

# Effectief procederen tegen anonieme internetgebruikers



**INFORMATIEPLICHT  
ONDERNEMINGS-  
PENSIOENFONDSEN**



**EUROPESE INVLOED  
OP REGELGEVING  
MEETBAAR**

# 29



# EFFEKTIEF PROCEDEREN TEGEN ANONIEME INTERNETGEBRUIKERS

1529 *Mr. R.D. Chavannes*

*Remy Chavannes is advocaat te Amsterdam. Hij trad in de hier beschreven procedure Lycos/Pessers in cassatie op voor Lycos. De tekst is afgesloten op 1 mei 2007.*

***De Hoge Raad heeft in het arrest Lycos/Pessers uit 2005 bevestigd dat een internetaanbieder onder bepaalde omstandigheden verplicht kan worden om de naam- en adres- (ook wel NAW-) gegevens van een klant te verstrekken aan een derde die meent dat de klant hem onrechtmatig heeft bejegend. Zodoende kan op last van de rechter de anonimiteit van internetgebruikers worden doorbroken. De wens om te voorkomen dat een internetgebruiker zich ongestraft anoniem kan misdragen is begrijpelijk. De in de jurisprudentie ontwikkelde procedure heeft echter als nadeel dat de anonieme gebruiker géén partij wordt in de procedure waarin zijn anonimiteit in het geding is en daarom onvoldoende mogelijkheden heeft om uiteen te zetten waarom hij die uiting – anoniem – mocht doen. Bovendien wordt zijn internetaanbieder opgescheept met de lastige en kostbare taak om een publicatie te beoordelen en verdedigen zonder voldoende kennis van de feiten. Het is tijd voor een wettelijke regeling die tegemoetkomt aan de belangen van de beschadigde derde, de anonieme internetgebruiker en de internetaanbieder.***

*Een uitgebreide versie van dit artikel is te vinden op [www.njb.nl](http://www.njb.nl) als link in dit artikel.*

Uit de zaak Lycos/Pessers<sup>1</sup> blijkt dat er bij zaken over verstrekking van NAW-gegevens door internetaanbieders (ISP's) twee wezenlijke belangen in botsing komen. Enerzijds gaat het om het recht van een derde die stelt benadeeld te zijn door een publicatie of andere handeling van een anonieme internetgebruiker, om die internetgebruiker in rechte aan te spreken en bijvoorbeeld staking, rectificatie of schadevergoeding te eisen. Er moet een mechanisme zijn om anonimiteit op te heffen, zo blijkt uit het arrest Lycos/Pessers, omdat het anders onmogelijk zou zijn op te treden tegen onrechtmatige handelingen van anonieme internetgebruikers. De voortschrijdende discussie in het kader van de fundamentele herbezinning van het burgerlijk procesrecht, over uitbreiding van de exhibitieplicht

en invoering van een vorm van disclosure, vormt een erkenning van het feit dat er zowel een algemeen als een individueel belang bestaat bij effectieve mogelijkheden om je recht te halen.<sup>2</sup> Het recht op anonimiteit vindt zijn beperking in de bescherming van rechten van derden.

Anderzijds heeft iedere burger in beginsel het recht zich publiekelijk uit te laten over zaken die hem bezighouden, zonder zijn identiteit prijs te geven. Juist in geval van 'kwetsbare' uitingen, waarin bijvoorbeeld maatschappelijke impopulaire standpunten worden verdedigd of misstanden aan de kaak worden gesteld die bepaalde betrokkenen liever onbesproken zien blijven, is het voor het maatschappelijke debat van belang dat de internetgebruiker zijn anonimiteit kan bewaken en zo gevrijwaard kan blijven van kostbare en beangstigende rechtszaken die tot doel hebben hem het zwijgen op te leggen. Als het niet mogelijk is zich publiekelijk te uiten zonder vrees voor represailles, zullen bepaalde uitingen niet meer gedaan worden, met verarming van het maatschappelijk debat als gevolg.

1. HR 25 november 2005, RvdW 2005, 133 (Lycos/Pessers).

2. Kamerstukken II 2006/07, 30 951, nr. 1. De minister spreekt van 'een tijdige (efficiënte) informatie-uitwisseling en een verdere informatie- en daarmee machtsevenwicht tussen partijen'.

De positie van ISP's in deze botsing van belangen is een bijzondere. De ISP is vaak (als enige) feitelijk in staat de gewenste NAW-gegevens te verstrekken. Net als de journalist kent de ISP zijn 'bron' en geeft hij het verhaal van de bron door. Anders dan de journalist heeft de ISP echter geen inhoudelijke betrokkenheid bij het 'verhaal' en is hem, volgens de Hoge Raad, ook niks 'toevertrouwd'.<sup>3</sup> Hij treedt slechts op als facilitator van het publieke communicatieproces en heeft dus (uitzonderingen daargelaten) geen inhoudelijke betrokkenheid bij – of noodzakelijkerwijs een mening over – de gewraakte uiting. Op grond van de Richtlijn elektronische handel (zoals geïmplementeerd in art. 6:196c BW) is hij in beginsel ook niet aansprakelijk voor de inhoud van die uiting. In zoverre is zijn positie vergelijkbaar met de beheerder van Hyde Park Corner in Londen of de Albert Heijn die een prikbord voor klanten ophangt. De positie van de ISP is dus ook een andere dan de winkelier die inbreukmakende goederen verkoopt en, op basis van bestaande jurisprudentie en de per 1 mei 2007 geïmplementeerde IE Handhavingsrichtlijn, gedwongen kan worden de gegevens van zijn leveranciers te noemen.<sup>4</sup> De nieuwe bevoegdheid van art. 1019f Rv is alleen beschikbaar in zaken betreffende inbreuk op intellectuele eigendom, waarbij de vermeende inbreukmaker bekend is en gedagvaard is – en waarbij de rechter (voorshands) oordeelt dat ook daadwerkelijk sprake is van inbreuk.<sup>5</sup> Voor het verkrijgen van NAW-gegevens bij ISP's blijft een kort geding langs de lijnen van Lycos/Pessers aangewezen.

In concrete gevallen moet de ISP zijn verplichtingen jegens zijn klant (op grond van de Wet bescherming persoonsgegevens en art. 8 EVRM) afwegen tegen zijn verplichtingen jegens de derde (op grond van de door de Hoge Raad erkende zorgvuldigheidnorm, die in concrete gevallen verstrekking van gegevens kan voorschrijven). In de literatuur wordt de lastige positie van de ISP doorgaans als spagaat aangeduid.<sup>6</sup> De rol van de ISP in het openbare communicatieproces geeft hem bovendien een eigen belang, dat individuele gevallen overstijgt. Dat belang kan in individuele gevallen het belang van de klant en de derde doorkruisen, wat de afweging die de rechter moet maken verder bemoeilijkt.

In het hiernavolgende bespreek ik allereerst het probleem: waarom is een recht op anonieme communicatie belangrijk en waarom wordt dat recht bedreigd door de huidige praktijk van een kort geding tussen ISP en derde langs de lijnen van Lycos/Pessers? Vervolgens bespreek ik een aantal oplossingen, vanuit de veronderstelling dat de materiële afwegingscriteria die de Hoge Raad in Lycos/Pessers heeft aanvaard op zich niet gewijzigd (kunnen of hoeven te) worden. Het gaat er vooral om, te zorgen dat de belangen van de anoniemus op adequate wijze worden betrokken bij de afweging die Lycos/Pessers voorschrijft, met andere woorden dat de anoniemus zich desgewenst effectief kan verzetten tegen opheffing van zijn anonimiteit.

Ik beperk mij in deze bijdrage tot wijzigingen van het Wetboek van Burgerlijke Rechtsvordering. In de uitge-

## *De ISP is vaak (als enige) feitelijk in staat de gewenste NAW-gegevens te verstrekken. Net als de journalist kent de ISP zijn 'bron' en geeft hij het verhaal van de bron door.*

breidere online versie van dit artikel (zie [www.njb.nl](http://www.njb.nl)) wordt ook een aantal minder vergaande (en mijns inziens minder effectieve) alternatieven besproken, zoals een bindend-adviesprocedure.

### 1. HET PROBLEEM

#### 1.1. Het belang van anonieme communicatie

De gedachte dat er zoiets is als een recht op anonieme communicatie, gaat in het Amerikaanse recht makkelijker dan in het Europese of het Nederlandse.<sup>7</sup> Het Supreme Court ziet het als een vitaal onderdeel van de bescherming van de vrijheid van meningsuiting:

*[A]n author is generally free to decide whether or not to disclose his or her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, [...] the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment. [...] Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority.<sup>8</sup>*

3. Zie r.o. 5.3.7 van het arrest.

4. Zie HR 27 november 1987, NJ 1988, 722, m.nt. LWH (Chloé/Peeters) en art. 1019f Rv, ingevoerd bij wet van 8 maart 2007, Stb. 2007, 108.

5. Aldus art. 8 lid 1 van de IE Handhavingsrichtlijn en de minister in Kamerstukken II 2005/06, 30 392, nr. 6, p. 7.

6. Zie laatstelijk L.A.R. Siemerink, *De overeenkomst van Internet Service Providers met consumenten* (diss. Leiden), 2007, par. 6.2.2.2.

7. Zie uitvoerig: A.H. Ekker, *Anoniem communiceren: van drukpers tot weblog. Een onderzoek naar de grondrechtelijke bescherming van anonieme openbare communicatie* (diss. UvA), 2006.

8. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 341-342, 356 (1995).

## *In het Nederlandse burgerlijke procesrecht is het vermoedelijk onmogelijk om een onbekende persoon te dagvaarden, jegens een onbekende een vonnis ten uitvoer te leggen of als anonieme partij verweer te voeren.*

Ook op internet is de mogelijkheid om anoniem te publiceren een essentieel onderdeel van de vrijheid van meningsuiting. Amerikaanse rechters hebben dat recht herhaaldelijk erkend – en afgewogen tegen de belangen van derden.<sup>9</sup> De ervaring heeft geleerd dat bedrijven soms ook gebruik maken van procedurele middelen om ongewenste kritiek de mond te snoeren. Vaak heeft de eiser voldoende belang en middelen om een zaak door te zetten, ook als de zaak juridisch zwak is, omdat (de dreiging van) jarenlange procedures en kosten de meeste potentiële critici aanzet tot zelfcensuur. Dergelijke zaken vormen een bedreiging voor de open discussie op internet dat juist, door de mogelijkheden die het biedt om met beperkte middelen een groot publiek te bereiken, bij uitstek een medium is dat vrijheid van meningsuiting ondersteunt.<sup>10</sup>

Dezelfde argumenten voor een (grond)recht op anonieme communicatie zijn in de Nederlandse context aangevoerd.<sup>11</sup> In Europees verband heeft het Comité

van Ministers van de Raad van Europa dat belang in 2003 erkend, daarbij slechts een uitzondering makend voor strafvordering:

*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. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.<sup>12</sup>*

In het arrest Lycos/Pessers spreekt de Hoge Raad niet van een 'recht' maar van een 'belang' bij anonimiteit; hij overweegt 'dat niet lichtvaardig mag worden voorbijgegaan aan het belang van de vrije meningsuiting, waaronder in bepaalde gevallen het belang van de websitehouder zijn mening anoniem te kunnen uiten'. Daaraan koppelt de Hoge Raad de eis van rechterlijke 'terughoudendheid' bij opheffing van anonimiteit. Ekker betoogt in zijn proefschrift dat de Hoge Raad in zijn eerdere jurisprudentie de kans heeft gemist om een heldere koppeling te leggen tussen anonimiteit en de uitingsvrijheid die het helpt beschermen.

### *1.2. Huidige praktijk en Lycos-criteria*

De huidige praktijk is dat de derde die een anonieme internetgebruiker wil aanspreken, zich wendt tot de ISP met een eis om verstrekking van de NAW-gegevens. Als de ISP dat weigert, kan een civiele procedure volgen (doorgaans een kort geding), waarin de derde de ISP dagvaardt en eist dat deze alsnog de gegevens verstrekt. De grondslag van die vordering is volgens de Hoge Raad (overweging 5.2.2 van het arrest Lycos/Pessers) een maatschappelijke zorgvuldigheidsnorm, die inhoudt dat een hosting provider in een geval, waarin het gaat om een op de website gepubliceerde, anoniem geuite, ernstige beschuldiging, onder omstandigheden onrechtmatig handelt door de bij haar bekende NAW-gegevens van de websitehouder niet aan de beschuldigde bekend te maken. De ISP is verplicht de gegevens van zijn klant te verstrekken, als de volgende omstandigheden zich voordoen:

a. de mogelijkheid dat de informatie, op zichzelf be-

9. Zie onder meer *American Civil Liberties Union v. Johnson* (D.N.M. 1998) 4 F. Supp.2d 1029, 1033; *American Civil Liberties Union v. Miller* (N.D. Ga. 1997) 977 F. Supp. 1228, 1230; *ApolloMEDIA Corp. v. Reno* (1999) 526 U.S. 1061, (C.D. Cal. 1998) 19 F. Supp.2d 1081. Het District Court in the Northern District of California benadrukt in de richtinggevende zaak *Seescandy* dat 'the need to provide injured parties with an forum in which they may seek redress for grievances (...) must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously. (...) People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity'. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999). <<http://www.legal.web.aol.com/aol/aolpol/seescandy.html>>.

10. Zie verder Ekker, *Anoniem communiceren*, hoofdstuk 4.5.

11. Zie Ekker, 'Anonimiteit en uitingsvrijheid op het Internet: het onthullen van identificerende gegevens door Internetproviders', *Mediaforum* 2002-11/12, p. 348-351; zie ook L.F. Asscher, 'Niemand als consument. Naar een evenwichtig grondrecht op anonimiteit', in: *De e-Consument. Consumentenbescherming in de Nieuwe Economie*, Den Haag: Elsevier Juridisch 2000, p. 7-20. <<http://www.ivir.nl/publicaties/asscher/niemand.html>>; Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving* (diss. Amsterdam), handelseditie Amsterdam, Otto Cramwinckel 2002; en het artikel van Asscher en Ekker in de *Volkskrant* van 26 augustus 2003, 'Anonimiteitswet is hard nodig', <<http://www.ivir.nl/publicaties/asscher/opiniecampinazaak.htm>>.

12. *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. <[http://www.osce.org/documents/rfm/2003/05/94\\_en.pdf](http://www.osce.org/documents/rfm/2003/05/94_en.pdf)>.



- schouwd, jegens de derde onrechtmatig en schadelijk is, is voldoende aannemelijk;
- b. de derde heeft een reëel belang bij de verkrijging van de NAW-gegevens;
  - c. aannemelijk is 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 serviceprovider en de websitehouder (voor zover kenbaar) brengt mee dat het belang van de derde behoort te prevaleren.

Een belangrijk nadeel van de huidige werkwijze is dat de ISP in eerste instantie gedwongen wordt zelf de hier geschetste afwegingscriteria toe te passen en een beslissing te nemen over het al dan niet verstrekken van gegevens. Daartoe voelen veel ISP's zich niet bevoegd en niet geëquipeerd. Als zij echter weigeren de gegevens te verstrekken, belanden zij in een situatie waarin zij zich in kort geding moeten verweren aan de hand van deze afwegingscriteria, waarbij zij in de praktijk zowel hun eigen afstandelijkheid als het anonimiteitsbelang van de anonieme klant moeten bepleiten. Dit terwijl zij onvoldoende kennis hebben van de feiten en belangen aan de kant van de klant. Een dergelijke werkwijze plaatst de ISP voor aanzienlijke onzekerheid en kosten – en betekent in de praktijk dat

het belang van de anonieme klant onvoldoende kan worden behartigd.

### *1.3. Geen bruikbare oplossing binnen het bestaande burgerlijke procesrecht*

Het probleem wordt vooral veroorzaakt, doordat het in het Nederlandse burgerlijke procesrecht vermoedelijk onmogelijk is om een onbekende persoon te dagvaarden, jegens een onbekende een vonnis ten uitvoer te leggen of als anonieme partij verweer te voeren.

Een geldige dagvaarding moet de naam en woonplaats van de gedaagde bevatten (art. 45 lid 2 Rv). Er bestaat wel een specifieke uitzondering voor kraakpanden (art. 45 lid 3 jo. 61 Rv), waarbij een dagvaarding kan worden betekend 'aan de bewoners van dit pand', zonder dat deze met naam genoemd hoeven te worden. Sommige schrijvers zouden ook een dagvaarding toelaten, waarbij een duidelijke en niet voor twijfel vatbare aanduiding van de gedaagde partij deze voldoende identificeert.<sup>13</sup> Of een rechter een e-mail adres of een website als zodanig zou aanmerken, is zeer twijfelachtig. Bovendien lijkt toepassing van deze mogelijkheid

<sup>13</sup> Zie bijvoorbeeld Kluwer, *Burgerlijke rechtsvordering (oud)*, losbladig, aantekening 6 bij art. 5 Rv (oud).

buiten krakerszaken überhaupt problematisch. In een recent arrest overweegt het Hof Amsterdam nog dat de uitzondering van art. 45 lid 3 jo. 61 Rv 'restrictief' moet worden uitgelegd – zo restrictief zelfs, dat zij niet eens van toepassing is bij de ontruiming van een ongebouwde onroerende zaak of een gedeelte daarvan.<sup>14</sup> Zelfs als het mogelijk zou zijn een geldige dagvaarding op geldige wijze te betekenen aan de anoniemus en de rechter bereid zou zijn tegen die gedaagde een verstekvonnis te wijzen, dan is het maar de vraag wat de eiser daaraan heeft: het is vermoedelijk niet goed mogelijk om een vonnis, gewezen tegen iemand waarvan bijvoorbeeld alleen een website- of e-mailadres bekend is, ten uitvoer te leggen. Om schadevergoe-

### **Lastgeving ter incasso?**

Denkbaar is nog dat de anonieme klant zijn ISP (of een derde) last geeft om op eigen naam ten behoeve van de klant te procederen, een figuur die bij de uitoefening van vorderingsrechten bekend is als lastgeving ter incasso. Voordeel van een dergelijke constructie zou zijn dat de rechter dan het belang van de lastgever ten volle kan meewegen. Het is echter de vraag of lastgever gedurende de principiële discussie over zijn recht op anonimiteit, die anonimiteit wel kan behouden. Ligt in de nemo plus-regel van art. 6:145 BW niet besloten dat de wederpartij bij een rechtsovergang al zijn processuele verweren behoudt en dus recht heeft om te weten tegen wie hij eigenlijk procedeert?<sup>15</sup>

## *In krakerszaken is doorgaans geoordeeld dat anonieme gedaagden alleen konden verschijnen door hun namen bekend te maken, vooral omdat de eiser moeilijk kan reageren op anoniem verweer.*

ding te verhalen, zal toch echt bekend moeten zijn bij wie. Ook als de rechter de anoniemus veroordeelt om zich bekend te maken, heeft de derde geen effectieve manier om dat af te dwingen of om dwangsommen te incasseren als de veroordeelde niet thuis geeft.

Wat de belangen van de anonieme gedaagde betreft, speelt nog het probleem dat hij in beginsel niet anoniem kan verschijnen in de procedure. Als hij verweer wil voeren, moet hij zijn naam bekend maken. Als hij vindt dat hij goede gronden heeft om zijn anonimiteit te behouden, bestaat er geen procedure om die aan de rechter kenbaar maken.

Het is dus zeer de vraag, of de wet toelaat dat een partij in het geding verschijnt, zelfs in kort geding waar de procesregels minder streng worden toegepast, zonder vermelding van zijn echte naam. Een rechter die bereid is de regels welwillend toe te passen met het oog op het maatschappelijke en praktische probleem waar derden, ISP's en hun anonieme klanten voor staan, zou wellicht bereid zijn hieraan mee te werken, maar deze weg zal vermoedelijk in veel gevallen doodlopen. Hoe dan ook zou het hoogstwaarschijnlijk niet mogelijk zijn om als anoniemus in beroep te gaan tegen een kortgedingvonnis, want een appeldagvaarding moet in elk geval de naam van de appellante bevatten. Al met al zou deze route een interessante proefprocedure opleveren, maar is deze vermoedelijk niet daadwerkelijk bruikbaar in de praktijk.

De lasthebber is bovendien zélf aansprakelijk voor de gevolgen: als er een schadevergoeding wordt toegekend, dient hij deze zelf te betalen. Die kan hij wel verhalen op de lastgever, maar daarin schuilt een duidelijk (incasso)risico. Ook voor de derde is deze oplossing onvolledig, omdat, als de rechter de uiting onrechtmatig acht, de derde jegens de lastnemer moeilijk een algemeen verbod kan krijgen – laat staan afdwingen – om zich in de toekomst van soortgelijke uitingen te onthouden. Voor een dergelijke vordering behoudt de derde dus een belang bij verstrekking van de NAW-gegevens van de lastgever.

## **2. EEN NEDERLANDSE JOHN DOE PROCEDURE**

In de Verenigde Staten is het probleem al eerder onderkend en zijn oplossingen ontwikkeld die wel worden aangeduid als 'John Doe'-procedure. Er zijn verschillende varianten, maar in de regel gaat het om een procedure waarin de derde de ISP verzoekt om de NAW-gegevens bekend te maken. De rechter wijst dat verzoek toe, tenzij de anoniemus zich binnen een bepaalde termijn in de procedure mengt en op overtuigende wijze zijn recht op anonimiteit verdedigt. Hoe zou een dergelijk systeem in het Nederlandse recht kunnen worden ingevoerd?

### *2.1. Invoering van anoniem dagvaarden en procederen*

Eén mogelijke oplossingsrichting zou kunnen zijn om de regels in het burgerlijk procesrecht over dagvaarding en procesdeelname zodanig aan te passen, dat het mogelijk is om een anoniemus te dagvaarden, als

14. Hof Amsterdam 8 maart 2007, NJF 2007, 300.

15. Zie ook HR 26 november 2004, NJ 2005, 41.

anonymus deel te nemen aan het proces en om een vonnis ten uitvoer te leggen jegens een anonymus.

#### **Anonieme dagvaarding**

Dagvaarding van een anonymus vergt vermoedelijk een verruiming van het bestaande art. 45 lid 3 Rv omtrent dagvaarding van krakers, of toevoeging van een aparte bepaling over dagvaarding van anoniemi. Vermoedelijk zal steeds de eis moeten blijven gelden, dat de dagvaarding waarin de gedaagde niet bij naam wordt genoemd, deze toch wel zodanig identificeert dat daarover geen twijfel of misverstand kan bestaan. Een aanduiding als 'degene die op 15 mei 2006 een bericht plaatste op het forum van website X' is niet voldoende, maar 'de houder op 15 mei 2006 van het e-mail adres xyz@isp.nl' vermoedelijk wel.

Betekening van de dagvaarding van de anonymus van wie de woonplaats bekend is, kan zonder wetswijziging plaatsvinden via de bestaande figuur van de openbare dagvaarding via een dagblad (art. 54 lid 2 Rv). Het lijkt echter wenselijk om daarnaast ook te eisen dat een afschrift van de dagvaarding per e-mail wordt verzonden als een e-mail adres van de gedaagde bekend is: de kans is immers veel groter dat daarmee het doel van de betekening wordt bereikt, te weten dat de gedaagde op de hoogte wordt gesteld van het feit dat er een zaak tegen hem is ingesteld. Als aanvullende zekerheid in dit verband zou van een derde van wie kan worden aangenomen dat hij beschikt over de daadwerkelijke identiteit of het daadwerkelijke (internet)adres van de gedaagde (zoals in dit geval de ISP), kunnen worden verlangd dat hij een afschrift van de dagvaarding aan de gedaagde toezendt.

#### **Anonieme procesdeelname**

Omdat de wet niet voorziet in anoniem dagvaarden, biedt de wet ook geen antwoord op de vraag of de anonymus met behoud van anonimiteit in het geding kan verschijnen. In krakerszaken is er doorgaans geoordeeld dat anonieme gedaagden alleen konden verschijnen door hun namen bekend te maken, vooral omdat de eiser moeilijk kan reageren op anoniem verweer.<sup>16</sup> Voor procesdeelname van de anonymus zal dus een wettelijke voorziening moeten worden getroffen, die inhoudt dat een partij die anoniem is gedagvaard bij procureur in het geding kan verschijnen onder de aanduiding waaronder hij is gedagvaard.

Een vervolgvraag is of het voor de anonymus mogelijk zou moeten zijn om ook na het vonnis in eerste aanleg anoniem door te procederen – als geïntimeerde of, als het toewijzende vonnis niet uitvoerbaar bij voorraad is verklaard, als appellant. Op zich lijken er mij geen principiële aanvullende redenen om niet ook in hoger beroep anoniem procederen mogelijk te maken. Dat vergt wel een verdere wetsaanpassing, in elk geval aan art. 45 lid 2 sub b Rv, dat bepaalt dat een exploit (waaronder een appeldagvaarding) de naam bevat van degene op wiens verzoek de betekening plaatsvindt.

## *Een verzoekschriftprocedure is niet per se sneller of goedkoper dan een kortgedingprocedure.*

#### **Tenuitvoerlegging jegens de anonymus**

Om tegemoet te komen aan het terechte bezwaar dat de eiser zijn vonnis niet ten uitvoer kan leggen tegen een anonymus, zou bepaald kunnen worden dat de anonymus slechts anoniem in het geding kan verschijnen als hij zich wel bekend maakt bij een onafhankelijke derde (bijvoorbeeld zijn ISP of wellicht een notaris), die vervolgens verplicht is de NAW-gegevens van de anonymus bekend te maken als de rechter dat in zijn vonnis bepaalt.

Daarmee is nog niet het probleem opgelost van de tenuitvoerlegging van een verstekvonnis tegen een niet verschenen anonieme gedaagde. Het lijkt mij echter op het eerste gezicht niet bezwaarlijk om te aanvaarden dat de ISP de NAW-gegevens verstrekt als de eiser hem een afschrift toont van een in kracht van gewijsde gegaan of bij voorbaat uitvoerbaar verklaard verstekvonnis tegen de klant, waarin deze onder meer wordt bevolen zijn identiteit bekend te maken. Anders gezegd, als de klant een processueel gewaarborgde mogelijkheid ongebruikt laat om zijn handelwijze met behoud van anonimiteit te verdedigen, kan hij moeilijk verwachten dat zijn ISP volhardt in de verdediging van die anonimiteit.

#### **Voor- en nadelen**

Het belangrijkste voordeel van de hier geschetste oplossingsrichting is dat op deze manier het geschil gevoerd kan worden tussen de twee partijen om wie het daadwerkelijk gaat: de internetgebruiker en degene die stelt door hem te zijn benadeeld. Beide kunnen hun stellingen aan de rechter voorleggen; de ISP blijft er verder buiten, in elk geval inhoudelijk. Het belangrijkste nadeel is dat het introduceren van anoniem dagvaarden en procederen een brede impact zou kunnen hebben (ook buiten zaken over NAW-gegevensverstrekking) en bovendien een systeembreuk in het burgerlijk procesrecht betekent.

Uiteraard zou de invoering van anoniem dagvaarden en procederen beperkt kunnen worden tot de hier bedoelde zaken over de verstrekking van NAW-gegevens van anonieme internetgebruikers. Systeemtechnisch is dat misschien 'lelijk', maar de specifieke bepalingen over krakers zijn wat dat betreft wel een bruikbaar precedent.

<sup>16</sup> Hof Amsterdam 8 juli 1993, KG 1993, 292, r.o. 3.8.

*2.2. Een specifieke verzoekschriftprocedure – het voorstel van Ekker*

Anton Ekker sluit zijn recente proefschrift *Anoniem communiceren* af met een specifiek voorstel voor een Nederlandse variant van de hierboven besproken John Doe procedure.<sup>17</sup>

Hij beschrijft een verzoekschriftprocedure tussen de derde en de ISP, met als inzet de verstrekking door de ISP van de NAW-gegevens. De ISP wordt verplicht om de anonieme klant te informeren en in de gelegenheid te stellen om zich te verweren. Dat eventuele verweer zendt de ISP in geanonimiseerde vorm door naar de rechter.

*Het verdient de voorkeur om, in zijn algemeenheid of alleen in zaken met betrekking tot internetuitingen, te voorzien in de mogelijkheid van anoniem procederen.*

**Voor- en nadelen**

De discussie over de verstrekking van NAW-gegevens wordt volgens Ekkers voorstel gevoerd in een afzonderlijke (voor)procedure, waarin de uiteindelijke eisen van de derde (staking, rectificatie, schadevergoeding, etc.) niet aan de orde komen. De ISP is verweerder in de verzoekschriftprocedure, zij het dat hij de inhoud van zijn verweer bij zijn klant kan betrekken. Ekker voert voor zijn voorstel een aantal voordelen aan, die ik hieronder citeer en becommentarieer:

*In de eerste plaats is indiening van een verzoekschrift sneller, doelmatiger en minder kostbaar dan een dagvaardingsprocedure terwijl ook de rechterlijke macht hierdoor minder wordt belast.*

Dit lijkt mij onjuist: een verzoekschriftprocedure is niet per se sneller of goedkoper dan een kortgedingprocedure. De materiële discussiepunten zijn dezelfde en zullen door de eiser/verzoeker moeten worden onderzocht en gepresenteerd. Beide procedures beginnen met een schriftelijk stuk, kennen een mondelinge behandeling en leiden tot een gemotiveerde rechterlijke uitspraak en zijn dus vermoedelijk voor de rechterlijke macht ongeveer even belastend (daargelaten dat het vermoedelijk niet om een zodanig groot aantal zaken gaat dat überhaupt sprake is van een significante belasting).

*De provider is daarnaast verplicht om aan te geven of hij over identificerende gegevens beschikt zodat wordt voorkomen dat pas na het toewijzen van een civiele vordering blijkt dat dit niet het geval is.*

Als de ISP geen (of alleen evident valse) gegevens bezit kan hij dat uiteraard ook vóór of tijdens de behandeling van een kort geding mededelen. Desnoods kan de rechter daar ter zitting expliciet naar vragen.

*In de derde plaats worden de grondrechtelijke aanspraken van de anoniemus door een rechterlijke instantie beoordeeld. Ook wordt tegemoetgekomen aan het uit privacyregelgeving voortvloeiende recht van de anoniemus om op de hoogte te worden gesteld van de verwerking en om zich daartegen te verzetten.*

Dit zijn zeer positieve kenmerken van deze procedure, zij het dat zij in gelijke mate kunnen worden behaald in de huidige kortgedingprocedure (zie hieronder). De Lycos-criteria hebben ook betrekking op het belang van de klant bij behoud van zijn anonimiteit – de uitdaging is om dat belang in de procedure verwoord te krijgen zonder dat daardoor die anonimiteit al moet worden prijsgegeven.

*Ten slotte wordt ook de elektronische tussenpersoon uit zijn benarde positie bevrijd. Hij wordt niet langer als gedaagde geconfronteerd met een civiele vordering tot verstrekking en hoeft het verzoek tot verstrekking niet langer zelf te beoordelen. De vraag of een provider jegens de derde partij aansprakelijk kan zijn voor een weigering om identificerende gegevens te verstrekken speelt hierdoor niet langer. De provider hoeft zich hierover in het geheel geen zorgen te maken zolang hij het verzoek, het notificatiebericht en de eventuele reactie van de internetgebruiker doorzendt. Dit systeem doet meer recht aan zijn functie als doorgeefluik van informatie. Zijn taak beperkt zich dan immers tot datgene waar hij zich eigenlijk mee bezighoudt: het mogelijk maken van communicatie.*

Ik maak hieruit op dat Ekker zijn voorstel ziet als vervanging van de bestaande gang van zaken, en dat de door de Hoge Raad in Lycos/Pessers erkende zorgvuldigheidsregel hierdoor dus komt te vervallen. Dat zou impliceren dat de ISP per definitie niet zonder rechterlijke tussenkomst overgaat tot verstrekking van NAW-gegevens, ook niet als hij daartoe volgens de Lycos-criteria (evident) verplicht is.

Ekkers oplossing onderscheidt zich van de hiervoor besproken variant (§ 2.1) doordat zij specifiek van toepassing is in de telecommunicatieomgeving. Ekker stelt voor deze regeling neer te leggen in de Telecommunicatiewet, door middel van een wijziging van

<sup>17</sup> A.H. Ekker, *Anoniem communiceren*, p. 239-240.

het bestaande art. 11.11 Telecommunicatiewet. Deze beperking kan helpen een systeemdificatie over de inrichting van het burgerlijk procesrecht te vermijden, maar sluit tegelijkertijd belangrijke gevallen uit. Zo is het op een website beschikbaar stellen van een forum op zich geen elektronische communicatiedienst en zou dus de beheerder van zo'n forum buiten de voorgestelde regeling vallen.

De belangrijkste beperking van Ekkers voorstel is dat het weliswaar voorziet in een bijzondere procedure voor de verstrekking van NAW-gegevens, maar, met uitzondering van de niet relevante wijziging van rechtsingang, in feite een codificatie of formalisering is van de normale gang van zaken in een kort geding langs de lijnen van Lycos/Pessers. Ook in kort geding kan de ISP zijn klant om input vragen en zijn verweer in kort geding geheel of gedeeltelijk daarop baseren. ISP's kunnen zichzelf in hun algemene voorwaarden verplichten de klant te informeren over de poging van een derde om zijn anonimiteit te doorbreken en om de zienswijze van de klant aan de rechter door te zenden. Belangrijker nog is dat in het voorstel van Ekker, net als in de huidige kortgedingprocedure, de anonus niet zelf procespartij is, zodat hij niet zelf zijn procesinbreng en -strategie kan bepalen. Net als in een kortgedingprocedure wordt de ISP (in elk geval formeel) partij in een geschil waar hij (in elk geval inhoudelijk) buiten staat.

#### **De anonus als belanghebbende in de verzoekschriftprocedure**

Op zich zou tegemoetgekomen kunnen worden aan het bezwaar dat de anonus in het voorstel van Ekker geen procespartij wordt. De verzoekschriftprocedure kent immers ook een belanghebbende, die als zodanig een schriftelijke zienswijze op de zaak kan geven en vertegenwoordigd kan zijn tijdens de mondelinge behandeling van het verzoek.

Art. 272 Rv gaat uit van oproeping per aangetekende brief, maar sluit (elektronische) alternatieven niet uit. De rechter moet dan (kunnen) toestaan, dat een procureur een verzoekschrift indient dat niet de naam en woonplaats van de belanghebbende bevat (art. 282 jo. 278 Rv). De bij de dagvaardingsprocedure beschreven

bezwaren tegen het toelaten van anoniem verweer (die vooral verband houden met tenuitvoerlegging van het vonnis) spelen in dit geval niet of nauwelijks, omdat (a) de zaak alleen gaat over de verstrekking van de NAW-gegevens en dus niet over de inhoudelijke vorderingen van de eiser; en (b) de ISP ook partij is en dus uiteindelijk de NAW-gegevens kan verstrekken als de rechter daartoe beslist.

#### **CONCLUSIE**

Er bestaat een algemeen maatschappelijk belang bij de ontwikkeling van een wettelijke procedure, op grond waarvan een burger die zich beschadigd voelt door een anonieme uiting op internet, op een snelle en effectieve wijze kan optreden tegen de internetgebruiker die voor die uiting verantwoordelijk is. Die procedure moet zodanig zijn ontworpen, dat de internetgebruiker zijn anoniem gedane uiting in rechte kan verdedigen, zonder daardoor meteen zijn anonimiteit prijs te geven. De huidige praktijk, een kort geding tussen de beschadigde derde en de internetaanbieder met als inzet de opheffing van de anonimiteit van de internetgebruiker, is inefficiënt want gaat niet over de eigenlijke vraag naar de (on)rechtmatigheid van diens uiting. Bovendien doet deze gang van zaken onvoldoende recht aan de posities en belangen van de betrokkenen en biedt deze onvoldoende waarborgen voor kwetsbare maar maatschappelijk belangrijke anonieme uitingen.

Het verdient mijns inziens de voorkeur om, in zijn algemeenheid of alleen in zaken met betrekking tot internetuitingen, te voorzien in de mogelijkheid van anoniem procederen. Dat impliceert vooral: het dagvaarden van een anonus, het als anonus in het geding verschijnen en het ten uitvoer leggen jegens een anonus. De zaak wordt dan daadwerkelijk gevoerd tussen de partijen om wie het draait: de auteur van een uiting en de derde die zegt daardoor te zijn beschadigd. De ISP is dan geen procespartij en vermijdt de bij die status behorende kosten en risico's. Daardoor krijgt de anonieme klant de mogelijkheid – én de verantwoordelijkheid – om ten volle voor zijn positie op te komen, zonder daardoor meteen zijn anonimiteit te verliezen. ■

Op [www.njblog.nl](http://www.njblog.nl) kan gediscussieerd worden over de stelling:

**Bij vermoedelijk onrechtmatige handelingen moet de anonimiteit van internetgebruikers volledig kunnen worden wegenomen om derdenbelangen te beschermen.**