

# Privacyrecht in een piratenwereld: de Lycos/Pessers-toets 17 jaar na dato

Marijn Kingma\*

In 2003 ontdekte postzegelhandelaar Pessers dat er op een website van [members.lycos.nl](http://members.lycos.nl) teksten waren geplaatst waarin hij werd beschuldigd van oplichting. Nu de eigenaar van de website onbekend was, stuurde Pessers een brief aan hosting-provider Lycos met de sommatie om de website offline te halen en om de NAW-gegevens van de websitehouder aan hem te verstrekken. Dit leidde tot de rechtszaak die uitmondde in het standaardarrest *Lycos/Pessers*<sup>1</sup> (sinds de invoering van de anonimiseringsrichtlijnen van de rechtspraak: 'Lycos/[...]',) geweest in 2005. Vlak voor het arrest van de Hoge Raad werd YouTube opgericht. Het zou nog drie jaar duren voordat Facebook naar Nederland kwam en nog twee jaar voordat de eerste iPhone werd geïntroduceerd. Het is een understatement om te zeggen dat de digitale wereld niet meer te vergelijken is met die uit 2005. Met de digitalisering heeft ook het aantal inbreuken op auteursrechten een vlucht genomen en heeft de handhaving zich verplaatst naar het internet. Tegelijkertijd is ook de regelgeving op het gebied van (digitale) privacy aangescherpt. Dit heeft geresulteerd in discussie in de literatuur en rechtspraak over de vraag wanneer een tussenpersoon gehouden is NAW-gegevens van inbreukmakers af te geven. Afgelopen jaar werden zowel door de Hoge Raad (*Dutch Filmworks/Ziggo*) als het Europese Hof van Justitie (*Mircom*) arresten gewezen over deze vraag. Hoog tijd om de balans op te maken en te bezien of het *Lycos/Pessers*-arrest de tand des tijds heeft doorstaan.

## Hoe zat het ook alweer?

Maar eerst terug naar 2005: postzegelhandelaar Pessers kreeg in alle instanties gelijk. De voorzieningenrechter van de Rechtbank Haarlem overweegt dat het niet afstaan van NAW-gegevens door een internet serviceprovider (ISP) die ervan in kennis is gesteld dat een van zijn gebruikers onrechtmatig handelt, onder omstandigheden onrechtmatig kan zijn.<sup>2</sup> Ook kan de provider volgens de voorzieningenrechter gehouden zijn de NAW-gegevens af te staan op grond van de 'rechtsplicht tot het noemen van zijn voorman zoals die in zaken van intellectueel eigendom is erkend',<sup>3</sup> of op grond van artikel 843a Rv. Het Hof Amsterdam bekrachtigt het vonnis van de voorzieningenrechter en oordeelt dat ook indien de gepubliceerde informatie niet 'onmiskenbaar' onrechtmatig is, een internetprovider

gehouden kan zijn tot verstrekking van NAW-gegevens.<sup>4</sup> Indien 'voldoende aannemelijk' is dat de 'gepubliceerde informatie jegens de derde wel onrechtmatig zou kunnen zijn en dat deze daardoor schade kan lijden', is het maatschappelijk ongewenst als er geen enkele mogelijkheid zou bestaan de websitehouder aan te spreken. Vervolgens formuleert het hof in rechtsoverweging 4.10 de bekende vier omstandigheden waaruit kan blijken of een weigering van de serviceprovider om de NAW-gegevens bekend te maken, in strijd is met de zorgvuldigheid:

- a. de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, is voldoende aannemelijk;
- b. de derde heeft een reëel belang bij de verkrijging van de NAW-gegevens;

\* Mr. M.E. Kingma is advocaat te Amsterdam (Höcker Advocaten) en redacteur van dit blad. Met veel dank aan Jytte Elfferich voor haar bijdrage aan de totstandkoming van dit artikel.

1 HR 25 november 2005, ECLI:NL:HR:2005:AU4019, NJ 2009/550, m.nt. Hugenholtz, *Computerrecht* 2006/11, m.nt. De Vries (*Lycos/Pessers*).

2 Rb. Haarlem (vzr.) 11 september 2003, ECLI:NL:RBHAA:2003:AL1882.

3 De voorzieningenrechter verwijst naar HR 27 november 1987, NJ 1988/722 en BIE 1987, nr. 25, p. 88-96.

4 Hof Amsterdam 24 juni 2004, *Computerrecht* 2004/49, m.nt. N.M. Wisman.

- c. het is aannemelijk dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen;
- d. afweging van de betrokken belangen van de derde, de service provider en de websitehouder (voor zover kenbaar) brengt mee dat het belang van de derde behoort te prevaleren.

In cassatie bevestigt de Hoge Raad de door het hof aangelegde maatstaf. Over de klacht van Lycos dat artikel 8 van de Wet bescherming persoonsgegevens (Wbp) in de weg zou staan aan verstrekking van de NAW-gegevens, oordeelt de Hoge Raad dat de door die bepaling voorgeschreven afweging van de betrokken belangen nu juist in de door het hof aangelegde toets is betrokken. De Hoge Raad concludeert dat het hof een nauwgezette afweging heeft gemaakt van alle betrokken belangen, waaronder het privacybelang van de websitehouder.<sup>5</sup> Deze afweging is in overeenstemming met de Wbp.

### (Ontwikkelingen in de) relevante wetgeving

De verplichting van tussenpersonen om onder omstandigheden NAW-gegevens af te geven, is in het *Lycos/Pessers*-arrest gebaseerd op artikel 6:162 BW in combinatie met artikel 3:296 BW (waarin is bepaald dat hij die jegens een ander verplicht wordt iets te geven, te doen of na te laten, daartoe door de rechter kan worden veroordeeld). Een mogelijke andere grondslag, die in 2005 al bestond, is het door de voorzieningenrechter in eerste aanleg genoemde artikel 843a Rv, dat bepaalt dat een partij die daartoe een rechtmatig belang heeft inzage, afschrift of uittreksel kan vorderen van bepaalde bescheiden over een rechtsbetrekking waarbij hij partij is. Sinds de implementatie van de Handhavingsrichtlijn<sup>6</sup> in 2007, is in artikel 1019a Rv specifiek bepaald dat een inbreuk op IE-rechten een rechtsbetrekking als bedoeld in artikel 843a Rv is. Voor IE-zaken geldt op grond van artikel 1019a Rv daarnaast een andere (strengere) afwijzingsgrond dan in artikel 843a Rv. De afwijzingsgrond van artikel 843a Rv bepaalt dat niet aan de vordering hoeft te worden voldaan indien daarvoor gewichtige redenen zijn, of als kan worden aangenomen dat een behoorlijke rechtsbedeling ook zonder de gevraagde gegevens is gewaarborgd. Deze afwijzingsgrond geldt niet voor een vordering uit hoofde van artikel 1019a Rv. In plaats daarvan bepaalt artikel 1019a Rv dat afgifte kan worden geweigerd voor zover de bescherming van vertrouwelijke informatie niet is gewaarborgd.

Auteursrechthebbenden kunnen daarnaast (tegenwoordig) ook een beroep doen op artikel 28 lid 9 van de Auteurswet. Dit lid implementeert artikel 8 van de Handhavings-

richtlijn en bepaalt onder meer dat een derde die op commerciële schaal diensten verleent die bij een inbreuk op auteursrechten worden gebruikt, door de rechter kan worden bevolen alles wat hem bekend is omtrent de herkomst en distributiekanaal daarvan te verstrekken. Tenslotte kunnen IE-rechthebbenden zich sinds de implementatie van de Handhavingsrichtlijn nog beroepen op artikel 1019f Rv, waarin is bepaald dat een derde die op commerciële schaal diensten verleent die bij de inbreuk worden gebruikt, door de rechter kan worden bevolen om mondeling of schriftelijk als getuige informatie te verstrekken over de herkomst en distributiekanaal van de inbreukmakende goederen of diensten.

De internet provider vindt op zijn beurt in de Europese en nationale wetgeving een arsenaal aan argumenten om zich te verweren tegen een vordering tot afgifte van NAW-gegevens. Allereerst is in artikel 6:196c lid 4 (de implementatie van artikel 14 E-commercerichtlijn<sup>7</sup>) bepaald dat een hosting provider niet aansprakelijk is voor de opgeslagen informatie, indien hij niet weet van de activiteit of informatie met een onrechtmatig karakter of daarvan niet redelijkerwijs behoort te weten, dan wel – zodra hij daarvan weet of redelijkerwijs behoort te weten – prompt de informatie verwijderd of de toegang daartoe onmogelijk maakt. Dit artikel mocht Lycos in 2005 echter niet baten. Haar verweer dat uit dit artikel moet worden afgeleid dat zij enkel NAW-gegevens hoeft af te staan als de informatie op de website *onmiskkenbaar* onrechtmatig is omdat zij in alle andere gevallen is gevrijwaard van aansprakelijkheid, werd door de Hoge Raad van tafel geveegd. De Hoge Raad overwoog dat uit de E-commercerichtlijn, de totstandkomingsgeschiedenis én de wetsgeschiedenis van de Nederlandse implementatie daarvan blijkt dat het niet in strijd is met de bedoeling van de richtlijn om aan tussenpersonen maatregelen op te kunnen leggen om onwettige activiteiten op te sporen en te voorkomen. Dit geldt ook voor situaties waarin de informatie niet onmiskkenbaar onrechtmatig is. Een andere opvatting zou volgens de Hoge Raad leiden tot het onwenselijke resultaat dat slechts een zeer beperkte groep benadeelden tegen onrechtmatige activiteiten kan optreden bij de burgerlijke rechter, en dat andere benadeelden op voorhand geen rechtsmiddelen kunnen inzetten.<sup>8</sup>

Daarnaast kan een provider zich beroepen op de regelgeving met betrekking tot bescherming van persoonsgegevens en privacy. In de Auteursrechtrichtlijn, de Handhavingsrichtlijn, de E-commercerichtlijn en de nieuwe richtlijnen in het kader van de *Digital Single Market* wordt steeds verwezen naar de privacywetgeving, en wordt overwogen dat die richtlijnen geen belemmering mogen vormen van de beginselen inzake de bescherming van per-

5 HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*), r.o. 5.3.1.-5.4.3.

6 Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele eigendomsrechten.

7 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.

8 HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*), r.o. 5.1.6.

soonsgegevens. Met name op dit gebied zijn er behoorlijk wat ontwikkelingen geweest sinds het arrest uit 2005.

De meest in het oog springende wijziging op het gebied van persoonsgegevens is natuurlijk de verordening die in 2018 voor een lucratief jaar voor juristen heeft gezorgd: de Algemene Verordening Gegevensbescherming (AVG). De grondslagen voor het verwerken van persoonsgegevens zijn in de AVG echter niet veranderd ten opzichte van de Richtlijn bescherming persoonsgegevens en de daarop gebaseerde Wbp. De grondslag waarop rechthebbenden zich kunnen beroepen bij een vordering tot afgifte van persoonsgegevens, blijft het gerechtvaardigd belang dat de rechthebbende heeft bij die verwerking. Dit belang moet opwegen tegen het privacybelang van de betrokkene. Die belangenafweging is – aldus de Hoge Raad – al opgenomen in de *Lycos/Pessers*-criteria.

De AVG heeft wel in zijn algemeenheid een groot aantal nieuwe verplichtingen gecreëerd voor verwerkingsverantwoordelijken, die met name met zich mee brengen dat steeds goed moet worden vastgelegd dat, en op welke manier, aan de AVG wordt voldaan (in goed Nederlands aangeduid met de term ‘*accountability*’). Dit brengt bijvoorbeeld met zich mee dat een verwerkingsverantwoordelijke (en dus ook een auteursrechthebbende die een IP-adres verwerkt dat wordt gebruikt om inbreuk te maken) een verwerkingsregister moet bijhouden waarin is vastgelegd welke gegevens hij verwerkt, met welk doel, aan wie hij de gegevens verstrekt en hoe lang hij deze bewaart. Een andere verplichting die voortvloeit uit de AVG is het uitvoeren van een *data protection impact assessment* (DPIA) als de verwerking een hoog privacyrisico met zich meebrengt. Meer in zijn algemeenheid moet het beleid ten aanzien van persoonsgegevens door verwerkingsverantwoordelijken worden vastgelegd, bijvoorbeeld in een protocol.

Tenslotte is in de AVG expliciet opgenomen dat persoonsgegevens moeten worden verwerkt op een wijze die transparant is voor de betrokkene (artikel 5 lid 1). Helemaal nieuw is dit transparantiebeginsel niet. Ook onder de Wbp moesten verwerkingsverantwoordelijken al bepaalde informatie over verwerkingen verstrekken aan betrokkenen, bijvoorbeeld via een privacyverklaring. Deze informatieverplichting is in de AVG opgenomen in artikelen 13 (voor gegevens die bij de betrokkene zelf worden verzameld) en 14 (voor gegevens die niet direct van de betrokkene zijn verkregen), en uitgebreid ten opzichte van de Wbp. In de AVG is in zijn algemeenheid meer nadruk gelegd op het belang van transparante verwerkingen. Zoals verderop wordt toegelicht speelde dit transparantiebeginsel een grote rol in

de zaak tussen Dutch Filmworks en Ziggo. Het beginsel van zoveel mogelijk transparantie geldt voor alle verwerkingen. In artikel 23 van de AVG in samenhang met artikel 41 van de Nederlandse Uitvoeringswet AVG (UAVG) zijn voor de informatieverplichtingen van artikelen 13 en 14 (en een aantal andere verplichtingen en rechten) uitzonderingen opgenomen. Een van die uitzonderingen is dat deze artikelen buiten toepassing gelaten kunnen worden indien dat noodzakelijk en evenredig is voor de inning van civielrechtelijke vorderingen (zie artikel 41 lid 1 sub j UAVG).

Specifieke regels voor de verwerking van persoonsgegevens via elektronische communicatiemiddelen zijn vastgelegd in de E-privacyrichtlijn<sup>9</sup> (die in 2018 al vervangen zou worden door de E-privacyverordening, maar dit proces lijkt volledig vastgeroest). In deze richtlijn uit 2002 is onder meer bepaald dat communicatie en daarmee verband houdende verkeersgegevens vertrouwelijk behandeld moeten worden (artikel 5 leden 1 en 2 e-Privacy-richtlijn) en dat persoonsgegevens moeten worden gewist of geanonimiseerd na afloop van de verwerking (artikel 6 lid 1 e-Privacyrichtlijn). In artikel 15 e-Privacyrichtlijn is bepaald dat lidstaten voor specifieke doeleinden wettelijke beperkingen op deze verplichtingen kunnen introduceren. Het beginsel van vertrouwelijke behandeling is (pas in 2012) in Nederland geïmplementeerd in artikel 11.2a Telecommunicatiewet.<sup>10</sup> In de literatuur<sup>11</sup> en door gedaagde internet providers<sup>12</sup> is dit beginsel aangegrepen om te beargumenteren dat de *Lycos/Pessers*-maatstaf achterhaald zou zijn. Zij beargumenteerden dat het arrest na de implementatie van artikel 5 E-privacyrichtlijn niet overleefde, omdat een specifieke civielrechtelijke regeling op grond waarvan tussenpersonen klantgegevens moeten afstaan, ontbreekt. Hierdoor zou er geen ruimte zijn om de verplichting tot vertrouwelijke behandeling opzij te zetten. Verderop in dit artikel zal ik bespreken waarom dit argument niet lijkt te slagen.

## Besluiten Autoriteit Persoonsgegevens

De publiekrechtelijke handhaving van de AVG geschiedt door de Autoriteit Persoonsgegevens, onder de Wbp nog College Bescherming Persoonsgegevens genaamd (hierna worden het College Bescherming Persoonsgegevens en de Autoriteit Persoonsgegevens allebei steeds aangeduid als: AP). De AP heeft zich in drie besluiten uitgelaten over de rechtmatigheid van het verwerken van IP-adressen van inbreukmakers en het vorderen van afgifte van de bijbehorende NAW-gegevens bij ISP's. Deze besluiten werden gegeven in het kader van zogenaamde voorafgaande onderzoeken. Zo'n voorafgaand onderzoek was onder de Wbp nog verplicht als er sprake was van het verzamelen

9 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).

10 Kamerstukken II 2010/11, 32549, nr. 16.

11 S.H. Kingma, 'De botsing tussen IE-rechten en privacyrechten. Het einde van het Lycos/ Pessers-tijdperk', *P&I* 2012-4, p. 170 e.v. en E.J. Dommering, 'De zaak Scarlet/Sabam – naar een horizontale integratie van het auteursrecht', *AMI* 2012-2.

12 Bijv. door Ziggo in Rb. Midden-Nederland (vzr.) 16 december 2015, ECLI:NL:RBMNE:2015:8974 (*BREIN/Ziggo*) en in de verderop behandelde procedure tegen Dutch Filmworks.

van persoonsgegevens door eigen waarneming, zonder dat de betrokkenen daarvan op de hoogte zijn (heimelijk onderzoek) of als er sprake was van het verwerken van strafrechtelijke persoonsgegevens ten behoeve van derden. In dat kader moesten rechthebbenden die IP-adressen van inbreukmakers verzamelden deze verwerking dus eerst aan de AP voorleggen. Het voorafgaand onderzoek is met de komst van de AVG afgeschaft. Dit betekent dat rechthebbenden de verwerking in beginsel niet meer eerst aan de AP kunnen voorleggen.<sup>13</sup> Daarmee kunnen rechthebbenden ook geen 'stempel van goedkeuring' van de AP meer krijgen, die ze vervolgens kunnen gebruiken in de civiele procedure tegen de ISP. Dat deze goedkeuring niet alles zegt, blijkt overigens uit het verderop te bespreken arrest *Dutch Filmworks/Ziggo*.

De AP heeft de verwerking van IP-adressen die zijn gebruikt voor het maken van inbreuk op auteursrechten drie keer rechtmatig verklaard. Twee keer werd een dergelijke rechtmatigheidsverklaring afgegeven aan Stichting BREIN,<sup>14</sup> en één keer aan Dutch Filmworks (hierna: DFW).<sup>15</sup> De besluiten van de AP bevatten een aantal interessante overwegingen.

Allereerst verdient opmerking dat de AP in deze drie besluiten oordeelt dat sprake is van strafrechtelijke persoonsgegevens, waarvoor in de AVG (en de Wbp) strengere regels zijn opgenomen. De AP overweegt in dat kader dat in artikel 33 Auteurswet is bepaald dat auteursrechtinbreuk (ook) een misdrijf is. Omdat de IP-adressen zien op persoonsgegevens van personen waartegen een min of meer gegronde verdenking bestaat van handelingen die inbreuk maken op auteursrecht, worden volgens de AP strafrechtelijke persoonsgegevens verwerkt.<sup>16</sup> Op grond van artikel 33 lid 2 sub b van de Uitvoeringswet AVG (UAVG) mogen persoonsgegevens van strafrechtelijke aard worden verwerkt door de verwerkingsverantwoordelijke die deze

gegevens ten eigen behoeve verwerkt, ter bescherming van zijn belangen. De AP concludeert in het besluit inzake DFW dat hier ook onder valt het constateren van inbreuk op de intellectuele eigendomsrechten ten aanzien waarvan DFW kan handhaven.<sup>17</sup> Rechtspersonen die kunnen handhaven, mogen dus op grond van artikel 33 lid 2 sub b van de UAVG strafrechtelijke persoonsgegevens ten aanzien van de inbreuken verwerken. Zij kunnen ook nog een beroep kunnen doen op artikel 32 sub d UAVG, dat bepaalt dat strafrechtelijke gegevens mogen worden verwerkt voor het instellen, uitoefenen of onderbouwen van een rechtsvoorde- ring.

In alle drie de rechtsmatigheidsbesluiten onderzoekt de AP of de rechthebbenden een gerechtvaardigd belang hebben bij de verwerking. De AP oordeelt dat onderzoek naar en handhaving tegen auteursrechtinbreuken een gerechtvaardigd belang is. Daarna toetst de AP of de gegevensbescherming noodzakelijk is, en betreft daarbij dat IP-adressen vaak het enige aanknopingspunt zijn om personen die vermoedelijk inbreukmakende handelingen verrichten op het spoor te komen. Vervolgens toetst de AP de gegevensverwerking aan de vereisten van noodzakelijkheid en subsidiariteit en weegt de betrokken belangen tegen elkaar af. In alle drie de besluiten komt de AP tot de conclusie dat het belang bij handhaving zwaarder weegt dan het privacybelang van de betrokkene, mede gelet op de door de rechthebbenden gehanteerde waarborgen. De voorgenomen verwerkingen zijn dus toegestaan onder de privacywetgeving.

## Europese rechtspraak

Het Europese Hof van Justitie (HvJ EU) heeft zich in verschillende zaken uitgelaten over verstrekking van NAW-gegevens bij handhaving van IE-rechten.<sup>18</sup> In de arresten

13 Tenzij zij een DPIA hebben uitgevoerd en daaruit is gebleken dat er een hoog risico blijft bestaan dat niet met maatregelen is weg te nemen (een *restrisiko*). In dat geval moet een rechthebbende de AP voorafgaand aan de verwerking raadplegen (een zogenaamde 'voorafgaande raadpleging', zie artikel 36 AVG). Voor de verwerking van strafrechtelijke gegevens ten behoeve van derden kan de AP tegenwoordig een vergunning verlenen (artikel 33 lid 4 Uitvoeringswet AVG). Ook in dat geval vindt dus nog steeds een voorafgaande toets door de AP plaats.

14 College Bescherming Persoonsgegevens 16 april 2004, verklaring rechtmatigheid Anti-piraterij bestand Stichting BREIN, z2003-1660 en College Bescherming Persoonsgegevens 6 januari 2016, Besluit inzake de verklaring omtrent de rechtmatigheid van de verwerking 'bittorrent onderzoeksbestand' van Stichting BREIN; z2015-00574.

15 Autoriteit Persoonsgegevens 5 december 2017, Definitief besluit inzake de verklaring omtrent de rechtmatigheid van online handhaving van intellectuele eigendomsrechten door Dutch FilmWorks B.V, z2017-02053.

16 Op deze vaststelling is m.i. wel wat af te dingen. Als er sprake is van een verwerking voor civielrechtelijke doeleinden, waarbij vast staat dat er geen strafrechtelijke vervolging zal plaatsvinden (al is het maar omdat het OM enkel vervolging instelt bij grootschalige inbreuken waarbij het algemeen belang straf-

rechtelijke handhaving vereist), voert het ver om gegevens over (mogelijke) inbreukmakers altijd te kwalificeren als strafrechtelijke persoonsgegevens. Wat mij betreft is het logischer om aan te sluiten bij de systematiek die de AP hanteert voor beeldmateriaal waarop bijzondere persoonsgegevens te zien zijn (dit is per definitie zo omdat je op een foto bijvoorbeeld het ras van de persoon die is afgebeeld ziet). De AP hanteert hiervoor de regel dat indien het beeldmateriaal niet gericht is op het maken van onderscheid op basis van deze gegevens, het niet voorzienbaar is dat iemand dit onderscheid zal maken, en het onvermijdelijk is dat bijzondere persoonsgegevens worden verwerkt bij het maken van het beeldmateriaal, er geen sprake is van bijzondere persoonsgegevens (zie de Beleidsregels cameratoezicht). Bij toepassing van deze criteria naar analogie, zou moeten worden geconcludeerd dat van verwerking van strafrechtelijke persoonsgegevens enkel sprake is indien er daadwerkelijk aangifte wordt gedaan.

17 Autoriteit Persoonsgegevens 5 december 2017, Definitief besluit inzake de verklaring omtrent de rechtmatigheid van online handhaving van intellectuele eigendomsrechten door Dutch FilmWorks B.V, z2017-02053, p. 1.

18 Zie voor een volledig overzicht al. 3.18 t/m 3.29 van de concl. A-G Drijber van 29 januari 2021 bij *Dutch Filmworks/Ziggo*, ECLI:NL:PHR:2021:83.

*Promusicae*<sup>19</sup> en *Bonnier*<sup>20</sup> oordeelde het Hof dat het Unierecht er niet aan in de weg staat dat lidstaten aan een tussenpersoon de verplichting opleggen om persoonsgegevens af te geven met het oog op civielrechtelijke handhaving van auteursrechtinbreuken, maar dat het Unierecht de lidstaten evenmin voorschrijft in een dergelijke verplichting te voorzien. Lidstaten mogen dus zelf weten of zij deze mogelijkheid wel of niet bieden. Uit het arrest *Coty Germany*<sup>21</sup> uit 2015 blijkt dat die keuze kennelijk enkel opgaat in de context van elektronische communicatie. Dit arrest ging niet over een ISP, maar over een bank die met een beroep op het bankgeheim afgifte van NAW-gegevens weigerde. Het HvJ EU oordeelde dat artikel 8 lid 3 van de Handhavingsrichtlijn zich verzet tegen een nationale bepaling op grond waarvan een bankinstelling zich onbeperkt en onvoorwaardelijk mag beroepen op het bankgeheim om niet over te gaan tot het verstrekken van informatie.

In het eerder genoemde arrest *Bonnier*, heeft het HvJ EU verduidelijkt dat een nationale regeling die een bevel tot afgifte van NAW-gegevens mogelijk maakt toelaatbaar is indien (1) duidelijke bewijzen van inbreuk zijn overgelegd, (2) de gevraagde gegevens de opsporing van inbreuk kunnen vergemakkelijken en (3) het belang van de redenen voor dit bevel opweegt tegen de ongemakken of andere nadelen ervan voor degene tot wie het is gericht, of tegen enig ander daarmee strijdig belang.

In twee arresten die niet gingen over verstrekking van NAW-gegevens, maakte het HvJ EU duidelijk dat een effectieve bescherming van het auteursrecht met zich mee kan brengen dat online inbreukmakers niet anoniem kunnen blijven. In *McFadden*<sup>22</sup> boog het Hof zich over de aansprakelijkheid van een winkelier voor het zonder toestemming uploaden van een muziekwerk door een gebruiker van een onbeveiligde wiferverbinding van de winkel. Het Hof concludeerde dat de winkelier inbreuken moet verhinderen of bemoeilijken, en dat de rechthebbende mag verlangen dat de wifi-verbinding wordt beveiligd met een wachtwoord waarbij de gebruikers verplicht zijn hun identiteit op te geven om dat wachtwoord te verkrijgen. In het arrest *Bastei Lübbe* oordeelde het Hof over Duitse rechtspraak waarin was bepaald dat de houder van een internetaansluiting niet meer aansprakelijk kon worden gehouden als hij stelde dat een gezinslid ook toegang had tot deze internetaansluiting, zonder dat hij verder gegevens over het gebruik van de aansluiting hoefde te verstrekken. Deze rechtspraak maakt volgens het Europese Hof de vaststelling van de vermeende inbreuk en de identificatie van de inbreukmaker onmogelijk.

De grondrechten op een doeltreffende voorziening in rechte en op intellectuele eigendom worden hierdoor ernstig aangetast, zodat niet is voldaan aan het vereiste dat een juist evenwicht wordt verzekerd tussen de verschillende grondrechten in kwestie.<sup>23</sup>

In juni vorig jaar sprak het HvJ EU zich voor het eerst sinds de invoering van de AVG uit over de rechtmatigheid van de verstrekking van NAW-gegevens door een internet provider, en over het systematisch verzamelen van IP-adressen door een rechthebbende. De zaak *Mircom*<sup>24</sup> ging over een Cypriotische *copyright troll* wiens werkwijze het is om sommatiebrieven te sturen aan gebruikers die via Bittorrent porno hebben gedeeld. *Mircom* vorderde van ISP Telenet afgifte van NAW-gegevens van deze gebruikers. Deze smakelijke casus riep verschillende interessante vragen op die ik in dit artikel verder niet bespreek.<sup>25</sup> Voor Europese rechthebbenden was deze casus in ieder geval niet het beste scenario om aan het HvJ EU voor te leggen. Toch komen de rechthebbenden er redelijk goed vanaf, en lijkt de omstandigheid dat het hier gaat om persoonsgegevens van pornogebruikers (toch een vrij gevoelig gegeven) het oordeel van het Hof niet te hebben beïnvloed.

Het Hof onderscheidt eerst de twee verwerkingen waar het in deze casus om gaat: (1) het registreren door *Mircom* (althans door een door haar ingehuurd derde) van de IP-adressen van de vermoedelijke inbreukmakers en (2) de door *Mircom* gewenste verstrekking van NAW-gegevens achter die IP-adressen door Telenet. Het Hof overweegt voor beide verwerkingen dat het innen van schuldvorderingen een gerechtvaardigd belang in de zin van artikel 6 lid 1 onder f AVG kan opleveren.<sup>26</sup> De verwerkingen moeten daarnaast noodzakelijk zijn. Aan die voorwaarde is voldaan als de rechthebbende geen andere mogelijkheid heeft om achter de identiteit van de houder van het IP-adres te komen.<sup>27</sup> Vervolgens moet (door de nationale rechter) een belangenafweging worden gemaakt aan de hand van de omstandigheden van het geval.

Het Hof stelt daarna vast dat de E-privacyrichtlijn van toepassing is op zowel de verwerking door *Mircom* als op de afgifte van persoonsgegevens door Telenet, en dat daaruit (kort gezegd) volgt dat verkeersgegevens vertrouwelijk behandeld moeten worden en worden gewist als deze niet langer nodig zijn voor het doel van de transmissie van communicatie, tenzij een van de uitzonderingen van artikel 15 E-privacyrichtlijn van toepassing is. Vervolgens merkt het Hof op dat in dat artikel wordt verwezen naar artikel 13 lid 1

19 HvJ EU 29 januari 2008, C-275/06, ECLI:EU:C:2008:54, AML 2008/5, m.nt. A.H. Ekker (*Promusicae*).

20 HvJ EU 19 april 2012, C-461/10, ECLI:EU:C:2012:219 (*Bonnier*).

21 HvJ EU 16 juli 2015, C-580/13, ECLI:EU:C:2015:485 (*Coty Germany/Stadtparkasse Magdeburg*).

22 HvJ EU 15 september 2016, C-484/14, ECLI:EU:C:2016:689 (*McFadden*).

23 HvJ EU 18 oktober 2018, C-149/17, ECLI:EU:C:2018:841 (*Bastei Lübbe*).

24 HvJ EU 17 juni 2021, C-597/19, ECLI:EU:C:2021:492, *Auteursrecht* 2021-4, m.nt. P. Teunissen (*Mircom/Telenet*).

25 Zie bijvoorbeeld de annotatie van Peter Teunissen in *Auteursrecht* 2021-4, nr. 8, p. 195 e.v. en de annotatie van Leon Dijkman in *IER* 2021/30.

26 *Mircom*, r.o. 109.

27 *Mircom*, r.o. 110.

van de richtlijn bescherming persoonsgegevens, dat inmiddels is vervangen door artikel 23 lid 1 van de AVG. Uit dit artikel volgt de mogelijkheid om de reikwijdte van de verplichting tot vertrouwelijke behandeling in te perken met wetgeving die de rechten en vrijheden van anderen beschermt. Daarnaast is in de AVG (anders dan in de eerdere richtlijn) expliciet opgenomen dat die inperkingsmogelijkheid ook ziet op de inning van civielrechtelijke vorderingen.<sup>28</sup> Het Hof concludeert dat als er inderdaad een nationale wettelijke maatregel is die de reikwijdte van de voorschriften van artikelen 5 en 6 van de E-richtlijn beperkt ten behoeve van het instellen van een civielrechtelijke vordering, zowel de systematische verzameling van IP-adressen door Mircom als de daaropvolgende afgifte door Telenet, niet in strijd zijn met de regelgeving op het gebied van persoonsgegevens.

Al met al laat het Europese Hof het dus aan de lidstaten zelf om te bepalen of een rechthebbende afgifte van NAW-gegevens kan vorderen bij een internet provider (*Bonnier*, *Promusicae* en *Mircom*). Het Hof is ook van oordeel dat effectieve bescherming van eigendomsrechten tot gevolg kan hebben dat inbreukmakers geïdentificeerd moeten kunnen worden (*McFadden* en *Bastei Lübbe*). Als een lidstaat een wettelijke basis voor vordering tot afgifte van NAW-gegevens biedt, is deze in overeenstemming met het Unierecht indien (1) duidelijke bewijzen van inbreuk zijn overgelegd (*Bonnier*), (2) de gevraagde gegevens de opsporing van inbreuk kunnen vergemakkelijken (*Bonnier*), (3) de afgifte noodzakelijk is, bijvoorbeeld omdat identificatie van de houder van het IP-adres anders niet mogelijk is (*Mircom*) en (4) de belangenafweging in het voordeel van de rechthebbende uitvalt (*Bonnier*, *Mircom*). Deze vier criteria komen, in net iets andere woorden, overeen met de *Lycos/Pessers*-criteria van de Hoge Raad in 2005.

### Toepassing Lycos/Pessers-criteria op IE-zaken: lagere rechtspraak tot 2021

In de Nederlandse rechtspraak zien we dan ook dat de *Lycos/Pessers*-criteria sinds 2005 vrij consequent worden toegepast op vorderingen tot afgifte van NAW-gegevens wegens inbreuk op IE-rechten. Van de 17 onderzochte (eind)uitspraken tussen 2005 en 2021, werd in 14 gevallen *Lycos/Pessers* toegepast.<sup>29</sup>

In slechts drie van de uitspraken paste de rechter de *Lycos/Pessers*-criteria niet toe. In één zaak (*BREIN cs/UPS cs* uit

2006<sup>30</sup>) overwoog het Hof Amsterdam expliciet dat de *Lycos/Pessers*-toets op die zaak niet van toepassing kon zijn. *BREIN* voerde in beroep aan dat de voorzieningenrechter ten onrechte had overwogen dat voor afgifte pas plaats is 'indien buiten redelijke twijfel is dat de IP-adressen betrekking hebben op gebruikers die daadwerkelijk illegaal muziek- of andere bestanden aanbieden op hun computer'. *BREIN* voerde aan dat dit een strengere toets is dan de *Lycos/Pessers*-toets dat 'voldoende aannemelijk' is dat de gepubliceerde informatie onrechtmatig is. Volgens het Hof gaat het hier echter om twee verschillende vragen, namelijk niet de vraag of de informatie onrechtmatig is, maar de vraag in hoeverre vast staat dat de IP-adressen ook echt zien op gebruikers die inbreuk hebben gemaakt. Voor die vraag moet volgens het hof een zwaarder criterium worden gehanteerd.

In de recente uitspraak *Dish Network/Worldstream* toetste de Haagse voorzieningenrechter een vordering tot afgifte van NAW-gegevens wegens inbreuk evenmin (expliciet) aan de criteria uit *Lycos/Pessers*.<sup>31</sup> De grondslag voor deze vordering was artikel 843a Rv. Na een uitvoerige bespreking van de relevante voorwaarden gaat de voorzieningenrechter in op de bepalingen van de AVG. De rechter concludeert dat *Dish Network* een gerechtvaardigd belang heeft, dat de verwerking noodzakelijk is en dat de belangen van *Dish Network* zwaarder moeten wegen dan die van de inbreukmakers. Doorgifte van persoonsgegevens aan het Amerikaanse *Dish Network* is eveneens toegestaan, nu zij een beroep kan doen op de uitzondering van artikel 49 lid 1 onder e AVG: de doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Onduidelijk is of bij een beroep op 843a Rv de *Lycos/Pessers*-criteria toegepast zouden moeten worden, nu de Hoge Raad deze heeft toegepast op een vordering uit hoofde van onrechtmatige daad. Toch lijken rechters over het algemeen wel de *Lycos/Pessers*-criteria na te lopen als een vordering op 843a Rv is gebaseerd.<sup>32</sup>

In de meeste onderzochte uitspraken past de rechter de *Lycos/Pessers*-criteria consistent toe. Voorbeelden daarvan kunnen worden gevonden in een reeks zaken tussen Stichting *BREIN* en verschillende tussenpersonen zoals *KPN*, *Leaseweb*, *Google*, en twee *Usenet*providers.<sup>33</sup> In al deze zaken werd de vordering tot verstreking van NAW-gegevens na toepassing van de *Lycos/Pessers*-criteria toegewezen.

28 *Mircom*, r.o. 116-117.

29 Bij uitspraken in hoger beroep is steeds alleen de uitspraak van het Hof meegerekend.

30 Hof Amsterdam, 13 juli 2006, ECLI:NL:GHAMS:2006:AY3854 (*BREIN cs/UPC*).

31 Rb. Den Haag (vzr.) 30 april 2020, ECLI:NL:RBDHA:2020:3980, *AMI 2020-5*, m.nt. P. Teunissen.

32 Zie bijv. Rb. Amsterdam (vzr.) 26 april 2021, ECLI:NL:RBAMS:2021:2050 en Rb. Den Haag (vzr.) 17 augustus 2016, ECLI:NL:RBDHA:2016:9685.

33 Rb. Den Haag (vzr.) 5 januari 2007, ECLI:NL:RBSGR:2007:AZ5678 (*BREIN/KPN*); Hof Amsterdam 3 juli 2008, ECLI:NL:GHAMS:2008:BD6223 (*Leaseweb/BREIN*); Rb. Den Haag (vzr.) 5 oktober 2015, ECLI:NL:RBDHA:2015:11408 (*BREIN/Google*); Hof Den Bosch 10 juli 2018, ECLI:NL:GHSHE:2018:2824 (*Usenet/BREIN*); Rb. Noord-Holland (vzr.) 7 juni 2017, ECLI:NL:RBNHO:2017:4435 (*BREIN/Ewaka Internet Services*).

In uitspraken waarin de vordering tot het verstrekken van NAW-gegevens wordt afgewezen, gebeurt dat om uiteenlopende redenen. In een zaak uit 2010 tussen 123 Video en Ziggo, vordert 123 Video van Ziggo de NAW-gegevens van een gebruiker die pornografisch filmmateriaal op het platform 123 Video had geplaatst, en daarmee inbreuk maakte op het auteursrecht van Kim Holland Productions waarvoor Kim Holland Productions schadevergoeding van 123 Video vorderde. Het Hof wijst de vordering van 123 Video af op grond van criterium c uit het *Lycos/Pessers*-arrest, en oordeelt dat 123 Video onvoldoende aannemelijk heeft gemaakt dat geen minder ingrijpende mogelijkheden bestonden om de door haar benodigde gegevens te achterhalen. Het was niet noodzakelijk die gegevens van Ziggo te verkrijgen, omdat 123 Video op grond van e-mailcorrespondentie en gegevens verkregen bij inschrijving, al over de naam en geboortedatum van de gebruiker beschikte.<sup>34</sup> In een zaak tussen BREIN en Ziggo waarin BREIN NAW-gegevens vorderde van een gebruiker van Ziggo die via Usenet auteursrechtinbreuken zou hebben gefaciliteerd, wijst de rechter de vordering af op grond van criterium a. De rechter oordeelt dat onvoldoende aannemelijk is geworden dat het de bedoeling van de gebruiker was om via Usenet derden te faciliteren en aan te moedigen om inbreuk te plegen op auteursrechten.<sup>35</sup> Interessant aan deze zaak is dat Ziggo aanvoerde dat *Lycos/Pessers* maar zeer beperkt relevant is, omdat het arrest dateert van voor de implementatie van de e-Privacyrichtlijn en artikel 15 van die richtlijn een specifieke wettelijke basis vereist voor het opvragen van privacygevoelige gegevens als NAW-gegevens. De voorzieningenrechter wijst dat argument af omdat artikel 6:162 BW, zoals uitgelegd in *Lycos/Pessers* als een wettelijke basis als bedoeld in artikel 15 fungeert.

In een zaak tussen BREIN en ING wees de voorzieningenrechter de vordering van BREIN tot het verstrekken van de NAW-gegevens door ING af, omdat banken een bijzondere positie hebben en de ING niet 'instrumenteel' is bij het plegen van de auteursrechtinbreuken.<sup>36</sup> De uitkomst van deze zaak zou gelet op het latere arrest van het Europese Hof van Justitie in *Coty Germany* nu hoogstwaarschijnlijk anders uitvallen.

## Dutch Filmworks/Ziggo

Een zaak die zowel in de juridische literatuur als in de media veel aandacht heeft gegenereerd is *DFW/Ziggo*. DFW kondigde in 2017 als eerste organisatie in Nederland aan dat zij handhavingsacties ging instellen tegen downloaders van illegale films. Zoals hiervoor is besproken, gaf de AP een rechtmatigheidsverklaring af voor deze voorgeno-

men verwerkingen. DFW liet vervolgens in de media weten dat zij aan ISP's gegevens van downloaders van de film *The Hitman's Bodyguard* zou opvragen en de gebruikers van de IP-adressen vervolgens zou gaan aanschrijven en hen een schikkingsbedrag van € 150,- zou aanbieden. Het noemen van dit bedrag, dat door de media een 'downloadboete' werd genoemd,<sup>37</sup> zou later geen slimme zet blijken.

Ziggo weigert de NAW-gegevens van de gebruikers van de 174 door DFW aangetroffen IP-adressen aan DFW te verstrekken. DFW vordert bij de rechter afgifte van de gegevens op grond van artikel 6:162 BW in samenhang met artikel 3:296 BW, ingevuld door de *Lycos/Pessers*-leer, maar vangt zowel bij de voorzieningenrechter Midden-Nederland als bij het Hof Arnhem-Leeuwarden bot.

Anders dan de voorzieningenrechter past het Hof-Arnhem Leeuwarden niet de *Lycos/Pessers*-toets toe op de vraag of Ziggo gehouden is de NAW-gegevens te verstrekken. In plaats daarvan onderzoekt het hof of de verwerking voldoet aan de grondslag van artikel 6 lid 1 sub f AVG (gerechtvaardigd belang). Het hof gaat daarvoor na of (a) DFW een gerechtvaardigd belang heeft (b) de verwerking noodzakelijk is en (c) het belang van DFW prevaleert boven het belang van de klanten van Ziggo. Net als de AP oordeelt het hof dat DFW een gerechtvaardigd belang heeft bij handhaving van haar auteursrechten, en dat de verstrekking van NAW-gegevens noodzakelijk is omdat er geen andere manier is om achter de identiteit van de inbreukmakers te komen. Anders dan de AP oordeelt het hof echter dat de belangen van de Ziggo-abonnees zwaarder moeten wegen dan de belangen van DFW. Het hof overweegt daartoe dat DFW niet voldoende transparant is geweest over (a) welke acties zij tegen de Ziggo-abonnees gaat ondernemen en welke criteria zij daarvoor hanteert, met name in de situatie dat onzeker is of de betrokken Ziggo-klant ook daadwerkelijk de inbreukmaker is en (b) welke bedragen zij van de Ziggo-klanten zal gaan vorderen. Hierdoor kan Ziggo volgens het hof op haar beurt tegenover haar klanten ook niet voldoen aan de informatieverplichtingen op grond van de AVG. Bij het oordeel over de te vorderen bedragen klinkt een zekere mate van chagrijn door over de door DFW in de media aangekondigde 'boetes' van € 150 of meer. Het hof zet deze bedragen af tegen de veel lagere bedragen die een consument normaal betaalt voor een legale download of stream. Kennelijk wil het hof de particuliere downloaders (het zal maar je neefje zijn!) behoeden voor Amerikaanse of Duitse praktijken waarbij op grote schaal sommaties met hoge 'boetes' worden verstuurd.<sup>38</sup>

34 Hof Amsterdam 14 december 2010, ECLI:NL:GHAMS:2010:BP7309 (*Ziggo/123 Video*).

35 Rb. Midden-Nederland (vzr.) 16 december 2015, ECLI:NL:RBMNE:2015:8974 (*BREIN/Ziggo*).

36 Rb. Amsterdam (vzr.) 14 mei 2013, ECLI:NL:RBAMS:2013:CA0350.

37 Zie bijv. <https://www.nu.nl/internet/5059076/dutch-filmworks-wil-downloadboetes-van-150-euro-uitdelen.html>.

38 Overigens zijn de in de VS en Duitsland gevorderde schadevergoedingsbedragen over het algemeen een veelvoud van de door DFW genoemde € 150.

Op het arrest van het hof kwam behoorlijk wat kritiek. Reus vindt bijvoorbeeld de uitkomst van de belangenafweging verrassend, onder meer omdat de AP de verwerking door DFW wél rechtmatig achtte en de gevolgen voor de betrokkenen minder groot zijn dan het hof het doet voorkomen. Hij acht het een stap te ver dat het hof zich mengt in de bedragen die DFW wil vorderen van inbreukmakers.<sup>39</sup> Teunissen vindt het onder andere ‘voor serieuze twijfel vatbaar’ of de overwegingen over de hoogte van de schade op hun plaats zijn in deze procedure, nu de relevante belangen van de Ziggo-klienten gelegen zijn in de bescherming van hun persoonsgegevens (en niet financieel zijn), en een oordeel over de hoogte van de schade is voorbehouden aan de rechter die de inbreuk beoordeelt.<sup>40</sup> Ook Seignette stelt vraagtekens bij de overwegingen van het hof over de schade, en acht de mogelijkheid dat een ander dan de Ziggo-abonnee het IP-adres heeft gebruikt, niet redengevend om het NAW-verzoek af te wijzen. De Ziggo-klant is het enige aanknopingspunt voor de rechthebbende, en is de meest gereede partij om aan te spreken. Als een ander de inbreuk heeft gepleegd kan hij dat aanvoeren, maar als het NAW-verzoek bij voorbaat al wordt afgewezen, wordt handhaving onmogelijk.<sup>41</sup>

De verwachtingen over het oordeel van de Hoge Raad waren dus hooggespannen. In een behoorlijke anticlimax deed de Hoge Raad de zaak echter af met toepassing van 81 R.O. Wat de Hoge Raad had gevonden, zullen we dus nooit weten. Wel schreef A-G Drijber een uitgebreide conclusie, die strekte tot verwerping van het cassatieberoep.<sup>42</sup>

Ik licht een paar interessante onderdelen uit de conclusie van de A-G. Allereerst constateert de A-G dat *Lycos/Pessers* nog steeds het relevante toetsingskader is. Het standpunt van Ziggo dat *Lycos/Pessers* is achterhaald door artikel 5 van de E-privacyrichtlijn is volgens de A-G onjuist. Net als de voorzieningenrechter in eerste aanleg, en de voorzieningenrechter in de eerder genoemde zaak tussen BREIN en Ziggo uit 2015,<sup>43</sup> overweegt de A-G dat artikel 6:162 BW zoals uitgelegd in *Lycos/Pessers* kan gelden als een wettelijke basis als bedoeld in artikel 15 E-privacyrichtlijn. Daarvoor is niet nodig dat het gaat om een specifieke nationale wetsbepaling die regelt onder welke voorwaarden provider klantgegevens moet verstrekken. Een algemene grondslag zoals art. 6:162 BW kan volgens de A-G ook als ‘nationale wettelijke regeling’ gelden, mits die kan worden uitgelegd en toegepast op een wijze die verenigbaar is met de toepasselijke Unierechtelijke regelgeving.

Ook interessant zijn de overwegingen van de A-G over het oordeel van het hof dat niet aan de transparantieplicht uit

de AVG is voldaan. DFW had onder meer geklaagd tegen de overweging van het hof dat het te vinden evenwicht tussen de belangen van DFW en de Ziggo-klienten met name is verstoord in de situatie dat onzeker is of de betrokken Ziggo-klant ook daadwerkelijk de inbreukmaker is. De A-G merkt op dat het hof weliswaar heeft overwogen dat dit evenwicht teveel is verstoord in *met name* de gevallen waarin onzeker is of de Ziggo-klant de inbreukmaker is, maar dat de vordering geheel is afgewezen (dus ook ten aanzien de gevallen waarin dit niet onzeker is).<sup>44</sup> Deze overweging van het hof was dus niet doorslaggevend voor de afwijzing. De vraag is dan wel hoe DFW nog meer verduidelijking moet geven over haar handhavingsacties (los van de te vorderen schade) om de vordering wél toewijsbaar te maken. Rechts-overweging 5.18 van het arrest van het hof, waar de klacht tegen was gericht, noemt namelijk geen andere punten waarop DFW transparanter had moeten zijn. Daarnaast lijkt mij het meewegen van de mogelijke omstandigheid dat er abonnees zijn die niet zelf inbreuk hebben gepleegd hoe dan ook problematisch met het oog op *Bastei Lübbe*. Uit *Bastei Lübbe* blijkt dat een regeling die ertoe leidt dat identificatie van de betrokken inbreukmaker onmogelijk is, het recht op intellectuele eigendom in de kern aantast en in strijd is met het Unierecht. Door het feit dat de identiteit van de inbreukmaker niet met (absolute) zekerheid kan worden vastgesteld mee te wegen in de afwijzing van de vordering, lijkt het oordeel van het HvJ EU in *Bastei Lübbe* te worden miskend.<sup>45</sup>

Met betrekking tot de transparantieplicht over de te vorderen schade lijkt de A-G niet enorm onder de indruk van het relaas van het hof: ‘Minder duidelijk vind ik het verband tussen de bescherming van privacybelangen en de voorwaarde dat de rechthebbende van te voren transparantie betracht over de handhavingsmaatregelen die zij voornemens is te nemen. Het gaat bij dat laatste overwegend om een financieel belang van de aangesproken internetgebruikers en, zou ik menen, niet zozeer om een aspect van hun privacy (ervan uitgaande dat de naam van de betrokkenen niet openbaar wordt gemaakt). De door het hof gestelde transparantie-eis vormt in het bestreden arrest slechts één reden waarom de balans voor DFW ongunstig uitvalt, maar acht ik niet de meest overtuigende reden.’<sup>46</sup> Volgens de A-G is het hof echter toch niet uitgegaan van een onjuiste rechtsopvatting. De informatieverplichting die Ziggo onder de AVG heeft, en waar zij alleen aan kan voldoen als zij informatie van DFW krijgt, ziet onder meer op de gevolgen van de verdere verwerking voor de betrokkene. Tot die gevolgen behoort ook het risico om te worden aangesproken op betaling van een (aanzienlijk) schadebedrag, zonder dat zij over de omvang van dat financiële

39 Annotatie van het hof-arrest van J.G. Reus in *Jurisprudentie Bescherming Persoonsgegevens* 2019/6, p. 872 e.v.

40 Annotatie van het hof-arrest van P. Teunissen in *AMI* 2020/2, nr. 4, p. 61 e.v.

41 Annotatie van het hof-arrest van J.M.B. Seignette, IEF 18807.

42 Concl. van A-G Drijber van 29 januari 2021, ECLI:NL:PHR:2021:83.

43 Zie voetnoot 35.

44 Concl. A-G al. 4.35-4.38.

45 Aldus ook Teunissen, *AMI* 2020-2, nr. 4, p. 61 e.v. en Seignette, IEF 18807. De A-G lijkt *Bastei/Lubbe* minder relevant te vinden, zie al. 3.27 van zijn conclusie: ‘Over de reikwijdte van de verplichting van een access provider om NAW-gegevens te verstrekken aan een IE-rechthebbende zegt dit arrest naar mijn mening betrekkelijk weinig.’

46 Concl. A-G al. 4.9.



risico duidelijkheid krijgen.<sup>47</sup> De A-G overweegt over de vergaande invulling van de transparantieplicht door het hof nog wel dat een voor DFW gunstiger beoordeling ook mogelijk was geweest. Bovendien is het tekortschieten van DFW volgens de A-G reparabel.

Net als de eerder genoemde auteurs die kritiek hadden op het arrest van het hof, vraag ik mij af of het recht van betrokkenen om geïnformeerd te worden over risico's van een verwerking van hun persoonsgegevens, zo moet worden uitgelegd dat dit ook ziet op de omvang van mogelijke financiële gevolgen. Het hof lijkt bij zijn beoordeling artikel 5 AVG (de algemene transparantieplicht) en de meer specifieke informatieverplichtingen van artikelen 13 en 14 AVG op één hoop te gooien. De informatieverplichtingen van artikelen 13 en 14 kunnen echter op grond van artikel 41 UAVG buiten toepassing worden gelaten bij verwerkingen in het kader van inning van civielrechtelijke vorderingen. Het is gezien die uitzondering de vraag of de AVG wel voorschrijft dat Ziggo desalniettemin (op grond van de meer algemene transparantieplicht van artikel 5 AVG) haar abonnees zó uitgebreid moet kunnen informeren dat zij ook duidelijkheid krijgen over de hoogte van een mogelijke schadevergoedingsaanspraak. Daarbij is ook relevant dat uit het arrest van het hof blijkt dat Ziggo er in haar algemene voorwaarden wel op wijst dat haar klanten moeten instaan voor aanspraken van derden wegens auteursrechtinbreuk. De abonnees konden dus weten dat zij mogelijk aansprakelijk konden worden gehouden voor onrechtmatig gebruik van de door Ziggo verleende diensten. Dat zij niet konden weten voor welk bedrag, lijkt mij niet een belang dat de AVG beoogt te beschermen.

### Conclusie: meer huiswerk voor rechthebbenden

Uit vrijwel alle uitspraken sinds 2005, en de conclusie van de A-G in *DFW/Ziggo*, blijkt dat de *Lycos/Pessers*-criteria nog springlevend zijn. De A-G concludeert dat uit de E-privacyrichtlijn niet volgt dat *Lycos/Pessers* niet langer een rechtsgrond voor het opvragen van NAW-gegevens is. Ook concludeert de A-G dat *Lycos/Pessers* een AVG- en grondrechtconforme uitleg toelaat. Ook uit de Europese jurisprudentie en het recente *Mircom*-arrest van het HvJ EU volgt niet dat de *Lycos/Pessers*-toets met de komst van de aangescherpte privacywetgeving achterhaald is. De door het HvJ EU aangelegde criteria komen, in net andere woorden, overeen met *Lycos/Pessers*.

Waar rechthebbenden 17 jaar na *Lycos/Pessers* wel rekening mee moeten houden zijn de aangescherpte verplichtingen op het gebied van *accountability* en transparantie.

Deze verplichtingen brengen met zich mee dat een rechthebbende, voordat IP-adressen van (mogelijke) inbreuk-

makers worden verwerkt, zijn beleid voor deze verwerking zal moeten vastleggen. Ook zal de rechthebbende moeten nagaan of het nodig is een DPIA uit te voeren.

De rechthebbende zal ook zo transparant mogelijk moeten zijn over de verwerking. De vraag is wel of daarbij steeds aan de vergaande transparantie-eis van het hof in *DFW/Ziggo* moet worden voldaan. Deze strenge invulling van de transparantieverplichting lijkt niet zozeer direct voort te vloeien uit de AVG, maar eerder uit de omstandigheid dat DFW afgifte van de NAW-gegevens van een groot aantal particuliere gebruikers vorderde, en daarbij in media aankondigde een vast bedrag aan schadevergoeding te gaan vorderen. Het lijkt mij in ieder geval niet de bedoeling van hof (of de AG) dat een rechthebbende bij *iedere* vordering tot opgave van NAW-gegevens precies moet gaan uitleggen wat hij vervolgens met die gegevens gaat doen, welke stappen hij zal zetten in alle mogelijke scenario's, en welke schade hij gaat vorderen. In de lagere rechtspraak lijkt de door het hof aangelegde strenge transparantie-toets inderdaad niet te worden toegepast op het vorderen van NAW-gegevens van één of enkele (semi) professionele inbreukmaker(s). In het eerder genoemde vonnis van de voorzieningenrechter Den Haag in de zaak *Dish Network/World Stream*, gaat de voorzieningenrechtbank voorbij aan het betoog van WorldStream dat Dish Network had moeten onderbouwen hoe zij de rechten van haar klanten zou waarborgen, welke schade zij zou gaan vorderen en welke acties zij per individuele klant zou gaan inzetten.<sup>48</sup> De rechtbank Den Haag oordeelde recent in de zaak *PVH/Facebook* dat uit de conclusie van A-G Drijber volgt dat de *Lycos/Pessers*-leer nog geldend recht is, en wees de vordering tot afgifte van NAW-gegevens (grotendeels) toe, zonder daarbij te betrekken welke acties PVH voornemens was tegen de gebruikers te treffen.<sup>49</sup> De rechtbank betreft bij haar oordeel nadrukkelijk de omstandigheid dat het gaat om partijen die vaak in herhaling vallen en dat die 'minder bescherming verdienen dan bijvoorbeeld een particulier die eenmalig een misstap begaat'.

Voor (organisaties van) rechthebbenden die op grotere schaal IP-adressen van particuliere inbreukmakers willen verwerken en de bijbehorende NAW-gegevens willen opvragen, betekent de komst van de AVG met name (nog) meer huiswerk. In die gevallen lijkt *DFW/Ziggo* er wél op te wijzen dat voorafgaand aan de verwerking zal moeten worden uiteengezet welke acties er tegen de inbreukmakers zullen worden ondernomen, hoe de schadevordering tot stand zal komen, en wat abonnees kunnen doen als zij zelf niet de inbreukmaker zijn. Hoewel er vraagtekens geplaatst kunnen worden bij de ruime toepassing van het transparantiebeginsel door het hof, lijkt dit voor rechthebbenden wel een oplosbaar probleem. Het zou dus zomaar kunnen dat DFW het met een aangepast protocol de volgende keer wel redt.

47 Concl. A-G al. 4.51.

48 Zie voetnoot 31.

49 Rb. Den Haag 17 maart 2021, ECLI:NL:RBDHA:2021:2422 (*PVH/Facebook*).