Brein/KPN: het gevaar van een bagatel?

Remy Chavannes*

Kan een internetaanbieder verplicht worden een klant af te sluiten als deze met gebruikmaking van zijn internetverbinding onrechtmatig handelt door om commercieel gewin auteursrechtinbreuk te faciliteren? Maakt het voor de criteria voor het verstrekken van identificerende gegevens van deze klant aan de rechthebbenden uit, dat de klant zijn onrechtmatige website niet bij de internetaanbieder heeft opgeslagen maar thuis op zijn eigen pc heeft gestald en van de aanbieder dus geen opslag (hosting) dienst afneemt maar alleen een toegangs (access) dienst? De antwoorden van de Haagse voorzieningenrechter in de zaak tussen Brein en KPN[1] zijn in het licht van de feiten te begrijpen, maar vormen een onjuist en onwenselijk precedent.

Inleiding

Aanleiding voor het geschil was een internetklant van KPN, die op zijn website www.dutchtorrent.org zogenoemde bittorrentbestanden beschikbaar stelde. Dergelijke indexbestandjes bevatten geen auteursrechtelijk beschermd materiaal, maar zijn een essentieel technisch hulpmiddel bij de (veelal inbreukmakende) uitwisseling op internet van muziek-, video- en softwarebestanden.[2]

In deze bijdrage besteed ik aandacht aan (1) de kwalificatie en rechtmatigheid van het aanbieden van *bittorrent*-bestanden, (2) de criteria voor de verstrekking van NAW-gegevens van internettoegangsklanten en (3) de criteria voor het op last van de rechter afsluiten van een internetverbinding.

Het aanbieden van torrentbestanden

In r.o. 4.2 – 4.4 oordeelt de voorzieningenrechter kort, krachtig en niet onbegrijpelijk dat het aanbieden van bittorrentbestanden op zich geen directe of indirecte auteursrechtinbreuk behelst, maar onder de omstandigheden wel maatschappelijk onzorgvuldig en dus onrechtmatig is jegens de rechthebbenden wiens rechten daardoor met speels gemak door gebruikers kunnen worden geschonden.

Een elektronische verwijzing naar de beschikbaarheid elders van inbreukmakend materiaal is natuurlijk niet per se onrechtmatig, net zo min als de mededeling op een borrel dat er op het Waterlooplein inbreukmakende spijkerbroeken te vinden zijn. Dat kan onder bijkomende omstandigheden echter anders zijn,[3] zeker als zij derden aanzetten tot het plegen van strafbare feiten.[4] De overwegingen die in dit vonnis de conclusie van onrechtmatigheid dragen, lijken sterk op die van het Hof Amsterdam in de zaak ZoekMP3.[5] Het Hof overwoog dat Techno Design, die de gespecialiseerde zoekmachine voor muziekbestanden ZoekMP3.nl exploiteerde, wist dat 'haar zoekmachine systematisch en structureel zou verwijzen naar ongeautoriseerde openbaarmakingen van auteurs- en nabuurrechtelijk beschermde mp3-muziek-bestanden.' Zij verwierf inkomsten uit advertenties op haar website, die juist bezoekers trok vanwege de beschikbaarheid van verwijzingen naar die inbreukmakende bestanden. De onrechtmatigheid van haar handelwijze was er dan ook met name in gelegen, dat zij 'haar inkomsten dus overwegend althans voor een belangrijk deel [verwierf] door structureel gebruik te maken van de beschikbaarheid op het 'World Wide Web' van ongeautoriseerde mp3-muziekbestanden, klaarblijkelijk zonder rekening te houden met de belangen van de auteurs- en nabuurrechthebbenden.'

Het is een *business model* dat op internet wel vaker voorkomt: geld verdienen aan reclame *banners* op een website door daarop een handige, gestructureerde lijst te presenteren van evident illegaal aanbod elders. Het 'u moet bij de bron zijn'-verweer gaat dan dus niet op.

* Mr. R.D. Chavannes is advocaat bij Brinkhof te Amsterdam en redacteur van dit blad. De titel van dit artikel ontleent hij graag aan de Leidse afscheidsrede van D.W.F. Verkade, *Het belang van een bagatel*, Ars Aequi Libri 2002.

1 Vzr. Rb. Den Haag 5 januari 2007 (*Brein/KPN*), elders in dit nummer gepubliceerd. De uitspraak is ook geannoteerd door O.L. van Daalen in *AMI* 2007-2, nr. 9 en door L.A.R. Siemerink in *Computerrecht* 2007-2.

2 BitTorrent is een peer-to-peer-systeem dat gebruik maakt van een centrale locatie die de downloads coördineert maar zelf geen bestanden levert. De download zelf gebeurt decentraal en bestaat uit het uitwisselen van stukken van bestanden tussen alle gebruikers die op dat moment meedoen aan het up- en downloaden van dat bestand. Zo'n gecoördineerde groep wordt een *torrent* genoemd. Het centrale distributiepunt wordt de *tracker* genoemd. Men wordt met de tracker verbonden zodra een torrentbestand wordt geopend door een BitTorrent-applicatie op de eigen pc. In dit torrentbestand staan de kenmerken van de torrent, zoals de locatie van de tracker en de omvang van het bestand of de bestanden die in de torrent worden uitgewisseld. (Bron: Wikipedia)

3 Zie verder o.a. mijn 'Hype of echt link? De hyperlinksaansprakelijkheid van informatieaanbieders, internetaanbieders en zoekmachines', *JAVI* 2003/1.

4 Zie bijvoorbeeld Pres. Rb. Amsterdam 15 februari 1990, *IER* 1990, 36 (*DNB/Aktueel*): gedetailleerde beschrijving in maandblad hoe bankbiljetten kunnen worden nagemaakt en voor echt uitgegeven is onrechtmatig jegens De Nederlandsche Bank; en Hof Amsterdam 21 februari 2002, *Mediaforum* 2002-4, nr. 10 (*VNU/Canal+*): publicatie van gedetailleerde handleiding hoe gratis Canal+ te kijken door decoder te kraken is onrechtmatig jegens Canal+.

5 Hof Amsterdam 15 juni 2006, *Mediaforum* 2006-10, nr. 33 m.nt. T.F.W. Overdijk (*Brein/Techno Design*), r.o.v. 4.8 e.v.

In de praktijk zal het overigens nog wel eens voorkomen dat inkomsten uit banners dermate laag zijn, dat geen sprake is van een daadwerkelijk commercieel aanbod, maar meer van een uit de hand gelopen hobby met hoogstens commerciële bijbedoelingen. Voor de voorzieningenrechter lijken de commerciële bedoelingen van de aanbieder van dutchtorrent.org niet meer dan een gezichtspunt te zijn. In de zaak *Brein/ZoekMP3* lag dat vermoedelijk anders: het Hof spreekt van de door ZoekMP3 'gedreven onderneming' en baseert zijn onrechtmatigheidsoordeel op het feit dat zij haar inkomsten overwegend verwierf door gebruik te maken van de beschikbaarheid van inbreukmakend materiaal elders op het internet.

Of het aanbieden van ZoekMP3 en dutchtorrent.org wél rechtmatig zou zijn geweest als zij volledig niet-commercieel waren geweest (geen lidmaatschapsbijdrage, geen reclame, etc.), is natuurlijk de vraag. Voor de schade die rechthebbenden lijden, maakt het uiteraard weinig uit of de gedaagde nu € 0,20 of € 20.000,– per maand verdient met zijn site. Inbreuk op auteursrecht is onrechtmatig, ook als de inbreukmaker handelt zonder commercieel oogmerk. Maar de rechter heeft juist expliciet vastgesteld dat het aanbieden van de sites op zich geen auteursrechtinbreuk oplevert, zodat de onrechtmatigheid moet worden geconstrueerd uit bijkomende omstandigheden.

De verstrekking van NAW-gegevens

Relevante toetsingscriteria

Ter beantwoording van de vraag of KPN verplicht kan worden om naam en adres van de onrechtmatig handelende klant te verstrekken, verwijst de voorzieningenrechter (r.o. 4.5) als uitgangspunt naar het arrest *Lycos/Pessers*.[6] Dat arrest erkent een maatschappelijke zorgvuldigheidsnorm die een ISP onder voorwaarden verplicht om NAW-gegevens van een klant te verstrekken, ook als de ISP zelf geen verwijt treft in verband met het gedrag van de klant. Een bij het Hof van Justitie lopende prejudiciële procedure zou deze norm kunnen beïnvloeden, maar in deze zaak valt pas in 2008 een arrest te wachten.[7] De vier voorwaarden zijn in het onderhavige vonnis weergegeven als criteria II, IV, V en VI in r.o. 4.6, waarbij criterium II wat scherper is geformuleerd dan het eerste criterium in *Lycos/Pessers*.

KPN voert echter aan dat in deze zaak twee aanvullende criteria moeten worden aangelegd, te weten: (I) de wijze waarop Brein de wél bekende gegevens omtrent de klant heeft verkregen, mag niet onrechtmatig zijn en (III) het dient buiten redelijke twijfel te zijn dat die gegevens inderdaad herleidbaar zijn tot degene die onrechtmatig heeft gehandeld.

KPN wijst er terecht op dat deze zaak zich onderscheidt van *Lycos/Pessers* en de meeste andere zaken over de verplichtingen van internetaanbieders bij (beweerdelijk) onrechtmatig gedrag van klanten (verwijderen van website, onthullen van NAW-gegevens, etc.), doordat KPN hier alleen optreedt als *access provider* en niet (ook) als *hosting provider*. Anders gezegd, de onrechtmatig bevonden website, die bereikbaar was via het adres www.dutchtorrent.org, stond op de eigen pc van de klant en dus niet op de server van KPN. KPN levert alleen de internetaansluiting waarmee de klant toegang krijgt tot internet en waarmee zijn website van buitenaf beschikbaar is. In beide gevallen is het voor de ISP technisch mogelijk om de website ontoegankelijk te maken. De aansprakelijkheidspositie van internetaanbieders verschilt echter significant al naar gelang het *access* of *hosting* betreft, in die zin dat de *access provider* in beginsel nooit aansprakelijk is voor de inhoud van het internetverkeer van zijn klant (onder de voorwaarden van artikel 6:196c lid 1 BW), terwijl de *hosting provider* onder omstandigheden actief in actie moet komen om niet aansprakelijk te worden voor wat zijn klant bij hem onderbrengt (zie artikel 6:196c lid 4 BW).[8]

Het door KPN voorgestelde criterium III is vermoedelijk afkomstig van de zaak *Brein/UPC* uit 2006, die ook ging over een vordering tot verstrekking van NAW-gegevens in een situatie waarin de ISP als *access provider* optrad, namelijk als ISP van gebruikers die muziek uitwisselden via peer-to-peer programma's. In zijn arrest legde het Hof Amsterdam een 'zwaarder' criterium aan dan dat uit *Lycos/Pessers*: 'Noodzakelijk is allereerst dat niet in redelijkheid kan worden betwijfeld dat de IP-adressen [waarvan de bijbehorende NAW-gegevens werden gevorderd, *RDC*] betrekking hebben op abonnees die illegaal muziekbestanden aanbieden'.[9]

Het Hof legt niet uit waarom in deze *toegangs*situatie een zwaarder criterium heeft te gelden dan in de *hosting*situatie van *Lycos/Pessers*. In zijn noot suggereert Overdijk dat in *hosting*situaties tenminste duidelijk is dat iemand bepaalde informatie op internet aanbiedt. Ik voeg daar nog aan toe dat een website per definitie enigszins statisch is, in die zin dat die doorgaans wel enige tijd online te *zien* is. Historische versies zijn achteraf vaak uit archieven en backups te reconstrueren. De kans is bovendien vrij klein dat een website die op de server van de ISP is geplaatst in de *directory* (folder) van klant X, *niet* van klant X zelf is: alleen die heeft toegang tot die *directory*. Een webadres of e-mailadres kan dus redelijk secuur worden herleid tot één klant, waarvan met enig mate van zekerheid kan worden aangenomen dat die daadwerkelijk verantwoordelijk is voor de bestreden uiting op de website.

Het via internet uitwisselen van bestanden is per definitie vluchtiger en laat minder sporen na. In de zaak *Brein/UPC* wilde Brein de NAW-gegevens die behoorden bij bepaalde IP-nummers van gebruikers waarvan een door Brein ingeschakeld onderzoeksbureau had geconstateerd dat zij op enig moment muziekbestanden hadden aanboden. Een dergelijk informatievergaringsproces is foutgevoeliger, zodat het risico groter is dat iemand die in het geheel geen informatie heeft aangeboden, door de ISP wordt geïdentificeerd en vervolgens blootgesteld aan een civiele actie van Brein. Vandaar de eis dat 'niet in

6 HR 25 november 2005, *Mediaforum* 2006-1, nr. 1 m.nt. A.H. Ekker *(Lycos/Pessers)*. De auteur trad in cassatie op voor Lycos.

7 Zie zaak C-275/06 (*Productores de Música de España/Telefónica*), waarin de Juzgado de lo Mercantil de Madrid op 26 juni 2006 de volgende prejudiciële vraag stelde: 'Is het de lidstaten volgens het gemeenschapsrecht en meer in het bijzonder de artikelen 15, lid 2, en 18 van [de richtlijn Elektronische handel, *RDC*], artikel 8, leden 1 en 2, van [de Auteursrechtrichtlijn, *RDC*], artikel 8 van [de IE Handhavingsrichtlijn, *RDC*], en de artikelen 17, lid 2, en 47 van het Handvest van de grondrechten van de Europese Unie, toegestaan om te bepalen dat operatoren van elektronische communicatienetwerken en -diensten, telecomproviders en hostingproviders de verbindings- en verkeersgegevens betreffende elektronische communicaties die tijdens de verstrekking van een dienst van de informatiemaatschappij tot stand zijn gebracht, slechts ten behoeve van een strafrechtelijk onderzoek of ter bescherming van de openbare of de nationale veiligheid, en dus niet ten behoeve van civiele procedures, dienen te bewaren en ter beschikking te stellen?'

8 Zie over deze kwestie verder uitbreid Van Daalen in zijn noot onder de uitspraak in *AMI* 2007-2, nr. 9.

9 Hof Amsterdam 13 juli 2006, *Mediaforum* 2006-9, nr. 27 m.nt. T.F.W. Overdijk *(Brein/UPC)*, r.o. 4.2.

redelijkheid kan worden betwijfeld' dat de IP-adressen daadwerkelijk betrekking hebben op abonnees die illegaal muziekbestanden aanbieden.

Het is maar de vraag of een dergelijke aanvullende terughoudendheid, verwoord in dit 'zwaardere' criterium, in deze zaak *Brein/KPN* nodig was. Ook hier ging het immers om de onrechtmatigheid van een min of meer statische website en niet van individuele, moeilijk te bewijzen of traceren verkeersstromen. Het risico dat KPN de gegevens van de 'verkeerde' klant aan Brein zou doorgeven, was dus gering. Hoe dat ook zij, de voorzieningenrechter beslist niet expliciet of dit criterium III hier van toepassing is. Hij verwerpt onder verwijzing naar dit criterium het verweer dat er mogelijk meerdere gebruikers onrechtmatig handelden in verband met dutchtorrent.org. Er bestond kennelijk geen onduidelijkheid over wie de klant was waarnaar Brein op zoek was.

Toepassing van de criteria

Opmerkelijk in deze zaak was nog dat de gevraagde NAW-gegevens op zich heel gemakkelijk door Brein konden worden achterhaald (en vermoedelijk al waren achterhaald). Op de website www.dutchtorrent.org kon je op een knopje klikken om de beheerder een financiële bijdrage toe te stoppen voor zijn werk aan de site. Daarbij was een e-mailadres bij een andere provider vermeld, gesteld in de vorm voornaam.achternaam@provider.nl. Dat was bepaald geen veel voorkomende naam: zowel de Telefoongids als Google gaven daarop één hit, met adres en telefoonnummer. Navraag bij de gemeentelijke basisadministratie door de advocaat van Brein kon dus al snel de actuele gegevens bevestigen.

Men kan zich afvragen in hoeverre is voldaan aan de *Lycos/Pessers*-criteria als de verzoeker de gevraagde gegevens met miniem eigen onderzoek met aan zekerheid grenzende waarschijnlijkheid kan achterhalen. Het derde *Lycos*-criterium (in dit vonnis criterium V) is dat 'aannemelijk is dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen.' De exacte betekenis van dit criterium is nooit helemaal duidelijk geworden – minder ingrijpend voor wie? –, maar het ligt voor de hand dat er in elk geval mede wordt gedoeld om de mate van ingrijpendheid voor de ISP. In zijn vonnis (r.o. 4.11) lijkt de voorzieningenrechter vooral oog te hebben voor de mate van bezwarendheid voor de verzoeker, maar als het criterium alleen daarop ziet dan heeft het geen toegevoegde waarde. Voor de *verzoeker* is het immers per definitie het minst bezwarend als de eerste de beste instantie aan wie men de NAW-gegevens vraagt, ze meteen geeft.

Op zich moet voorkomen worden dat een ISP de verzoeker al te gemakkelijk van het kastje naar de muur kan sturen onder verwijzing naar allerlei andere instanties die de gegevens mogelijk zouden hebben. Van belang is daarom ook het vierde criterium (VI in dit vonnis), dat in algemene zin een 'afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder' eist. Het is mij niet bekend waarom Brein de – gemakkelijk te identificeren – persoon niet gewoon heeft gedagvaard. Uiteraard kon voorafgaande bevestiging van de gegevens door de ISP de kans verkleinen dat Brein een juridisch blauwtje zou lopen door aanvankelijk de verkeerde te dagvaarden, maar men kan zich de vraag stellen of dat een zo groot belang is, dat daarvoor de belangen van de (ontegenzeglijk: niet onrechtmatig handelende) ISP opzij geschoven moeten worden. Ik mis in het vonnis een weging van de belangen aan de zijde van KPN, waaronder het bredere belang om niet lichtvaardig te worden geconfronteerd met informatieverstrekkingsverzoeken van beweerdelijk beschadigde derden. Dergelijke verzoeken brengen immers onderzoeks- en juridische kosten met zich mee, terwijl de beslissing om al dan niet te voldoen aan het verzoek steeds juridische en publicitaire risico's met zich brengt (zie ook r.o. 4.13).

Verhouding tot artikel 1019f Rv

De vraag zou kunnen rijzen in hoeverre er in intellectuele eigendomszaken nog plaats is voor de *Lycos/Pessers*-criteria nu de IE Handhavingsrichtlijn per 1 mei is geïmplementeerd.[10] Artikel 1019f Rv, de implementatie van artikel 8 van de richtlijn, luidt als volgt:

> *1. Indien de eiser informatie wenst te verkrijgen van een derde die op commerciële schaal inbreukmakende goederen in zijn bezit heeft of gebruikt, die op commerciële schaal diensten verleent die bij de inbreuk worden gebruikt, of die door een van deze derden is aangewezen als zijnde betrokken bij de productie, fabricage of distributie van deze goederen of bij het verlenen van deze diensten, kan de rechter op gerechtvaardigde en redelijke vordering van de eiser een getuigenverhoor bevelen over al hetgeen de derde bekend is over de herkomst en de distributiekanalen van de inbreukmakende goederen of diensten. Dit verhoor heeft enkel betrekking op het verkrijgen van de in dit lid bedoelde informatie.*
>
> *2. Naast of in plaats van verhoor van een getuige ter terechtzitting, kan ook overlegging gevraagd worden van de in het tweede lid bedoelde informatie in schriftelijke vorm door de getuige.*

Zou Brein de volgende keer de ISP als getuige kunnen oproepen en zou de ISP dan de NAW-gegevens moeten verstrekken, zonder dat aan de hierboven besproken criteria voldaan zou hoeven worden? Ik denk het niet. Uit de parlementaire geschiedenis volgt dat de bevoegdheid van artikel 1019f Rv alleen beschikbaar is in zaken waarin de vermeende inbreukmaker bekend is en gedagvaard is, en niet bedoeld is voor zaken zoals deze:

> *Het vorderen van NAW-gegevens zoals opgenomen in artikel 8 van de richtlijn en zoals dienovereenkomstig geïmplementeerd in dit wetsvoorstel, betreft een vordering die onderdeel is van een procedure waarbij de inbreukmaker is gedagvaard, beëindiging van de inbreuk wordt gevorderd en daarnaast nevenvorderingen kunnen worden ingesteld, zoals de vordering tot het verstrekken van NAW-gegevens over derden die onderdeel zijn van de inbreukketen.*
> *[...]*
> *Dit artikel is niet bedoeld om een internetprovider te dagvaarden met het doel de NAW-gegevens van websitehouders te achterhalen. Daarvoor blijft het huidige kort geding of een bodemprocedure de aangewezen procedure. Overigens kunnen artikel 8 van de richtlijn en artikel 1019f Rv wel van invloed zijn op dergelijke civiele procedures. Nu met zoveel woorden in de wet is opgenomen dat tussenpersonen en andere betrokkenen bij een inbreuk tijdens een procedure tegen de inbreukmaker kunnen worden opgeroepen om aan de rechthebbende informatie over andere schakels in de inbreukketen te verstrekken, valt niet in te zien waarom zij dat onder omstandigheden (zie Hoge Raad 25 november 2005, RvdW 2005, 133, Lycos/Pessers) niet ook zouden kunnen in een op zichzelf staande (kortgeding)procedure*

10 Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (*PbEG* L 195), geïmplementeerd bij Wet van 8 maart 2007, *Stb.* 2007, 108. Voor de parlementaire geschiedenis, zie *Kamerstukken* 30 392.

waarin de internetprovider wordt gedagvaard teneinde NAW-gegevens van een websitehouder te verstrekken.[11]

Zo lang de wet niet voorziet in de mogelijkheid om iemand anoniem te dagvaarden en om anoniem in een procedure te verschijnen – zodat Brein de internetgebruiker rechtstreeks zou kunnen dagvaarden –, blijft men dus aangewezen op een kort geding tussen rechthebbende en ISP zoals hier gevoerd.

De afsluiting van de internetverbinding

In het kader van het voorkomen van verder onrechtmatig handelen door de KPN-klant, vordert Brein ook dat KPN de internetaansluiting van de klant afsluit en afgesloten houdt. De voorzieningenrechter overweegt (r.o. 4.14) dat in beginsel voldoende tegemoet wordt gekomen aan het belang van Brein doordat de NAW-gegevens worden verstrekt: daarmee kan Brein immers de website-aanbieder dagvaarden. De voorzieningenrechter vervolgt echter met een in algemene bewoordingen gestelde norm:

Indien KPN echter gewezen wordt op kennelijk (onmiskenbaar) onrechtmatige gedragingen van haar abonnees op het internet, kan zij niet volstaan met het verstrekken van de NAW-gegevens, maar is zij daarnaast gehouden de betreffende verbinding af te sluiten.

De voorzieningenrechter lost het vervolgens heel elegant op door vordering slechts gedeeltelijk – voorwaardelijk – toe te wijzen: KPN hoeft te klant pas af te sluiten als deze in de toekomst via een KPN-verbinding dezelfde onrechtmatige website gaat aanbieden. Dat is voor deze zaak een uitkomst waarmee goed valt te leven. Dat laat onverlet dat de algemene norm mijns inziens onjuist en onwenselijk is. Zo gesteld lijkt het er namelijk op dat de rechtsregel voor *hosting providers* – die een website moeten afsluiten als zij worden gewezen op het onmiskenbaar onrechtmatige karakter daarvan, op straffe van aansprakelijkheid voor de inhoud van de website – één-op-één wordt toegepast op *access providers*. Een dergelijke norm is mijns inziens te algemeen geformuleerd en daarom in strijd met artikel 12 lid 3 van de E-commerce richtlijn en met artikel 10 EVRM. Kort gezegd: het enkele feit dat een internetgebruiker (onmiskenbaar) onrechtmatig handelt, rechtvaardigt niet het afsluiten van zijn internetverbinding.

De voorzieningenrechter motiveert de gestelde norm door verwijzingen naar de uitspraken inzake Scientology en Deutsche Bahn. Deze lijken mij in deze context echter niet doorslaggevend, omdat die zaken betrekking hebben op *hosting* providers, waarin het materiaal gehost was bij de provider zelf. Artikel 6:196c lid 5 BW stelt weliswaar in algemene zin, dus ten aanzien van zowel *access providers* als *hosting providers,* dat de voorgaande beperkingen van aansprakelijkheid niet in de weg staan aan het verkrijgen van een rechterlijk verbod of bevel. Die bepaling dient echter te worden geïnterpreteerd in overeenstemming met de bepalingen van de E-commerce richtlijn waarvan zij de implementatie vormt, te weten de artikelen 12 lid 3 respectievelijk 14 lid 2. Die bepalingen zijn, anders dan artikel 6:196c lid 5 BW, beperkt geformuleerd want voorzien slechts in de mogelijkheid om te eisen dat de aanbieder 'een inbreuk beëindigt of voorkomt.' Ten aanzien van *hosting providers* laat artikel 14 lid 2 bovendien nog de mogelijkheid open voor lidstaten 'om procedures vast te stellen om informatie te verwijderen of de toegang daartoe onmogelijk te maken.' Deze bepalingen rechtvaardigen dus niet ieder rechterlijk verbod of bevel maar alleen een verbod of bevel dat ziet op het voorkomen of beëindigen van *concrete* inbreuken.

Artikel 12 lid 3 van de richtlijn staat dus toe dat de rechter KPN verplicht om toegang tot de onrechtmatig bevonden website te voorkomen, maar niet om de klant geheel af te sluiten.

Dat brengt mij vanzelf op een andere reden waarom de verwijzing naar de zaken *Scientology* en *Deutsche Bahn* in dit geval maar beperkt relevant zijn. Een verwijderingsbevel aan een *hosting provider* is een veel beperktere ingreep dan een afsluitingsbevel aan een *access provider*. Een *verwijderings*bevel treft immers slechts de – onmiskenbaar onrechtmatig bevonden – website, terwijl een *afsluitings*bevel de klant volledig afsluit van het internet en dus niet alleen die ene onrechtmatige uiting raakt maar ook alle andere (toekomstige) communicatie van de klant, waaronder alle rechtmatige communicatie. Een afsluitingsbevel betekent dat de gebruiker niet meer kan e-mailen, internetbankieren, deelnemen aan discussiegroepen, etc. Het gaat dus aanzienlijk verder dan slechts het beëindigen of voorkomen van een inbreuk en treft ook allerlei volkomen legitieme gedragingen van de klant, zowel eigen uitingen als de ontvangst van informatie van derden.

Het volledig afsluiten van een internetverbinding is dus niet alleen een verdergaande maatregel dan artikel 12 lid 3 van de E-commerce richtlijn toelaat, maar tegelijkertijd een aanzienlijke beperking van zowel de uitings- als de ontvangstvrijheid. Toegang tot het internet is in het huidige tijdperk misschien niet een even basale levensbehoefte als water of elektriciteit. Het belang van internet en dus internettoegang voor de alledaagse informatievoorziening, het handelsverkeer en (volwaardige deelname aan) het publieke leven en het publieke debat, is echter onmiskenbaar. Dat betekent dat slechts in tamelijk uitzonderlijke situaties plaats is voor het op last van de rechter volledig afsluiten van iemands internetverbinding.

De in deze uitspraak geformuleerde, algemene norm – afsluiten bij kennelijk onrechtmatig gedrag op het internet – leidt in de praktijk tot de oplegging van een maatregel die mijns inziens niet proportioneel is. Nog los van de vraag of het belang van Brein zwaarder moet wegen dan het hier geschetste belang van het hebben van internettoegang, geldt dat er een minder vergaande maatregel denkbaar is die ook tegemoet komt aan het belang van Brein, te weten een gebod om toegang tot de website onmogelijk te maken. KPN zou zo'n gebod bijvoorbeeld kunnen uitvoeren door inkomend verkeer naar de eigen webserver van de klant te blokkeren, of door de klant simpelweg te verplichten om zijn webserver op te doeken. Het bij wijze van bijvangst beperken van zogenoemde *legitimate speech* is voor het Supreme Court herhaaldelijk aanleiding geweest om wetten ongrondwettelijk te verklaren.[12] Ook naar Nederlands en Europees recht dient een beperking nauwkeurig geformuleerd te worden en niet verder te gaan dan noodzakelijk. In dit geval is daar mijns inziens niet aan voldaan.

11 Nota naar aanleiding van het verslag, *Kamerstukken II* 2005-2006, 30 392, nr. 6, pp. 3 en 7.

12 Zie bijvoorbeeld *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) en, zeer recent, over de ongeldigheid wegens strijd met de vrijheid van meningsuiting van de Child Online Protection Act: *ACLU vs. Gonzales*, Eastern District of Pennsylvania, Final Order, 98-5591, 22 maart 2007, http://www.paed.uscourts.gov/documents/opinions/07D0346P.pdf.

De implementatie van de IE Handhavingsrichtlijn heeft ons ook artikel 26d Auteurswet gebracht: 'De rechter kan op vordering van de maker, tussenpersonen wier diensten door derden worden gebruikt om inbreuk op het auteursrecht te maken, bevelen de diensten die worden gebruikt om die inbreuk te maken, te staken.' Los van het feit dat in geval de website-houder géén auteursrechtinbreuk pleegde, geldt ook bij de toepassing van deze bevoegdheid een strikte proportionaliteitstoets.[13]

Overigens is een afsluitingsbevel betrekkelijk zinloos, omdat de gebruiker elders een abonnement kan afsluiten en de website kan hosten op een buitenlandse server. De enige echt effectieve oplossing zou zijn om een soort algemeen internettoegangsverbod in de wet op te nemen. Onder de noemer '*three strikes and you're out*' zou kunnen worden bepaald dat een internetgebruiker waarvan drie keer is vastgesteld dat deze zich online ernstig onrechtmatig heeft gedragen, op een zwarte lijst komt te staan en geen internettoegang meer mag. Het enge is dat zo'n bevoegdheid redelijk werkbaar zou zijn, omdat het bieden van internettoegang – anders dan het bieden van hosting ruimte – per definitie locatiegebonden is (je kunt moeilijk internettoegang afnemen van een buitenlandse aanbieder want die biedt niet aan in Nederland). Het zou dus in theorie mogelijk zijn om in de Telecommunicatiewet een verplichting op te nemen om geen internettoegangsdiensten te leveren aan personen die op een bepaalde zwarte lijst voorkomen. Natuurlijk kunnen zij dan nog naar internetcafés en in het buitenland internetten, maar dat zijn geen dagelijks bruikbare alternatieven.

Er zullen ongetwijfeld belanghebbenden zijn die een dergelijke bevoegdheid zouden verwelkomen – op zo'n manier kunnen we ook mensen die herhaaldelijk opruiende teksten op internet plaatsen of die bepaalde genocides ontkennen, tijdelijk of permanent uit hun actief en passief internetrecht ontzetten. Dat hier de grenzen van artikel 10 EVRM ruimschoots worden overschreden, moge duidelijk zijn.

Conclusie

Maken wij ons in bladen zoals *Mediaforum* te druk over kortgedinguitspraken zoals deze, gewezen door een voorzieningenrechter die, gezien de functie en beperkingen van de procedure in kort geding, vooral oog heeft voor de beslechting van het aan hem voorgelegde geschil en zich, zeker in eerste aanleg, niet hoeft te bekommeren over de bruikbaarheid van de door hem gehanteerde criteria of methoden in andere feitencomplexen? Het is op zich begrijpelijk dat de voorzieningenrechter weinig zin had om de vordering tot verstrekking van NAW-gegevens af te wijzen, gegeven dat er een gedaagde tegenover hem stond die over de gegevens beschikte en wiens klant kennelijk onrechtmatige activiteiten ontplooide. Ik kan mij vinden in de elegante beslissing op de vordering tot afsluiting. Als de uitspraak in het geheel geen precedentwaarde zou hebben, had een korte annotatie volstaan.

De realiteit van het 'internetrecht' is echter dat er vrijwel uitsluitend uitspraken in kort geding zijn die, bij gebrek aan hardere precedenten, in volgende zaken worden aangehaald, door partijen en door rechters. Dat betekent dat een uitspraak als deze wel degelijk belangrijk is, met name voor wat betreft (a) *welke* criteria worden gehanteerd bij de beoordeling van vorderingen tot verstrekking van NAW-gegevens en afsluiting van internetverbindingen; en, even belangrijk (b) *hoe streng* die criteria *in concreto* worden toegepast. Wat dat betreft schept deze uitspraak mijns inziens een onwenselijk precedent: de norm voor afsluiting is te algemeen en absoluut, terwijl ten aanzien van de NAW-gegevens de lat voor Brein te laag is gelegd door verstrekking te bevelen van gegevens die Brein al had of vrij makkelijk zelf had kunnen vinden. Als de criteria uit *Lycos/Pessers* op deze manier gehanteerd (moeten) worden, dan brengt dat het risico met zich mee dat ISP's zullen concluderen dat het op deze manier opkomen voor de privacy klanten een dure en onzekere – zo niet zinloze – exercitie is. Sinds de inwerkingtreding van de Wet bevoegdheden vorderen gegevens telecommunicatie en de Wet vorderen gegevens moeten zij al blind voldoen aan NAW-verzoeken van iedere opsporingsambtenaar van Nederland – waarom nog weerwoord bieden aan civiele vorderingen van (beweerdelijk) beschadigde burgers?

13 *Kamerstukken II* 2005-2006, 30 392, nr. 6, p. 10: 'Zoals is aangegeven in de memorie van toelichting bij de Aanpassingswet richtlijn inzake elektronische handel (*Kamerstukken II* 2001/02, 29 197, nr. 3, p. 51 en 65) moet de verwijdering van de website redelijkerwijs kunnen worden gevergd. De verlangde maatregel moet derhalve evenredig zijn ten opzichte van de inbreuk. Het moet voor de tussenpersoon mogelijk zijn om tegen aanvaardbare kosten en met personele en technische maatregelen op te treden. *Er mogen geen andere, minder verstrekkende mogelijkheden openstaan om een einde te maken aan de onrechtmatige situatie en de gevorderde maatregelen mogen niet verder strekken dan strikt noodzakelijk*.'