De provider als speurhond van de muziekindustrie. Kan hij gedwongen worden tot afgifte van identificerende informatie?

gepubliceerd in *JAVI* 2003/4, p. 129-134

Anton Ekker en Ot van Daalen[1]

1. Inleiding

Nu de strijd tegen de producenten van Kazaa en Napster lijkt te zijn verloren richt de muziekindustrie zich op de gebruikers van filesharingsoftware. De identiteit van deze gebruikers is vaak onbekend, en kan dan slechts met de hulp van een provider worden achterhaald. Het Amerikaanse District Court van Columbia oordeelde onlangs in de zaak *RIAA v. Verizon* dat een provider verplicht kan zijn om de gegevens van een Kazaa-gebruiker te onthullen op verzoek van een rechthebbende.

Dit artikel behandelt onder welke omstandigheden naar Nederlands recht voor een provider een verplichting bestaat om in gevallen van auteursrechtinbreuk identificerende informatie af te staan. Eerst wordt ingegaan op de *Verizon* zaak. Vervolgens komen de Richtlijn elektronische handel, de implementatiewet van de richtlijn, en de rechtspraak aan de orde.

Het artikel concludeert dat een provider niet verplicht is om zonder tussenkomst van de rechter de gegevens te onthullen van een Kazaa-gebruiker die auteursrechtinbreuk pleegt. De rechter dient een dergelijk bevel slechts met grote terughoudendheid te geven. De schrijvers doen vervolgens enige suggesties ter bescherming van de belangen van de internetgebruiker.

2. Filesharing: de achtergrond

---

[1]Anton Ekker schrijft een proefschrift over anonimiteit en uitingsvrijheid op het internet bij het Instituut voor Informatierecht van de Universiteit van Amsterdam. Ot van Daalen doet bij hetzelfde instituut onderzoek naar het telecommunicatierecht. Dit document is gedeeltelijk geschreven in LateX-formaat met behulp van GNU Emacs op GNU/Linux.

Opslagdienst en doorgeefluik

De meeste providers vervullen twee taken. Enerzijds bieden zij hun abonnees schijfruimte en bandbreedte waarmee informatie toegankelijk kan worden gemaakt op het internet, bijvoorbeeld door middel van een website. Deze vorm van dienstverlening noemt men *hosting*. Daarnaast verlenen de meeste providers hun abonnees ook internettoegang. Hierbij fungeert de provider slechts als doorgeefluik van de data die de computer van de gebruiker verzendt en ontvangt. Deze vorm van dienstverlening noemt men *mere conduit*.

Om de doorgifte van informatie mogelijk te maken kent de provider aan de computer van de abonnee een uniek internet-adres, of 'IP-adres' toe. Aan de hand van dit adres kan de provider de identiteit achterhalen van een abonnee die bepaalde informatie aanbiedt of ontvangt. Een rechthebbende die de gegevens van een internetgebruiker wil achterhalen wendt zich daarom al snel tot de provider.

Filesharing

Een filesharingprogramma (ook wel peer-to-peer of P2P-systeem genoemd) stelt gebruikers in staat om via het internet bestanden uit te wisselen.[2] Gebruikers van hetzelfde programma hebben toegang tot elkaars bestanden en kunnen die ook kopiëren. Napster was lange tijd het meest gebruikte filesharingprogramma totdat het tengevolge van juridische gevechten haar diensten moest staken. Kazaa heeft de rol van Napster overgenomen en is nu het meest gebruikte filesharingprogramma. In de praktijk wordt Kazaa ook gebruikt voor de uitwisseling van muziekbestanden zonder toestemming van de rechthebbenden.

De Recording Industry Association of America (RIAA), de Amerikaanse muziekrechthebbendenorganisatie, probeert de uitwisseling van haar muziek via deze uitwisselnetwerken tegen

---

[2] Voor een meer diepgaande behandeling van de technische en juridische aspecten van filesharing verwijzen wij hier naar 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.

te gaan. Deze pogingen hebben aanleiding gegeven tot de beslissing in *RIAA v. Verizon*, die hieronder aan de orde komt.

3. De zaak *RIAA v. Verizon*

Het Amerikaanse Congres, de federale wetgever, heeft in 1998 de Digital Millenium Copyright Act (DMCA) aangenomen.[3] Deze wet zou de Amerikaanse auteurswet voorbereiden op het digitale tijdperk. De DMCA introduceerde een nieuw artikel 512, dat de aansprakelijkheid van providers voor auteursrechtinbreuk beperkt.[4] Het Congres heeft in dit artikel gekozen voor een 'safe harbor' systeem: een provider is niet aansprakelijk voor auteursrechtinbreuk — een safe harbor — mits hij voldoet aan bepaalde voorwaarden. In dit verband is lid (h) van artikel 512 van belang, dat de afgifte van persoonsgegevens door ISPs regelt.

Artikel 512(h)

Om inbreukmakers te kunnen opsporen, kan een rechthebbende via artikel 512(h) een 'subpoena to identify an infringer' verkrijgen. Dit is een bevel om een inbreukmaker te onthullen (hierna: identificatiebevel). Ter verkrijging van een identificatiebevel dient een rechthebbende een verzoek in bij het District Court, de lagere rechter, dat vergezeld moet zijn van:

1. een kopie van de kennisgeving aan de provider dat sprake is van een auteursrechtinbreuk,

2. een voorstel voor het uit te vaardigen bevel en,

3. een verklaring van de auteursrechthebbende dat het bevel alleen bedoeld is om een inbreukmaker te identificeren en dat de verkregen informatie alleen zal worden gebruikt om de auteursrechten van de indiener te beschermen.

Het District Court toetst het verzoek niet inhoudelijk. Als aan de bovenstaande formele eisen is voldaan, wordt het bevel afgegeven. De provider die een dergelijk bevel ontvangt, is verplicht om de identiteit van de inbreukmaker onmiddellijk

---

[3] Pub. L. 105-304 (1998).
[4] 17 U.S.C. § 512.

aan de auteursrechthebbende of diens vertegenwoordiger bekend te maken.

Er bestaat in de Verenigde Staten een aantal uitspraken over het onthullen van identificerende gegevens door providers in gevallen van belediging, racisme of andere onrechtmatige uitingen.[5] De rechter hanteert in deze zogenaamde 'John Doe' procedures strenge criteria voor de afgifte van gegevens, teneinde de anonimiteit van een internetgebruiker te beschermen. De terughoudende aanpak in deze John Doe procedures staat in contrast met de regeling van artikel 512(h). Een *vermoeden* van auteursrechtinbreuk is al voldoende om een identificatiebevel te verkrijgen op grond van dit artikel. Overigens moet wel worden opgemerkt dat artikel 512(f) een schadevergoedingsactie schept voor degene die schade heeft geleden door een ongegronde kennisgeving van auteursrechtinbreuk en een daaruit voortvloeiende verstrekking van identificerende gegevens. Het leed is dan echter al geschied.

Artikel 512(h) is al eerder gebruikt om de gegevens van abonnees te achterhalen. Tot een rechtszaak over de geldigheid van zo een bevel was het echter nog niet gekomen. Dit verandert op 6 augustus 2002 wanneer provider Verizon weigert te voldoen aan een identificatiebevel van de RIAA. Na een vruchteloze correspondentie vordert de RIAA op 20 augustus een gebod bij de rechter om het identificatiebevel te handhaven.

Het District Court

Op 21 januari 2003 wijst het District Court for the District of Columbia het handhavingsverzoek toe.[6] Na een opschorting van deze beslissing, hangende een beroep bij het Court of Appeals, vaardigt het District Court op 4 februari 2003 een nieuw identificatiebevel uit. Een verzoek van Verizon aan het District Court om het nieuwe bevel te vernietigen is ook afgewezen op

---

[5] Zie bijvoorbeeld *Doe v. 2TheMart.com, Inc.,* 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001); *In re Subpoena Duces Tecum to America On-line, Inc.,* 52 Va. Cir. 26 (Cir. Ct. Fairfax County 2000); *Dendrite International, Inc. v. Doe,* 342 N.J. Super. 134 (App. Div. 2001).

[6] In re: Verizon Internet Services, Inc., Subpoena Enforcement Matter, 240 F. Supp. 2d 24 (D.D.C. 2003). Zie ook het archief van de EFF over deze zaak: http://www.eff.org.

24 april 2003.[7] De twee vonnissen worden hieronder gezamenlijk behandeld.

Verizon beroept zich ten eerste op de tekst en strekking van artikel 512(h). Dit artikel zou zich beperken tot situaties waar sprake is van hosting, en niet van toepassing zijn op ISPs die fungeren als doorgeefluik. Zo zou een internetgebruiker een hogere 'expectation of privacy' hebben met betrekking tot informatie die op zijn eigen computer is opgeslagen. Het District Court verwerpt dit argument. Uit de tekst, geschiedenis en doelstelling van artikel 512(h) blijkt dat dit artikel zich niet beperkt tot de identificatie van abonnees van hostingproviders, aldus de rechter. Een dergelijke beperkte interpretatie van het artikel "would create a huge loophole in Congress's effort to prevent copyright infringement on the Internet."

Verizon betoogt daarnaast dat artikel 512(h) in strijd is met het First Amendment, dat het recht op vrijheid van meningsuiting beschermt. Dit recht omvat ook het recht op anonimiteit. Artikel 512(h) voorziet niet in voldoende procedurele waarborgen om de vrijheid van meningsuiting van internetgebruikers te beschermen, omdat het District Court een identificatiebevel uitvaardigt zonder inhoudelijke toetsing van het verzoek. Het identificatiebevel kan daarnaast worden verkregen zonder dat de desbetreffende internetgebruiker op de hoogte wordt gesteld van de poging om zijn identiteit te achterhalen en zonder een voorafgaande mogelijkheid voor de ontvanger van het bevel om gehoord te worden. Ook dit argument vindt geen weerklank bij de rechter. Auteursrechtinbreuk is niet een uiting die het First Amendment beschermt. De rechter kan daarnaast auteursrechtelijke wetgeving slechts marginaal toetsen. Deze conclusie baseert de rechter op de uitspraak van het Supreme Court in Eldred v. Ashcroft.[8]

Verizon is tegen beide beslissingen in beroep gegaan. Inmiddels hebben 47 belangenorganisaties zich als 'amici curiae' in het beroep geschaard aan de zijde van Verizon. In afwachting van een definitieve uitspraak in beroep heeft het Court of Appeals op 4 juni 2003 een verzoek om de uitvoering van het identificatiebevel op te schorten, afgewezen. Verizon heeft

---

[7] In re Verizon Internet Services, 2003 U.S. Dist. LEXIS 6769 (D.D.C. 2003).
[8] Eldred v. Ashcroft, 537 U.S. 186 (2003).

daarom besloten om de namen van de bewuste gebruikers vrij te geven. Voorlopig heeft de muziekindustrie dus gewonnen.

4. De Richtlijn Elektronische Handel

Op Europees niveau bestaat geen regeling die vergelijkbaar is met artikel 512(h) van de Amerikaanse Copyright Act. Noch de algemene privacyrichtlijn, noch de Richtlijn privacy in de telecommunicatiesector bevat regels over het afgeven van identificerende gegevens door een provider.[9] De Richtlijn Elektronische Handel bevat evenmin een dergelijke bepaling.[10]

De laatste Richtlijn biedt wel enige aanknopingspunten voor een beoordeling van een plicht om identificerende gegevens af te staan. In overweging 14 van de Richtlijn wordt terecht geconstateerd dat de richtlijn het anonieme gebruik van open netwerken zoals internet niet kan voorkomen. Artikel 15 lid 2 bepaalt daarnaast dat de lidstaten kunnen voorschrijven dat dienstverleners de bevoegde autoriteiten op hun verzoek informatie dienen te verstrekken waarmee de afnemers van hun dienst met wie zij opslagovereenkomsten hebben gesloten, kunnen worden geïdentificeerd. Deze bepaling is gericht op de strafvordering, zo blijkt uit de toelichting bij het Gemeenschappelijk Standpunt van Raad.[11]

Daarnaast heeft het Europese Parlement in eerste lezing een amendement voorgesteld voor een nieuwe overweging 9bis.[12] Overweging 9bis zou stellen dat de verleners van diensten van de informatiemaatschappij in staat moeten zijn om alle nuttige informatie te verstrekken voor het opsporen en identificeren van leveranciers van onwettige inhouden. Dit amendement is echter niet in het gewijzigd voorstel opgenomen omdat een dergelijke overweging zou kunnen worden geïnterpreteerd op een wijze die in strijd is met de regels inzake de bescherming van persoonlijke gegevens, aldus de Raad.[13] Het Parlement geeft in haar verslag in tweede lezing toe dat de voorgestelde

---

[9] Richtlijn 95/46/EG, *PbEG* 1995 L 281/31 en Richtlijn 2002/22/EG, *PbEG* 2002 L 201/37.
[10] Richtlijn 2000/31/EG, *PbEG* 2000 L 178/1.
[11] *PbEG* 2000 C 128/32, overweging B.1.b.
[12] *PbEG* 1999 C 279/389.
[13] Zie paragraaf 2.3.2 van de toelichting bij het gewijzigd voorstel d.d. 17 augustus 1998, COM(1999) 427 def., *PbEG* 2000 C 248/96.

wijzigingen in eerste lezing zich inderdaad slecht verhouden met het recht op privacy.[14]

5. De Implementatiewet

De implementatiewet van de Richtlijn elektronische handel, die op dit moment bij de Tweede Kamer ligt, bevat twee artikelen die de aansprakelijkheid van tussenpersonen voor doorgifte en opslag van informatie regelen. De civielrechtelijke aansprakelijkheid zal worden bestreken door een nieuw artikel 6:196c van het Burgerlijk Wetboek. Dit artikel is een vrijwel letterlijke kopie van de artikelen 12 tot en met 14 van de richtlijn. Een nieuw in te voegen artikel 54a Wetboek van Strafrecht zou de strafrechtelijke aansprakelijkheid van tussenpersonen op het internet regelen. Hieronder komt de ontstaansgeschiedenis van beide bepalingen kort aan de orde.

Artikel 6:196c BW

In de Memorie van Toelichting bij de implementatiewet gaat de Minister in op de mogelijkheid dat de civiele rechter een provider opdraagt om de bron van onrechtmatige informatie bekend te maken.[15] Een dergelijk bevel kan alleen worden gegeven indien de provider redelijkerwijs in staat is om aan die verplichting te voldoen.[16] Hiervan is sprake, zo blijkt uit de toelichting, als de provider in een contractuele relatie staat met de abonnee, "los van de precieze inhoud daarvan", waarvan de persoonsgegevens worden opgevraagd. Een dergelijke contractuele relatie is waarschijnlijk aanwezig tussen de ISP die internettoegang verschaft en de abonnee. Een redenering *a contrario* leidt tot de conclusie dat zonder bevel van de rechter de provider niet verplicht is tot het afstaan van persoonsgegevens.

De wetgever hanteert daarnaast een technologieneutrale interpretatie van artikel 15 lid 2 van de richtlijn. Hoewel artikel 15 lid 2 spreekt van "opslagdiensten," kan volgens de Minister "worden aangenomen dat ook de dienstverlener die doorgifte-overeenkomsten heeft gesloten, onder omstandigheden binnen de reikwijdte van die bepaling kan vallen, bijvoorbeeld in

---

[14] A5-0106/2000, p. 10.
[15] *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 28.
[16] *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 51.

gevallen waarin door technische ontwikkelingen niet langer gebruik gemaakt behoeft te worden van «host»-diensten en de bedoelde gegevens slechts te achterhalen zijn via de dienstverlener die een doorgifte-overeenkomst met de afnemer heeft gesloten."[17] De Minister suggereert dat een dergelijke technologieneutrale interpretatie ook in civielrechtelijke context op zijn plaats is.

Men kan bij deze technologieneutrale interpretatie twee vraagtekens stellen.[18] Ten eerste staat technologieneutrale regulering binnen strafrechtelijke context op gespannen voet met het rechtszekerheidsbeginsel. Maar daarnaast is niet zeker dat een dergelijke interpretatie wel in overeenstemming is met de richtlijn. De tekst van de richtlijn is immers duidelijk: het betreft hier *opslagovereenkomsten*. Dit artikel hanteert echter het uitgangspunt dat een dergelijke interpretatie richtlijnconform is.

Artikel 54a WvSr

Het nieuwe artikel 54a Wetboek van Strafrecht ziet op de strafrechtelijke aansprakelijkheid van tussenpersonen voor onrechtmatige of strafbare informatie op het internet. Aangezien auteursrechtinbreuk ook een strafbaar feit is, kan dit artikel relevant zijn bij vervolging door het Openbaar Ministerie. Een tussenpersoon wordt krachtens artikel 54a niet vervolgd als hij alle maatregelen neemt die redelijkerwijs van hem kunnen worden gevergd om onrechtmatige informatie ontoegankelijk te maken. Uit het artikel volgt echter geen verplichting om identificerende gegevens bekend te maken. Zoals in de Memorie van Toelichting wordt opgemerkt staat de Richtlijn elektronische handel in de weg aan een bepaling die aan de niet-vervolgbaarheid van de provider de voorwaarde verbindt dat de dader bekend wordt gemaakt.[19] Het wetsvoorstel Vorderen gegevens telecommunicatie voorziet overigens *wel* in een wettelijke bevoegdheid tot het vorderen van gebruiksgegevens betreffende personen die gebruik maken van telecommunicatienetwerken of –diensten bij verdenking van

---

[17] *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 28.
[18] Anders: C.B. van der Net, "De civielrechtelijke aansprakelijkheid van de internetprovider na de Richtlijn elektronische handel", *JAVI* 2002/1, p. 13.
[19] *Kamerstukken II* 2001/02, 28 197, nrs. 3, p. 66.

strafbare feiten.[20] Op de verstrekking van identificerende gegevens in de strafrechtelijke sfeer wordt hier verder niet ingegaan.

6. De IE-Richtlijn

In het voorstel voor de nieuwe Europese Richtlijn inzake maatregelen en procedures om de handhaving van intellectuele eigendomsrechten te waarborgen (hierna: IE-Richtlijn) is een bepaling opgenomen die een vordering tegen de provider wellicht mogelijk zou maken.[21] Artikel 9 van deze Richtlijn is een uitwerking van het recht op informatie van de auteursrechthebbende en de daarmee corresponderende verplichting van de inbreukmaker tot het noemen van zijn voorman, zoals vastgelegd in artikel 47 van het TRIPS-verdrag. De lidstaten moeten in hun nationale wetgeving bepalen dat rechterlijke autoriteiten op verzoek van de rechthebbende iedere persoon kunnen gelasten informatie te verstrekken over de herkomst en de distributiekanalen van de goederen of diensten die worden verondersteld inbreuk te maken op een intellectuele-eigendomsrecht.[22] Dit geldt, als deze persoon a) de litigieuze goederen voor commerciële doeleinden in zijn bezit blijkt te hebben, b) de litigieuze diensten voor commerciële doeleinden blijkt te gebruiken, of c) door een onder a) of onder b) bedoelde persoon is aangewezen als degene van wie deze goederen of diensten afkomstig zijn, of als schakel in het distributienet van deze goederen of diensten. Het gaat hier om de namen en adressen van producenten, distributeurs, leveranciers en andere eerdere bezitters van het product of de dienst.

Artikel 9 lijkt zich met name te richten op klassieke vormen van *counterfeiting*, en ziet waarschijnlijk niet op de illegale verspreiding van informatieproducten op het internet. Het is bijvoorbeeld de vraag of het fungeren als doorgeefluik is aan te merken als het gebruiken van een litigieuze dienst voor

---

[20] *Kamerstukken II* 2000/01, 28 059.

[21] COM(2003) 46 def.

[22] In Nederland kennen wij een dergelijke wettelijke bepaling nog niet. Wel kan in een procedure over inbreuken op intellectuele eigendomsrechten volgens vaste jurisprudentie een bevel worden verkregen tot het verstrekken van een lijst met namen en adressen van afnemers en leveranciers.

commerciële doeleinden. Artikel 9 lijkt daarnaast weinig geschikt om in de digitale omgeving te worden toegepast. Bij de bestrijding van counterfeiting spelen de belangen van het recht op privacy en de communicatievrijheid doorgaans geen rol. Waarborgen om deze belangen te beschermen geeft het artikel dan ook niet. Omdat het hier gaat over een voorstel wordt verder niet ingegaan op artikel 9 IE-richtlijn.

7. Jurisprudentie

De identificatieplicht van de provider is tot nu toe in vier rechtszaken aan de orde gekomen. Het ging in twee zaken over een provider van hostingdiensten, en in twee zaken over een provider van e-maildiensten. De vier rechtszaken komen hieronder aan de orde.

De vraag of een provider gedwongen kan worden om identificerende gegevens van een abonnee af te staan is voor het eerst aan de orde gekomen in de zaak *Scientology/XS4ALL*.[23] Hier oordeelde de Haagse Rechtbank over de onrechtmatige publicatie van auteursrechtelijk beschermde werken via de hostingdienst van, onder andere, XS4ALL. Scientology, de rechthebbende, vorderde dat XS4ALL de bestanden ontoegankelijk zou maken en de namen en adressen van de betreffende abonnees zou afstaan. De Rechtbank besliste dat een provider verplicht is om naam en adres van een gebruiker af te staan als hij van het onrechtmatige karakter van de informatie in kennis is gesteld, en aan de juistheid van deze kennisgeving in redelijkheid niet valt te twijfelen. Uit de toelichting bij de implementatiewet van de Richtlijn elektronische handel blijkt dat aan de juistheid van de kennisgeving niet kan worden getwijfeld als de kennisgeving afkomstig is van een rechter, of als de informatie op de website onmiskenbaar onrechtmatig is.[24]

In de zaak *Deutsche Bahn/XS4All* is de uitspraak van de Rechtbank Den Haag verder uitgewerkt.[25] Ook hier ging het om de gegevens van een abonnee die gebruik maakte van de

---

[23] Rb. Den Haag 9 juni 1999, *Mediaforum* 1999/7-8, p. 205-209 m.nt. D.J.G. Visser (*Scientology/XS4ALL*).
[24] *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 49.
[25] Vzr. Amsterdam 25 april 2002, *Mediaforum* 2002/6, p. 226-227 (*Deutsche Bahn/XS4ALL*).

hosting-dienst van XS4ALL. Ditmaal was echter geen sprake van auteursrechtinbreuk, maar van de publicatie van twee artikelen van het linkse blad Radikal, die aanwijzingen bevatten over het saboteren van de Duitse spoorwegen. In deze zaak oordeelde het Hof Amsterdam dat de provider abonneegegevens direct moet bekendmaken als:

1. de gepubliceerde informatie onmiskenbaar onrechtmatig is en,

2. de gegevens nodig zijn ter voorkoming, dan wel beperking, van verdere kansen op aanzienlijke schade. Dit is bijvoorbeeld het geval als aannemelijk is dat de abonnee zal trachten de informatie via andere websites te publiceren, en dit kan leiden tot aanzienlijke schade.

Het Hof is in de bovenstaande zaak van mening dat deze plicht tot afgifte van de persoonsgegevens niet in strijd is met de Wet bescherming persoonsgegevens (Wbp), omdat deze wet een uitzondering schept 'ter bescherming van de rechten en vrijheden van anderen en ter voorkoming van strafbare feiten.'

In de zaak *Teleatlas N.V./Planet Media Group N.V.* vorderde Teleatlas afgifte door provider Planet van de gegevens van een e-mailgebruiker.[26] Deze abonnee zou op grote schaal illegale kopieën maken van software waarop Teleatlas het auteursrecht had. Teleatlas baseerde haar vordering op artikel 8 sub f van de Wbp. Dit artikel bepaalt dat verstrekking van persoonsgegevens door een verantwoordelijke (in dit geval Planet Media) aan derden alleen kan geschieden indien dit noodzakelijk is voor de behartiging van het gerechtvaardigde belang van die derde, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert. Bij de beoordeling van de toelaatbaarheid van de verstrekking dient onder meer de vraag beantwoord te worden of het doel dat met de verwerking wordt nagestreefd ook langs andere weg kan worden bereikt. Planet bracht in haar verweer naar voren dat Teleatlas onvoldoende naar alternatieve wegen had gezocht. Zij noemde onder andere de mogelijkheid om de toegang van de klant tot het internet te

---

[26] Vzr. Utrecht 9 juli 2002, *Computerrecht* 2002/5, p. 297-298, m.nt. W.A.M. Steenbruggen *(Teleatlas N.V./Planet Media Group N.V.)*.

blokkeren en het aanspreken van eBay, een veilingsite waarvan de anonieme boosdoener gebruik had gemaakt om de software te verspreiden. De rechter wees de vordering af omdat niet was komen vast te staan dat Teleatlas de gegevens niet op een andere, minder ingrijpende wijze had kunnen achterhalen.

Ook in de zaak *Rutloh/Concept ICT* van 25 juni 2002 gaat het over de identificatieplicht van een provider van e-maildiensten.[27] Het betrof e-mailberichten afkomstig van een onbekende persoon, die de indruk wekten afkomstig te zijn van Rutloh. De berichten stelden Rutloh in een kwaad daglicht. Het Hof Den Bosch concludeert:

> 'Er bestaat geen algemene rechtsregel op grond waarvan een ISP zo spoedig mogelijk nadat zij kennis heeft gekregen van onrechtmatige handelingen verplicht is mee te werken aan het ter beschikking stellen van gegevens die nodig zijn om vast te stellen wie voor die handelingen verantwoordelijk is.'

Omdat het account van de gebruiker was afgesloten en de onrechtmatige handelingen niet verder werden verricht, was de rechter in dit geval van oordeel dat de provider de gegevens niet hoefde te verstrekken.

8. Conclusie

Naar onze mening bestaat alleen een plicht tot afgifte van persoonsgegevens door een provider na tussenkomst van de rechter. De ontstaansgeschiedenis van de Richtlijn elektronische handel en de bijbehorende implementatiewet stelt deze eis weliswaar niet expliciet, maar zij biedt in ieder geval aanknopingspunten voor een dergelijke interpretatie. Een plicht voor de provider om buiten de rechter om tot verstrekking over te gaan wanneer sprake is van 'onmiskenbaar onrechtmatige informatie' lijkt in het algemeen niet hanteerbaar. In ieder geval is de bewering dat sprake is van auteursrechtinbreuk niet voldoende grond voor de vaststelling dat informatie onmiskenbaar onrechtmatig is, zoals de rechter ook oordeelde in de zaak *Deutsche Bahn/XS4ALL*.

---

[27] Hof Den Bosch 25 juli 2002, *KG* 2002, 259 (*Rutloh/Concept ICT*).

De rechter die een dergelijke vordering beoordeelt dient het belang van de auteursrechthebbende af te wegen tegen dat van de internetgebruiker. De auteursrechthebbende heeft belang bij het voorkomen van schade door auteursrechtinbreuk. Deze schade kan worden voorkomen door het filteren van P2P-verkeer, het afsluiten van een IP-adres of het onthullen van de identiteit van de inbreukmaker, opdat de rechthebbende de inbreukmaker kan aanspreken. Deze eerste twee maatregelen verhouden zich slecht tot het communicatiegeheim en de vrijheid van meningsuiting. De afgifte van persoonsgegevens staat op gespannen voet met het recht op privacy en anonimiteit.

Hoe moet de rechter de belangen van de betrokkenen in de praktijk tegen elkaar afwegen? In de jurisprudentie komen geen eenduidige criteria naar voren om conflicten tussen deze belangen te beslechten. De volgende criteria lijken van belang te zijn:

- Een vordering tot onthulling van identiteit dient afzonderlijk te worden beoordeeld van een vordering tot verwijdering of ontoegankelijk maken van informatie.[28] Dit uitgangspunt is in de zaken tegen XS4ALL echter niet gehanteerd.

- Wanneer de onrechtmatigheid van de informatie is vastgesteld en de provider daarvan op de hoogte is, zodat ontoegankelijk maken geboden is, dan dient de eiser een aanvullend belang aannemelijk te maken dat onthulling van identiteit rechtvaardigt. Pas wanneer hij dit gedaan heeft, handelt de provider onrechtmatig door te weigeren naam en adres vrij te geven.

Wij zijn van mening dat de rechter in zijn afweging de vrijheid van meningsuiting en het belang van anonimiteit moet betrekken. De mogelijkheid om anoniem te blijven is in de informatiesamenleving een essentiële voorwaarde voor het ongestoord uiten van meningen en voor het uitwisselen en ontvangen van informatie. Bovendien is anonimiteit bij

---

[28] Zie hierover uitgebreider Anonimiteit en uitingsvrijheid op het Internet; het onthullen van identificerende gegevens door Internetproviders, *Mediaforum* 2002-11/12, p. 348-351. Zie ook: www.ivir.nl/publicaties/ekker/anonimiteit-uitingsvrijheid.html.

handelingen op het internet een effectief middel om de individuele privacy te beschermen. Het internet kan als vrij communicatiemedium alleen blijven bestaan wanneer internetgebruikers niet worden gehinderd door het idee dat anderen over hun schouder meekijken, en door de angst voor represailles. De Raad van Europa heeft het belang van anonimiteit onlangs uitdrukkelijk erkend:

In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. […][29]

Om de genoemde belangen te beschermen moet de verstrekking van identificerende persoonsgegevens door providers aan private partijen met voldoende waarborgen worden omkleed.

Uit de *Verizon* zaak kan worden afgeleid wat de belangrijkste knelpunten zijn bij het formuleren van wettelijke regels die een provider verplichten om de identiteit van een abonnee vrij te geven. In de eerste plaats dienen waarborgen te bestaan voor de 'due process' rechten van internetgebruikers. De enkele bewering dat sprake is van auteursrechtinbreuk is naar onze mening niet voldoende. In een Nederlandse regeling zouden zwaardere eisen moeten worden gesteld aan auteursrechthebbenden om aan te tonen dat er daadwerkelijk sprake is van inbreukmakend handelen. Om de vermeende inbreukmaker de kans te geven zich te verweren zou daarnaast een notificatieplicht in kunnen worden gevoerd, inhoudende dat de provider zijn abonnee op de hoogte dient te stellen van de poging om zijn anonimiteit te doorbreken. Ook P2P-gebruikers hebben een gerechtvaardigd belang bij anonimiteit.

---

[29] Declaration on freedom of communication on the Internet adopted by the Committee of Ministers at the 840th meeting of the Ministers' Deputies, Straatsburg 28 mei 2003.