Gezamenlijke noot onder Hof van Justitie EU 24 november 2011, C-70/10 (Scarlet Extended NV/SABAM) en Hof van Justitie EU 16 februari 2012, C-360/10 (SABAM/Netlog NV)

P.B. Hugenholtz
gepubliceerd in: *NJ* 2012, nrs. 479 en 480, p. 5395-5397

De kolossale omvang die de auteursrechtinbreuk op het internet in het afgelopen decennium heeft aangenomen, is moeilijk in getallen uit te drukken. Blijkens een rapport van TNO, SEO en IViR maakt bijna de helft van de Nederlandse internetbevolking (zo'n 4,7 miljoen personen) zich wel eens schuldig aan file sharing (A. Huygen et al., 'Ups and downs. Economische en culturele gevolgen van file sharing voor muziek, film en games' (2009)). Volgens andere schattingen betreft meer dan een kwart van het totale internetverkeer 'illegale content' – vooral door *peer-to-peer file sharing*.

Hoewel de auteursrechthebbenden in hun strijd tegen deze 'piraterij' incidenteel successen boeken door verbodsacties tegen grootschalige 'uploaders' of aanbieders van peer-to-peer netwerken, blijft de handhaving van het auteursrecht op het internet dweilen met de kraan open. Individuele inbreukmakers opereren bij voorkeur anoniem en zijn dus moeilijk te identificeren. En peer-to-peer netwerken opereren dikwijls van buiten Nederland, en zijn nauwelijks effectief aan te pakken.

Geen wonder dat de rechtshandhaving zich de afgelopen jaren gaandeweg verplaatst heeft in de richting van de internetproviders (zie noot P.B. Hugenholtz onder NJ 2009, 551). Weliswaar kunnen deze tussenpersonen op grond van de Europese Richtlijn inzake elektronische handel ('E-commercerichtlijn') resp. art. 6:196c BW niet aansprakelijk worden gehouden voor (auteursrecht)inbreuk door derden, deze immuniteit sluit een gerechtelijk verbod of gebod niet uit (zie artikelen 12 lid 3, 13 lid 2 en 14 lid 3 E-commercerichtlijn; art. 6:196c lid 5 BW). Sterker, op grond van art. 8 lid 3 van de Auteursrechtrichtlijn en art. 11 van de Handhavingsrichtlijn moeten de lidstaten juist voorzien in de mogelijkheid van een gerechtelijk bevel tegen tussenpersonen die door derden voor inbreukdoeleinden worden gebruikt. Bijgevolg zijn de internetproviders steeds vaker het doelwit van op het 'schoonvegen' van het internet gerichte ge- en verbodsacties . Maar hoever moeten de providers – en mogen de rechters – hierin gaan? Deze vraag staat in deze zaken centraal.

Auteursrechthebbenden dromen wel eens van een perfecte wereld waarin de handhaving van het auteursrecht zich volautomatisch voltrekt door een combinatie van computergestuurde detectie, filtering en blokkering van inbreukmakende bestanden. Voor de providers en de gebruikers van het internet is deze *perfect world* echter een nachtmerrie. Van het open en 'neutrale' internet, dat de afgelopen decennia wereldwijd voor ongekende uitingsvrijheid heeft gezorgd, blijft dan weinig over, zo wordt gevreesd. Ook bestaan er twijfels of zo'n filtersysteem technisch realiseerbaar en betaalbaar is, gezien de gigantische hoeveelheid gegevens die het systeem in 'real time' zou moeten controleren. Hier komt bij dat het onderscheid tussen legaal en illegaal gebruik van auteursrechtelijk beschermde werken niet altijd evident is (denk aan parodiërend gebruik van een muziekwerk), en door een computergestuurd proces dus eigenlijk niet goed te maken is.

Ondanks deze evidente bezwaren trok muziekrechtenorganisatie SABAM, de Belgische evenknie

van Buma, al in 2004 de stoute schoenen aan door van internet access provider Tiscali (later: Scarlet) in kort geding te vorderen dat zij voortaan alle inbreukmakende uitwisseling van muziekbestanden door haar klanten zou blokkeren. Nadat een door de Brusselse rechtbank aangewezen deskundige had verklaard dat het filteren van peer-to-peer verkeer weliswaar zeer kostbaar maar niet onuitvoerbaar zou zijn (Conclusie A-G Cruz Villalón, § 21), wees de rechtbank het stakingsbevel in beginsel toe. In hoger beroep rezen echter ernstige twijfels over de verenigbaarheid van een dergelijk filtergebod met diverse tot het Unierecht behorende fundamentele vrijheden, en vooral met het in de E-Commercerichtlijn opgenomen verbod om internetproviders te onderwerpen aan een algemene toezichtplicht. De door het Brusselse Hof van Beroep gestelde prejudiciële vragen leidden uiteindelijk tot een arrest dat in de internetwereld met groot gejuich is begroet.

Omdat het door SABAM gevorderde filtersysteem nooit door Scarlet of enige andere access provider geïmplementeerd is, en de precieze technische werking ervan dus onduidelijk blijft, is de door het Hof van Beroep gegeven omschrijving van het systeem nogal algemeen. Zoals door het Hof van Justitie geherformuleerd, betreffen de prejudiciële vragen een gerechtelijk gebod dat een internetprovider zou verplichten om een filtersysteem in te voeren "voor alle elektronische communicatie via zijn diensten, met name door het gebruik van "peer-to-peer"-programma's; dat zonder onderscheid op al zijn klanten wordt toegepast; dat preventief werkt; dat uitsluitend door hem wordt bekostigd, en dat geen beperking in de tijd kent, dat in staat is om op het netwerk van deze provider het verkeer van elektronische bestanden die een muzikaal, cinematografisch of audiovisueel werk bevatten waarop de verzoeker intellectuele-eigendomsrechten zou hebben, te identificeren, om de overbrenging van bestanden waarvan de uitwisseling het auteursrecht schendt, te blokkeren […]" (r.o. 29).

Het Hof van Justitie laat van dit algemene filtergebod weinig heel. Weliswaar stelt het Hof onder verwijzing naar het arrest L'Oréal/eBay (C-324/09) voorop dat een tegen een internetprovider gericht gerechtelijk gebod ook preventieve maatregelen mag betreffen teneinde toekomstige inbreuken te voorkomen, het daarna volgende oordeel dat een algemeen filtergebod te ver gaat, komt niet als een verrassing. Naar het oordeel van het Hof komt zo'n gebod door zijn ruime en algemene strekking in feite neer op een door art. 15 lid 1 van de E-Commercerichtlijn verboden algemene toezichtverplichting. Immers, "een dergelijk preventief toezicht vereist dus een actieve observatie van alle elektronische communicatie op het netwerk van de betrokken internetprovider en omvat bijgevolg alle door te geven informatie en alle klanten die dat netwerk gebruiken." (r.o. 39).

Hoewel de belangrijkste vraag van de verwijzende rechter hiermee in feite beantwoord is, gaat het Hof van Justitie vervolgens in op de lastigere vraag hoe een filterverbod zich verhoudt tot de fundamentele rechten en vrijheden die sinds enkele jaren in het Handvest zijn verankerd. Dit vormt het interessantste deel van het arrest. Het Hof begint zijn toetsing met het recht van intellectuele eigendom dat in art. 17 lid 2 Handvest (Hv) grondrechtelijke erkenning heeft gekregen. Hoewel dit recht in het Handvest in absolute termen is vervat ("Intellectuele eigendom is beschermd"), overweegt het Hof dat "noch uit deze bepaling, noch uit de rechtspraak van het Hof [voortvloeit] dat dit recht onaantastbaar is en daarom absolute bescherming moet genieten." Dit is een juiste en belangrijke constatering. IE-rechten, zoals het auteursrecht en het octrooirecht, zijn eigenlijk geen eigendomsrechten, maar vermogensrechten van beperkte duur en reikwijdte. Op nationaal niveau kent het auteursrecht vele wettelijke beperkingen (uitzonderingen), zoals het citaatrecht, de persexceptie en de thuiskopieregeling. Bovendien laat art. 52 lid 1 Hv de lidstaten vrij om de in het Handvest gewaarborgde grondrechten bij wet te beperken, mits de kern ervan niet wordt aangetast en met inachtneming van het evenredigheidsbeginsel.

In casu zal de handhaving van het auteursrecht moeten worden afgewogen tegen andere in het Handvest gewaarborgde grondrechten; er zal een 'juist evenwicht' (*fair balance*) tussen deze rechten gevonden moeten worden. Een enigszins vergelijkbare exercitie had het Hof al eens gedaan in het Promusicae-arrest (C-275/06, *NJ* 2009, 551), waar de handhaving van het auteursrecht werd afgezet tegen de bescherming van de privacy en persoonsgegevens van (mogelijk) inbreukmakende internetgebruikers. In zijn uitvoerige conclusie bij het Scarlet-arrest toetst A-G Cruz Villalón het gerechtelijk bevel tot filteren aan de artikelen 7 (privacy en communicatiegeheim), 8 (persoonsgegevens) en 11 (informatievrijheid) Hv. De A-G concludeert uiteindelijk dat voor het bevel een adequate wettelijke grondslag ontbreekt. De grondrechtelijke toetsing door het Hof verloopt anders. Enigszins verrassend stelt het Hof de *vrijheid van ondernemerschap* van art. 16 Hv voorop. Dit is – zeker voor Nederlandse juristen – even wennen; een dergelijke vrijheid staat niet in onze Grondwet en evenmin in het EVRM dat overigens als bron van inspiratie voor het Handvest heeft gediend. Volgens het Hof zou een gerechtelijk filtergebod de internetproviders op hoge kosten jagen en daardoor leiden tot "een ernstige beperking van de vrijheid van ondernemerschap van de betrokken internetprovider" (r.o. 48). Hierdoor zou het 'juiste evenwicht' tussen de bescherming van het IE-recht en de vrijheid van ondernemerschap niet worden bereikt (r.o. 49).

Na deze ode aan de ondernemingsvrijheid komt het Hof pas toe aan de 'harde' grondrechten, waarbij opvalt dat het Hof het communicatiegeheim (art. 7 Hv) buiten beschouwing laat. Omdat het filteren onvermijdelijk gepaard zou gaan met de identificatie en registratie van de IP-adressen van illegale 'uploaders', en omdat IP-adressen tot personen herleidbaar zijn, is de bescherming van persoonsgegevens (art. 8 Hv) in het geding (r.o. 51). Dat IP-adressen inderdaad als persoonsgegevens zijn aan te merken, had het Hof nog niet eerder met zoveel woorden verklaard. Tevens vormt het filtersysteem een aantasting van de informatievrijheid (art. 11 Hv) doordat het geen onderscheid kan maken tussen verboden en toegestaan gebruik. Het Hof wijst hier niet alleen op de wettelijke beperkingen van het auteursrecht, die van land tot land kunnen verschillen, maar ook op variabele termijnen van bescherming (art. 52). Met dat al kan het door SABAM gevorderde stakingsbevel de toetsing aan de E-Commercerichtlijn en het Handvest op geen enkele wijze doorstaan.

Enkele maanden na het arrest in de Scarlet-zaak gaf het Hof in vrijwel identieke bewoordingen antwoord op vrijwel identieke vragen van de Brusselse rechtbank in de zaak SABAM/Netlog NV. Het arrest is hierboven in sterk verkorte vorm afgedrukt. Hoewel dit doet vermoeden dat het onderliggende feitencomplex gelijk is aan dat van de Scarlet-zaak, is dat niet het geval. Netlog is geen internet access provider, zoals Scarlet, maar exploitant van een sociaal netwerk vergelijkbaar met in Nederland populaire diensten als Myspace en Facebook. Dat dergelijke dienstverleners ook kunnen profiteren van de immuniteiten van de E-Commercerichtlijn was door het Hof van Justitie nog niet eerder gezegd. Erg lang lijkt het Hof – bij ontstentenis van een conclusie van een advocaat-generaal – hier ook niet over te hebben nagedacht, getuige de achteloze wijze waarop het Hof in r.o. 27 poneert dat Netlog door de profielinformatie van zijn gebruikers op zijn servers op te slaan "dus" een hostingprovider in de zin van artikel 14 van de richtlijn is. Bijgevolg mag ook Netlog niet aan een algemene toezichtplicht (art. 15 lid 1) – en een algemeen filtergebod – worden onderworpen.

Dat een sociale-netwerksite als hostingprovider is aan te merken is, gezien de overwegend passieve rol die een dergelijke dienstverlener normaliter vervult ten aanzien van de door de gebruikers op hun eigen pagina's geplaatste inhoud, weliswaar goed te begrijpen, maar is bepaald niet evident. In eerdere arresten had het Hof ten aanzien van de aanbieder van een zoekmachine (Google France, gevoegde zaken C-236/08, C-237/08 en C-238/08) en de exploitant van een

elektronische marktplaats (L'Oréal SA/eBay, zaak C-324/09) in zeer voorzichtige bewoordingen geoordeeld dat deze dienstverleners als hosting provider in de zin van art. 14 van de richtlijn kunnen worden aangemerkt, en dan dus de immuniteiten van de richtlijn genieten, mits "de rol van deze dienstverlener in die zin neutraal is dat zijn handelingen louter technisch, automatisch en passief zijn, wat impliceert dat hij geen kennis heeft van of controle heeft over de gegevens die hij opslaat" (Google France, r.o. 114). Het valt op dat het Hof in de Netlog-zaak toetsing aan dit criterium achterwege laat. Mogelijk wreekt zich hier de beslissing van het Hof om de zaak zonder conclusie te berechten.

Nu de door SABAM gedroomde *perfect world* van automatische rechtshandhaving niet door een gerechtelijk verbod geëffectueerd kan worden, rijst natuurlijk de vraag wat voor gerechtelijke bevelen wel door de Europeesrechtelijke beugel kunnen. Is een gebod dat er toe strekt om alle internetverkeer dat uit één notoir inbreuk faciliterende bron afkomstig is, wel voldoende specifiek, of schept zo'n maatregel ook een algemene (en dus verboden) toezichtplicht? Deze vraag is in Nederland bijzonder actueel in verband met de hardnekkige pogingen van de Stichting Brein (die optreedt namens een groot aantal rechthebbenden) om de *Pirate Bay* – een vanuit het buitenland opererende website die stelselmatig naar vindplaatsen van illegale bestanden verwijst – effectief te blokkeren. Recent heeft het Oostenrijkse Oberste Gerichtshof prejudiciële vragen van deze strekking aan het Hof gesteld (zaak C-314/12). Het antwoord zal van grote invloed zijn op de toekomstige handhaving van het auteursrecht op het internet. Indien het Hof ook een dergelijke, tegen een specifieke bron van inbreuk gerichte maatregel te ruim geformuleerd acht, zal de 'contentindustrie' zich moeten afvragen of verdere handhavingsinspanningen nog wel zo zinvol zijn.

Eerdere commentaren op het arrest verschenen in *NTER* 2012-2, p. 75-82 (N. Helberger en J. van Hoboken); *Mediaforum* 2012/3, p. 98-100 (S. Kulk en F. Zuiderveen Borgesius); en *AMI*, 2012-2, p. 49-53 (E.J. Dommering).