 'ieder hulpmiddel dat de consument of de handelaar in staat stelt om persoonlijk aan hem gerichte informatie op te slaan op een wijze die deze informatie toegankelijk maakt voor toekomstig gebruik gedurende een periode die is aangepast aan het doel waarvoor de informatie is bestemd, en die een ongewijzigde weergave van de opgeslagen informatie mogelijk maakt'.
14. In deze zaak gaat het primair om de duurzame drager. Daarnaast wordt ingegaan op het onderscheid tussen beschikken over informatie en het ontvangen van informatie. In Oostenrijk is in tegenstelling tot de meeste andere lidstaten voor de laatste variant gekozen, die een passieve houding van de consument verondersteld dan wel een actieve rol van de verkoper of dienstverlener. Na het plaatsen van informatie op een website zal eerder geconcludeerd worden dat de consument daarvoor beschikt dan dat deze ontvangen is (r.o. 35-37).
15. Van belang is dat informatie niet gewijzigd kan worden en gedurende een passende termijn toegankelijk is (r.o. 43). Hierbij wordt aansluiting gezocht bij de hierboven gegeven formulering uit de Consumentenrichtlijn 2011/83/EU. Mijns inziens zou de link in de aanvankelijke e-mail kunnen worden gezien als het ter beschikking stellen op een duurzame drager. Zo de consument dit zou willen wordt deze immers in staat gesteld deze informatie niet alleen te bekijken maar ook op te slaan en daarmee te 'verduurzamen'. Het is natuurlijk beter de informatie direct in de e-mail op te nemen en niet via een link. Bij latere raadpleging zou deze informatie immers gewijzigd kunnen zijn.
16. Wel onderschat in mijn ogen het hof de vaardigheden van de gemiddelde internetgebruiker (r.o. 46): 'Uit de stukken blijkt echter niet dat de website van de verkoper waarnaar de aan de consument getoonde link verwijst, *laatstgenoemde in staat stelt de aan hem persoonlijk gerichte informatie op zodanige wijze op te slaan dat hij er toegang toe heeft* en deze informatie ongewijzigd kan weergeven gedurende een passende termijn zonder enige mogelijkheid voor de verkoper de inhoud ervan eenzijdig te wijzigen.' Als de gebruiker de informatie bekijkt dan kan hij deze toch per definitie opslaan? Welke internetgebruiker kan niet een pagina opslaan? Het hof denkt hier dus blijkbaar anders over. Ik zie ook niet echt verschil met informatie op papier. Een brief kun je bekijken en bewaren of direct bij het oud papier leggen. Op internet is dit niet anders, behalve dat dan de default bij het oud papier leggen is. Voor de consument die wil bewaren is dit echter net zo eenvoudig mogelijk als het is om een papieren brief te bewaren.
17. Merkwaardig zijn r.o. 47-49 waarin door Content Services wordt aangevoerd dat er tegenwoordig websites zijn die onder uitsluitende controle van de consument staan en waarvan de inhoud niet gewijzigd kan worden. Ze voeren ter onderbouwing rapporten aan om te vervolgen met … dat ze zelf nog verouderde techniek gebruiken?!
18. Aardig is nog te vermelden dat de Oostenrijkse wettekst de volgende zinsnede kent: 'de termijn voor herroeping bedraagt zeven werkdagen. Zaterdag wordt niet als een werkdag beschouwd.' Mogelijk dat elders in de wet staat dat een werkweek zes dagen kent, want anders is onduidelijk waarom, zeker tegenwoordig, zondag niet ook genoemd wordt.
19. Al met al is dit een zaak die vragen oproept die niet beantwoord worden (de prejudiciële vraag is in dezen leidend), niet veel toevoegt aan de Richtlijn 2011/83/EU en blijk geeft van een ouderwetse kijk op de gemiddelde internetgebruiker.

De Anti-Wilders Hyve: een strafzaak over verantwoordelijkheid voor bedreigingen op internet

Martijn van Bemmel[*]

Annotatie bij Rechtbank Amsterdam 27 augustus 2012, *LJN* BX5755 (Anti-Wilders Hyve)

De rechtbank Amsterdam oordeelt over een strafzaak waarin bedreigingen op de sociaalnetwerksite Hyves centraal staan. Een 55-jarige man had op Hyves een groepspagina aangemaakt waarop derden bedreigingen hadden geplaatst aan het adres van Geert Wilders. De rechtbank spreekt de verdachte, die de groepspagina had aangemaakt, vrij van het medeplegen van en medeplichtigheid aan de bedreigingen.
Het is niet de eerste keer dat bedreigingen tegen Wilders het onderwerp zijn van een rechtszaak.[1] In deze zaak staat echter niet de bedreiger terecht, maar de beheerder van een internetpagina. Het vormt daarmee een interessant voorbeeld van verantwoordelijkheid voor andermans content op internet, die vergelijkingen oproept met de civielrechtelijke regeling voor aansprakelijkheid bij informatiediensten.[2]

Feiten

Hyves is een Nederlandse sociaalnetwerksite, vergelijkbaar met de Amerikaanse site Facebook. Op Hyves kunnen leden niet alleen een eigen profielpagina maken, ze kunnen ook groepen (zogenaamde 'Hyves') creëren. Andere leden kunnen vervolgens lid worden van de Hyve en hier berichten op plaatsen (het zogenaamde 'krabbelen' en vergelijkbaar met een 'wall post' op Facebook). De verdachte had een Hyve aangemaakt met de naam 'de Anti-Wilders Hyve'. Hij had echter de mogelijkheid tot 'krabbelen' uitgeschakeld, waardoor derden weliswaar lid konden worden van de Hyve, maar niet op de hoofdpagina berichten konden plaatsen. Bovendien had hij gedragsregels opgenomen waarin expliciet stond dat het verboden was op de Hyve Wilders te bedreigen. De verdachte had echter ook een logo (een foto) geplaatst op de Hyve en wanneer gebruikers daarop klikten konden zij op een aparte pagina opmerkingen plaatsen bij die foto. Diverse gebruikers hebben op deze onderliggende fotopagina bedreigingen richting Wilders geplaatst. Een aantal personen is hiervoor veroordeeld.[3]
De verdachte stelt dat hij niet wist dat er op de foto gereageerd kon worden en dat hij om die reden nooit op de onderliggende fotopagina heeft gekeken en de bedreigende teksten niet heeft verwijderd.

Vraag

De vraag is of verdachte verantwoordelijk moet worden gehouden voor de bedreigingen geuit door derden. Primair is tenlastegelegd het medeplegen van de bedreiging en subsidiair de medeplichtigheid aan de bedreigingen.

Juridisch kader

Het staat in deze zaak niet ter discussie dat er sprake is geweest van strafbare bedreigingen. Hiervoor is zoals aangegeven ook een aantal personen veroordeeld. Wil er echter sprake zijn van medeplegen of medeplichtigheid van de verdacht dan dient te worden voldaan aan de eisen van art. 47 respectievelijk 48 Sr.
Voor medeplegen gelden de volgende voorwaarden:[4]

- Bewuste samenwerking en gezamenlijke uitvoering;
- Dubbele opzet (op de samenwerking en op het uiteindelijke gevolg of de handeling); en
- Het delict zelf of een strafbare poging daartoe moet zijn gevolgd.

Voor medeplichtigheid gelden de volgende voorwaarden:[5]

- Er moet daadwerkelijk een bijdrage zijn verleend (voorafgaand of tijdens het misdrijf);
- Dubbele opzet (op zijn bijdrage en op het uiteindelijke gevolg of de handeling); en
- Het delict zelf of een strafbare poging daartoe moet zijn gevolgd.

De grens tussen medeplegen en medeplichtigheid is niet altijd duidelijk. Aan de hand van de mate van samenwerking

---

* Mr. M.A. van Bemmel is advocaat bij Kennedy Van der Laan te Amsterdam.

1. Zo moest de rapper Mohammad B. zich verantwoorden voor doodsbedreigingen tegen Wilders in zijn rapteksten. De zaak is door de Hoge Raad terugverwezen om opnieuw te worden behandeld (Hoge Raad 22 mei 2012, *LJN* BW6181). In een andere zaak werd de 15-jarige Giorgos N. veroordeeld nadat hij in een Hyves-bericht doodsbedreigingen had gestuurd aan Wilders (Hoge Raad 22 mei 2012, *LJN* BW6177).
2. Art. 6:196c BW.
3. Niet gepubliceerd, maar vermeld in persbericht Rechtbank Amsterdam, 'Vrijspraak voor oprichter anti-Wilders Hyve', 27 augustus 2012 (gepubliceerd op rechtspraak.nl).
4. Art. 47 Sr.
5. Art. 48 Sr.

bepaalt de rechter of er sprake is van medeplegen, dan wel medeplichtigheid.

De uitspraak

Volgens de rechtbank is zowel het medeplegen als de medeplichtigheid niet bewezen en dient verdachte te worden vrijgesproken.
De rechtbank is van oordeel (net als de verdachte én de Officier van Justitie) dat er geen sprake is van enige bewuste en nauwe samenwerking tussen verdachte en de personen die de bedreigingen op de Hyve hebben geplaatst. De verdachte is dus niet aan te merken als mededader (medeplegen).
Ook medeplichtigheid acht de rechtbank niet bewezen omdat niet wordt voldaan aan het vereiste van dubbele opzet. Het oprichten en beheren van de Hyve betekent namelijk niet dat de verdachte (voorwaardelijk) opzet had op de bedreigingen. De rechtbank oordeelt dat de Anti-Wilders Hyve niet bedoeld was als platform voor bedreigingen, zeker gezien de gedragsregels die de verdachte op de Hyve had gepubliceerd die bedreigingen uitdrukkelijk verboden.
De nalatigheid om de bedreigingen te verwijderen betekent ook niet dat verdachte (voorwaardelijk) opzet had op de bedreigingen. Volgens de rechtbank had verdachte weliswaar op de hoogte dienen te zijn van de bedreigingen, maar het niet verwijderen daarvan is onvoldoende om vast te stellen dat verdachte opzet had op het openbaar maken van de uiteindelijke bedreigingen; dit geldt te meer nu niet is komen vast te staan dat hij de bedreigingen daadwerkelijk heeft gezien.
Ondanks dat de verdachte door het oprichten en beheren van de Hyve en het nalaten om te verwijderen heeft bijgedragen aan de strafbare bedreigingen, is hij daarvoor dus niet strafrechtelijk medeverantwoordelijk.

Wél controleplicht?

Een interessante overweging van de rechtbank heeft betrekking op de rol van de verdachte als paginabeheerder:

> 'Als paginabeheerder had verdachte echter een verstrekkende verantwoordelijkheid om de volledige inhoud van die pagina voldoende grondig en frequent te controleren op ontoelaatbare en/of strafbare berichten. (…) 'Bij verdachte is veeleer sprake van schuld in de zin dat hij heeft tekortgeschoten in zijn taak als paginabeheerder om de inhoud van zijn pagina voldoende te controleren.'[6]

Volgens de strafrechter dient een paginabeheerder de content van derden grondig en frequent te controleren. De strafrechter lijkt daarmee te willen stimuleren dat beheerders van internetpagina's actief modereren en toezicht houden.
Een iets minder vergaand standpunt is eerder ingenomen in de strafzaak tegen een beheerder van het forum van de extreemrechtse partij de Nationale Alliantie. De strafrechter overwoog:

> 'Gelet op de inhoud van de teksten en de hoeveelheid daarvan wordt het geheel van teksten, in onderlinge samenhang bezien, door de rechtbank als discriminatoir, haatzaaiend en beledigend tegen Joden en Moslims aangemerkt. De verdachte heeft gefaciliteerd dat deze teksten openbaar werden gemaakt, nu hij de betreffende site als voorzitter van de Nationale Alliantie heeft opgezet, de rekeningen voor de instandhouding daarvan heeft betaald en heeft nagelaten deze teksten van het forum te verwijderen, hoewel hij daartoe uit hoofde van zijn bevoegdheden op het forum gehouden was in zijn functie als administrator/moderator.'[7]

De strafrechter veronderstelt een zorgplicht van de forumbeheerder voor de teksten op zijn forum. Dit is met name interessant wanneer gekeken wordt naar aansprakelijkheid in de civielrechtelijke context.
De civielrechtelijke aansprakelijkheid op internet is ingeperkt door art. 6:196c BW. Voor aanbieders van diensten van de informatiemaatschappij[8] geldt een Safe Harbour voor drie specifieke activiteiten: (i) voor mere conduit (waarbij de dienstverlener slechts als doorgeefluik van informatie fungeert, bijvoorbeeld door toegang te geven tot een communicatienetwerk); (ii) voor caching (waarbij de dienstverlener slechts informatie tijdelijk opslaat om latere doorgifte daarvan aan anderen doeltreffender te maken; (iii) voor hosting (waarbij de dienstverlener informatie van haar klant opslaat).
Er gelden diverse voorwaarden voor de vrijstelling van aansprakelijkheid. In hun functie als doorgeefluik (mere conduit) mag de dienstverlener bijvoorbeeld de informatie niet selecteren of wijzigen. Ook bij caching mag een dienstverlener de informatie niet wijzigen. Bij hosting geldt bijvoorbeeld dat een dienstverlener enkel in aanmerking komt voor de vrijstelling wanneer hij geen kennis heeft van de (onrechtmatige) informatie.
De voorwaarden van art. 6:196c BW leiden ertoe dat dienstverleners niet aansprakelijk zijn indien zij niet op de hoogte zijn van het onrechtmatige karakter van de content die derden plaatsen, mits wel wordt gehandeld om de content te verwijderen of ontoegankelijk te maken zodra het onrechtmatige karakter wel onmiskenbaar duidelijk is (*e.g.* in 'notice-and-takedowns' situaties). Dit is in lijn met art. 15 van de onderliggende E-Commerce Richtlijn: op grond van dat artikel legt een lidstaat op een internetprovider geen 'algemene verplichting op om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.'[9]
Onder het civielrecht is echter in een enkel geval ook een verplichting opgelegd aan een dienstverlener om zich actief te bemoeien met de inhoud van de content. Een voorbeeld van een dergelijke extra verplichting betreft een Nederlandse pedofielenwebsite. Deze site had een forum, waar leden berichten en afbeeldingen konden plaatsen. De rechter oordeelde dat de beheerder zich niet kon beroepen op art. 6:196c BW omdat zij actief selecteerde welke personen toegang kregen tot haar forum.[10] De beheerder is daarmee niet een passief opererende dienstverlener en de rechtbank leg-

6. R.o. 4.3.
7. Rechtbank Rotterdam 2 september 2009, *LJN* BH1711 (*Nationale Alliantie*), zie bewezenverklaring.
8. In de zin van art. 3:15d lid 3 BW.
9. Richtlijn 200/31/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* 2000 L 178/1.
10. De rechtbank oordeelde: 'Het beroep van gedaagde op het bepaalde in art. 6:196c BW gaat niet op. Zij is geen

de, mede gezien het bijzondere karakter van de website, een controleplicht op:

> 'Dit betekent dat op grond van het bijzondere karakter van de website van gedaagde zij bedacht moet zijn op, en beducht moet zijn voor misbruik en ook door haar ongewenst gebruik van haar website. Om die reden mag van gedaagde – anders dan wellicht van eigenaren of beheerders van websites die door hun aard niet op dergelijk misbruik en onbedoeld gebruik bedacht behoeven te zijn – worden verlangd dat zij bij het beheren van die website en van dat forum zodanige voorzieningen treft dat niet dankzij door haar geopende publicatiemogelijkheden personen, die de grenzen aan hun vrijheid van meningsuiting niet kennen, van die website gebruik kunnen maken om publicaties die inbreuken op de rechten van anderen opleveren te verspreiden.'[11]

Hiermee lijkt een civielrechtelijke controleplicht in uitzonderlijke gevallen toegepast te kunnen worden. Echter, auteursrechthebbenden en belangenorganisaties pleiten al lange tijd voor meer monitor- en filterverplichtingen om te voorkomen dat inbreukmakend materiaal verspreid wordt. Het is de vraag of dergelijke plichten de uitzondering blijven[12] of in de toekomst vaker worden opgelegd. Het Duitse Bundesgerichtshof lijkt in een recente zaak de mogelijkheid van controleplichten nadrukkelijk open te houden. Het betreft hier een zaak tussen Atari en RapidShare. De gamesfabrikant Atari heeft onder meer gevorderd dat RapidShare, een bestandenhoster, voorkomt dat het spel 'Alone in the Dark' door gebruikers wordt geupload en dat RapidShare de uploads vooraf filtert. Het Bundesgerichtshof heeft geoordeeld dat RapidShare het 'technisch en economisch redelijke' moet doen om te voorkomen dat gebruikers het spel op de servers van RapidShare aanbieden. Het Bundesgerichtshof merkt daarbij op dat RapidShare deze plicht mogelijk al geschonden heeft door geen (woord)filter in te voeren. De mededeling van de persdienst vermeldt:

> 'Vielmehr musste sie auch das technisch und wirtschaftlich Zumutbare tun, um - ohne Gefährdung ihres Geschäftsmodells - zu verhindern, dass das Spiel von anderen Nutzern erneut über ihre Server Dritten angeboten wurde. Diese Pflicht hat die Beklagte möglicherweise verletzt, weil sie keinen Wortfilter für den zusammenhängenden Begriff 'Alone in the Dark' zur Überprüfung der bei ihr gespeicherten Dateinamen eingesetzt hatte.'[13]

Er zou een tendens kunnen ontstaan waarbij civiele rechters eenzelfde weg in zullen slaan als de strafrechter in deze Anti-Wilders Hyve zaak heeft gedaan. Voor bijzondere websites (zoals een pedofielenforum) zijn zwaardere maatregelen snel voor te stellen, maar een algemene toename van controleplichten doet afbreuk aan de rol van tussenpersonen. Louter passief opererende tussenpersonen die geen enkele bemoeienis hebben met de inhoud van het materiaal worden dan geconfronteerd met aansprakelijkheden. Dit gaat mogelijk ten koste van rol die dergelijke dienstverleners spelen in de informatiemaatschappij en de diensten die zij aanbieden. Het is interessant om te zien of deze ontwikkeling zich in de nabije toekomst zal voortzetten.

internet dienstverlener die uitsluitend (technische) toegang verschaft tot een communicatienetwerk of behulpzaam is bij het tijdelijk, tussentijds geautomatiseerd opslaan van gegevens van een ander. Zij selecteert immers de personen die zij tot haar forum actief toegang verleent en plaatst dat forum in de context van haar eigen doelstellingen.' Rechtbank Amsterdam 1 november 2007, *LJN* BB6926.

11. Rechtbank Amsterdam 1 november 2007, *LJN* BB6926, zie beoordeling.
12. Het Hof van Justitie EU heeft meerdere malen monitor- dan wel filterverplichtingen van de hand gewezen. Zie bijvoorbeeld HvJ EU 24 november 2011, zaak C-70/10 (*Sabam/Scarlet*) en HvJ EU 16 februari 2012, zaak C-360/10 (*Sabam/Netlog*).
13. Bundesgerichtshof, Mitteilung der Pressestelle, 'Bundesgerichtshof zur Haftung von File-Hosting-Diensten für Urheberrechtsverletzungen', Nr. 114/2012, met betrekking tot de uitspraak van 12 juli 2012, I ZR 18/11. De uitspraak zelf is nog niet gepubliceerd.

Jurisprudentie

Onder redactie van M. van der Linden-Smith, met medewerking van C.C.M. de Raaij

161. Notariskamer Hof Amsterdam 15 mei 2012 (Notaris), *LJN* BX9030

Domeinnaam, e-mailadres, notaris, naar buiten optreden, verordening beroeps- en gedragsregels

Het gebruiken van een domeinnaam en een daaraan gekoppeld e-mailadres en de vermelding van een kantoornaam op het briefpapier moeten worden beschouwd als naar buiten optreden in de zin van art. 24 van de Verordening beroeps- en gedragsregels. De omstandigheid dat van die uitingen veelal eerst wordt kennisgenomen als het contact het notariskantoor reeds is gelegd, kan hieraan niet afdoen, omdat het bij 'naar buiten optreden' gaat om alle uitlatingen gedaan jegens derden.
Het gebruik van het litigieuze woord in de domeinnaam en het daarbij behorende e-mailadres bij het publiek de - onjuiste - indruk wekt dat appellant de enige notaris in de betreffende plaats is. Door dat gebruik presenteert appellant zijn kantoor derhalve niet juist, hetgeen in strijd is met art. 24 van de Verordening. Het beroep op de marktwerking en het recht te concurreren kan aan die strijdigheid niet afdoen, omdat het recht te concurreren niet mede het recht omvat het publiek ten koste van de concurrent een onjuiste voorstelling van zaken te geven.

162. Sector kanton rechtbank Arnhem 4 juni 2012 (Reflectie), *LJN* BW7967

Auteursrecht, artikel op internet, breder publiek, persoonlijkheidsrecht

Gedaagde heeft zonder toestemming van eiser een groot aantal gedeelten uit het artikel overgenomen, deze gedeelten heeft gedaagde gewijzigd, verbonden en aangevuld met teksten van eigen hand, terwijl gedaagde het geheel de vorm van een nieuw werk heeft gegeven. Door de bronvermelding onder het artikel heeft gedaagde de inhoud van het artikel vervolgens ten onrechte aan eiser toegeschreven. Dat het blad Reflectie, waarin het gewijzigde artikel gepubliceerd is, alleen bestemd is voor IT-ers doet aan de stelling van eiser nie af, nu het artikel ook op internet beschikbaar is geweest voor een breder publiek.

163. Sector kanton rechtbank 's-Hertogenbosch 7 juni 2012 (levering computerprogramma), *LJN* BW8396

Auteursrecht, nieuwsbrief, levering software, akte, art. 2 Aw

Naar het oordeel van de kantonrechter is eiser er niet in geslaagd te bewijzen dat het TMS–programma aan gedaagde is geleverd. Op grond van art. 2 Auteurswet juncto art. 3:96 BW dienen zaken als de onderhavige te worden geleverd door een daartoe bestemde akte. De enkele vermelding van de wijze waarop een computerprogramma kan worden geïnstalleerd in een nieuwsbrief kan niet worden gekwalificeerd als een leveringsakte.

164. Sector kanton rechtbank Middelburg 11 juni 2012 (foto van eigen medewerkers), *LJN* BX4106

Auteursrecht, foto op website, hoogte schadevergoeding

Door publicatie zonder toestemming op de website van gedaagde heeft eiser schade geleden. Voor begroting van de schade zal de kantonrechter aansluiting zoeken bij de doorgaans gehanteerde tarieven, maar deze zijn niet leidend. Er zijn immers geen tarieven overeengekomen.
Hierbij acht de kantonrechter van belang dat er geen sprake is van recent werk. Niet in geschil is dat de foto dateert uit 2002. Aangenomen mag worden dat de foto inmiddels opbrengst heeft kunnen opleveren voor eiser en dat de opbrengst van toekomstig gebruik beperkt zal zijn. Bovendien gaat het hierbij om een foto van (medewerkers van) gedaagde zelf op een werk van gedaagde. De kantonrechter acht, mede in aanmerking genomen het door een aantal fotografen gehanteerde tarief voor publicatie op internet, een vergoeding van € 250 in dit geval redelijk.
Eiser heeft daarnaast voldoende onderbouwd dat door inbreuk op zijn auteursrecht hem de mogelijkheid is ontnomen om vooraf over de exploitatie van zijn werk te onderhandelen. Voorts heeft hij tijd en kosten moeten maken om staking van de inbreuk en betaling van een vergoeding te bewerkstelligen. Deze schade, als door eiser gesteld en voldoende aannemelijk gemaakt, kan niet inbegrepen worden geacht in de vergoeding die hem ook zonder inbreuk zou zijn toegekomen. De kantonrechter acht in dit geval eenzelfde vergoeding gerechtvaardigd zoals de hiervoor naar redelijkheid vastgestelde gederfde licentievergoeding voor het plaatsen van de foto, derhalve eveneens € 250.

165. Rechtbank 's-Gravenhage 12 juni 2012 (modder gooien via FB), *LJN* BW8727

Personen- en familierecht, Facebook, communicatie, belang van minderjarige

Geschil over onder meer gezamenlijk gezag van gescheiden ouders. De rechtbank verwerpt het verweer van de man dat overgelegde prints van Facebook en andere zogenoemde sociale media geen (juridische) waarde zouden hebben omdat zij alleen zijn overgelegd als stemmingmakerij. De Facebook-berichten zijn naar het oordeel van de rechtbank duidelijk gericht op de Facebook-vrienden van de man en hebben ten aanzien van de vrouw als moeder een negatieve lading. De rechtbank acht het ook in de richting van de vrouw als andere ouder zonder meer ongepast om een - nota bene door de rechtbank gestempelde - leesbare foto van een processtuk (in dit geval: de eerste pagina van het inleidende verzoekschrift met de naam en voornamen van de vrouw) op Facebook te plaatsen met daarbij

het onderschrift: 'Daar is ie dan toch de brief van de rechtbank via de tegenpartij zijnde de moeder van mijn (ons) kind.' De man geeft zich naar het oordeel van de rechtbank met dergelijke berichten, die voor de Facebook-vrienden van de man openbaar zijn en bovendien doorgezonden kunnen worden aan anderen ('vrienden' van 'vrienden') onvoldoende rekenschap van de eisen die gezamenlijk ouderschap en de belangen van de minderjarige met zich meebrengen.
De rechtbank benadrukt dat het in het belang van de minderjarige moet worden geacht dat beide partijen eerst hulp zoeken om beter te gaan communiceren, het vertrouwen in elkaar te herstellen en te stoppen met het 'modder gooien'. Eerst dan, wanneer de ouders elkaar niet meer beschouwen als ex-partners, maar als ouders van de minderjarige, kan er na verloop van tijd een situatie ontstaan waarin van een gezamenlijke gezagsuitoefening sprake kan zijn zonder dat de minderjarige klem of verloren dreigt te raken.
Verzoek van de man om hem gezamenlijk met het gezag te belasten afgewezen.

166. Rechtbank Rotterdam 20 juni 2012 ('onbeperkt' breedband internet), *LJN* BX4167

Verbintenissenrecht, mobiel internet, datalimiet

Rechtsvraag: had gedaagde, gelet op de reclame-uitingen van Telfort, erop bedacht moeten zijn dat er aan het product 'Maximaal online' een datalimiet was verbonden en dat zij bij overschrijding van deze limiet extra kosten voor internet verschuldigd zou zijn? Rechtbank: nee. Blijkens de door gedaagde in het geding gebrachte stukken heeft Telfort op haar website bij de omschrijving van het abonnement 'maximaal online' vermeld dat 'onbeperkt' breedband internet deel uitmaakt van het abonnement. Voorts is van betekenis, dat niet in het contract of in de algemene voorwaarden staat vermeld dat sprake is van een datalimiet, maar dat dit alleen wordt genoemd in een aparte tarievenlijst die als bijlage bij de algemene voorwaarden is gevoegd.
De stelling van Telfort dat bij de omschrijving van het abonnement het woord 'onbeperkt' tussen aanhalingstekens staat en daaruit volgt dat dit woord niet onbeperkt in de absolute zin van het woord betekent, wordt verworpen. De rechtbank is van oordeel dat gedaagde hieruit niet heeft kunnen afleiden dat mogelijk sprake zou zijn van een verbruikslimiet. Wanneer in reclame-uitingen sprake is van een abonnement met een onbeperkte limiet voor het gebruik dient de verkoper van het abonnement zich daar aan te houden, tenzij zij op een duidelijke wijze kenbaar maakt dat er toch van een limiet sprake is. Door alleen in een bijlage bij de algemene voorwaarden de limiet op te nemen, heeft Telfort het moeilijk gemaakt om kennis te nemen van deze, toch essentiële, beperking van het abonnement. In relatie tot de ondubbelzinnige reclame-uiting die op het tegendeel wijst, heeft Telfort niet, althans onvoldoende, voldaan aan de plicht om de koper op een duidelijke wijze over de beperkingen van het abonnement te informeren.

167. Hof van Justitie EU 5 juli 2012 (Content Services), zaak C-49/11

E-commerce, algemene voorwaarden, hyperlink, vertrekking, website, duurzame drager, art. 5 Richtlijn verkoop op afstand

Art. 5, lid 1, van richtlijn 97/7/EG van het Europees Parlement en de Raad van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten moet aldus worden uitgelegd dat een handelspraktijk die erin bestaat de in deze bepaling bedoelde informatie voor de consument enkel toegankelijk te maken via een hyperlink op een website van de betrokken onderneming, niet aan de vereisten van deze bepaling voldoet, aangezien deze informatie niet door deze onderneming wordt „verstrekt' en evenmin door de consument wordt „ontvangen' in de zin van deze bepaling, en dat een website als aan de orde in het hoofdgeding niet als een 'duurzame drager' in de zin van dit art. 5, lid 1, kan worden beschouwd.

168. Rechtbank Utrecht 6 juli 2012 (stalking door exman), *LJN* BX1227

Strafrecht, belaging, stalking, email, Facebook, Hyves, contactverbod, art. 285b Sr

Verdachte heeft zich schuldig gemaakt aan stalking van zijn ex-echtgenote, zijn twee zoons en de nieuwe partner van zijn ex-echtgenote. Daartoe stuurde hij hen gedurende een periode van een aantal jaren veelvuldig met wisselende frequentie e-mailberichten met grievende, beledigende, dreigende en intimiderende teksten. Verdachte heeft daarmee stelselmatig inbreuk gemaakt op de persoonlijke levenssfeer van deze personen.
Volgt veroordeling tot 4 maanden voorwaardelijke gevangenisstraf, met contactverbod als bijzondere voorwaarde.

169. Rechtbank 's-Gravenhage 11 juli 2012 (ex parte TPB), IT828

Auteursrecht, TPB, The Pirate Bay, reverse proxy, tussenpersoon

Het is voldoende aannemelijk gemaakt dat gerekwestreerde is te beschouwen als tussenpersoon wiens diensten worden gebruikt voor inbreuken op auteursrechten en naburige rechten. Gerekwestreerde verleent derden namelijk een dienst (aanbod van een reverse proxy) die deze derden gebruiken om via de website The Pirate Bay auteursrechtelijk beschermde werken te uploaden. Gezien het vonnis van 11 januari 2012 (LJN BV0549) bestaat voldoende duidelijkheid met betrekking tot het inbreukmakende handelen van deze derden en de juridische mogelijkheid in een geval als dit aan de tussenpersoon een bevel tot staking van de dienstverlening te geven.

170. Rechtbank 's-Gravenhage 11 juli 2012 (Forum Tros-Pretium), *LJN* BX1975

Onrechtmatige uiting, forum, forumbeheer, notice-and-take-down verzoek, gedragsregels

Voor zover voor internetrecht van belang: De rechtbank stelt voorop dat het openstellen van een internetforum waarop berichten kunnen worden geplaatst over Pretium Telecom, op zichzelf niet als onrechtmatig is aan te merken. Bij de vraag of een onrechtmatige inhoud van postings op het forum aan de Tros kan worden toegerekend, is van belang of de Tros actief postings selecteert, redigeert of voor publicatie beoordeelt, dan wel enkel achteraf, al dan niet op verzoek van bezoekers of derden, de rechtmatigheid daarvan controleert. In het onderhavige geval is er sprake van de laatstgenoemde situatie. In dat geval kan het handelen van de Tros onrechtmatig zijn, wanneer zij nalaat op eerste verzoek van Pretium Telecom binnen redelijke termijn postings te verwijderen die een jegens Pretium Telecom evident onrechtmatige inhoud hebben. Dat impliceert ook dat postings die Pretium Telecom onwelgevallig zijn maar de grens van de maatschappelijke zorgvuldigheid niet overschrijden, door de Tros niet verwijderd hoeven te worden.
Niet is komen vast te staan dat de Tros aan voldoende concrete en gerechtvaardigde verzoeken tot verwijdering van Pretium Telecom geen gevolg geeft of heeft gegeven.
Of de Tros zou handelen in strijd met de door haar zelf gestelde gedragsregels voor gebruikers van het forum kan in het midden blijven. De Tros heeft met recht naar voren gebracht dat een derde zoals Pretium Telecom niet (rechtstreeks) enig recht aan die gedragsregels kan ontlenen in haar relatie met de Tros, omdat door de Tros met deze regels is beoogd een ordentelijk verloop op het forum te bewerkstelligen.

171. Rechtbank Breda 17 juli 2012 (jonge tienermeisjes), *LJN* BX1668

Strafrecht, grooming, webcam, kinderporno, art. 240b Sr, art. 246 Sr, art. 248a Sr

Verdachte heeft onder meer via een website, waarin fotomodellen zich aanbieden, contact gezocht met jonge tienermeisjes. Ter zitting heeft hij verklaard dat hij zo probeerde om die meisjes uit de kleren te praten en seksuele handelingen met zichzelf te laten verrichten. Van een aantal van die contacten heeft verdachte middels een webcam van die meisjes opnamen gemaakt en opgeslagen op zijn laptop. In twee gevallen heeft verdachte gedreigd de opnamen op internet te plaatsen. In een aantal andere gevallen heeft hij de meisjes geld geboden of modellenopdrachten in het vooruitzicht gesteld.
Verdachte heeft zich hierdoor schuldig gemaakt aan het vervaardigen van kinderporno en aanzetten van (jonge) meisjes tot het plegen van seksuele handelingen voor een webcam. Verdachte heeft weliswaar verklaard dat hij de opnamen van de seksuele handelingen niet op internet heeft geplaatst, echter bij de meisjes zal altijd de vrees blijven bestaan dat de gemaakte opnamen toch nog een keer op internet zullen verschijnen.
Volgt veroordeling tot 30 maanden gevangenisstraf, waarvan 10 maanden voorwaardelijk.

172. Rechtbank Arnhem 18 juli 2012 (fietsporno), *LJN* BX3401

Onrechtmatige daad, domeinnaam, redirect, dwarszitten concurrent, pesterij

Gedaagde-fietsenzaak heeft domeinnaam geregistreerd die vrijwel identiek is aan die van eiser-fietsenzaak, en die leidt naar een porno-website.
Gedaagde voert aan dat zij om haar moverende redenen de domeinnaam geregistreerd heeft. Ter comparitie heeft gedaagde uitgelegd dat hij de concurrentie van eiser vreest en de domeinnaam geregistreerd heeft om die aan eiser te kunnen verkopen 'als er rare dingen zouden gebeuren'. De rechtbank vermag niet in te zien wat gedaagde hiermee bedoelt.
Nu gedaagde zich niet uitlaat over een valide reden voor deze registratie van de naam die evident gekoppeld is aan haar concurrent eiser, is de rechtbank van oordeel dat er geen andere reden geweest kan zijn dan het dwarszitten van haar concurrent. Dit dwarszitten kan gelet op de concurrentiestrijd tussen partijen gericht zijn geweest op misleiding van klanten en potentiële klanten van eiser.
Voor de link naar de pornosite geeft gedaagde geen verklaring. Er kan een hacker aan het werk zijn geweest, stelt zij. Het evidente bestaan van een concurrentiestrijd tussen partijen leidt tot het vermoeden dat gedaagde zelf achter de link zit. Daarbij komt dat zij zelf verantwoordelijk is voor het gebruik van de door haar geregistreerde domeinnaam. Het voorgaande betekent naar het oordeel van de rechtbank dat vaststaat dat er sprake is van pesterij van haar concurrent door gedaagde. Zulke pesterij, uitgevoerd in het kader van een concurrentiestrijd, kan de goede naam van eiser schaden. Daarom acht de rechtbank deze pesterij onrechtmatig.

173. Rechtbank Breda 24 juli 2012 (Zembla), *LJN* BX2328

Strafrecht, smaad, laster, televisieprogramma op internet, voortdurend delict

Voor zover voor internetrecht van belang: De officier van justitie heeft betoogd dat verdachte, door in het programma Zembla de genoemde beschuldigingen te uiten, terwijl zij wist dat slachtoffer voor die feiten integraal was vrijgesproken, zich heeft schuldig gemaakt aan een voortdurend delict. De uitzending van Zembla is immers tot op de dag van vandaag via internet te bekijken.
De rechtbank volgt hem daarin niet. De uitlatingen van verdachte in het televisieprogramma Zembla betreffen immers één en dezelfde gedraging, te weten de uitlatingen voor de camera tijdens het interview ten behoeve van dit programma. Als verdachte al had kunnen voorzien dat deze Zembla-uitzending later via internet alsnog te bekijken zou kunnen zijn, dan kan zij in het onderhavige geval niet verantwoordelijk worden gehouden voor de beslissing van de VARA om de inhoud van het programma op internet te plaatsen.

174. Rechtbank Middelburg 26 juli 2012 (dreigrap Wilders), *LJN* BX2749

Strafrecht, bedreiging, YouTube, videoclip, openbaar toegankelijk en veel bekeken medium, art. 285 Sr

De teksten die de rechtbank op de videoclip heeft gehoord, de daarbij getoonde beelden en de overige geluidsfragmenten verwijzen ondubbelzinnig naar de dood van aangever. De rechtbank acht de inhoud van de videoclip van dien aard dat daardoor bij aangever de redelijke vrees kon ontstaan dat hij het leven zou verliezen. Blijkens de aangifte is aangever op de hoogte geraakt van de videoclip en voelde hij zich hierdoor ook daadwerkelijk bedreigd.
Voor zover de verdediging met verwijzing naar YouTube en muzikale expressie heeft bedoeld zich te beroepen op de ontzenuwende rol van de context, verwerpt de rechtbank dat verweer. De aard en inhoud van de videoclip die op een openbaar toegankelijk en veel bekeken medium is geplaatst en die uitsluitend en individueel gericht is tegen aangever, een lid van de Tweede Kamer van wie algemeen bekend is dat hij vaker wordt bedreigd en derhalve streng beveiligd wordt, is van dien aard dat veeleer gesproken kan worden van een de bedreiging versterkende dan van een ontzenuwende context.
Volgt veroordeling tot 2 maanden voorwaardelijke gevangenisstraf en een werkstraf van 50 uur.

175. Hof 's-Gravenhage 31 juli 2012 (imam in Fitna), *LJN* BX2991

Onrechtmatige uiting, Fitna, bedreiging via internet, portretrecht, vrijheid van meningsuiting, eer en goede naam, publiek debat, art. 8 EVRM, art. 10 EVRM

Appellant is imam. Een fragment van een Netwerk-interview met hem is in Fitna opgenomen.
Appellant heeft niet (duidelijk) aangevoerd dat de passages die aan het fragment van zijn Netwerk-interview voorafgaan, een voor zijn goede naam schadelijke context opleveren.
De enkele en niet nader uitgewerkte stelling van appellant dat 'als gevolg van zijn negatieve aanwezigheid in de film, hij op het internet met grote regelmaat is bedreigd, die het daglicht niet kunnen dragen' is onvoldoende om te kunnen aannemen dat hij door het gebruik van zijn beeltenis en uitlatingen in Fitna daadwerkelijk voldoende ernstig nadeel heeft ondervonden. Bij gebreke aan concrete informatie over de aard en inhoud van de gestelde bedreigingen kan de ernst daarvan niet worden vastgesteld.
Nu appellant zich zelf met controversiële uitspraken in het publieke debat heeft begeven is zijn belang op zichzelf beschouwd van onvoldoende gewicht om Stichting PVV het haar door art. 10 lid 1 EVRM gewaarborgde recht te ontzeggen om één van die controversiële uitspraken te gebruiken in haar bijdrage aan het publieke debat. In aanmerking nemende dat dit niet is gedaan in een voor appellant schadelijke context, appellant niet voldoende heeft onderbouwd dat hij daarvan anderszins nadelige gevolgen van voldoende betekenis heeft ondervonden en zijn strikte privésfeer daardoor niet is getroffen, moet appellant zich dat laten welgevallen.

176. Rechtbank 's-Hertogenbosch 1 augustus 2012 (Nexpak), *LJN* BX3380

IPR, bevoegdheid Nederlandse rechter, algemene voorwaarden, Weens koopverdrag, verwijzing naar algemene voorwaarden op website, niet digitaal tot stand gekomen overeenkomst

De rechtbank oordeelt dat uit het systeem van het Weens Koopverdrag volgt dat de wederpartij van de gebruiker van algemene voorwaarden de mogelijkheid moet hebben op passende wijze van de algemene voorwaarden kennis te nemen en dat het aan de gebruiker van de algemene voorwaarden is om de algemene voorwaarden aan de wederpartij toe te zenden of anderszins toegankelijk te maken. Aan dit vereiste is niet voldaan met de mededeling op orderbevestigingen dat de algemene voorwaarden zijn gedeponeerd bij de Kamer van Koophandel en dat deze op verzoek zullen worden toegezonden. Of de wederpartij op passende wijze van de algemene voorwaarden heeft kunnen kennis nemen door een verwijzing op een orderbevestiging naar een website waar de algemene voorwaarden kunnen worden geraadpleegd of gedownload, hangt naar het oordeel van de rechtbank af van een aantal omstandigheden, waaronder met name de wijze van totstandkoming van de overeenkomst (schriftelijk, digitaal of anderszins). Indien de overeenkomst niet digitaal is tot stand gekomen, mag de gebruiker van algemene voorwaarden er niet zonder meer van uitgaan dat de wederpartij op eenvoudige wijze toegang heeft tot het internet en tot de website van de gebruiker, te minder indien de wederpartij is gevestigd in een land waarin internetgebruik nog minder gangbaar is. De wederpartij mag verwachten dat de algemene voorwaarden op de website van de gebruiker in een voor hem begrijpelijke taal, te weten zijn eigen taal of de taal waarin partijen met elkaar hebben gecorrespondeerd, duidelijk en zonder omwegen worden aangeboden.

177. Rechtbank Arnhem 2 augustus 2012 (Fietsplus), *LJN* BX3401

Domeinnaam, handelsnaam, onrechtmatig, schadevergoeding

Concurrent van fietshandelaar X registreert een vergelijkbare domeinnaam als de domeinnaam van de website van de fietshandelaar. Deze vergelijkbare domeinnaam is doorgelinkt naar een pornosite. De rechter oordeelt dat het evidente bestaan van een concurrentiestrijd tussen partijen leidt tot het vermoeden dat er sprake is van een pesterij. Het is onvoldoende aannemelijk gemaakt dat er sprake is van inbreuk op de handelsnaam of enig aan fietshandelaar X toebehorend merk. Wel oordeelt de rechter dat het registreren van de domeinnaam, welke dusdanig vergelijkbaar is met de door fietshandelaar X geregistreerde domeinnaam, onrechtmatig is. Ook het doorlinken van de domeinnaam naar pornografische content acht de rechter onrechtmatig. De vordering tot schadevergoeding wordt afgewezen nu geen vorm van schade is gebleken.

178. Voorzieningenrechter Haarlem 2 augustus 2012 (foute advocaten), *LJN* BX9028

Onrechtmatige uiting, klaagsite, domeinnaam, wederhoor, maatschappelijk belang, zoekmachine, zoekresultaten

De uitlatingen op de website moeten, gelet op de gebezigde kwalificaties als 'intimiderend, sluw, eigenbelang prevaleert, onbetrouwbaar, leugenaar, graaier, fantast' zonder meer als zeer negatief en diffamerend worden aangemerkt. Daar komt bij dat, gelet op de domeinnaam 'fouteadvocaten', aannemelijk is dat de website uitsluitend is bedoeld om negatieve kritiek op advocaten te publiceren. Van die kritiek wordt geen enkele feitelijke onderbouwing gegeven en daar wordt van de kant van de website ook niet om gevraagd. Lezers worden min of meer aangemoedigd om termen als 'achterbaks, laks, onkundig, liegt, bedriegt' en dergelijke te gebruiken. De uitlatingen worden geplaatst zonder dat wederhoor wordt toegepast. Degenen op wie de uitlatingen betrekking hebben hebben ook achteraf niet de mogelijkheid om hun zienswijze kenbaar te maken. Voor zover met de website wordt beoogd een maatschappelijk belang te dienen - bijvoorbeeld om misstanden in de advocatuur aan de kaak te stellen en het publiek daarover te informeren- valt niet in te zien dat dat belang met deze werkwijze gediend kan zijn. Dus: onrechtmatige uitlatingen.
De zeer kwetsende aard van de uitlatingen rechtvaardigen een veroordeling van gedaagde om de gehele website en de inhoud ervan van het internet te doen verwijderen, evenals een machtiging om dat zelf te bewerkstelligen indien gedaagde daarmee in gebreke blijft.
De aard van de uitlatingen rechtvaardigt ook dat gedaagde wordt veroordeeld om te bewerkstelligen dat alle zoekresultaten van het internet worden verwijderd waarin melding wordt gemaakt van de website. De vrees voor is herhaling reëel: verbod om een website op te richten of te publiceren met een soortgelijke domeinnaam of met een soortgelijke inhoud, als die van www.fouteadvocaten.org.

179. Hof 's-Gravenhage 3 augustus 2012 (gewoontebelediging), *LJN* BX3873

Strafvordering, MDI, Meldpunt Discriminatie Internet, buiten heterdaad, onrechtmatige inbeslagname, art. 137c lid 2 Sr, art. 137d lid 2 Sr, art. 137e lid 2 Sr

Naar het oordeel van het hof bieden de ten tijde van de aanhouding van de verdachte en de inbeslagname van diens computers beschikbare gegevens, te weten de aangifte van het MDI en de resultaten van het onderzoek van het KLPD, onvoldoende grondslag voor een verdenking van overtreding van het tweede lid van art. 137c, 137d dan wel 137e van het Wetboek van Strafrecht. Pas bij onderzoek van de gegevens op de computer is duidelijkheid verkregen over de omvang van de bestanden.
De ten tijde van de aanhouding en inbeslagname beschikbare gegevens bieden naar 's hofs oordeel wel voldoende grondslag voor een verdenking van overtreding van het eerste lid van art. 137c, 137d dan wel 137e van het Wetboek van Strafrecht.
Nu op grond van laatstgenoemde artikelen geen bevel tot voorlopige hechtenis kan worden gegeven, stelt het hof vast dat de wettelijke grondslag voor de aanhouding buiten heterdaad van de verdachte en de inbeslagname van diens computers ontbrak.
Het hof is dan ook van oordeel dat de aanhouding van de verdachte en de inbeslagname van diens computers onrechtmatig zijn. Naar het oordeel van het hof doet zich aldus de situatie voor dat belangrijke strafvorderlijke voorschriften in aanzienlijke mate zijn geschonden. Het gevolg hiervan is dat niet kan worden volstaan met de constatering van die schending of verdiscontering daarvan in de strafmaat maar dat de resultaten van de onrechtmatige bewijsvergaring van het bewijs dienen te worden uitgesloten. Volgt vrijspraak.

180. Voorzieningenrechter Alkmaar 8 augustus 2012 (Rots-Vast), *LJN* BX 3995

Merkenrecht, handelsnaam, proceskostenvergoeding, verwarringsgevaar, verwatering, art. 1019h Rv, art. 2.20 BVIE, art. 5 jo 5a Handelsnaamwet

Inbreuk op merk en handelsnaam door gebruik te maken van een teken dat op verwarrende wijze overeenstemt met het geregistreerde merk van eiseres voor dezelfde diensten. De rechter is van mening dat er sprake is van visuele, auditieve en begripsmatige overeenstemming uitgaande van de totaalindruk. Daarbij moet meer gewicht worden toegedicht aan de overeenkomsten dan aan de verschillen. Risico voor verwarringsgevaar is aannemelijk nu de verschillen gering zijn en partijen hun handelspraktijk in dezelfde regio uitoefenen. Ook met betrekking tot de handelsnaam oordeelt de rechter dat bij het publiek verwarring kan ontstaan tussen de ondernemingen. Door de naam ook te gebruiken in de domeinnaam (namelijk www.rotsidbvastgoed.nl) maakt gedaagde ook hier inbreuk op de handelsnaam. Weliswaar is een domeinnaam in beginsel niet meer dan een adres van de domeinnaamhouder, maar gedaagde gebruikt haar domeinnaam ook als handelsnaam voor haar kamerverhuuractiviteiten. Door op deze wijze gebruik te maken van haar domeinnaam maakt gedaagde eveneens inbreuk op de handelsnaam van de Rots-Vast Groep.

181. Raad van State 8 augustus 2012 (Irakees op YouTube), *LJN* BX4824

Vreemdelingenrecht, filmpje op internet, internet-surveillance

Voor zover voor internetrecht van belang: Uit het arrest van het EHRM van 15 mei 2012 in zaak nr. 52077/10, S.F. en anderen tegen Zweden (www.echr.coe.int/echr), blijkt dat Iraanse autoriteiten communicatie via het internet en critici van het regime in de gaten houden, zowel binnen als buiten Iran. Ook blijkt uit dit arrest dat Iraniërs die terugkeren naar Iran bij aankomst worden onderzocht.
De vreemdeling heeft deelgenomen aan een demonstratie voor de Iraanse ambassade te Den Haag op de herdenkingsdag van de overwinning van de islamitische revolutie op het bewind van de Sjah. De vreemdeling heeft in deze demonstratie geen bijzondere rol gehad. Zijn deelname aan deze demonstratie heeft voorts geen speciale aandacht ge-

kregen in de media. Weliswaar is de vreemdeling en profil te zien op een filmpje op internet, maar daarbij zijn zijn personalia niet vermeld. De rechtbank heeft voorts overwogen dat de minister zich in redelijkheid op het standpunt heeft kunnen stellen dat het asielrelaas van de vreemdeling ongeloofwaardig is. Ook overigens heeft de minister in hetgeen door de vreemdeling naar voren heeft gebracht terecht geen grond gezien voor het oordeel dat aannemelijk is dat de vreemdeling in de gaten wordt gehouden door de Iraanse autoriteiten dan wel bij terugkeer naar Iran zal worden onderzocht.
De minister heeft zich terecht op het standpunt gesteld dat de vreemdeling niet aannemelijk heeft gemaakt dat hij bij uitzetting naar Iran een reëel risico loopt op een met art. 3 van het EVRM strijdige behandeling.

182. Sector kanton rechtbank Rotterdam 10 augustus 2012 (geparkeerde vrachtwagens), Boek9 11563

Auteursrecht, foto op website, koppeling, link, hyperlink hoogte schadevergoeding

Gedaagde heeft in het nieuwsoverzicht op haar website een koppeling met een nieuw bericht van de Telegraaf tot stand gebracht, waardoor een foto waar eiser het auteursrecht op heeft, automatisch is meegekoppeld: inbreuk op auteursrecht. Eiser heeft als schadevergoeding, onder verwijzing naar de algemene voorwaarden van de Fotografenfederatie, driemaal de licentievergoeding gevorderd. Die algemene voorwaarden zijn weliswaar niet van toepassing op de (niet contractuele) relatie tussen eiser en gedaagde, maar vormen wel een rechtens aanvaardbaar en geaccepteerd uitgangspunt om op die basis de schade te begroten.
Het moet niet aantrekkelijk gemaakt worden voor gebruikers van auteursrechtelijk beschermd werk om een inbreuk te herstellen door achteraf alsnog te betalen en dan niet slechter af te zijn dan als zij tevoren toestemming zouden hebben gevraagd. Een dergelijk gebruik van zijn werk levert de auteursrechthebbende immers ook schade op. De gevorderde € 765 aan schadevergoeding wordt toegewezen.

183. Rechtbank Amsterdam 15 augustus 2012 (rauwe bewoordingen), *LJN* BX5688

Strafrecht, Facebook, bedreiging, redelijke vrees, kring van geadresseerden, vrienden op Facebook, art. 285 Sr

Voor het bewezen verklaren van een bedreiging in de zin van art. 285 van het Wetboek van Strafrecht is vereist dat de bedreigde daadwerkelijk op de hoogte moet zijn geraakt van de bedreiging en dat de bedreiging van dien aard dient te zijn en onder zodanige omstandigheden moet zijn geschied dat bij de bedreigde de redelijke vrees kon ontstaan dat het misdrijf waarmee werd gedreigd, daadwerkelijk zou worden uitgevoerd.
Verdachte heeft de teksten zoals omschreven in de tenlastelegging op zijn profielpagina op facebook geplaatst. Die pagina is toegankelijk voor een beperkte, door verdachte zelf geselecteerde groep mensen. Daarnaast heeft hij de teksten in algemene bewoordingen gesteld, die bovendien, zoals verdachte heeft verklaard, voor een deel aan teksten van bekende rappers zijn ontleend of daarvan zelfs letterlijk zijn geciteerd. Er valt geen geadresseerde aan te wijzen. De onbekend gebleven vrouw die zich bij het politiebureau meldde, heeft verklaard dat zij bang werd van de dingen die verdachte opschreef en dat zij hoopte dat de politie daarmee iets zou doen, omdat het erop leek dat verdachte helemaal de weg kwijt was. Zij maakte zich zorgen over de berichten en over verdachte, maar niet over eventuele gevolgen voor haarzelf.
Uit deze verklaring van de onbekende vrouw kan dus niet worden afgeleid dat zij – of iemand anders – als bedreigde van de teksten op de hoogte is geraakt. Tot slot blijkt uit het dossier niet dat verdachte de intentie heeft gehad iemand met het plaatsen van de teksten te bedreigen. Gelet op de kring van geadresseerden mag worden aangenomen dat de lezers van de teksten begrepen dat verdachte daarmee op een voor hem eigen wijze teksten van rappers wilde citeren en parafraseren. Daaraan doet niet af dat het om voor een gemiddeld publiek rauwe bewoordingen gaat. Volgt vrijspraak.

184. Sector kanton rechtbank Amsterdam 17 augustus 2012 (DWI), LJN BX4940

Ondernemingsrecht, inzage in e-mail, instemmingsrecht ondernemingsraad, art. 27 WOR

Geschil over besluit van de Dienst Werk en Inkomen van de gemeente Amsterdam, waarbij werknemers verplicht worden een collega dan wel hun leidinggevende te machtigen tot inzage in hun mailbox (bij gebreke waarvan de leidinggevende die inzage toch krijgt). De ondernemingsraad had een instemmingsrecht ten aanzien van dit besluit, omdat het een wijziging van de bestaande regeling is, inzage in email geschikt is voor waarneming van of controle op aanwezigheid, gedrag of prestaties van werknemers, en omdat het privacyaspecten heeft.

185. Voorzieningenrechter 's-Gravenhage 21 augustus 2012 (nephorloges), *LJN* BX5303

Merkenrecht, positie tussenpersoon, hosting provider, hosting, art. 2.22 BVIE

Gedaagde AltusHost host websites waar replica's c.q. fake horloges te koop worden aangeboden: merkinbreuk. Merkhouders hebben onweersproken gesteld dat Nederland op de websites is aangemerkt als een land van waaruit de producten besteld kunnen worden en waar de producten naar toe kunnen worden gestuurd (via een zogenaamde 'drop down lijst'). Voorts kan betaald worden met euro's en zijn de websites in het Engels gesteld, welke taal in Nederland door nagenoeg iedereen met een internetaansluiting begrepen wordt. De voorzieningenrechter beschouwt AltusHost zodoende voorshands als een tussenpersoon in de zin van art. 2.22 lid 3 en lid 6 BVIE, wiens diensten worden gebruikt voor inbreuk op de aan Merkhouders toebehorende merken.
De voorzieningrechter is van oordeel dat de procedure tot schorsing van de gewraakte domeinnamen bij ICANN voorshands onvoldoende soelaas biedt, enerzijds omdat ICANN zich volgens Merkhouders niet met de inhoud van websites bezig houdt maar met wie de rechthebbende is op de betreffende domeinnaam en anderzijds omdat deze procedure onweersproken tamelijk langdurig van aard is.

Bevel om diensten ten aanzien van een aantal met name genoemde websites te staken, door deze af te sluiten en afgesloten te houden voor toegang door derden vanuit de Benelux, en het hosten van die websites te staken en gestaakt te houden.

186. Voorzieningenrechter Amsterdam 23 augustus 2012 (Linq), B9 11590

Merkenrecht, internet-domein, domeinnaam, Google, zoekmachines, verwijzingen, notice-and-take-down verzoek

Conflict tussen eiser Linq Holding en gedaagde Linqwise executive search.
In casu is verwarringsgevaar voldoende aannemelijk. Dat reeds daadwerkelijk verwarring moet zijn geconstateerd is voor het aannemen van een merkinbreuk geen vereiste.
De vordering om 'elke inbreuk op de genoemde merkrechten van Linq te staken en gestaakt te houden' wordt slechts toegewezen voor zover dit het gebruik door Linqwise van het teken Linq (met de kenmerkende q aan het eind) betreft.
Veroordeling om het gebruik van het internet-domein <linqwise.nl> te staken en gestaakt te houden en zich alle inspanningen te getroosten om verwijzingen in zoekmachines te doen verwijderen, door de beheerders van die zoekmachines (waaronder in ieder geval Google) aan te schrijven.

187. Rechtbank 's-Hertogenbosch 24 augustus 2012 (nachtelijk internetverbod), *LJN* BX5364

Strafrecht, Twitter, bedreiging, belediging, art. 111, art. 285

Verdachte heeft middels een aantal twitterberichten H.K.H. Beatrix, Koningin der Nederlanden, bedreigd. Aangenomen mag worden dat deze bedreiging voor H.K.H. Beatrix, Koningin der Nederlanden, - mede gezien haar kwetsbare publieke positie - beangstigend zal zijn geweest. Verdachte heeft H.K.H. Beatrix, Koningin der Nederlanden, bovendien middels twitterberichten beledigd. Verdachte heeft door zijn beledigingen de waardigheid van de Koningin aangetast. De waardigheid van de Koningin en het met haar positie verweven staatsbelang genieten een bijzondere mate van beschermwaardigheid, hetgeen tot uitdrukking komt in een specifiek op de bescherming van dat belang toegespitste strafbepaling en bijpassend strafmaximum.
De rechtbank houdt voorts ten bezware van verdachte rekening met de uitermate grove en - mede daardoor - kwetsende bewoordingen die hij in zijn twitterberichten heeft gebezigd.
Volgt veroordeling tot 6 maanden voorwaardelijke gevangenisstraf, met als bijzondere voorwaarde dat veroordeelde geen gebruik van internet en sociale media zal maken tussen 00.00 en 08.00 uur, zulks indien en voor zover de reclassering dit noodzakelijk acht.

188. Voorzieningenrechter Rotterdam 29 augustus 2012 (The Training Room), *LJN* BX7261

Arbeidsrecht, Facebook, relatiebeding, bericht op Facebook

Eiser, oud-werknemer zou relatiebeding overtreden hebben door berichten op Facebook, waarmee hij klanten van zijn oud-werkgever Gosh (gedaagde) heeft kunnen bereiken.
Dat deze berichten specifieke, met naam genoemde, klanten van Gosh daadwerkelijk hebben bereikt, acht de voorzieningenrechter daarbij niet van belang.
Voorshands is onvoldoende aannemelijk geworden dat eiser met het plaatsen van deze berichten zich doelbewust en met zakelijk oogmerk tot specifieke klanten van Gosh heeft gericht,om deze als lid van The Training Room te verwerven. Evenmin aannemelijk is geworden dat eiser daadwerkelijk klanten van Gosh als leden van The Training Room heeft verworven.

189. Rechtbank Groningen 5 september 2012 (vermeende dochter Michael Jackson), *LJN* BX6804

Onrechtmatige uiting, artikel op internet, eer en goede naam, vrijheid van meningsuiting, privacy, zelf openbaarheid opzoeken, maatschappelijk belang, belangenafweging

Eiseres beweert de dochter van Michael Jackson te zijn.
Gedaagde heeft op de website van de Telegraaf een artikel over eiseres gepubliceerd dat naar haar oordeel onrechtmatig is. De rechter oordeelt dat eiseres zelf de openbaarheid zocht.
Door een website te openen en te onderhouden waarmee eiseres haar gehele verhaal in de openbaarheid heeft gebracht, heeft zij haar recht om zich te beroepen op bescherming van haar persoonlijke levenssfeer aanzienlijk ingeperkt. Eiseres was geen bekend persoon, maar zij heeft zich daartoe proberen op te werken door via het internet publiekelijk uiting te geven aan haar stellige overtuiging dat zij zeer naaste familie is van de beroemdheid Michael Jackson.
Anders dan gedaagden aanvoeren, is met de zaak van eiseres geen groot algemeen belang gemoeid. Het delen van zijn inzichten door gedaagde is derhalve ook geen essentiele publieksvoorlichting. De aandacht voor de zaak van eiseres is vooral ingegeven door de amusementsbehoefte van het publiek. Die behoefte is weliswaar reëel en als zodanig van enig belang, maar zij zal snel onderdoen voor andere belangen, zoals de privacy van een persoon; daarin ligt een essentieel verschil met kwesties van algemeen belang die de grondvesten van de maatschappij raken en (daarom) de aandacht van de 'serieuze' pers plegen te hebben.
Daargelaten dat het plegen van hoor en wederhoor niet in alle gevallen een aan journalisten te stellen strikte eis is, heeft De Telegraaf enigermate getracht eiseres zelf aan het woord te laten.
Belangenafweging: De vrijheid van meningsuiting prevaleert boven het recht van eiseres op eerbiediging van haar privéleven. De publicatie en/of de bijdrage daarvan van gedaagde is niet aan te merken als onrechtmatig jegens eiseres.

190. Rechtbank Rotterdam 5 september 2012 (belastingfraude met DigiD), *LJN* BX6605

Strafrecht, DigiD, identiteitsfraude, witwassen, opzet-witwassen, gewoontewitwassen, valsheid in geschrifte, art. 225 Sr, art. 420bis Sr, art. 420ter Sr

De verdachte heeft deel uitgemaakt van een criminele organisatie die zich bezighield met het op grote schaal valselijk opmaken en indienen van aanvraag- en wijzigingsformulieren betreffende diverse, door de Belastingdienst uit te keren toeslagen en het witwassen van de aldus verkregen geldbedragen. De verdachte en zijn mededaders maakten bij het – langs digitale weg – aanvragen dan wel wijzigen van de toeslagen onrechtmatig en zonder medeweten gebruik van burgerservicenummers en DigiD's van anderen.
Door aldus te handelen heeft de verdachte zich aanzienlijke geldbedragen toegeëigend en heeft hij daarmee niet alleen de Belastingdienst maar meer nog de desbetreffende toeslaggerechtigden ernstig benadeeld. Immers, zij wisten niet van de aanvragen en wijzigingen zoals door de verdachte en zijn mededaders ingediend en werden plotseling geconfronteerd met het niet meer ontvangen van voor hen vaak essentiële toeslagen dan wel met naheffing van de Belastingdienst wegens onterecht uitgekeerde toeslagen.
Dat het om wijd verbreide criminaliteit is gegaan, blijkt verder uit de wijze waarop de verdachte en de medeverdachten aan de persoonsgegevens van hun slachtoffers kwamen. Er werd post uit brievenbussen gehengeld, er werd gebruik gemaakt van post die aan de TNT was toevertrouwd maar kennelijk was verduisterd en er werd gebruik gemaakt van bescheiden die bij inbraken bij bedrijven werden ontvreemd.
Daar komt bij, dat misbruik is gemaakt van het vertrouwen van anderen, die aan de verdachte en zijn medeverdachten gegevens van hun bankrekeningen toevertrouwden. Daarbij hebben de verdachte en zijn mededaders meer dan eens druk uitgeoefend op hun slachtoffers en gedreigd met geweld tegen hen of hun familieleden.
Volgt veroordeling tot 30 maanden gevangenisstraf.

191. Rechtbank Amsterdam 12 september 2012 (link naar Playboy-foto's), *LJN* BX7043

Auteursrecht, hyperlink, link, openbaarmaking, nieuw publiek, toegankelijk voor publiek, vindbaar voor publiek, solitary URL, ontsluiting, portretrecht, redelijk belang, toestemming

GeenStijl.nl had gelinkt naar naaktfoto's bestemd voor de Playboy, die nog niet waren gepubliceerd. Is dat een openbaarmaking in auteursrechtelijke zin?
Uit jurisprudentie van het HvJ (bv. HvJ EU 15 maart 2012, zaak C-135/10, SCF) blijkt dat rekening moet worden gehouden met de omstandigheden van het geval. Van belang is met name of er sprake is van een interventie, een (nieuw) publiek en winstoogmerk.
Het plaatsen van een hyperlink, die verwijst naar de locatie op het internet waar een bepaald werk voor publiek toegankelijk is gemaakt, is in beginsel geen zelfstandige openbaarmaking. De feitelijke terbeschikkingstelling aan het publiek vindt plaats op de website waar de hyperlink naar verwijst.
In het onderhavige geval was de fotoreportage echter niet op zodanige wijze voor het publiek beschikbaar gesteld, dat deze voor publiek toegankelijk en vindbaar was. Door het plaatsen van een hyperlink op haar website heeft GeenStijl de gehele fotoreportage, die tot dan toe slechts voor een onbeduidend aantal personen vindbaar was, ontsloten. Dus: openbaarmaking.
M.b.t. portretrecht: Dat eiseres toestemming heeft gegeven om de fotoreportage in het tijdschrift en op de websites van Playboy openbaar te maken, heeft tot gevolg dat zij haar privacy in zekere mate heeft prijsgegeven. Dat ontneemt haar echter niet het belang om zich te verzetten tegen de openbaarmaking door GeenStijl. Zij heeft immers geen toestemming verleend voor openbaarmaking door anderen dan Playboy op een moment en op een wijze zoals thans heeft plaatsgevonden, te weten door middel van een link naar een website, in de context van berichten van GeenStijl met een diskwalificerende toon, nog vóór de door eiseres wel toegestane publicatie in Playboy.

192. Voorzieningenrechter Groningen 14 september 2012 (Universiteitskrant Groningen), *LJN* BX7924

Onrechtmatige uiting, digitaal archief, online archief, eer en goede naam, vrijheid van meningsuiting, onrechtmatige daad, belangenafweging, vindbaarheid, Google, publieke belang, vrije nieuwsgaring

Conflict over weigering om artikel uit digitaal archief te verwijderen. In de onderhavige casus zou het publicatierecht van gedaagde kunnen worden beperkt wanneer het gewraakte artikel aantoonbaar onjuistheden bevat, dan wel op onzorgvuldige wijze tot stand is gekomen en in die zin onrechtmatig is in de zin van art. 6:162 BW.
Maar ook kan de op zichzelf rechtmatige publicatie van gedaagde zozeer botsen met het grondrecht van eiseres op eerbiediging van haar eer en goede naam, dat het in haar archief en op internet geplaatst houden van dit artikel alsnog als onrechtmatig handelen in de zin van art. 6:162 BW is aan te merken.
De gewraakte passage bevat naar het oordeel van de voorzieningenrechter geen onjuistheden, althans niet zodanige onjuistheden dat dit onrechtmatigheid in de zin van art. 6: 162 BW oplevert. Dit geldt ook voor het opnemen van de passage in het gewraakte artikel als zodanig.
Hoewel de toon van de passage scherp kan worden genoemd en het betreffende incident al enigszins gedateerd; niet kan worden aangenomen dat verwijzing daarnaar in de gegeven omstandigheden zonder doel en mitsdien onnodig beschadigend was.
Bij de afweging tussen enerzijds het door UK bepleite publieke belang van vrije nieuwsgaring en volledige archivering daarvan en anderzijds het private belang van eiseres bij bescherming van haar eer en goede naam, sluit de voorzieningenrechter aan bij hetgeen de voorzieningenrechter te Amsterdam in een uitspraak van 31 maart 2010 heeft overwogen:
'(...) de samenleving moet kunnen vertrouwen op een volledige en integere (online) archivering. Media hebben bij het dienen van dit publieke belang een belangrijke taak. De pers heeft namelijk de primaire rol van publieke waakhond, maar een belangrijke secundaire functie is het beschikbaar maken van nieuws in archieven. Daarmee is een verplichting tot het verwijderen van artikelen, die op zichzelf rechtmatig zijn, uitsluitend vanwege een negatieve lading, niet goed te verenigen. De archivering zou dan geen betrouwbare getuigenis van het verleden meer vormen. '
(LJN BM4462).

Conclusie het belang van eiseres bij bescherming van haar eer en goede naam weegt niet op tegen het recht van gedaagde op vrijheid van meningsuiting, met inbegrip van de integrale archivering daarvan.

193. Sector kanton Rechtbank 's-Hertogenbosch 27 september 2012 (zoekmotor), *LJN* BX7760

Verbintenissenrecht, zoekmotor, zoekmachine, Google, aanmelding bij zoekmachine

Ingevolge het bepaalde in de overeenkomst strekt de verbintenis van Proximedia niet verder dan het verzorgen van de eerste aanmelding van de website van haar abonnee bij de belangrijkste gratis zoekmotoren. Bovendien is daarbij nog met zoveel woorden opgenomen dat Proximedia niet verantwoordelijk kan worden gesteld van het resultaat van die aanmelding, aangezien die aanmelding bij de zoekmotoren de bevoegdheid is van de commerciële ondernemingen die deze uitbaten. Nu gedaagde de overeenkomst ondertekend heeft, moet het ervoor worden gehouden dat zij met die bepaling en met de aldus beperkte reikwijdte van de strekking van de verplichting van Proximedia, accoord is gegaan. Haar verweer dat anders afgesproken is, valt daarmee niet te verenigen. Voorts heeft Proximedia onweersproken gesteld dat zij de website van gedaagde aangemeld heeft bij de desbetreffende zoekmotoren, zodat ervan uitgegaan moet worden dat zij aldus aan haar contractuele verplichting terzake voldaan heeft.

Wet- en regelgeving

Onder redactie van M. Lassche

NATIONALE WETGEVING

Instelling Cyber Security Raad

Naar aanleiding van de Nationale Cyber Security Strategie van 21 februari 2011 is een Cyber Security Raad ingesteld. Doel is het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen.
In de Cyber Security Raad hebben vertegenwoordigers van alle relevante partijen uit de publieke en private sector alsmede de wetenschap zitting. Centraal staat de uitvoering en de uitwerking van de Nationale Cyber Security Strategie.
De Cyber Security Raad is geen formeel besluitvormingsorgaan, maar handelt op basis van het gezag van de deelnemers. De aanbevelingen van de Cyber Security Raad zijn niet bindend. Bij het opstellen van de aanbevelingen wordt zoveel mogelijk rekening gehouden met de verschillende belangen zodat er een breed draagvlak bestaat voor deze aanbevelingen, zowel bij de publieke als de private partijen.
Bron:Besluit van de Minister van Veiligheid en Justitie (kenmerk 5727629/12) van 9 juli 2012, houdende instelling van een Cyber Security Raad. (*Stcrt.*nr. 17780)
http://goo.gl/ALFAo

Instellingsbesluit besturing eHerkenning

Het instellingsbesluit legt officieel vast welke zeggenschap de betrokken partijen hebben over de inhoud en ontwikkeling van het Afsprakenstelsel. Het is de bedoeling Herkenning. elektronische identificatie van bedrijven veilig, continu en tegen redelijke prijzen beschikbaar is, zodat betrouwbare elektronische communicatie met de overheid en in het handelsverkeer kan plaatsvinden. In de nieuwe besturingsstructuur van eHerkenning zijn de belangen van alle betrokken partijen nog meer gewaargborgd.
Bron: Besluit van de Minister van Economische Zaken, Landbouw en Innovatie van 25 juni 2012, met kenmerk WJZ/12040241, houdende instelling van de besturing van eHerkenning (Instellingsbesluit besturing eHerkenning) (*Stcrt.*nr. 13382)
http://goo.gl/xpgeS

Vragen over toezicht Facebook op gebruikers

Minister Opstelten erkent dat hij kennis heeft van het feit dat Facebook de activiteiten van zijn gebruikers scant op mogelijke criminele activiteiten. Hij vind echter dat het niet zijn taak is om hier opheldering over te vragen. Dit zou de taak zijn van de privacytoezichthouders van de lidstaten. Het CBP heeft te kennen gegeven dat de privacytoezichthouder in Ierland, waar het Europese kantoor van Facebook is gevestigd, mede namens de privacytoezichthouders van de 26 overige EU-lidstaten onderzoek doet naar Facebook.
Bron: Vragen van het lid Schouw (D66) aan de minister en de staatssecretaris van Veiligheid en Justitie over het bericht dat Facebook de activiteiten van zijn gebruikers scant op mogelijke criminele activiteiten (ingezonden 9 augustus 2012). Antwoord van minister Opstelten (Veiligheid en Justitie), mede namens de staatssecretaris van Veiligheid en Justitie) (ontvangen 4 september 2012). (*Aanhangsel Handelingen II*, 2011/12, nr. 3361)
http://goo.gl/ftTzD

Signaleringen

Onder redactie van B.W. Schermer

Britse auteursrechthebbenden willen dat 4G onder DEA gedragscode komt te vallen

Ofcom, de Britse onafhankelijke telecomautoriteit en toezichthouder, is momenteel bezig met het opstellen van een 'Obligation Code' voor netwerkbeheerders. Dit is een gedragscode waarin de meest controversiële aspecten van de 'Digital Economy Act'(DEA) worden uitgewerkt in het belang van de handhaving. Onder deze code kunnen netwerkbeheerders verplicht worden om bepaalde maatregelen te nemen, bijvoorbeeld in geval van auteursrechtinbreuken op hun netwerk. Britse auteursrechthebbenden hebben Ofcom gevraagd om de reikwijdte van deze aankomende regeling uit te breiden zodat ook mobiele netwerkbeheerders eronder vallen. Vooral met het oog op de aankomende uitrol van 4G-netwerken in het Verenigd Koninkrijk eind dit jaar, waardoor ongeveer tien maal hogere downloadsnelheden gehaald kunnen worden, zien auteursrechthebbenden de noodzaak hiervoor; zij vrezen dat het onrechtmatig downloaden sterk zal toenemen door de hogere snelheden van mobiele netwerk. Ofcom heeft aangegeven dat de initiële reikwijdte van de code al bepaald is, maar dat zij deze kan herzien indien rekening moet worden gehouden met nieuwe technieken. Vooralsnog is Ofcom echter van mening dat het grootste deel van de auteursrechtinbreuken plaats vindt via vaste (breedband)netwerken en niet via mobiel internet.
Bron: The Telegraph (http://bit.ly/OhLShP)

Europese Raad van Ministers stemt in met 'Richtlijn Verweesde werken'

Zowel de Europese Commissie als de Europese Raad van Ministers hebben het voorstel voor een nieuwe Richtlijn met betrekking tot zogenaamde 'verweesde werken' aangenomen. Verweesde werken zijn werken die auteursrechtelijk beschermd zijn, maar waarvan de rechthebbende niet kan worden geïdentificeerd. Onder de nieuwe richtlijn kunnen instellingen zoals bibliotheken, universiteiten en musea verweesde werken onder bepaalde omstandigheden digitaliseren of openbaar maken uit het oogpunt van het publieke belang. Een van de vereisten is dat er eerst een 'diligent search' naar de rechthebbende moet plaatsvinden in het land waar het werk voor het eerst is gepubliceerd of opgevoerd. Hoewel de Richtlijn nu is aangenomen, zal het nog zeker twee jaar duren voordat deze is geïmplementeerd en in werking treedt.
Bron: Europese Unie:(http://bit.ly/RN6XRf)

Opstelten beantwoordt Kamervragen over criminaliteitsscan Facebook

D66 Kamerlid Gerard Schouw heeft op 9 augustus Kamervragen ingediend over het bericht dat Facebook activiteiten van gebruikers scant op mogelijke criminele activiteiten. De software van Facebook filtert gesprekken op verdachte inhoud en vergelijkt deze met eerder verkregen chatlogs van criminelen, waaronder zogeheten 'sexual predators'. Hierbij moet met name worden gedacht aan seksueel getinte gesprekken. De software richt zich voornamelijk op leden die een 'losse' relatie hebben, bijvoorbeeld wanneer twee gebruikers geen gemeenschappelijke vrienden hebben, heel weinig met elkaar communiceren, een significant leeftijdsverschil hebben en/of ver uit elkaar wonen. Als de analyse van de gesprekken en de relatie tussen de gebruikers reden tot alarm geeft, controleert een werknemer van Facebook de communicatie en maakt de uiteindelijke beslissing het dossier al dan niet door te spelen naar de autoriteiten.
Schouw wilde weten of het initiatief van Facebook is toegestaan op grond van de Europese en Nederlandse dataprotectiewetgeving en of het opsporen van (potentiële) criminelen niet uitsluitend een bevoegdheid van de Nederlandse overheid is. Minister van Veiligheid en Justitie Ivo Opstelten heeft de vragen van Schouw op 4 september beantwoordt. Hij stelt dat het opsporen van criminelen inderdaad uitsluitend een taak is van de overheid. Of de werkwijze van Facebook binnen het kader van de Nederlandse wetgeving valt, is volgens hem ter beoordeling aan de autoriteiten waar deze gegevensverwerking plaatsvindt. Hij verwijst in dit verband naar het nog lopende onderzoek door de Ierse privacytoezichthouder.
Bronnen: Officielebekendmakingen.nl (http://bit.ly/P7p-ZRY)

OPTA stuurt brief aan overheidsinstanties over voldoen aan nieuwe cookiewet

In de eerste week van september heeft OPTA 121 overheidsinstanties een brief gestuurd om ze te informeren over de nieuwe cookiewet die op 2 juni in werking is getreden. OPTA richt zich in eerste instantie op websites van de overheid en websites die daar door burgers mee geassocieerd worden, omdat deze een voorbeeldfunctie vervullen. Volgens OPTA mag van websites van de overheid verwacht worden dat ze voldoen aan de geldende wet- en regelgeving en zullen andere partijen bij een beslissing om bepaalde regels te implementeren in hun afweging meenemen of en hoe de overheid zelf met deze regels omgaat.
OPTA heeft 96 websites erop gewezen dat ze cookies plaatsen zonder vooraf te informeren en/of om toestemming te vragen. Websites die alleen functionele cookies plaatsen of helemaal niet met cookies werken hebben eveneens een brief gekregen om ervoor te zorgen dat ze ook in de toekomst blijven voldoen aan de cookiewetgeving. Dit signaal aan de betreffende instanties is niet vrijblijvend. OPTA waarschuwt in de brief dat er boetes tot maximaal €45.000 opgelegd kunnen worden als de cookiewet niet nageleefd wordt.
Bron: OPTA (http://bit.ly/ROsbdF)

Europese Commissie wil frequentiespectrum efficiënter verdelen

Dankzij de enorme groei van mobiel en draadloos internet wordt er steeds meer gebruik gemaakt van radiofrequenties. Het spectrum van frequenties is echter beperkt en schaarste dreigt. Als de frequenties op een efficiëntere manier verdeeld worden, kan dit probleem opgevangen worden. Dit maakt het tevens aantrekkelijker om te investeren in nieuwe technologieën die gebruik maken van het frequentiespec-

trum. Daarom wil de Europese Commissie met maatregelen komen om het delen van frequenties te bevorderen. Een van de maatregelen is het bevorderen van consistente regelgeving in de gehele EU voor gedeelde gebruiksrechten van het frequentiespectrum, wat idealiter tot rechtszekerheid leidt voor alle huidige en nieuwe gebruikers. In sommige lidstaten komt het delen van frequenties op nationaal niveau al voor, maar op Europees niveau is hiervoor niets geregeld. Volgens de Europese Commissie moet er een interne markt voor frequenties komen om te kunnen blijven omgaan met de groeiende vraag naar frequenties en om draadloze innovatie te stimuleren.
Bron: Europese Commissie (http://bit.ly/OghVLG) (http://bit.ly/OghVLG)

Duitse Hoge Raad doet uitspraak in zaak Rapidshare/Atari

Begin juli werd het geschil tussen filehostingdienst Rapidshare en softwareproducent Atari behandeld voor de Duitse Hoge Raad. Atari maakte op 19 augustus 2008 melding van een inbreukmakende verwijzing naar hun spel 'Alone in the Dark' bij Rapidshare. Rapidshare verwijderde daarop die specifieke inbreukmakende verwijzing. Volgens de Hoge Raad was het echter niet toereikend dat Rapidshare de concreet genoemde data ontoegankelijk heeft gemaakt. Verder overwoog de Hoge Raad dat Rapidshare heeft nagelaten om te onderzoeken of het spel door andere gebruikers op hun servers was opgeslagen en daardoor alsnog kon worden opgevraagd. Volgens de Hoge Raad heeft Rapidshare als dienstaanbieder een controlefunctie. Deze plicht heeft Rapidshare mogelijkerwijs verzaakt, omdat zij geen woordfilter voor het samenhangende begrip 'Alone in the Dark' inzette om de bij haar opgeslagen data te doorzoeken. Het is aan Rapidshare om 'redelijke economische en technische' maatregelen te nemen om te voorkomen dat het spel opnieuw via hun servers aan derden beschikbaar wordt gesteld. De Hoge Raad wees de zaak terug naar het Hof Düsseldorf om vast te stellen welke maatregelen een filehostingdienst redelijkerwijs moet nemen om niet aansprakelijk te zijn voor auteursrechtinbreuken van gebruikers.
Bron: Bundesgerichtshof (bit.ly/PV6Apf)

Cour de Cassation: Google moet auto-complete functie aanpassen

De Franse Hoge Raad heeft geoordeeld dat Google zoektermen als 'torrent', 'rapidshare' en 'megaupload' niet meer in de instant- en autocomplete-functie van haar zoekdienst mag gebruiken. Een lagere rechtbank wees het verzoek van SNEP, de belangenbehartiger van de muziekindustrie in Frankrijk, eerder af omdat de termen zelf geen inbreuk op het auteursrecht van SNEP vormen. De Hoge Raad heeft deze uitspraak teruggedraaid, overwegende dat de vordering waarschijnlijk inbreuk voorkomt of gedeeltelijk staakt. Door deze zoektermen niet aan te bieden maakt Google het moeilijker voor gebruikers om illegaal materiaal te vinden, aldus de Hoge Raad. Google is teleurgesteld over de uitspraak. Eind 2010 nam Google eigen maatregelen, onder andere door nauw aan piraterij verwante zoektermen te verwijderen uit de autocomplete-functie. Google zou daarbij echter niet consequent handelen; terwijl 'BitTorrent' als term niet meer voorkomt, worden er nog wel suggesties gedaan voor andere populaire torrentclients.
Bron: Cour de Cassation (bit.ly/Ld6gKL), FutureOfCopyright (bit.ly/P77ttw)

Kroes komt met standaarden voor cloud computing

Neelie Kroes, vice-president van de Europese Commissie en verantwoordelijk voor de Digitale Agenda, werkt aan standaarden voor clouddiensten. Ze wil hiermee meer duidelijkheid scheppen over juridische kwesties, zoals modelcontracten, dataportabiliteit en aansprakelijkheid. Ook stelt ze dat de wetgeving binnen Europa homogener moet worden, zodat gebruikers weten waar ze aan toe zijn en aanbieders van clouddiensten niet in elk land rekening hoeven te houden met andere regels. Door beleidsmaatregelen te treffen hoopt Kroes meer carrièremogelijkheden en arbeidsmobiliteit te scheppen en het economische groeipotentieel van clouddiensten beter te benutten. Daarnaast wil ze onderzoek en innovatie stimuleren, zodat applicaties die nu niet in de cloud werken dat uiteindelijk wel gaan doen en er nieuwe diensten ontwikkeld zullen worden. Het complete overzicht met voorstellen moet uiterlijk begin 2013 zijn gepubliceerd.
Bron: TheParliament.com (bit.ly/MXSCNX)