tegenstelling tot de (schaarse) rechtspraak tot nog toe – betoogd dat de richtlijn die niet heeft willen omvatten. De geschriftenbescherming valt daarentegen volgens mij wél onder het toepassingsbereik.
Met vrij veel zekerheid kan in ieder geval worden geconcludeerd dat de volgende gevallen onder het toepassingsbereik vallen: handelsnaamgeschillen (op grond van art. 5 of art. 5a Hw); domeinnaamgeschillen waarin een merk of handelsnaam wordt ingeroepen; vergelijkende reclame waarin het merk van de concurrent wordt gebruikt; wapperverboden; executiegeschillen; en geschillen over overeenkomsten die sterk samenhangen met IE-rechten. Uitgesloten van de nieuwe regeling zijn: slaafse nabootsing en andere op art. 6:162 BW gebaseerde vorderingen.
De toekomst zal moeten uitwijzen, hoe de rechtspraak het toepassingsbereik interpreteert. In hoogste instantie zal het Hof van Justitie daar aan te pas kunnen komen.

Nr. 97

Richtlijnconform filteren van peer-to-peer verkeer

Arnoud Engelfriet[1]

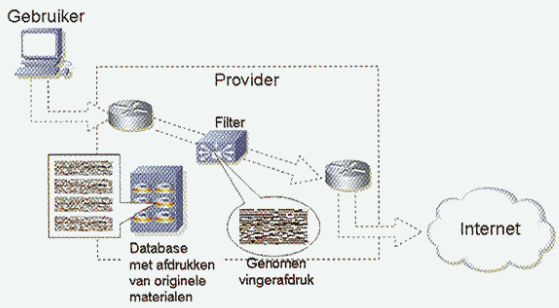
1. Inleiding

Het digitaal auteursrechtfilter is technisch haalbaar. Moeten providers dan nu peer-to-peer (P2P) verkeer van klanten gaan filteren? Ja, en wel op straffe van een dwangsom, zo oordeelde de Belgische rechter in de zaak tussen de auteursrechtenorganisatie SABAM en internetprovider Scarlet (voorheen Tiscali).[2] Nee, zo zeggen art. 12 en 15 Richtlijn elektronische handel.[3] Zijn deze opvattingen te verenigen? Is richtlijnconform filteren van internetverkeer mogelijk?

De roep om blokkades en filters bij P2P-uitwisseling van werken bestaat al sinds de Amerikaanse P2P-dienst Napster in juridische problemen raakte.[4] Napster voerde onder druk van rechtszaken een filter in dat het delen van inbreukmakend materiaal moest tegengaan. Dit filter bleek echter totaal niet effectief, omdat het uitsluitend op titels en namen filterde. Gebruikers boden vanaf dat moment simpelweg het nummer 'Haertbreak h0tel' van de onbekende artiest 'Elivs Presley' aan.

Filters anno 2007 letten niet op titels maar filteren op inhoud. Muziek en filmwerken blijken herkenbaar aan hun digitale vingerafdruk. Bovendien is gespecialiseerde technologie beschikbaar die alle in- en uitgaand verkeer kan bestuderen: *deep packet inspection*. Daarmee zijn de technische ingrediënten beschikbaar om P2P-verkeer preventief te filteren en aldus inbreuk op auteursrecht te voorkomen. Hoe ziet dit er in de praktijk uit?

2. De pakketinspecteur



Figuur 1 laat schematisch een filtersysteem zien zoals een provider dat kan installeren. Het filter zit aangesloten op de verbinding tussen de klant en het internet, waarlangs alle gegevens moeten die de klant via het internet wil versturen. De gegevens komen binnen als pakketjes (IP-pakketten) die stuk voor stuk doorgegeven worden. Elk pakketje bevat een aanduiding van de afzender en de bestemming, plus een fragment van het originele werk en een volgnummer. De ontvanger verzamelt alle pakketjes en assembleert het originele werk met behulp van de volgnummers. Wil een provider kunnen nagaan wat haar klanten versturen of ontvangen, dan moet deze alle langskomende pakketjes inspecteren. Dit lijkt ondoenlijk: het Nederlandse internetverkeer alleen al is ongeveer 360 gigabyte – 77 dvd's – *per seconde*.[5]
Het blijkt echter wel degelijk mogelijk om zulke gigantische hoeveelheden pakketjes te inspecteren. De benodigde technologie heet *deep packet inspection*, omdat niet alleen gekeken wordt naar de aanduidingen op de

1. Arnoud Engelfriet is jurist en octrooigemachtigde bij Philips. E-mail: Arnoud@Engelfriet.net – Site: <http://www.iusmentis.com/>.
2. Rechtbank van Eerste Aanleg van Brussel 29 juni 2007 (*SABAM/Tiscali*).
3. Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000, *PbEG* L 178 van 17 juli 2000.
4. Vgl. D.J.G. Visser, 'Napsteren', 'Gnutellen' en de afwezigheid van legale muziek op Internet', *Computerrecht* 2001/3, p. 131-133 en J.M.B. Seignette, 'Napster en de controle van de rechthebbende over de distributie van zijn werk', *AMI/Informatierecht* 2001/2, p. 29-34.
5. Voor de beeldvorming: dat kost € 35 per seconde alleen al voor de thuiskopievergoeding voor de data dvd's om dit verkeer op te bewaren. Cijfers afkomstig van de Amsterdam Internet Exchange, <http://www.ams-ix.net/technical/stats/>.

pakketjes, maar ook naar de inhoud ervan.[6] Een pakketje met P2P-verkeer ziet er anders uit dan een pakketje met een fragment van een e-mail. Door nu de P2P-pakketjes er uit te vissen, kan het werk dat wordt gedeeld weer worden gereconstrueerd. De e-mail kan worden overgeslagen, en daarmee blijft de hoeveelheid werk behapbaar.[7]

3. De digitale vingerafdruk

De volgende stap is het inhoudelijk controleren van de via P2P uitgewisselde werken. Dit gebeurt via hun unieke 'digitale vingerafdruk'. Er zijn diverse technieken ontwikkeld om digitale vingerafdrukken van werken te nemen.[8] Algemeen gesproken werken ze hetzelfde: unieke kenmerken van het werk worden op een gestandaardiseerde manier vastgelegd, zodat ze kunnen worden vergeleken met eerder genomen vingerafdrukken waarvan het bekend is bij welk werk ze horen.

Waar vingerafdrukken van mensen gevormd worden door unieke ribbeltjes op de vingers, wordt de digitale vingerafdruk van muziek of film gevormd door unieke kenmerken van het audio- of videosignaal, zoals uitschieters in de signaalsterkte binnen een bepaalde tijd of het stijgen dan wel dalen van de signaalsterkte binnen bepaalde frequentiebanden. Deze kenmerken blijken uniek voor elk werk en kunnen daarmee ingezet worden bij herkenning.
Wat digitale vingerafdrukken bijzonder maakt, is dat ze niet veranderen bij wijziging of omzetten van het werk. De vingerafdruk van een werk op cd is hetzelfde als die van het sterk gecomprimeerde MP3-bestand, zelfs wanneer daar in is geknipt.

Figuur 2 laat bijvoorbeeld de vingerafdruk zien van een werk op cd (boven) en hetzelfde werk als MP3-bestand (onder). Hoewel de twee duidelijk niet identiek zijn, bestaan er voldoende overeenkomsten om te kunnen concluderen dat het om hetzelfde werk gaat.

De vingerafdruk wordt genomen van de eerste tien tot dertig seconden van het werk. Dit is genoeg voor een meestal betrouwbare detectie en geeft voldoende tijd om in te grijpen als het werk niet verspreid mag worden. De provider beschikt over of heeft toegang tot een database met door rechthebbenden aangeleverde vingerafdrukken van beschermde werken. Als de genomen vingerafdruk overeenkomt met één van deze geregistreerde vingerafdrukken, dan wordt het werk zonder toestemming van deze rechthebbenden verspreid. De verdere verzending van dit werk wordt dan automatisch geblokkeerd.[9] Hiermee wordt elke mogelijke inbreuk voorkomen: werken waarvan vingerafdrukken in de database voorkomen, kunnen niet langer worden uitgewisseld.

De technische ingrediënten zijn er dus. Het probleem is alleen dat deze manier van grootschalig preventief filteren ingaat tegen de regeling over aansprakelijkheid van providers uit de Richtlijn elektronische handel.

4. Van doorgeefluik naar portier

Een *access provider* is in beginsel een doorgeefluik, een *mere conduit*. Bestanden die haar klanten via P2P verspreiden, zijn afkomstig van de systemen van klanten en passeren slechts de provider op weg naar hun bestemming elders. De bestanden worden niet opgeslagen (*gecached*) bij de provider. Art. 6:196c BW, de implementatie van art. 12 lid 1 Richtlijn 2000/31/EG, bepaalt dat de provider dan niet aansprakelijk is, mits hij niet het initiatief voor de doorgifte neemt, hij de ontvanger niet selecteert en hij de doorgegeven informatie niet selecteert of wijzigt.[10]

Door een preventief filter zoals hierboven beschreven te implementeren, komt de provider echter in een positie waarin hij juist *wel* de doorgegeven informatie selecteert. Informatie wordt tegengehouden vanwege de mogelijkheid van inbreuk op rechten van derden. Er is geen sprake van optreden naar aanleiding van een klacht of mededeling van de kant van de rechthebbende. De provider treedt zelf op en blokkeert, uitsluitend op basis van de vingerafdruk. Het doorgeefluik wordt daarmee een portier. Een portier die aansprakelijk gehouden kan worden voor alle werken die zijn klanten toch nog succesvol blijken te verspreiden. Juist door de selectie middels het filter kan de provider niet langer gebruik maken van de uitsluiting van aansprakelijkheid krachtens art. 6:196c BW.

---

6. De benodigde apparatuur is verkrijgbaar bij tientallen leveranciers, onder andere Cisco, IBM en Ericsson.
7. Zie ook Nate Anderson, 'Deep packet inspection meets 'Net neutrality, CALEA', *Ars Technica* 25 juli 2007, <http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars>.
8. Een voorbeeld is J. Haitsma en T. Kalker, 'A Highly Robust Audio Fingerprinting System With an Efficient Search Strategy', *Journal of New Music Research* 32(2), juni 2003, p. 211-221. Een overzicht van technieken is P. Cano e.a., 'A Review of Audio Fingerprinting', *The Journal of VLSI Signal Processing* 41(3), p. 271-283. Bedrijven die deze technologie aanbieden, zijn o.a. Gracenote, Audible Magic en Relatable.
9. Het kan gebeuren dat het filter ten onrechte verspreidingen blokkeert. Dit zal vooral spelen wanneer fragmenten van een beschermd werk rechtmatig worden hergebruikt als onderdeel van een ander werk. Het fragment kan bijvoorbeeld een citaat (art. 15a Aw) zijn, een opname in een *podcast*-reportage (art. 16a Aw), een parodie (art. 18b Aw) of een incidentele verwerking van ondergeschikte aard (art. 18a Aw) in een ander werk.
10. C.B. van der Net, 'De civielrechtelijke aansprakelijkheid van. internetproviders na de Richtlijn elektronische handel', *JAVI* 2002/1, p. 10-15. Zie ook P.B. Hugenholtz, 'Het Internet: het auteursrecht voorbij?', Preadvies Nederlandse Juristenvereniging, *Handelingen NJV* 1998-I, p. 226-228.

En dat was nu net niet de bedoeling van de Richtlijn. De Richtlijn wilde ontwikkeling van de grensoverschrijdende dienstverlening stimuleren en providers dan ook slechts 'in bepaalde gevallen' verplichten op te treden (zie overweging 40). Dat er destijds geen werkbare filters beschikbaar waren, en nu wel, doet daar niet aan af. Er is immers geen voorbehoud gemaakt voor het geval zulke technologie beschikbaar komt.[11] Er moet sprake zijn van een concrete inbreuk die met een specifieke maatregel beëindigd kan worden. Van de provider kan immers niet gevraagd worden om in te schatten of sprake is van inbreuk.

Die maatregel moet ook proportioneel zijn.[12] Alle verkeer filteren en preventief alle verdachte werken blokkeren gaat veel te ver. Al was het maar omdat de gebruiker bij een onterecht ingrijpen dan tussen wal en schip valt. De provider kan de beweringen van de gebruiker niet verifiëren. De rechthebbende heeft de verspreiding niet gezien en kan er dus niets over zeggen. Het enkele feit dat de vingerafdruk van het werk overeenkomt met een eerder door hem aangeleverde vingerafdruk is nog lang geen bewijs van inbreuk op het auteursrecht.

Bovendien kan een preventief filter niet anders worden gezien dan als een 'algemene verplichting tot toezien op informatie of actief zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden', welke verboden is op grond van art. 15 lid 1 Richtlijn 2000/31/EG. Een preventief filter filtert alle langskomende informatie, en controleert op strijd met auteursrechten van derden. Veel actiever dan alles controleren kan een provider niet worden.

Men zou nog kunnen betogen dat art. 8 lid 3 Richtlijn 2001/29/EG (Auteursrechtrichtlijn) toch de mogelijkheid biedt om een provider een verbod op te leggen bij inbreuk op auteursrecht.[13] Echter, een dergelijk verbod kan, zoals blijkt uit overweging 16 van die Richtlijn, geen afbreuk doen aan de aansprakelijkheid zoals geregeld in de Richtlijn elektronische handel. Een maatregel opgelegd aan een *access provider* mag dus alleen strekken tot het beëindigen van een specifieke inbreuk en voorkoming van verdere schade.

Een verplichting om een preventief filter als dit in te voeren, mag dan ook niet aan *access providers* worden opgelegd.

5. Richtlijnconform filteren

Filters kunnen wel degelijk ingezet worden op een manier die in overeenstemming is met de bedoeling van de Richtlijn. Daarvoor moet het filter niet preventief worden ingezet, maar juist reactief. Art. 12 lid 5 Richtlijn 2000/31/EG staat het nemen van maatregelen *achteraf* toe om een inbreuk te beëindigen of te voorkomen.[14] Hieronder valt bijvoorbeeld het blokkeren van toegang tot of doorgifte van een specifiek werk. Ook mogelijk zijn het afsluiten van een inbreukmaker of het verstrekken van diens adresgegevens aan de rechthebbende.[15] Een dergelijke maatregel mag niet ontaarden in de hierboven genoemde algemene verplichting tot toezien actief zoeken.

Een reactief mechanisme bestaat al voor *hosting providers*. Deze zijn gehouden om, wanneer zij op een inbreuk worden gewezen, het inbreukmakende materiaal te blokkeren of te verwijderen (art. 6:196c lid 4 BW). Dankzij de digitale vingerafdruk kan dit mechanisme nu ook bij *access providers* worden toegepast, zodat ook zij kunnen ingrijpen bij specifieke gevallen van inbreuk.

De procedure werkt dan als volgt. De provider beschikt nog steeds over een P2P-filter zoals in figuur 1. Echter, de database is initieel leeg. Wanneer de provider een klacht ontvangt over verspreiding van een bepaald werk, neemt hij de vingerafdruk van dat werk op in de database. Daarmee wordt verdere verspreiding van dat werk onmogelijk. Bovendien kan dan meteen de abonnee in kwestie – die in de klacht moet worden geïdentificeerd via zijn IP-adres – de wacht worden aangezegd. Mocht er toch sprake zijn van een legitieme verspreiding (bijvoorbeeld omdat sprake was van een parodie op het werk), kan deze reageren en dan kan het werk weer uit de database worden verwijderd.

Er is in deze procedure geen sprake van preventief filteren van *alle* aangeboden werken. Elk blokkeren gebeurt op basis van een concrete klacht met betrekking tot een specifiek werk. Daarmee is het filter reactief geworden: een maatregel ter beëindiging van *verdere* inbreuk.

6. 'Take down, stay down'

Recent is Google's filmpjessite Youtube overgegaan tot invoeren van deze procedure, overigens met een zelf ontwikkelde technologie voor het nemen van vingerafdrukken.[16] Er is geen sprake van preventief filteren: de rechthebbende moet nog steeds bij elk werk een klacht indienen. Na een klacht wordt het werk verwijderd en wordt de vingerafdruk van het werk aan het filter toegevoegd zodat dit werk niet meer herplaatst kan worden, ook niet via een andere account. Daarnaast kunnen rechthebbenden met vingerafdrukken van hun eigen werk op Youtube zoeken naar alle aangeboden films die met die vingerafdruk overeenkomen.

11. K. Koelman, 'Online Intermediary Liability', in: P.B. Hugenholtz (ed.), *Copyright and Electronic Commerce. Legal Aspects of Electronic Copyright Management*, London/The Hague/Boston: Kluwer Law International 2000, p. 7-57.
12. Van der Net, *supra* noot 10, p. 14.
13. Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij.
14. Zie ook Van der Net, *supra* noot 10, p. 13-14.
15. Zie bijvoorbeeld HR 25 november 2005, *LJN*: AU4019 (*Lycos/Pessers*) en Rb. Zwolle 3 mei 2006, *LJN*: AW6288 (*Stokke/Marktplaats*).
16. David King, 'Latest content ID tool for YouTube', Google blog 17 oktober 2007. <http://googleblog.blogspot.com/2007/10/latest-content-id-tool-for-youtube.html>.

Zij kunnen dan via het bestaande 'Notice and take-down'-systeem een klacht indienen.[17]

In mei 2007 heeft de Amerikaanse profielensite Myspace een vergelijkbaar systeem ingevoerd.[18] Zij noemt dit toepasselijk genoeg 'Take down, stay down'.[19] Gebruikers kunnen muziek en beeld aan hun profiel toevoegen, zonder voorafgaande controle. Ontvangt Myspace een klacht, dan wordt het werk verwijderd en een vingerafdruk daarvan toegevoegd aan het filter. Vanaf dat moment kan geen enkele gebruiker een werk met dezelfde vingerafdruk meer publiceren bij zijn of haar profiel.

7. Conclusie

Filteren via vingerafdrukken levert een zinvolle bijdrage aan de bestrijding van inbreuk op auteursrecht op internet. Maar om daarvoor de neutrale positie van de access provider op te geven, gaat mij te ver. Providers vervullen slechts de louter technische rol van doorgeefluik. En zo moet het ook blijven. Providers kunnen en mogen niet in een positie gebracht worden waar zij zelf moeten bepalen of wellicht sprake is van een inbreukmakende handeling, zonder zelfs maar een claim van de rechthebbende.

Het 'Notice and take down' mechanisme uit de Richtlijn bewaart bij *hosting providers* het evenwicht tussen de bestrijding van inbreuk en het ontwikkelen van nieuwe digitale diensten. De rechthebbende constateert een vermeende inbreuk, en meldt deze zodat de provider dan kan ingrijpen. Bij een onjuiste constatering kan de gebruiker reageren naar de rechthebbende. Van de provider wordt nu niet verwacht dat hij preventief optreedt en zelf moet beoordelen of er sprake is van een onrechtmatig handelen van een gebruiker. Dankzij de digitale vingerafdruk en *deep packet inspection* kan dit mechanisme nu ook voor *access providers* worden gehanteerd. En zo wordt dit evenwicht ook bij *access providers* gehandhaafd.

17. 'YouTube Video Identification Beta', Youtube website 18 oktober 2007, http://www.youtube.com/t/video_id_about.
18. Zowel Youtube als Myspace zijn natuurlijk *hosting providers* en geen *access providers*, maar het principe blijft hetzelfde.
19. 'MySpace Launches 'Take Down Stay Down' Copyright Protection', Audible Magic persbericht 11 mei 2007, <http://www.audiblemagic.com/news/press-releases/pr-2007-05-11.asp>.