Effectief procederen tegen anonieme internetgebruikers

Alternatieve mechanismen voor de beslechting van geschillen over de verstrekking van NAW-gegevens door internet providers aan derden

Remy Chavannes*

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 adresgegevens 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 de tegemoet komt aan de belangen van de beschadigde derde, de anonieme internetgebruiker en de internetaanbieder.

1 INLEIDING

Uit de zaak Lycos/Pessers[1] blijkt dat er bij zaken over verstrekking van NAW-gegevens door internetaanbieders (ISP's) twee zeer 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.[2] 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 bezig houden, zonder zijn identiteit prijs te geven. Juist in geval van

* Advocaat bij Brinkhof te Amsterdam. De auteur trad in de hier beschreven procedure Lycos/Pessers in cassatie op voor Lycos. Een ingekorte versie van dit artikel verscheen in het Nederlands Juristenblad van 24 augustus 2007. De tekst is afgesloten per 1 mei 2007.

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

2 *Kamerstukken II* 2006-2007, 30951, nr. 1. De Minister spreekt van "een tijdige (efficiënte) informatie-uitwisseling en een verdere informatie- en daarmee machtsevenwicht tussen partijen."

'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.

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'.[3] 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 artikel 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 heel andere dan de detaillist die inbreukmakende goederen verkoopt en, op basis van bestaande jurisprudentie en de per 1 mei 2007 geïmplementeerde IE Handhavingsrichtlijn, gedwongen kan worden ook de gegevens van zijn leveranciers te noemen.[4] De nieuwe bevoegdheid van artikel 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.[5] Voor het verkrijgen van NAW-gegevens bij ISP's blijft een kort geding langs de lijnen van Lycos/Pessers aangewezen. Beide procedures kennen overigens hetzelfde gebrek, dat zij niet voorzien in inhoudelijke betrokkenheid van de anonymus en dus in gedegen kennisname van diens mogelijke belang bij anonimiteit.[6]

3 Volgens de Hoge Raad in ov. 5.3.7 van het arrest: "Daarbij moet in aanmerking worden genomen dat, hoezeer ook een hosting provider een faciliterende rol vervult bij de verspreiding van informatie op internet, zijn rol niet kan worden gelijkgesteld aan, en evenmin vergelijkbaar is met die welke de pers in een democratische samenleving vervult, zodat aan de hosting provider niet een verschoningsrecht toekomt als dat waarop de journalist met het oog op de bescherming van zijn bronnen aanspraak kan maken, reeds omdat via een website verspreide informatie niet kan gelden als informatie die door de websitehouder aan de hosting provider is toevertrouwd."

4 Zie HR 27 november 1987, *NJ* 1988, 722 m.nt. LWH *(Chloé/Peeters)* en artikel 1019f Rv, ingevoerd bij Wet van 8 maart 2007, *Stb.* 2007, 108. Bij nota van wijziging *(Kamerstukken II* 2005-2006, 30 392, nr. 7) is de materiële bevoegdheid van de rechthebbende om deze informatie bij de derde op te vragen, verplaatst van artikel 1019f Rv naar de verschillende intellectuele eigendomswetten (artikel 28 lid 9 Aw, artikel 17 lid 6 WNR, artikel 5c lid 5 Dw, etc.). De procesrechtelijke gang van zaken blijft geregeld in artikel 1019f Rv.

5 Aldus artikel 8 lid 1 van de IE Handhavingsrichtlijn en de Minister in de Nota naar aanleiding van het verslag, *Kamerstukken II* 2005-2006, 30 392, nr. 6, p. 7.

6 Het ligt wel voor de hand, dat een dergelijk belang in de regel eerder aanwezig zal zijn bij de openbaarmaking van content die vanwege zijn inhoud onrechtmatig kan zijn (smaad, laster, aantasting eer en

In concrete gevallen moet de ISP zijn verplichtingen jegens zijn klant (op grond van de Wet bescherming persoonsgegevens en artikel 8 EVRM) afwegen tegen zijn verplichtingen jegens de derde (op grond van de door de Hoge Raad erkende zorgvuldigheidsnorm, die in concrete gevallen verstrekking van gegevens kan voorschrijven). In de literatuur wordt de lastige positie van de ISP doorgaans als spagaat aangeduid.[7] 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 van 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

1 dat de belangen van de anonymus op adequate wijze worden betrokken bij de afweging die Lycos/Pessers voorschrijft, met andere woorden dat de anonymus zich desgewenst effectief kan verzetten tegen opheffing van zijn anonimiteit; en

2 dat de betrokkenheid van de ISP zo veel mogelijk wordt beperkt tot een rol als facilitator en doorgeefluik, en dat de beslissing over verstrekking dus wordt genomen door een rechter of andere daarvoor geëquipeerde geschilbeslechter.

De besproken alternatieven gaan van zeer formeel (wetswijziging) tot informeel (inspraakrecht voor de klant). Daarbij gaat het in feite steeds om dezelfde vragen:

- Welke instantie gaat de belangenafweging uitvoeren?

- Hoe wordt de anonymus in staat gesteld zich – uiteraard met behoud van zijn anonimiteit – inhoudelijk te verweren tegen de verstrekking van zijn NAW-gegevens door zijn ISP aan de derde?

- Welke procedurele voorzieningen moeten worden getroffen om deze afweging te laten plaatsvinden, en op welk niveau (wetgeving, zelfregulering, contract; rechter, adviescommissie, bindend advies?)

goede naam) dan bij de openbaarmaking van content waarop de derde het auteursrecht stelt te bezitten.

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

- Welke stappen dienen gezet te worden om deze werkwijze te implementeren of geïmplementeerd te krijgen?

2 HET PROBLEEM

2.1 Het belang van anonieme communicatie

De gedachte dat er zoiets is als een recht op anonieme communicatie, gaat in het Amerikaanse rechter makkelijker dan in het Europese of het Nederlandse.[8] De jurisprudentie van het Supreme Court biedt ook de mooiste rechtvaardigingen van dat recht, als vitaal onderdeel van de bescherming van de vrijheid van meningsuiting. In de zaak *McIntyre* overwoog het Supreme Court:

> *[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.*[9]

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.[10] In het Amerikaanse recht kent men bovendien het begrip SLAPP: 'Strategic Lawsuits Against Public Participation', rechtszaken van bedrijven tegen hen onwelgevallige publieke uitingen van individuen.[11] De ervaring heeft geleerd dat be-

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

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

10 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://legal.web.aol.com/aol/aolpol/seescandy.html.

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

drijven soms ook gebruik maken van procedurele middelen om ongewenste maar op zich legitieme kritiek de mond te snoeren. Vaak heeft de eiser daarbij voldoende belang en middelen om een zaak door te zetten, ook als de kans van slagen uiteindelijk klein 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. Die vrees heeft zelfs geleid tot een aantal zogenoemde anti-SLAPP statutes, een specifieke procesrechtelijke regeling die een verzoek tot verstrekking van NAW-gegevens als onderdeel van pre-trial discovery kan blokkeren.[12]

Dezelfde argumenten voor een (grond)recht op anonieme communicatie zijn in de Nederlandse context aan te voeren en ook daadwerkelijk aangevoerd.[13] 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.*[14]

12 Zie onder meer § 425.16 van de California Code of Civil Procedure.

13 Zie Ekker, 'Anonimiteit en uitingsvrijheid op het Internet; het onthullen van identificerende gegevens door Internetproviders', *Mediaforum* 2002-11/12, pp. 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, pp. 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:
"Anonimiteit [heeft] een onmiskenbaar maatschappelijk nut. Het openbare debat is gebaat bij een vrije uitwisseling van ideeën en informatie. Allerlei kritische geluiden zouden niet gehoord worden wanneer de afzender te allen tijde verplicht zou zijn om zich met naam en toenaam bekend te maken. De anonymus zal in sommige gevallen alleen eerlijk en ongegeneerd voor zijn mening durven uitkomen als hij niet hoeft te vrezen voor represailles van kwaadwillende overheidsinstanties, zijn werkgever, of de buren.
Anonimiteit is een belangrijke waarborg voor de anonieme klokkenluider die maatschappelijke misstanden aan de kaak stelt, voor de vertolker van de niet politiek correcte mening en voor de criticus van een totalitair regime in China, Birma of Iran. Een volwassen democratische samenleving moet zo stevig zijn dat zij anonieme uitingen niet alleen tolereert maar ze zelfs waardeert en beschermt als onderdeel van de meningsvorming."

14 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. De toelichting luidt als volgt:
"The aim of this principle is first and foremost to underline that the will of users to remain anonymous should be respected. There are two aspects to this principle. Firstly, users may have a valid reason not to reveal their identity when they have statements published on the Internet. Obliging them to do so

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 een de uitingsvrijheid die het helpt beschermen.

2.2 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 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;

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 beslis-

could restrict excessively their freedom of expression. It would also deprive society of potentially valuable information and ideas. Secondly, users need protection against unwarranted on-line surveillance by public or private entities. Member States should therefore, for example, allow the use of anonymity tools or software which enable users to protect themselves. This principle has, however, its limitations. Member States should have the possibility of obtaining information about persons responsible for illegal activities within the limits laid down under national law, the Convention for the Protection of Human Rights and Fundamental Freedoms, in particular Article 8, and other relevant international treaties such as the Convention on Cybercrime."

sing 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.

2.3 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 (artikel 45 lid 2 Rv). Er bestaat wel een specifieke uitzondering voor kraakpanden (artikel 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.[15] Of een rechter een e-mail adres of een website als zodanig zou aanmerken, is zeer twijfelachtig. Bovendien lijkt toepassing van deze mogelijkheid 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.[16]

Als geen woon- of verblijfplaats bekend is, kan de dagvaarding langs openbare weg worden betekend, d.w.z., kort gezegd, betekend aan het parket van de rechtbank waar de zaak gaat dienen met publicatie van een afschrift in een landelijk dagblad (artikel 54 lid 2 Rv).

Zelfs als het mogelijk zou zijn een geldige dagvaarding op geldige wijze te betekenen aan de anonymus 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 schadevergoeding te verhalen, zal toch echt bekend moeten zijn bij wie. Ook als de rechter de anonymus veroordeelt om zich bekend te maken, heeft de derde geen effectieve manier

[15] Zie bijvoorbeeld Kluwer, Burgerlijke rechtsvordering (oud), losbladig, aantekening 6 bij art. 5 Rv (oud).
[16] Hof Amsterdam 8 maart 2007, *NJF* 2007, 300.

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 duidelijke procedure om die aan de rechter kenbaar maken.

In theorie is nog denkbaar, dat de derde een kort geding aanspant tegen de anonymus, waarin de derde onder meer vordert dat de anonymus gedoogt dat de ISP de gegevens verstrekt. Als de kort geding rechter een openbaar uitgebrachte dagvaarding, waarin de gedaagde met e-mail adres wordt aangeduid, als geldig zou beschouwen, zou vervolgens de vraag zijn of hij zou toestaan dat een advocaat namens de aldus aangeduide gedaagde verschijnt en het woord voert. Zo ja, dan kan op die manier in beginsel het inhoudelijke debat over de verstrekking van NAW-gegevens worden gevoerd. Als de rechter concludeert dat de gedaagde onvoldoende belang heeft bij behoud van zijn anonimiteit, en hem gebiedt te gedogen dat de ISP zijn gegevens verstrekt, kan de ISP dat vermoedelijk zonder vrees of nadere afweging doen.

De hier geschetste route is echter uiterst onzeker. Vooral is het maar 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 anonymus in beroep te gaan tegen een kort geding vonnis, want een appeldagvaarding moet in elk geval de naam van de appellant bevatten. Al met al zou deze route een interessante proefprocedure opleveren, maar is deze vermoedelijk niet daadwerkelijk bruikbaar in de praktijk.

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 artikel 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?[17]

17 Zie ook HR 26 november 2004, *NJ* 2005, 41.

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: als de rechter de uiting onrechtmatig acht, kan hij de lastnemer moeilijk een algemeen verbod opleggen op herhaling in de toekomst. Voor een dergelijke vordering behoudt de derde dus een belang bij verstrekking van de NAW-gegevens van de lastgever.

3 EEN NEDERLANDSE JOHN DOE PROCEDURE

In de Verenigde Staten is dit probleem al eerder onderkend en zijn oplossingen ontwikkeld die wel worden aangeduid als 'John Doe'-procedures. Die maken onderdeel uit van de in het Nederlandse procesrecht niet bestaande, bewijsgarende voorfase van een civiele procedure, 'discovery'. Het is een procesrechtelijke figuur die tot dusver niet op federaal niveau bestaat, en in diverse staten op verschillende wijzen is geregeld. Het mechanisme werkt echter in de meeste gevallen ongeveer als volgt:

- De derde zendt zijn verzoek om verstrekking van gegevens aan de ISP in de vorm van een *subpoena*;

- De ISP stelt de klant op de hoogte van de *subpoena* en biedt de klant enkele dagen of weken de gelegenheid de rechter te verzoeken de *subpoena* te vernietigen (met als gevolg dat de ISP de gegevens niet verstrekt);

- Als de klant niet reageert of de rechter diens vernietigingsverzoek weigert, verstrekt de ISP de NAW-gegevens aan de derde.

Hoe zou een dergelijk systeem in het Nederlandse recht kunnen worden ingevoerd?

3.1 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 anonymus te dagvaarden, als 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 artikel 45 lid 3 Rv omtrent dagvaarding van krakers, of toevoeging van een aparte bepaling over dagvaarding van anonymi. 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 besproken figuur van de openbare dagvaarding via een dagblad. 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

Wat betreft deelname van de anonymus als gedaagde aan een procedure geldt het volgende. 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 echter over het algemeen vanuit gegaan, dat een groep anoniem gedagvaarde krakers slechts aan het geding kon deelnemen door hun namen bekend te maken. Daartoe is onder meer verwezen naar het feit dat de eiser aldus de gelegenheid krijgt om – tegenover de feitelijke stellingen van de gedaagden waarop zij hun verweer tegen de gevorderde ontruiming baseren – zijnerzijds inhoudelijk verweer kan voeren, hetgeen bij handhaving van de anonimiteit van de gedaagden niet goed mogelijk is. Bovendien heeft de eiser een gerechtvaardigd belang bij de mogelijkheid om de proceskosten – die bij een contentieuze procedure hoger uitvallen dan bij een verstekprocedure – op de verschenen gedaagden te verhalen.[18]

Voor procesdeelname van de anonymus zal dus een wettelijke voorziening moeten worden getroffen, die inhoudt dat een partij die anoniem is gedagvaard (overeenkomstig het uitgebreide artikel 45 lid 3 Rv) 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 – door zelf hoger beroep in te stellen of door zich te verweren tegen het hoger beroep van de eiser in eerste aanleg. Dit is uiteraard geen *issue* als de eiser in eerste aanleg heeft gewonnen en het vonnis uitvoerbaar bij voorraad is verklaard, omdat de anonimiteit van de gedaagde dan al is opgeheven. Als de gedaagde anonymus in eerste aanleg heeft gewonnen of als het veroordelende vonnis niet uitvoerbaar bij voorraad is verklaard, lijkt mij dat er geen principiële aanvullende reden is om hem dan niet ook in hoger beroep anoniem te laten procederen. Dat vergt wel de een verdere wetsaanpassing, in elk geval aan arti-

18 Hof Amsterdam 8 juli 1993, *KG* 1993, 292, rov. 3.8.

kel 45 lid 2 sub b Rv, dat bepaalt dat een exploot (waaronder een appeldagvaarding) de naam bevat van degene op wiens verzoek de betekening plaatsvindt.

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 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 (in kracht van gewijsde gegane of bij voorbaat uitvoerbaar verklaarde) vonnis bepaalt. Denkbaar is ook dat een advocaat in het geding kan verschijnen namens een (eventueel) nader bekend te maken opdrachtgever, wiens gegevens wel reeds bij de griffie zijn gedeponeerd.

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 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 zeer brede impact zou kunnen hebben (ook buiten zaken over NAW-gegevensverstrekking) en bovendien een majeure systeembreuk in het burgerlijk procesrecht zou betekenen. Dat betekent dat er de nodige weerstand en complicaties kunnen worden verwacht. De grootste horde is wellicht de eerste: om uit te leggen waar deze ingreep voor nodig is.

Uiteraard zouden de impact en de weerstand verkleind kunnen worden, door de invoering van anoniem dagvaarden en procederen slechts te bepleiten voor 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. Dat brengt mij vanzelf op een tweede variant van een Nederlandse John Doe procedure.

3.2 Een specifieke verzoekschriftprocedure – het voorstel van Ekker

In zijn recente proefschrift *Anoniem communiceren* heeft Anton Ekker verslag gedaan van zijn onderzoek naar de grondrechtelijke bescherming van anonieme openbare communicatie. In dat kader analyseert hij onder meer uitgebreid de hierboven genoemde Amerikaanse John Doe procedures. Hij sluit zijn onderzoek af met een specifiek voorstel voor een Nederlandse variant:[19]

> *1. De persoon of instantie die schade meent te leiden als gevolg van anonieme informatie en die de identiteit van de verantwoordelijke gebruiker wenst te achterhalen, verzoekt de rechter om de aanbieder van het telecommunicatienetwerk of de telecommunicatiedienst waarmee de bewuste informatie toegankelijk is gemaakt of is doorgezonden en van wie redelijkerwijs wordt vermoed dat hij over de NAW-gegevens van deze gebruiker beschikt, te bevelen tot het verstrekken van diens naam-, adres- en woonplaatsgegevens.*
> *2. De verzoeker dient in het verzoekschrift te motiveren waarom hij de NAW-gegevens wenst te verkrijgen. Daarnaast dient hij nauwkeurig te vermelden waar en wanneer de beweerdelijk onrechtmatige informatie beschikbaar is of was.*
> *3. De verzoeker stuurt een kopie van het verzoekschrift naar de aanbieder. Deze stuurt de kopie en een notificatiebericht door naar de anonieme internet- of e-mailgebruiker. In het notificatiebericht wordt de gebruiker op de hoogte gesteld van de poging om zijn identiteit te achterhalen en van de mogelijkheid om zich hiertegen te verzetten. Indien de provider niet beschikt over de daarvoor benodigde naam-, adres-, en woonplaatsgegevens stelt hij de verzoeker en de rechter daarvan terstond op de hoogte.*
> *4. Indien de gebruiker zich binnen de daarvoor gestelde termijn tegen het verzoek verzet stuurt de provider zijn reactie, met waarborging van anonimiteit, door aan de rechter.*
> *5. Na het verstrijken van de genoemde termijn weegt de rechter, eventueel met inachtneming van de door de internetgebruiker naar voren gebracht bezwaren, de bij de verstrekking betrokken belangen af met toepassing van in de jurisprudentie ontwikkelde criteria.*

Voor- en nadelen

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.*

19 A.H. Ekker, *Anoniem communiceren*, pp. 239-240.

Dit lijkt mij over het algemeen onjuist: een verzoekschriftprocedure is niet per se sneller of goedkoper dan een kort geding procedure. De materiële discussiepunten zijn dezelfde en zullen door de eiser dus 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.

> *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.*

Dit is op zich juist, maar 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.

> *Introductie van de geschetste procedure zou in de tweede plaats een einde maken aan de onder juristen bestaande discussie over de juridische grondslag van een op de online tussenpersoon rustende verplichting tot verstrekking van identificerende gegevens.*

De Hoge Raad heeft deze vraag beantwoord in het arrest Lycos/Pessers.

> *In de derde plaats worden de grondrechtelijke aanspraken van de anonymus door een rechterlijke instantie beoordeeld. Ook wordt tegemoet gekomen aan het uit privacyregelgeving voortvloeiende recht van de anonymus 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 kort geding procedure (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.

> *Tenslotte 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 bezig houdt: 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 Lyocs/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.

Deze oplossing onderscheidt zich van de hiervoor besproken variant (§ 3.1) 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 het bestaande artikel 11.11 Tw. Deze plaatsing en de specifieke beperking tot elektronische communicatiediensten, heeft als voordeel dat een algemene systeemdiscussie over de inrichting van het burgerlijk procesrecht vermoedelijk kan worden vermeden. Er wordt niet getracht een algemene mogelijkheid van anoniem procederen in te vullen. De introductie van een dergelijk systeem kan worden gepresenteerd als een specifieke wettelijke regeling die tegemoet komt aan een specifiek probleem in een bepaalde sector.

De discussie over de verstrekking van NAW-gegevens wordt volgens dit voorstel gevoerd in een afzonderlijke (voor)procedure, waarin de uiteindelijke eisen van de derde (staking, rectificatie, schadevergoeding, etc.) niet aan de orde komen. Ekker kiest voor een verzoekschriftprocedure in plaats van een dagvaardingsprocedure, wat op zich begrijpelijk is, omdat in zijn voorstel de ISP wel van meet af van aan procespartij is en een verzoekschriftprocedure zich beter leent voor een procedure waarin de betrokken partijen niet per definitie diametraal tegenover elkaar staan. De ISP is verweerder in de verzoekschriftprocedure, zij het dat hij de inhoud van zijn verweer bij zijn klant kan betrekken. Dat de ISP procespartij moet zijn, is tegelijkertijd ook een significant nadeel van de door Ekker geschetste procedure.

Deze optie voorziet in een bijzondere procedure voor de verstrekking van NAW-gegevens, maar – en dat is meteen de grootste beperking ervan – is in feite een codificatie of formalisering van de normale gang van zaken in een kort geding langs de lijnen van Lycos/Pessers. Ook in kort geding staat het de ISP uiteraard vrij om zijn klant om input te vragen en zijn verweer in kort geding geheel of gedeeltelijk daarop te baseren. ISP's kunnen ook in hun algemene voorwaarden zichzelf een verplichting opleggen om 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 kort geding procedure, de anonymus niet zelf procespartij is, zodat hij niet zelf zijn procesinbreng en -strategie kan bepalen. Net als in een kort geding procedure wordt de ISP (in elk geval formeel) partij in een geschil waar hij (in elk geval inhoudelijk) buiten staat. Hij wordt bovendien gedwongen om juridische kosten te maken en (in elk geval formeel) een standpunt in te nemen.

De anonymus als belanghebbende in de verzoekschriftprocedure

Op zich zou vermoedelijk tegemoet gekomen kunnen worden aan het zojuist genoemde bezwaar, dat de anonymus in het voorstel van Ekker geen procespartij wordt maar zijn argumenten alleen via de ISP kan aanvoeren. De verzoekschriftprocedure kent een verzoeker, een verweerder en eventueel een belanghebbende.[20] In het voorstel van Ekker is de derde uiteraard de verzoeker en de ISP de verweerder. Als de anonieme klant echter als belanghebbende zou worden aangemerkt, zou hij een schriftelijke zienswijze op de zaak kunnen geven en vertegenwoordigd kunnen zijn tijdens de mondelinge behandeling van het verzoek.

De regels over oproeping van belanghebbenden in een verzoekschriftprocedure zijn minder formeel dan de regels over het uitbrengen van exploten aan de gedaagde in een dagvaardingsprocedure. Zo blijkt uit artikel 272 Rv dat de oproeping van belanghebbenden weliswaar *in beginsel* plaatsvindt per aangetekende brief, maar dat de rechter ook een *andere* wijze van oproeping kan bepalen. Dat laat ruimte voor oproeping per e-mail, via de ISP, etc.

Een verweerschrift, in beginsel in te dienen door een procureur, dient de naam en woonplaats van de belanghebbende te bevatten (artikel 282 jo 278 Rv). Op schending van deze eis staat echter geen formele sanctie. Denkbaar is dus dat de rechter in een geval als deze toestaat dat een procureur een verweerschrift indient en ter zitting verschijnt namens een belanghebbende die niet bij naam wordt genoemd. Deze specifieke afwijking van artikel 278 lid 1 Rv kan desnoods ook in een specifieke bepaling (in het voorgestelde nieuwe artikel 11.11 Tw) worden vastgelegd. 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 in mindere mate, 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.

3.3 Tussenconclusie

Bezien vanuit zowel de ISP als zijn anonieme klant, verdient de hierboven als eerste genoemde oplossingsrichting mijns inziens de voorkeur, omdat daarin de zaak daadwerkelijk wordt gevoerd tussen de klant en de derde. De ISP is daarin geen partij en vermijdt dus 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. In de als tweede beschreven verzoekschriftprocedure is de ISP nog steeds procespartij en heeft de klant nog steeds geen zelfstandige procespositie, tenzij hij met behoud van anonimiteit als belanghebbende kan optreden.

20 De wet geeft geen definitie van het begrip 'belanghebbende' in de verzoekschriftprocedure, zodat daaraan steeds passende invulling kan worden gegeven al naar gelang de aard van de procedure.

Daar staat tegenover dat de invoering in de Telecommunicatiewet van een specifieke verzoekschriftprocedure zoals hier beschreven, een veel minder vergaande ingreep is in het burgerlijk procesrecht dan de invoering van anoniem dagvaarden en procederen, zelfs als dat specifiek zou worden beperkt tot bepaalde zaken. Bijgevolg zijn de *kansen* om een dergelijke verzoekschriftprocedure ingevoerd te krijgen, vermoedelijk hoger. Vergeleken met de bestaande kort geding praktijk is de verzoekschriftprocedure wel een vooruitgang, omdat hiermee een geformaliseerde procedure wordt geschapen met een duidelijke rolverdeling. Het is echter de vraag of ISP's daarmee gevrijwaard zouden zijn van een kort geding volgens de Lycos-route. Zeker in zaken die evident en spoedeisend zijn, zou een kort geding rechter nog steeds kunnen oordelen dat de ISP NAW-gegevens moet verstrekken. De wettelijke regeling (of de toelichting daarop) zou deze weg dus expliciet moeten afsnijden.

4 BUITENGERECHTELIJKE MECHANISMEN VOOR DE BESLECHTING VAN GESCHILLEN OVER VERSTREKKING VAN NAW-GEGEVENS

Een wettelijke regeling biedt duidelijkheid en rechtszekerheid en daardoor ook een redelijke bescherming van de positie van alle betrokkenen. De totstandkoming van een wetswijziging is echter een langdurig proces, waarvoor voldoende steun zou moeten worden vergaard bij het Ministerie van Justitie, het kabinet en het parlement. Ik bespreek daarom nu ook een aantal mogelijke mechanismen voor de beslechting van geschillen over de verstrekking van NAW-gegevens waarvoor een wetswijziging niet noodzakelijk is.

4.1 Bindend advies

Partijen kunnen overeenkomen dat zij een geschil niet zullen voorleggen aan de rechter maar één of meer derden. Het advies is geen vonnis en kan niet ten uitvoer gelegd worden, maar schept een vaststellingsovereenkomst tussen de betrokken partijen die alleen onder uitzonderlijke omstandigheden nog door de rechter kan worden gewijzigd of vernietigd.

Kort gezegd zou men een regeling kunnen ontwerpen die voorziet in een bindend advies over de vraag of de ISP in een concreet geval de NAW-gegevens van een klant zal verstrekken. De regeling dient te voorzien in de benoeming van één of meer personen die het advies gaan uitbrengen, alsmede in een procedure. Deze procedure dient alle partijen in de gelegenheid te stellen hun zienswijze te geven, uiteraard zonder dat de klant daardoor zijn anonimiteit prijs hoeft te geven.

Het grote voordeel van een dergelijke procedure zou zijn deze door betrokkenen (ISP-'s, gebruikers en wellicht een aantal potentiële bevragers, zoals vertegenwoordigers van rechthebbenbenden), deze zelf in het leven kunnen roepen en dus ook zelf de procedureregels kunnen ontwerpen. De formele hobbels tegen 'anoniem procederen' in het burgerlijk procesrecht spelen hierbij geen rol, net als de overige wettelijke pro-

cesregels. Bovendien is de procedure laagdrempelig en daardoor relatief goedkoop. Daartegenover staan drie nieuwe vragen:

- Hoe kan worden verzekerd dat ISP, klant én de derde bereid zijn zich aan bindend advies te onderwerpen?
- In hoeverre kan worden voorkomen dat de derde die in het bindend advies zijn zin niet krijgt, alsnog naar de civiele rechter gaat?
- Wie gaat het bindend advies geven?

Instemming met bindend advies

Bindend advies vergt als gezegd een *overeenkomst* tussen de betrokkenen. Met de anonieme klant heeft de ISP uiteraard een contractuele relatie, zodat zij met de klant in elk geval kan afspreken dat deze de gelegenheid krijgt zich in de procedure te mengen en zich bij de uitkomst van de zaak zal neerleggen, ook in die zin dat de ISP niet aansprakelijk is voor (de gevolgen van) verstrekking van de NAW-gegevens als het bindende advies daartoe strekt.

Er is nog discussie mogelijk over de vraag of aldus de klant wordt afgehouden van de rechter die de wet hem toekent en dus over de vraag of een dergelijke regeling niet in strijd is met artikel 17 van de Grondwet. Vermoedelijk is dat niet het geval, omdat het bindend advies de weg naar de rechter niet afsluit en de klant er bovendien (door aanvaarding van de algemene voorwaarden) mee instemt. Op grond van de regeling van algemene voorwaarden, meer in het bijzonder artikel 6:236, aanhef en sub n BW, dient de gebruiker echter vermoedelijk wel de gelegenheid te hebben alsnog te kiezen voor beslechting door de gewone rechter.[21] Het is denkbaar dat daarom bijvoorbeeld wordt opgenomen dat, als een klant daarvoor kiest, de ISP het recht heeft de NAW-gegevens terstond te verstrekken, tenzij de klant de kosten van rechtsbijstand betaalt. Bovendien kan sowieso de vraag gesteld worden, of het wel mogelijk is om een klant bij algemene voorwaarden te laten instemmen met bindend advies. In haar onlangs verdedigde proefschrift stelt Siemerink dat een beding in algemene voorwaarden dat bepaalt dat de klant door het aanvaarden van de algemene voorwaarden 'instemt' met iets, per definitie onredelijk bezwarend is.[22]

Aangezien de ISP over het algemeen geen klantrelatie of andere contractuele band zal hebben met beweerdelijk beschadigde derden, zal zij daaromtrent te zijner tijd met de derde een afspraak over moeten maken. De vraag of een derde hiertoe bereid zal zijn, hangt uiteraard mede af van het gezag van de bindend adviseurs en de kwaliteit van hun bindende adviezen. Mocht de ISP een bindend advies procedure inrichten en een derde weigert om daarmee in te stemmen, zou de ISP in het daarop volgende kort geding het verweer moeten voeren dat de vordering dient te worden afgewezen op de derde van de vier Lycos-criteria, omdat er in het concrete geval wel

21 Betoogd zou nog kunnen worden dat het hier niet gaat om een geschil tussen de ISP en de klant, zodat deze bepaling hier niet van toepassing is.

22 Siemerink, *De overeenkomst van Internet Service Providers met consumenten*, par. 3.4.4.1 en stelling 3.

degelijk een minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen. Of dit verweer zou slagen, kan op voorhand niet worden gezegd – het hangt uiteraard ook weer samen met de kwaliteit en het gezag van de bindend adviezen en -adviseurs.

Verhouding tot civiele rechter

Als partijen bindend advies zijn overeenkomen in een kwestie die tot hun vrije beschikking staat, dan zal de overheidsrechter een eiser die niet eerst de weg van het bindend advies heeft gevolgd, niet-ontvankelijk verklaren in zijn vordering.[23] Nadat bindend advies is uitgebracht, is het advies als onderdeel van een vaststellingsovereenkomst tussen de betrokken partijen slechts onderworpen aan een marginale rechterlijke controle. Het advies kan blijkens artikel 7:904 BW worden vernietigd als gebondenheid daaraan in verband met inhoud of wijze van totstandkoming in de gegeven omstandigheden naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zou zijn. Wat de inhoud betreft is de beslissing dus onaantastbaar als deze blijft binnen de grenzen waarbinnen redelijk denkende mensen van mening kunnen verschillen. De rechter dient met name niet zijn eigen oordeel voor dat van de bindend adviseur in de plaats te stellen.[24]

Wat de wijze van totstandkoming betreft moet vooral worden gedacht aan schending van fundamentele rechtsbeginselen. Dat komt er kort gezegd op neer:

- dat partijen in de gelegenheid worden gesteld hun standpunt kenbaar te maken;
- dat de gegevens waarop het advies berust ter kennis van beide partijen worden gebracht;
- dat de beslissing op een deugdelijk onderzoek is gebaseerd; en
- dat de beslissing deugdelijk gemotiveerd is.

Het ontwerp van de bindend advies procedure vergt ook hierom de nodige zorg.

De bindend adviseur(s)

Een bijzondere uitdaging vormt uiteraard de benoeming van één of meer bindend adviseurs. Hun gezag en kwaliteit is mede bepalend voor het succes van deze route. In dit verband is overigens denkbaar dat wordt gewerkt aan de branche-brede oplossing, in die zin dat meerdere ISP's meewerken aan de totstandkoming van het bindend advies mechanisme en het vervolgens hanteren. Denkbaar is ook dat één ISP een dergelijk mechanisme opzet, maar dat anderen zich er vrijwillig bij kunnen aansluiten. Een *Bindend Adviescommissie Gegevensverstrekking Internet* die onafhankelijk is van een individuele provider heeft mogelijk een grotere kans om gezag op te bouwen, bij derden en bij de rechter. Bovendien kunnen daardoor uiteraard de kosten worden

23 HR 22 november 1985, *NJ* 1986, 275 m.nt. PAS.
24 HR 18 juni 1993, *NJ* 1993, 615 *(Fysiotherapie Gruythuysen/Stichting Centraal Ziekenhuis).*

gespreid en kan op termijn wellicht ook een secretariaat worden ingericht dat bijvoorbeeld de evident gegronde of ongegronde verzoeken op eigen gezag kan afdoen.

Overigens zou een dergelijke bindend adviescommissie (specifiek voor één ISP of branche-breed) natuurlijk ook worden ingeschakeld voor *notice and take down* zaken, waarin een derde eist dat de beweerdelijk onrechtmatige website van een klant van de ISP wordt verwijderd. Daar spelen immers vergelijkbare problemen voor ISPs die niet voor rechter willen hoeven spelen – en van klanten die hun website willen kunnen verdedigen zonder verlies van anonimiteit. Ik ga hier niet verder in op dit onderwerp, maar merk op dat een geschillenprocedure en -commissie ook met het oog hierop zou kunnen worden ingezet.

4.2 Een adviescommissie NAW-gegevensverstrekking

Het is ook mogelijk om te kiezen voor een minder vergaande vorm van advisering. Men kan een externe adviescommissie in het leven roepen, aan wie verzoeken om NAW-gegevens te verstrekken, worden voorgelegd. De anonieme klant wordt in de gelegenheid gesteld zijn zienswijze aan de adviescommissie voor te leggen – en wellicht op een zitting te verschijnen. De ISP kan in zijn algemene voorwaarden opnemen dat de hij deze procedure hanteert en gegevens ook daadwerkelijk zal verstrekken als adviescommissie daartoe adviseert.

Een dergelijke advisering vergt niet de instemming van de derde die om NAW-gegevens vraagt. Het is dan ook slechts een manier voor de ISP om de materiële beoordeling uit handen te geven en haar aansprakelijkheid jegens de klant uit te sluiten. Het gevolg is dat, als de adviescommissie negatief adviseert en de ISP dus weigert de gegevens te verstrekken, de derde alsnog naar de civiele rechter kan. Zeker in het begin zal het advies van de adviescommissie mogelijk geen doorslaggevend gewicht in de schaal leggen. Voordeel is echter, dat de ISP op deze manier een deel van de zaken kan oplossen, terwijl zij in zaken die wel doorgaan naar de civiele rechter, in elk geval beschikt over een gedegen advies waarin het standpunt en de belangen van de anonieme klant zijn betrokken. De kans dat de derde naar de rechter gaat, kan mogelijk worden verkleind als ook deze derde zijn zienswijze aan de adviescommissie kan geven en het advies zodanig goed en gezaghebbend is, dat de derde moet vrezen voor zijn kansen bij de civiele rechter.

Op deze manier kan op zich niet worden voorkomen dat de derde het advies van de adviescommissie niet eens afwacht, maar meteen een kort geding begint. Hij is immers niet contractueel betrokken bij de adviescommissie, maar ontleent zijn recht op verstrekking van de gegevens aan de wet (d.w.z. aan de door de Hoge Raad erkende maatschappelijke zorgvuldigheidsnorm van de ISP op grond van artikel 6:162 BW). Het is daarom van belang dat de adviescommissie desnoods heel snel kan adviseren, zodanig dat de redelijk denkende derde dat advies wel zal afwachten (althans de rechter zal oordelen dat hij dat zou moeten doen).

Een nadeel van deze procedure is dat de ISP en de anonieme klant in beginsel zijn overgeleverd aan het oordeel van de adviescommissie. De klant heeft geen beroepsmogelijkheid als hij het niet eens is met het advies, en zijn anonimiteit kan uiteraard maar één keer worden opgeheven. Uiteraard is denkbaar dat er ook nog een beroepscommissie in het leven wordt geroepen waar de klant de zaak aan kan voorleggen, waarbij de ISP de gegevens pas verstrekt als de beroepscommissie heeft beslecht. Dat maakt de zaak uiteraard ingewikkelder en doet – tenzij een zeer snelle procedure kan worden ontwikkeld – ook de kans toenemen dat de derde ondertussen naar de civiele rechter gaat.

4.3 Versterking van de participatie van de anonymus

De minst vergaande ingreep die toch in enige mate tegemoet komt aan de in de inleiding geschetste problematiek, zou zijn als de ISP de gang van zaken bij NAW-bevragingen in zekere mate formaliseert. Daarmee bedoel ik, dat de wijze waarop de ISP omgaat met verzoeken om verstrekking van NAW-gegevens van klanten, neerlegt in een publiek beschikbaar document en haar algemene voorwaarden. Op die manier kan bijvoorbeeld worden vastgelegd dat de ISP de klant altijd onmiddellijk op de hoogte stelt van een dergelijk verzoek en deze binnen een redelijke termijn (afhankelijk van de omstandigheden van het geval) in de gelegenheid stelt zijn mening te geven over het verzoek. Vastgelegd kan worden, dat de ISP de gegevens verstrekt als de klant niet binnen de gestelde termijn een verweer verschaft. Denkbaar is ook dat wordt vastgelegd dat, als wel een verweer wordt ingediend, de ISP zelfstandig beslist over verstrekking en, als het besluit om dat te weigeren, in het mogelijk daarop volgende kort geding dat verweer integraal overlegt (met behoud van anonimiteit).

Denkbaar is zelfs dat de ISP zich *alleen* op dat verweer van de klant baseert, zodat de klant de verantwoordelijkheid heeft om een sluitend verweer te produceren dat de rechterlijke toetsing aan de hand van de Lycos-criteria kan doorstaan. Daardoor wordt een zwaardere verantwoordelijkheid op de schouders van de klant geplaatst, maar het kan verdedigd worden dat hij die zich anoniem uitlaat, zodanig dat een ander daardoor schade kan lijden, een behoorlijke verantwoordelijkheid heeft om zich te verweren als de derde daartegen vervolgens daadwerkelijk in actie komt.

Nadeel is dat de kort geding procedure niet geschikt is voor een procespartij die een inhoudelijk afstandelijke houding aanneemt. Wil een gedaagde voorkomen dat een vordering wordt toegewezen, zal hij daartegen over het algemeen verweer moeten voeren. Een gedaagde die volstaat met te verwijzen naar het standpunt van een niet bij de zaak betrokken derde (zoals in dit geval de kant) en zich verder refereert aan het oordeel van de rechter, zal over het algemeen worden veroordeeld. Het institutionaliseren van de participatie van de klant is dus absoluut aan te raden, zolang geschillen over de verstrekking van NAW-gegevens in de praktijk worden gevoerd in een kort geding procedure tussen de derde en de ISP. Daarmee wordt de ISP echter niet gevrijwaard van de noodzaak om voorafgaand aan de kort geding procedure voor zichzelf te bepalen of hij op grond van de Lycos-criteria verplicht is de gegevens te verstrekken en, als het antwoord ontkennend is, dat antwoord voor de rechter te verde-

digen. De input van de klant is daarvoor een belangrijk hulpstuk, maar niet een alternatief.

CONCLUSIE

Er bestaat een algemeen maatschappelijk belang bij de ontwikkeling van een 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.

In dit artikel zijn diverse mogelijke wettelijke en buitenwettelijke procedures geschetst en vergeleken. De buitenwettelijke procedures bieden naar mijn oordeel onvoldoende zekerheid, duidelijkheid en afdwingbaarheid om een volledig alternatief te kunnen zijn voor de huidige praktijk. Mijns inziens verdient het dan ook de voorkeur om, in zijn algemeenheid of alleen in zaken met betrekking tot internetuitingen, expliciet te voorzien in de mogelijkheid van anoniem procederen. Dat impliceert vooral: het dagvaarden van een anonymus, het als anonymus in het geding verschijnen en het ten uitvoer leggen jegens een anonymus. 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.