

De botsing tussen IE- en privacyrechten

Het einde van het *Lycos/Pessers*-tijdperk

145

Trefwoorden:

Dataretentierichtlijn, Richtlijn handhaving intellectuele rechten, *Lycos/Pessers*

Vorig jaar heeft de hoogste civielrechtelijke instantie van Zweden, in de zaak *Bonnier Audio AB c.s./Perfect Communication Sweden AB*,¹ prejudiciële vragen gesteld aan het Europees Hof van Justitie (HvJ) over het toepassingsbereik van en de verhouding tussen de Dataretentierichtlijn² en artikel 8 van de Handhavingsrichtlijn.³ Inmiddels heeft het HvJ ter zake arrest gewezen.⁴ Het arrest van het HvJ en meer in het bijzonder de conclusie van advocaat-generaal Jääskinen bij dit arrest,⁵ gaf aanleiding voor het schrijven van dit artikel. De uitkomst van het arrest druist in tegen de in Nederland geldende rechtspraak op dit punt en verdient daarom onze aandacht. Na een bespreking van de relevante (Europese) regelgeving en jurisprudentie, wordt de inhoud van het door het HvJ ter zake gewezen arrest besproken. Vervolgens wordt in dit artikel ingegaan op de vraag of de voor de praktijk erg ongunstige conclusie van de A-G terecht is. Ten slotte zal worden nagegaan welke gevolgen de in mijn ogen juiste conclusie van de A-G heeft voor de Nederlandse rechtspraktijk.

1 Inleiding

De Zweedse rechter heeft in zijn verzoek aan het HvJ gevraagd of de Dataretentierichtlijn eraan in de weg staat dat informatie over een abonnee aan wie een IP-adres is toegewezen, aan civiele partijen wordt medegedeeld. Tot op heden wordt deze vraag voor Nederland veelal beant-

woord aan de hand van het in het *Lycos/Pessers*-arrest⁶ bepaalde toetsingskader. Dit door de Hoge Raad der Nederlanden gewezen arrest stamt echter van voor de inwerkingtreding van de Dataretentierichtlijn. Het is dus interessant na te gaan of met de komst van de Dataretentierichtlijn de *Lycos/Pessers*-criteria naar de prullenbak kunnen worden verwezen.

Het bovengenoemde artikel 8 van de Handhavingsrichtlijn regelt, kort gezegd, dat lidstaten erin moeten voorzien dat een rechter op verzoek van een houder van een intellectuele-eigendomsrecht (IE-recht) de in een procedure betrokken partij kan bevelen informatie over de herkomst en de distributiekanaal van goederen en diensten te verstrekken die inbreuk maken op een IE-recht.⁷ De Dataretentierichtlijn heeft tot doel de nationale bepalingen van de lidstaten te harmoniseren voor wat betreft de bewaringsverplichtingen van onder andere ISP's ten aanzien van gegevens van haar abonnees. Dit ten behoeve van de bestrijding van criminaliteit.

Hieronder volgt eerst een korte uiteenzetting over de relevante Europese regelgeving.

2 Relevante Europese regelgeving

Om het onderwerp van dit artikel in het juiste perspectief te kunnen plaatsen, is het goed te beginnen met een korte uiteenzetting van de voor de onderhavige zaak relevante Europese richtlijnen. Deze richtlijnen bestaan enerzijds uit die welke bescherming bieden aan houders van intellectuele-eigendomsrechten en anderzijds uit een aantal belangrijke richtlijnen die het recht op een persoonlijke levenssfeer beschermen. De richtlijnen die in de laatstgenoemde categorie vallen, worden hieronder als eerste in chronologische volgorde besproken.

* Sil Kingma is advocaat te Amsterdam en gespecialiseerd in IE-, IT- en privacyrecht.

1 HvJ EU 19 april 2012, nr. C-461/10 (*Bonnier Audio AB c.s./Perfect Communication Sweden AB*).

2 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbare beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG.

3 Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (*PbEU* 2004, L 157/45, en – rectificatie – *PbEU* 2004, L 195/16).

4 HvJ EU 19 april 2012, nr. C-461/10 (*Bonnier Audio AB c.s./Perfect Communication Sweden AB*) (*prejudiciële vragen Högsta domstol, Zweden*) te vinden via de navolgende link: <http://curia.europa.eu/juris/liste.jsf?language=nl&num=C-461/10>.

5 Conclusie van A-G N. Jääskinen bij *Bonnier Audio AB c.s./Perfect Communication Sweden AB*, te vinden via de navolgende link: <http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=nl&num=7988882C19100461&doc=T&ouvert=T&seance=CONCL>.

6 HR 25 november 2005, *IER* 2006, 2, *Mediaforum* 2006-1 (*Lycos/Pessers*).

7 Artikel 8 lid 1 onder c van de Handhavingsrichtlijn.

2.1 IE-rechtelijke richtlijnen

2.1.1 E-Commercerichtlijn

De E-Commercerichtlijn⁸ is een van de eerste richtlijnen die specifiek rekening houdt met de opkomst van het internet en de metamorfose die onze maatschappij als gevolg daarvan de afgelopen decennia heeft ondergaan. Het doel van deze richtlijn is de juridische veiligheid van elektronische handel te versterken, deze te harmoniseren en zo het vertrouwen van de internetgebruikers te vergroten. Verder heeft zij tot doel de interne markt te bevorderen, door de belemmeringen weg te nemen die in de weg staan aan de ontwikkeling van elektronische handel. In dat kader voorziet de richtlijn in regels met betrekking tot de rechtspositie van tussenpersonen of intermediairs, die anderen in staat stellen om kennis te nemen van informatie. Daarbij valt te denken aan internet-serviceproviders (ISP's).

2.1.2 Handhavingsrichtlijn

Harmonisatie van de handhavingsrechten van houders van intellectuele-eigendomsrechten was de voornaamste reden voor de intrede van de Handhavingsrichtlijn.⁹ De richtlijn bevat maatregelen, procedures en rechtsmiddelen die noodzakelijk zijn om de handhaving van intellectuele-eigendomsrechten te waarborgen. De richtlijn schrijft aan de lidstaten voor te voorzien in een wettelijke maatregel op basis waarvan een in een procedure betrokken partij op rechterlijke last kan worden gehouden om informatie omtrent de herkomst en de distributiekanaalen van goederen en diensten die inbreuk maken op een IE-recht te verstrekken.¹⁰ De komst van de richtlijn werd aangewakkerd door de angst dat de Europese markt zou worden overspoeld met namaakproducten uit de voormalige Oostbloklanden. Alvorens bedoelde landen zouden toetreden, was het dus noodzakelijk om de regels omtrent piraterijbestrijding op orde te hebben.

2.2 Privacyrichtlijnen

Beide hiervoor besproken richtlijnen bepalen, expliciet dan wel impliciet, dat de bescherming die deze richtlijnen aan houders van intellectuele-eigendomsrechten bieden, geen afbreuk mag doen aan de vereisten inzake de bescherming van persoonsgegevens.¹¹ Om deze reden is het van belang om hier ook de voor de door de Zweedse verwijzende rechter gestelde vraag van belang zijnde richtlijnen betreffende de bescherming van persoonsgegevens kort te introduceren.

2.2.1 E-Privacyrichtlijn

De E-Privacyrichtlijn¹² zet de beginselen van de Algemene Privacyrichtlijn¹³ om in specifieke regels voor de sector elektronische communicatie en complementeert daarmee laatstgenoemde richtlijn op een aantal punten. Op basis van de E-Privacyrichtlijn zijn de lidstaten ertoe gehouden om ISP's ertoe te verplichten om gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken, vertrouwelijk te behandelen. Deze geheimhoudingsverplichting is niet absoluut. Het is mogelijk om wettelijke maatregelen te treffen ter beperking van de reikwijdte van deze geheimhoudingsverplichting, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is.¹⁴ Daarbij geldt overigens dat de geheimhoudingsverplichting enkel kan worden ingeperkt voor een welbepaald aantal doeleinden waaronder het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

2.2.2 Daretentierichtlijn

Op haar beurt vormt de E-Privacyrichtlijn de grondslag voor de Daretentierichtlijn die een Europese algemene bewaarplicht van telecommunicatiegegevens regelt. Deze bewaarplicht moet garanderen dat bepaalde – in die richtlijn opgesomde categorieën – gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgeving van de lidstaten. De naam en het adres van de abonnee of de geregistreerde gebruiker aan wie een IP-adres is toegewezen, zijn gegevens die op basis van de Daretentierichtlijn door de ISP dienen te worden bewaard. Ten aanzien van de in de Daretentierichtlijn opgesomde categorieën telecommunicatiegegevens geldt de hiervoor omschreven beperkingsmogelijkheid van de uit de E-Privacyrichtlijn voortvloeiende geheimhoudingsverplichting niet. Wel bepaalt de Daretentierichtlijn dat de lidstaten bepalingen aannemen om te waarborgen dat de overeenkomstig deze richtlijn bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde autoriteiten worden verstrekt.¹⁵

3 Relevante Nederlandse wetgeving

De Daretentierichtlijn is voor Nederland omgezet in de zogenaamde Wet bewaarplicht telecommunicatiegegevens en geïmplementeerd in de Telecommunicatiewet. In de memorie van toelichting (MvT) op deze wet heeft

8 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('E-Commercerichtlijn') (PbEG 2000, L 178/1).

9 Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (PbEU 2004, L 157/45 en – rectificatie – PbEU 2004, L 195/16).

10 Artikel 8 van Richtlijn 2004/48/EG.

11 Overweging 14 van Richtlijn 2000/31/EG en artikel 2 van Richtlijn 2004/48/EG.

12 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juni 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie) (PbEG 2002, L 201/37).

13 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

14 Artikel 15 lid 1 van Richtlijn 2002/58.

15 Artikel 4 van Richtlijn 2006/24/EG.

de Nederlandse wetgever zich op het standpunt gesteld dat de Nederlandse wetgeving reeds de waarborgen kent dat verkeersgegevens, die worden verwerkt door de ISP's, alleen in welbepaalde gevallen en onder wettelijk vastgelegde voorwaarden kunnen worden verstrekt aan de bevoegde autoriteiten.¹⁶ Volgens de minister betreffen dit enkel de regels over het vorderen van verkeersgegevens in het Wetboek van Strafvordering in combinatie met de relevante (spiegel)bepalingen uit de Telecommunicatiewet. Voor het verstrekken van verkeersgegevens door ISP's aan civiele partijen zou onder Nederlands recht dus geen plaats zijn.

4 Relevante rechtspraak

4.1 Nationaal

Desondanks hebben civiele partijen via rechtelijke procedures in het verleden met succes toegang bedongen tot door ISP's opgeslagen verkeersgegevens. Zo heeft de voorzieningenrechter Amsterdam Google veroordeeld tot het verstrekken van persoonsgegevens aan Iceshop.¹⁷ De voorzieningenrechter rechtvaardigde zijn beslissing met het argument dat aannemelijk is dat de betreffende gebruiker van Google onrechtmatig jegens Iceshop heeft gehandeld. Ook is het Stichting Brein een aantal keren gelukt om via een kortgedingprocedure toegang te verkrijgen tot door KPN en UPC bewaarde verkeersgegevens van hun abonnees.¹⁸

4.1.1 Lycos/Pessers

De vraag of een ISP gehouden is om persoonsgegevens aan een belanghebbende te verstrekken wordt veelal beantwoord aan de hand van het in het *Lycos/Pessers*-arrest¹⁹ bepaalde toetsingskader.²⁰ In dit arrest geeft de Hoge Raad antwoord op de vraag of de E-Commercerichtlijn zich verzet tegen een aan een ISP als Lycos gerichte veroordeling tot het verstrekken van persoonsgegevens.

In de procedure stelt Lycos zich op het standpunt dat de E-Commercerichtlijn zich in ieder geval tegen een zodanige veroordeling zou verzetten, wanneer de gewraakte informatie niet onmiskenbaar onrechtmatig is jegens degene die de vordering instelt. Aan dit standpunt ligt – kort gezegd – de opvatting ten grondslag dat hoewel de E-Commercerichtlijn met artikel 15 lid 2 voorziet in de mogelijkheid dat bepaalde persoonsgegevens door ISP's aan bevoegde autoriteiten worden verstrekt, dit artikel niet toelaat dat een ISP gehouden kan worden de persoonsgegevens van een betrokken inbreukmaker aan civiele partijen te verstrekken.

Dit verdedigde standpunt kan volgens de Hoge Raad echter niet als juist worden aanvaard. De Hoge Raad stelt dat de E-Commercerichtlijn, kort gezegd, geen uitputten-

de regeling inzake de verstrekking van NAW-gegevens bevat. Daar komt bij dat de E-Commercerichtlijn niet bedoeld zou zijn om benadeelden van anonieme onrechtmatige uitingen de gang naar de rechter te ontzeggen. De Hoge Raad concludeert vervolgens dat de in de richtlijn vastgelegde beperking van de aansprakelijkheid van dienstverleners, die als tussenpersoon optreden, geen afbreuk doet aan de mogelijkheid dat de nationale rechter die maatregelen treft die van deze tussenpersonen redelijkerwijs kunnen worden verlangd in verband met op hen rustende zorgvuldigheidsverplichtingen om onwettige activiteiten op te sporen en te voorkomen.²¹

Vervolgens komt de vraag aan bod of op de ISP een plicht rust om desgevorderd NAW-gegevens te verschaffen, ook indien geen sprake is van een onmiskenbaar onrechtmatige (anonieme) uiting. Het Amsterdamse Hof kwam in appèl reeds tot de conclusie dat het weigeren van het verstrekken van NAW-gegevens door een ISP onder een aantal omstandigheden die meespelen bij de weging van de betrokken grondrechten, onrechtmatig kan zijn. Volgens het hof kan dit met name het geval zijn indien zich de volgende omstandigheden voordoen:

- de mogelijkheid dat de informatie, op zich zelf beschouwd, jegens de derde onrechtmatig en schadelijk is, is voldoende aannemelijk;
- de derde heeft een reëel belang bij de verkrijging van de NAW-gegevens;
- aannemelijk is dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen;
- afweging van de betrokken belangen van de derde en de websitehouder brengt mee dat het belang van de derde behoort te prevaleren boven de vordering die de houder van een intellectuele-eigendomsrecht kan instellen om informatie van de inbreukmaker over de inbreukketen te verkrijgen.

De Hoge Raad onderstreept in zijn arrest het door het Amsterdamse Hof ontwikkelde toetsingskader, maar benadrukt tegelijkertijd dat het Hof zijn oordeel heeft toegesneden op het onderhavige, specifieke geval.

Dit door de Hoge Raad gewezen arrest, stamt echter van voor de inwerkingtreding van de Handhavingsrichtlijn, de E-Privacy- en Dataretentierichtlijn. Als gevolg daarvan zijn de bepalingen uit deze richtlijnen logischerwijs niet in de beoordeling van de Hoge Raad meegenomen. Het is dus interessant na te gaan of met de komst van laatstbedoelde richtlijnen de *Lycos/Pessers*-criteria nog standhouden.

Overigens heeft Dommering in een recent artikel al betoogd dat het *Lycos/Pessers*-arrest lijkt te zijn ingehaald door het, op de E-Privacyrichtlijn gebaseerde, *Promusi-*

16 Zie p. 19 van de MvT op de Wet bewaarplicht telecommunicatiegegevens.

17 Rb. Amsterdam (vzr.) 9 oktober 2008, LjN BF7448 (*Iceshop/Google*).

18 Rb. Amsterdam (vzr.) 9 oktober 2008 (*Stichting Brein/Euroaccess Enterprises Ltd.*); Rb. 's-Gravenhage (vzr.) 5 januari 2007, AMI 2007-2, nr. 9 (*Stichting Brein/KPN*); Rb. Amsterdam (vzr.) 24 augustus 2006, LjN AY6903 (*Stichting Brein/UPC*).

19 HR 25 november 2005, IER 2006, 2, *Mediaforum* 2006-1 (*Lycos/Pessers*).

20 Zie in dit verband ook Rb. Haarlem (vzr.) 31 december 2010, IEPT20101231, waarin de informatieplicht van een expediteur naar analogie van het *Lycos/Pessers*-arrest door de rechter werd aangenomen.

21 Rechtsoverweging 5.1.4 van het *Lycos/Pessers*-arrest.

cae-arrest.²² Dommering laat het op dit punt echter bij deze signalering. Reden temeer om na te gaan of het *Promusicae*-arrest en het meer recentelijk door het HvJ gewezen *Bonnier Audio c.s.*-arrest, deze conclusie inderdaad rechtvaardigen. Begrip van de beide arresten is hiervoor noodzakelijk.

4.2 Europees

4.2.1 *Promusicae*-arrest

Het *Promusicae*-arrest behandelt een vordering van de gelijknamige vereniging, waarvan de leden muziekproducenten zijn. In een procedure vordert *Promusicae* bij de Spaanse rechtbank om Telefónica te veroordelen om de NAW-gegevens van enkele inbreukmakende abonnees te verstrekken. Volgens *Promusicae* gebruiken deze personen het zogenaamde peer-to-peerprogramma KaZaA, waarmee databestanden kunnen worden uitgewisseld. Via een map die gedeeld wordt vanaf hun personal computer, biedt KaZaA aan anderen toegang tot muzieknummers waarvan de exploitatierechten toebehoren aan de leden van *Promusicae*. De gevorderde gegevens heeft *Promusicae* nodig om tegen de betrokken personen civiele procedures te kunnen instellen.

Telefónica heeft aangevoerd dat volgens de Spaanse wet de door *Promusicae* gevraagde gegevens slechts mogen worden verstrekt in het kader van een strafrechtelijk onderzoek of wanneer dit nodig is ter waarborging van de openbare veiligheid en landsverdediging.²³ Hoewel dit standpunt door de Madrileense rechter werd erkend, wilde de verwijzende rechter toch graag van het HvJ weten of het gemeenschapsrecht wellicht tot een andere conclusie zou leiden. Onder verwijzing naar de E-Commercerichtlijn, de Auteursrechtlijn²⁴ en de Handhavingsrichtlijn was de Madrileense rechter daarbij vooral geïnteresseerd in het antwoord op de vraag of het gemeenschapsrecht²⁵ het doorgeven van persoonsgebonden verkeersgegevens over het gebruik van internet aan houders van intellectuele-eigendomsrechten toestaat of zelfs eist.

Het HvJ focust zich voor het antwoord op de door de Madrileense rechter gestelde vraag met name op de E-Privacyrichtlijn. Artikel 15 van de E-Privacyrichtlijn bevat een uitdrukkelijke verwijzing naar artikel 13 lid 1 van de Algemene Privacyrichtlijn. Laatstgenoemd artikel voorziet voor bepaalde gevallen in de mogelijkheid om persoonsgegevens buiten het doel waarvoor ze zijn verkregen te verwerken. Een van die uitzonderingen

betreft de verwerking van persoonsgegevens ter bescherming van andermans rechten en vrijheden. De richtlijn precificeert niet om welke rechten en vrijheden het gaat. Op basis hiervan neemt het HvJ aan dat deze bepaling de verplichting van een ISP om NAW-gegevens aan een belanghebbende te verstrekken niet uitsluit. Mochten lidstaten tot implementatie van de betreffende of andere uit de hier aangehaalde richtlijnen bepalingen besluiten, dan is dit dus niet in strijd met het gemeenschapsrecht. Tenminste voor zover zij zich niet baseren op een uitlegging van deze richtlijnen die in conflict zou komen met grondrechten of andere algemene beginselen van gemeenschapsrecht, zoals het evenredigheidsbeginsel.²⁶

Echter, volgens het HvJ dwingen deze bepalingen de lidstaten evenmin om een dergelijke verplichting op te leggen, hetgeen mogelijk verklaart, dat de bedoelde uitzondering niet door de Spaanse wetgever is geïmplementeerd.²⁷ In de later door het HvJ uitgesproken *LSG*-beschikking,²⁸ waarin het fenomeen *filesharing* centraal staat, wordt dit ongedwongen karakter van de hierboven aangehaalde bepalingen uit de E-Privacyrichtlijn bevestigd.

5 *Bonnier Audio c.s.*

In het *Bonnier Audio c.s.*-arrest wenst de verwijzende Zweedse rechter van het HvJ te vernemen of de uitleg in de zaken die aanleiding hebben gegeven tot het *Promusicae*-arrest en de *LSG*-beschikking, die met name waren gestoeld op de E-Privacyrichtlijn, na de vaststelling van de Datarentierichtlijn moet worden aangevuld.

Bonnier Audio c.s. zijn uitgevers die onder meer het exclusieve recht bezitten op het reproduceren, uitgeven en distribueren van 27 luisterboeken. *Bonnier Audio c.s.* stellen dat inbreuk is gemaakt op hun exclusieve rechten doordat deze 27 boeken zonder hun toestemming publiekelijk zijn gemaakt door middel van een FTP-server (*file transfer protocol*: protocol voor het binnenhalen van gegevens), een *filesharing*-programma, dat de overdracht van gegevens tussen computers via internet mogelijk maakt. *ePhone* is de ISP die de gestelde onrechtmatige uitwisseling van gegevens mogelijk heeft gemaakt.

Bonnier Audio c.s. hebben zich tot de bevoegde gerechtelijke instantie gewend met het verzoek tot het gelasten van mededeling van de naam en het adres van de gebruiker van het IP-adres dat geacht wordt te zijn gebruikt om de betrokken bestanden door te geven. *ePhone* heeft als verweer tegen deze vordering onder meer aangevoerd dat het verzochte bevel in strijd is met de Datarentierichtlijn.

22 E.J. Dommering, 'De zaak Scarlet/Sabam – Naar een horizontale integratie van het auteursrecht', *AMI* 2011-2, p. 49-53. Zie hierover ook M.W. Kellog, 'Ook een ontaarde ruzie over postzegels kent zijn grenzen!', *Boek9.nl*, 15 oktober 2007, B9-4876.

23 Perscommuniqué nr. 5/08, 29 januari 2008, arrest van het Hof van Justitie in nr. C-275/06 (*Productores de musica de espana (Promusicae)/Telefonica de Espana SAU*).

24 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 (*PbEG* 2001, L 167/10).

25 Onder verwijzing naar de E-Commercerichtlijn, de Auteursrechtlijn en de Handhavingsrichtlijn.

26 Rechtsoverweging 68 van het *Promusicae*-arrest.

27 Rechtsoverweging 70 van het *Promusicae*-arrest.

28 Zie wat het verband met de bescherming van intellectuele eigendom betreft, HvJ EG 29 januari 2008, nr. C-275/06, *Jur.* 2008, p. I-271 (*Promusicae*); beschikking van 19 februari 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* (nr. C-557/07, *Jur.* 2009, p. I-1227), en conclusie van A-G Cruz Villalón van 14 april 2011 in de zaak *Scarlet Extended/Sabam* (nr. C-70/10, nog aanhangig bij het Hof).

Het geschil wordt momenteel uitgevochten ten overstaan van de hoogste Zweeds rechterlijke instantie. De zogeheten 'Högsta domstol' heeft de behandeling van de zaak geschorst en prejudiciële vragen aan het HvJ gesteld. De verwijzende rechter wenste onder meer te vernemen of de Dataretentierichtlijn in de weg staat aan de toepassing van een op artikel 8 van de Handhavingsrichtlijn gebaseerde nationale bepaling die een ISP een dergelijke informatieverplichting oplegt. Dit onder de gegeven omstandigheid dat vaststaat dat het IP-adres dat de ISP heeft toegewezen gebruikt is om inbreuk te maken op een auteursrecht, er duidelijk bewijs van inbreuk is overgelegd en die maatregel in overeenstemming is met het evenredigheidsbeginsel.

5.1 Conclusie HvJ

Al snel komt het HvJ tot de conclusie dat Dataretentierichtlijn niet op het hoofdgeding van toepassing is. De Dataretentierichtlijn heeft enkel betrekking op de bewaring van gegevens ten behoeve van de overheid met het oog op de opsporing van ernstige criminaliteit. Deze richtlijn is bijgevolg niet van toepassing, waar het gaat om een civiele procedure. Vervolgens bevestigt het HvJ zijn eerdere *Promusicae*-uitspraak met de overweging dat artikel 8 van de Handhavingsrichtlijn gelezen in samenhang met de E-Privacyrichtlijn zich er niet tegen verzet dat lidstaten de verplichting opleggen persoonsgegevens aan particulieren door te geven met het oog op civielrechtelijke vervolging.²⁹

Ten slotte gaat het HvJ specifiek in op de vraag of de betrokken bepalingen van de Zweedse omzettingwet geoorloofd zijn in de zin dat de toepasselijke fundamentele rechten daarmee voldoende gewaarborgd zijn. Onder verwijzing naar het *Promusicae*-arrest, komt het HvJ tot de conclusie dat het antwoord bevestigend kan luiden. Dit omdat in het onderhavige geval aan de volgende voorwaarden lijkt te zijn voldaan:

- er zijn duidelijke bewijzen van een inbreuk op een intellectuele-eigendomsrecht op een werk overgelegd;
- de gevraagde gegevens kunnen de opsporing van een inbreuk op het auteursrecht vergemakkelijken; en
- het belang van de redenen voor dit bevel weegt op tegen de ongemakken of andere nadelen ervan voor degene tot het wie het is gericht, of tegen enig ander daarmee strijdig belang.³⁰

Een wettelijke regeling die aan dergelijke voorwaarden voldoet stelt de nationale rechterlijke instantie in staat om de in het geding zijnde tegengestelde belangen af te wegen op basis van de concrete omstandigheden van de zaak en daarbij terdege rekening te houden met de uit

het evenredigheidsbeginsel voortvloeiende vereisten. In deze situatie kan worden aangenomen dat een dergelijke wettelijke regeling in beginsel een juist evenwicht tussen de bescherming van het intellectuele-eigendomsrecht van de auteursrechthouders en de bescherming van de persoonsgegevens van een internet abonnee of -gebruiker kan waarborgen, aldus het HvJ.

Met dit oordeel lijkt het HvJ een andere weg in te slaan dan A-G Jääskinen in zijn conclusie bij het arrest. Evenals het HvJ komt hij tot de conclusie dat er in beginsel een plicht op een ISP kan rusten om persoonsgegevens aan een houder van IE-rechten te verstrekken. Echter, volgens hem is de ISP hiertoe enkel gehouden wanneer de betreffende persoonsgegevens zijn bewaard om voor dat doel te kunnen worden verstrekt en gebruikt overeenkomstig gedetailleerde nationale bepalingen die zijn vastgesteld met eerbiediging van het Unierecht op het gebied van de bescherming van persoonsgegevens.³¹ De A-G motiveert dit standpunt met de stelling dat houders van intellectuele-eigendomsrechten niet mogen worden bevooroordeeld door hun toe te staan persoonsgegevens te gebruiken die rechtmatig zijn verzameld of bewaard voor doeleinden die geen verband houden met de bescherming van hun rechten.

5.2 Conclusie A-G

De kritiek die op de conclusie van de A-G wordt geuit, is dat hij ten onrechte een strikte verdeling tussen de werking van intellectuele-eigendomsrechten en privacy-rechten aanneemt, waarbij geen plaats is voor ongeregelde botsingen tussen de beide rechtsgebieden.³² Daarbij onderschat de A-G dat, hoewel op verzoek van een particuliere partij, de toegang tot de persoonsgegevens door een rechter wordt gelast, zo luidt het bezwaar.

De criticasters vreesden dat wanneer de door de A-G uiteengezette lijn als juist zou worden gezien, houders van IE-rechten de mogelijkheid om via een civiele procedure NAW-gegevens van een inbreukmakende abonnee van een ISP te verkrijgen, vaarwel konden zeggen. Zelden tot nooit worden de NAW-gegevens immers door een ISP voor dergelijke doeleinden bewaard. Het lijkt erop dat deze critici na het door het HvJ ter zake gewezen arrest opgelucht adem kunnen halen.

6 Analyse uitspraak HvJ

Of het HvJ ter zake tot een juiste uitspraak is gekomen, valt te betwijfelen. Volgens mij is een wettelijke regeling als de Zweedse omzettingwet namelijk niet voldoende om er op basis van artikel 15 van de E-Privacyrichtlijn de reikwijdte van het uit het privacyrecht voortvloeiende doelbindingsbeginsel of de geheimhoudingsplicht mee

29 Rechtsoverweging 55 van het *Bonnier Audio c.s.*-arrest.

30 Rechtsoverweging 58 van het *Bonnier Audio c.s.*-arrest.

31 Daaronder vallen ook artikel 7 en 8 van het Europees Handvest en artikel 8 EVRM.

32 Riccardo Sciaudone (Grimaldi e Associati), 'Personal data protection and IP rights enforcement: two worlds apart?', *Journal of Intellectual Property Law & Practice* 30 January 2012, <http://jiplp.blogspot.com/2012/01/personal-data-protection-and-ip-rights.html>.

te kunnen beperken. Ook niet wanneer is voldaan aan de door het HvJ gegeven hierboven opgesomde voorwaarden.

Voorsnog ben ik eerder geneigd om de door A-G Jääskinen uitgezette lijn als juist te accepteren. Niet voor niets bepaalt artikel 2 van de Handhavingsrichtlijn namelijk dat de bescherming die deze richtlijn houders van IE-rechten biedt geen afbreuk mag doen aan de vereisten inzake de bescherming van persoonsgegevens. Anders dan de critici beweren is van een ongeregelde botsing tussen de beide rechtsgebieden dus geen sprake.

Verder geldt dat wel wordt aangenomen dat de E-Privacyrichtlijn geen gronden geeft waarop een verwerking van verkeersgegevens (zoals een IP-adres) is toegestaan op verzoek van een civiele partij teneinde een civiele procedure te kunnen starten. Immers de in artikel 13 lid 1 van de Algemene Privacyrichtlijn bedoelde gronden op het gebied van de elektronische communicatie gelden slechts voor zover zij in artikel 15 lid 1 van de E-Privacyrichtlijn uitdrukkelijk worden genoemd.³³ De in artikel 13 lid 1 onder g van de Algemene Privacyrichtlijn opgenomen grond ontbreekt daarin echter.

Maar zelfs wanneer wordt aangenomen dat het de nationale wetgever, al dan niet op basis van artikel 15 E-Privacyrichtlijn, is toegestaan om in deze mogelijkheid te voorzien, dan moet een dergelijke wet wel voldoen aan de vereisten van het arrest van het HvJ in de zaak *Österreichischer Rundfunk*.³⁴ Daarin is bepaald dat een inbreuk op artikel 8 EVRM alleen is toegestaan:

‘(...) indien zij bij wet is voorzien, één van de in lid 2 van deze bepaling genoemde legitieme doelstellingen nastreeft en in een democratische samenleving noodzakelijk is om dat doel of die doelstellingen te bereiken... (alsmede dat een dergelijke bepaling) voldoende nauwkeurig is geformuleerd opdat degenen tot wie de wet is gericht hun gedrag kunnen bepalen en derhalve voldoet aan het vereiste van voorzienbaarheid zoals dat in de rechtspraak van het Europees Hof voor de rechten van de mens is neergelegd.’

Een dergelijk wettelijk vastgelegd gebruikersdoel moet dus voldoen aan het voorzienbaarheidsbeginsel en onstotelijk duidelijk maken aan gebruikers van een elektronische-communicatiedienst dat hun verkeersgegevens ook kunnen worden verwerkt ten behoeve van een civiele partij die een civiele actie tegen hen wil instellen.³⁵

Het gaat mij een brug te ver om aan te nemen dat die expliciete wettelijke maatregelen reeds in de in artikel 13 lid 1 van de Algemene Privacyrichtlijn dan wel de Zweedse omzettingwetgeving vastgelegde en algemeen

geformuleerde uitzonderingen kunnen worden gelezen. Hiervoor is een meer specifieke nationale regeling noodzakelijk die uitputtend rekening houdt met de uit de privacyregelgeving voortvloeiende (bewaar- en beveiligings)verplichtingen.

7 Rechtsgevolgen voor Nederland

Wat hier ook van zij, vaststaat dat een door het HvJ noodzakelijk geachte specifieke bepaling (voorsnog) in de Nederlandse wetgeving ontbreekt. De wet mag dan wel (ten dele) artikel 8 van de Handhavingsrichtlijn implementeren en voorzien in de mogelijkheid om middels een getuigenverhoor ten overstaan van een rechter NAW-gegevens over derden die onderdeel van een inbreukketen maken te verkrijgen,³⁶ dit is echter enkel van toepassing in het geval dat de ISP ook zelf onrechtmatig ten opzichte van de verzoeker van het getuigenverhoor handelt.³⁷

Verder rechtvaardigt al het bovenstaande de conclusie dat, bij het ontbreken van een wettelijke bepaling die specifiek in die mogelijkheid voorziet, op basis van het *Lycos/Pessers*-arrest ten onrechte wordt aangenomen dat een ISP ook kan worden gedagvaard om van hem de NAW-gegevens van een abonnee te vorderen.³⁸ Het feit dat toewijzing van een dergelijke vordering een belangenafweging op basis van het door het *Lycos/Pessers* gegeven toetsingskader vereist in verband met de privacy van de betrokkenen en het gelaedeerde belang, maakt dit niet anders.³⁹ Daar komt bij dat de Hoge Raad bij het afwegen van de belangen de relevante privacybepalingen onjuist heeft toegepast. Ook om die reden mag het *Lycos/Pessers*-arrest geen precedentwerking meer hebben. Ter toelichting op dit standpunt dient het volgende.

In het *Lycos/Pessers*-arrest oordeelt de Hoge Raad dat inbreuk op artikel 9 van de Wbp mogelijk is op basis van artikel 8 aanhef en onder f van de Wbp. Dit artikel versterkt echter uitsluitend en limitatief de rechtvaardigingsgronden op basis waarvan een verantwoordelijke persoonsgegevens voor door hem vooraf welbepaalde doeleinden mag verzamelen en verder mag verwerken. Het verzamelen en verder verwerken van persoonsgegevens in het kader van een verzoek aan een ISP tot verstrekking van persoonsgegevens is daar niet een van. Een inbreuk op artikel 9 van de Wbp is dan ook niet te rechtvaardigen met een beroep op artikel 8 aanhef onder f van de Wbp.

Wie de Wbp goed leest weet dat schending van artikel 9 Wbp door een verantwoordelijke in de zin van de Wbp enkel is toestaan op basis van een beperkt aantal in artikel 43 van de Wbp opgenomen zwaarwegende belangen.

33 Paragraaf 86 van de conclusie van A-G Kokott.

34 HvJ EG 20 mei 2003, gevoegde zaken nr. C-465/00, C-138/01 en C-139/01, *Jur.* 2003, p. I-4989 (*Österreichischer Rundfunk*).

35 Zie in die zin ook overweging 109 uit de conclusie van A-G Kokott van 18 juli 2007 bij het *Promusicae*-arrest.

36 Artikel 1019f Wetboek van Burgerlijke Rechtsvordering.

37 Zie in dit kader ook J.J.C. Kabel, commentaar op *Lycos/Pessers*, *IER* 2006-1, p. 1-3.

38 A.I.M. van Mierlo e.a., *Tekst & Commentaar Burgerlijke Rechtsvordering*, Deventer: Kluwer 2012 (vijfde druk), punt 5 van de toelichting bij artikel 1019f Rv.

39 *Kamerstukken II* 2005/06, 30 392, nr. 6, p. 3 (NV). Artikel 8 onder f Wet bescherming persoonsgegevens; zie ook HR 25 november 2005, *IER* 2006, 2, *Mediaforum* 2006-1 (*Lycos/Pessers*).

Een van die belangen betreft de bescherming van rechten van derden, zoals het auteursrecht. Artikel 43 Wbp verbindt aan de mogelijkheid tot doorbreking van het doelbindingsprincipe echter dezelfde voorwaarden als artikel 8 lid 2 EVRM. Dat betekent derhalve dat: het voorschrift voldoende nauwkeurig moet zijn omschreven; het voorschrift adequate en effectieve waarborgen moet bevatten tegen ongeoorloofde inbreuken; de inbreuk moet worden gerechtvaardigd door een *pressing social need* en in overeenstemming moet zijn met de beginselen van proportionaliteit en subsidiariteit. Een strikte uitleg van deze begrippen is van belang omdat de gronden (de zwaarwegende belangen) zelf slechts in algemene zin kunnen worden geformuleerd.

Bij een juiste toepassing van de Wbp had de Hoge Raad derhalve ook via deze weg tot de conclusie dienen te komen dat de nationale wetgever vooraf gedetailleerde bepalingen dient te hebben vastgesteld om het in het privacyrecht gewortelde doelbindingsbeginsel te kunnen omzeilen.

8 Conclusie

De vraag of het een ISP vrijstaat om op verzoek van een houder van intellectuele-eigendomsrechten aan deze houder persoonsgegevens van een vermeende inbreukmaker te verschaffen, dient te worden beantwoord aan de hand van de toepasselijke privacyrichtlijnen.

Op basis van artikel 15 van de E-Privacyrichtlijn heeft het HvJ aangenomen dat deze bepaling de verplichting van een ISP om NAW-gegevens aan een belanghebbende te verstrekken niet uitsluit. Mochten lidstaten tot implementatie van de betreffende of andere uit de hier aangehaalde richtlijnen bepalingen besluiten, dan is dit dus niet in strijd met het gemeenschapsrecht, tenminste voor zover zij zich niet baseren op een uitlegging van deze richtlijnen die in conflict zou komen met de relevante grondrechten of andere algemene beginselen van gemeenschapsrecht.

Een aan een ISP gericht verzoek tot verstrekking van persoonsgegevens mag door een nationale rechter enkel worden gehonoreerd, indien de nationale wetgever vooraf gedetailleerde bepalingen heeft vastgesteld overeenkomstig artikel 15 van de E-Privacyrichtlijn die in een dergelijke verstrekking voorzien. In de Nederlandse wetgeving ontbreekt momenteel een dergelijke bepaling.

Verder geldt sinds de inwerkingtreding van de E-Privacyrichtlijn dat voor de in het *Lycos/Pessers*-arrest gehanteerde criteria en de op basis daarvan te maken belangenafweging geen plaats (meer) is. Het voorgaande houdt in dat de vele uitspraken waarin ISP's op basis van het *Lycos/Pessers*-arrest zijn veroordeeld tot het verstrekken van NAW-gegevens en/of IP-adressen in strijd met de wet zijn geweest.⁴⁰

Naast het wetmatige argument valt ook overigens wel wat voor deze conclusie te zeggen. Het komt de informatievrijheid immers ten goede wanneer een ISP terug kan vallen op het adagium 'don't shoot the messenger' en niet bang hoeft te zijn om in een civielrechtelijke strijd verwickeld te raken enkel omdat de inhoudelijke boodschap die zij bezorgt onrechtmatig jegens anderen is.

40 Zie onder andere Rb. 's-Hertogenbosch (vzr.) 8 juli 2008, KG ZA 08-261 (*Stichting Brein/Euroaccess Enterprises Ltd.*); Rb. Amsterdam (vzr.) 9 oktober 2008, LJN BF7448 (*Iceshop/Google Inc.*); Rb. 's-Gravenhage (vzr.) 5 januari 2007, AMI 2007-2, nr. 9 (*Stichting Brein/KPN*); Rb. Amsterdam (vzr.) 24 augustus 2006, LJN AY6903 (*Stichting Brein/UPC*).