Anoniem communiceren: van drukpers tot weblog : een onderzoek naar de grondrechtelijke bescherming van anonieme openbare communicatie

Ekker, A.H.

Publication date
2006

Document Version
Final published version

Anoniem communiceren: van drukpers tot weblog

ANONIEM COMMUNICEREN: VAN DRUKPERS TOT WEBLOG

EEN ONDERZOEK NAAR DE GRONDRECHTELIJKE BESCHERMING VAN ANONIEME OPENBARE COMMUNICATIE

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. mr. P.F. van der Heijden
ten overstaan van een door het college voor promoties ingestelde
commissie, in het openbaar te verdedigen in de Aula der Universiteit
op dinsdag 14 maart 2006, te 12.00 uur

door

Antonie Hendrik Ekker

geboren te Nootdorp

Prof. mr. E.J. Dommering (promotor)
Prof. mr. J.J.C. Kabel (co-promotor)
Faculteit der Rechtsgeleerdheid

Van deze uitgave verschijnt een handelseditie onder ISBN 90-1211-256-7

Voorwoord

Bij deze bedank ik allen die hebben bijgedragen aan de totstandkoming van dit proefschrift. Lodewijk Asscher verdient bijzondere vermelding omdat ik er zonder hem nooit aan begonnen was. Hij begeleidde mij bij het schrijven van mijn scriptie en vroeg mij daarna om het ITeR-onderzoek te doen dat uiteindelijk zou resulteren in een promotieonderzoek. Ook was hij, als onderzoeksbegeleider, zeer behulpzaam bij het schrijven van artikelen en annotaties en bij het organiseren van een verblijf in het buitenland. Met Wilfred Steenbruggen, die lange tijd mijn kamergenoot was, heb ik veel gelachen en eindeloos gediscussieerd over allerlei juridische onderwerpen. Voor het ventileren van de met het schrijven van een proefschrift gepaard gaande frustraties kon ik daarnaast terecht bij mijn lotgenoten Nirmala Sitompoel, Sjoerd van Geffen, Hans Fischer, Tarlach McGonagle en Natali Helberger. Anja Dobbelsteen was er altijd voor goede raad en gezelligheid. Elvira Caneda en Rosanne van der Waal gaven broodnodige ondersteuning bij het vinden van informatie. Bernt Hugenholtz, Lucie Guibault, Nico van Eijk, Gerard Mom, Aernout Nieuwenhuis en Sabina Gorini gaven vele nuttige adviezen en inhoudelijk commentaar. Alle collega's bij het Instituut voor Informatierecht die ik hier nog niet genoemd heb dank ik ten slotte omdat zij mijn jaren bij het instituut met hun aanwezigheid tot een zeer plezierige ervaring hebben gemaakt.

Een deel van het onderzoek werd verricht in de Verenigde Staten. Julie Cohen van Georgetown University te Washington wil ik bedanken omdat zij mij hielp bij het leggen van contacten. Peter Swire van George Washington University en Marc Rotenberg en David Sobel van de Electronic Frontier Foundation (EFF) waren bereid tot beantwoorden van vele vragen. Mijn verblijf aan Boalt Hall Law School, University of Berkeley, California werd mogelijk gemaakt door Pamela Samuelson. Ook ontving ik een bijdrage uit het reisfonds Maatschappij- en Gedragswetenschappen (MaGW) van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).

Het onderzoek werd afgesloten in augustus 2005. Daarna zijn slechts enkele aanvullingen opgenomen.

Amsterdam, november 2005

Inhoud

Inleiding

Wij leven in een transparante maatschappij. In alle hoeken en gaten van onze leefwereld hebben zich technologieën genesteld waarmee wij onszelf en elkaar kunnen observeren en registreren. Camera's bewaken het openbare leven op straat en in winkels. Flitspalen controleren ons gedrag op de snelweg. Zelfs mobiele telefoons herbergen geminiaturiseerde apparatuur voor opname van beeld en geluid. Ons handelen laat daarnaast een spoor van gegevens achter. Wij worden in de loop van ons leven opgenomen in tienduizenden gegevensbestanden. Personal computers, telecommunicatienetwerken en pinautomaten creëren een digitaal logboek van ons dagelijks leven. Fragmenten die uit ons eigen geheugen reeds verdwenen zijn, echoën voor onbepaalde tijd na in een collectief geheugen van videobestanden, fotoarchieven en databanken.

De doorzichtigheid van onze omgeving wordt nog eens verhoogd door de opkomst van kunstmatig intelligente systemen die de mens kunnen identificeren op basis van zijn gedrags- en lichaamskenmerken. Voorbeelden van dergelijke biometrische toepassingen zijn spraak- en gezichtsherkenning, de herkenning van warmteprofielen en de irisscan. Wanneer de communicatietechnologie camera's, microfoons en biometrische toepassingen verbindt, zullen kijken, luisteren, digitaal registreren en herkennen samenvloeien. Lenzen, microfoons en toetsenborden worden dan de tentakels van een immer uitdijend organisme met communicatiekabels en schakelstations als zenuwstelsel en een zee van gegevens(bestanden) als brein.

Het individu neemt ten aanzien van de technische ontwikkelingen een ambivalente houding aan. Hij hecht waarde aan zijn privacy, maar het gebruiksgemak van technologische toepassingen doet principiële bezwaren vaak verdwijnen. Daarnaast wordt de behoefte om alleen en onbespied te zijn meer dan eens overstemd door het verlangen om juist wel gezien, gehoord en herkend te worden. De dichteres Neeltje Maria Min schreef:

"Mijn moeder is mijn naam vergeten
Mijn kind weet nog niet hoe ik heet
Hoe moet ik mij geborgen weten?"

De veiligheid van het sociale contact met anderen is een essentiële voorwaarde voor menselijke ontplooiing. Soms komt de wens om bekeken te worden echter voort uit andere motieven. IJdelheid is eveneens een belangrijke drijfveer. Het verlangen naar 'one minute

of fame' brengt mensen ertoe op televisie of het internet vrijwillig iedere vorm van privacy op te geven.

Nu vele facetten van menselijk gedrag meer dan vroeger registreerbaar, reproduceerbaar en controleerbaar zijn geworden, rijst niettemin de vraag in hoeverre men de keuze moet hebben om zich aan de waarneming van anderen te onttrekken. Vanuit juridisch perspectief is deze vraag relevant nu de wens om anoniem te blijven op gespannen voet kan staan met andere maatschappelijke belangen. In vele gebieden van het recht bestaan dan ook vraagstukken rondom de identificeerbaarheid en de anonimiteit van rechtssubjecten. Voorbeelden zijn de koppeling van gegevensbestanden voor de bestrijding van uitkeringsfraude, de invoering van een wettelijke identificatieplicht, het verschijnsel van de anonieme getuige in het strafrecht en het recht van adoptiekinderen om te weten wie hun biologische ouders zijn. Zonder veel moeite zou aan deze opsomming nog een lange lijst van gelijksoortige problemen kunnen worden toegevoegd.

Achter de genoemde juridische vraagstukken gaat een conflict schuil tussen twee maatschappelijke principes. Het eerste principe, dat ik hier aan zou willen duiden als het principe van 'kenbaarheid', houdt in dat het individu zijn identiteit aan anderen bekend dient te maken. Er zijn veel situaties waarin dit principe prevaleert. In de relatie tussen overheid en burger is het onder andere tot uitdrukking gebracht in de verplichting om een pasgeboren kind in te schrijven in het bevolkingsregister.[1] Bij de aangifte van geboorte dient voor hem een naam te worden gekozen die voor alle andere burgers kenbaar is. In het economisch verkeer vraagt de rechtszekerheid om kenbaarheid van identiteit.[2] Om hun rechtspositie te kunnen bepalen dienen burgers wetenschap te hebben omtrent de identiteit van andere rechtssubjecten. Zo is de identiteit van contractspartijen bij de totstandkoming van overeenkomsten een relevant gegeven. Om aan de maatschappelijke behoefte aan kenbaarheid tegemoet te komen is van veel registers de openbaarheid bij wet voorgeschreven. Ik noem hier het handelsregister, het huwelijksgoederenregister en de kadastrale registratie.[3] Daarnaast zijn er registers die feitelijk openbaar zijn, zoals bijvoorbeeld het telefoonboek. Een belangrijke functie van dergelijke registers is de koppeling van juridisch relevante informatie aan identificeerbare personen.

Tegenover het beginsel van kenbaarheid staat het eveneens zwaarwegende maatschappelijke beginsel dat het individu het recht heeft om bepaalde elementen van zijn identiteit verborgen te houden voor anderen. Dit beginsel, dat men het beginsel van 'vertrouwelijkheid' of 'anonimiteit' zou kunnen noemen, vloeit voort uit de waarden van individuele autonomie en persoonlijke vrijheid, die op hun beurt deel uitmaken van de

1. Zie artikel 1:19e BW.
2. Over de betekenis van (online) anonimiteit voor het verbintenissenrecht is geschreven door Prins. Prins 2000a, 2000b.
3. Rechtspersonen zijn krachtens artikel 3 t/m 5 van de Handelsregisterwet verplicht om zich in het handelsregister te laten inschrijven.

grondbeginselen van de rechtsstaat. Het komt hierna nog in vele verschijningvormen aan de orde.

Afbakening

Om te komen tot een coherent geheel van juridisch relevante onderwerpen is er voor gekozen in dit onderzoek alleen in te gaan op anonimiteitsvraagstukken in de sfeer van communicatie. Ook dit domein kenmerkt zich in toenemende mate door registratie en controle. Verschillende maatschappelijke en private belangen creëren in het communicatieproces, evenals in de reeds genoemde maatschappelijke sferen, een behoefte aan kenbaarheid. Zo dient de overheid, onder andere ter handhaving van het strafrecht, te beschikken over bevoegdheden om de identiteit van zenders en ontvangers van informatie te achterhalen. Ook private partijen moeten kunnen vaststellen wie verantwoordelijk is voor een inbreuk op hun rechten. Anderzijds manifesteert zich ook in het communicatieproces de behoefte om niet geobserveerd en geregistreerd te worden. Bij het verzenden en ontvangen van berichten en bij het verzamelen van informatie wil men niet het gevoel hebben dat anderen meekijken. De principes van kenbaarheid en vertrouwelijkheid botsen zodoende in alle hevigheid.

De focus op communicatie vraagt om een afbakening van dat begrip. Een precieze definitie is echter moeilijk te geven. Men kan communicatie ruim opvatten als 'de uitwisseling van informatie tussen een zender en een ontvanger'. In die betekenis, hoe vaag zij ook is, omvat het begrip alle communicatietechnologieën die hier aan de orde zullen komen: drukpers, telefonie en telegraaf, radio en televisie, internet, e-mail, mobiele telefonie en andere elektronische communicatietechnieken, zoals SMS en instant messaging.

Belangrijker is het onderscheid tussen openbare en niet-openbare communicatie. De regulering van anonimiteit wordt in het onderstaande namelijk allereerst behandeld voor zover het openbare communicatie betreft. Hoewel het begrip openbaarheid in juridische zin geen duidelijk omlijnde betekenis heeft, kan men, waar het communicatie betreft, in zijn algemeenheid stellen dat het al dan niet openbare karakter van een uitlating of een communicatiemiddel afhangt van het bereik waarop de uitlating of het communicatiemiddel zich richt. Voor de afbakening tussen openbaar en niet-openbaar kunnen daarnaast de bedoeling van de verzender of de uiter, de adressering van de boodschap en de aard van het medium van belang zijn.[4] Van een openbare uiting is in ieder geval sprake wanneer daarvan feitelijk kennis kan worden genomen door een onbepaald publiek. Openbare communicatiemiddelen zijn die middelen waartoe een ieder in principe toegang heeft, zoals radio, televisie, kranten en tijdschriften en het internet. Niet-openbaar zijn die middelen die voornamelijk bedoeld zijn om communicatie tussen een bepaald aantal individuen mogelijk te maken, zoals de klassieke telefonie en e-mail. De scheids-

4. Deze criteria spelen onder andere een rol bij het communicatiegeheim. Zie daarover Asscher 2002, p. 95-104.

lijn tussen openbare en niet-openbare communicatie is niet altijd duidelijk te trekken. Bij een bericht dat via een niet-openbaar communicatiemiddel, bijvoorbeeld de brief, wordt verstuurd aan meerdere ontvangers wordt het onderscheid al snel problematisch. In de digitale omgeving vloeien openbare en niet-openbare vormen van communicatie bovendien in toenemende mate samen. De grens tussen openbaar en niet-openbaar is als zodanig echter geen onderwerp van onderzoek.

De keuze om in het hiernavolgende de nadruk te leggen op openbare communicatie hangt samen met de centrale plaats van de uitingsvrijheid in dit onderzoek. Bij openbare communicatie spelen de aan dat recht ten grondslag liggende democratische en publieke belangen immers, meer dan bij besloten vormen van communicatie, een rol, met name wanneer uitingen betrekking hebben op publieke aangelegenheden en de uiter door anoniem te blijven een ongehinderde deelname aan het publieke debat mogelijk wenst te maken. Anonimiteit roept in de publieke sfeer de meest fundamentele juridische vragen op en de maatschappelijke en juridische discussie over de wenselijkheid van anonimiteit is in de context van openbare uitlatingen doorgaans het hevigst.

De focus op openbare communicatie staat er niet aan in de weg dat ook de functie van anonimiteit bij niet-openbare communicatie en de verhouding met andere grondrechtelijke belangen dan de uitingsvrijheid, zoals bijvoorbeeld de vrijheid van vereniging, vergadering en betoging en het recht op (informationele) privacy aan de orde komen. Zoals gezegd is een strikte scheiding tussen openbare en niet-openbare communicatie niet altijd mogelijk. Bovendien zijn de verschillende constitutionele belangen vaak moeilijk geheel los van elkaar te zien. De behandeling van deze andere grondrechten staat echter ten dienste van een op openbare communicatie en de uitingsvrijheid gebaseerde benadering.

Bij de behandeling van bovengenoemde onderwerpen is het van belang een onderscheid te maken tussen verschillende actoren in het communicatieproces. Anonimiteit is in de eerste plaats relevant voor de uiter, dat wil zeggen de persoon of instantie die een bepaalde mening verkondigt of informatie openbaarmaakt. Sprekers, demonstranten, internetgebruikers en auteurs van boeken en andere geschriften kunnen allen om een veelheid van redenen besluiten anoniem te blijven. Daarnaast nemen tussenpersonen in dit onderzoek een belangrijke plaats in. Onder een tussenpersoon wordt hier verstaan: elke natuurlijke persoon of rechtspersoon die communicatie mogelijk maakt of, anders gezegd, die zich bezighoudt met het verspreiden, doorgeven of toegankelijk maken van informatie. In de meeste gevallen betreft het instanties die een distributienetwerk of een (elektronisch) communicatienetwerk beheren en exploiteren. In de fysieke wereld zijn drukkers en uitgevers de belangrijkste tussenpersonen. In de digitale wereld moet men denken aan aanbieders van telecommunicatiediensten zoals telefonie en internet. Als schakel tussen zenders en ontvangers zijn tussenpersonen een spil in de hier behandelde problematiek omdat zij in staat zijn om communicatie aan individuen te relateren en anonimiteit te doorbreken. Hoewel de journalist niet zelfstandig een distributie- of communicatienetwerk in stand houdt, wordt hij, als onmisbare verbinding tussen de journa-

listieke bron en openbaarheid en als meest aangewezen persoon om deze te identificeren, in dit onderzoek ook als tussenpersoon aangemerkt. De mogelijkheid om anoniem te zijn is ten slotte van belang voor de actoren aan de ontvangstkant van het communicatieproces. Ook ontvangers en verzamelaars van informatie krijgen in veel gevallen te maken met identificatie en registratie van hun communicatiehandelingen. Dit geldt bijvoorbeeld voor leners van boeken in een bibliotheek en bezoekers van websites.

Rondom de genoemde actoren doet zich een aantal *materiële* en *procedurele* anonimiteitsvraagstukken voor. Het meest elementaire materiële anonimiteitsvraagstuk is in hoeverre uit de uitingsvrijheid en daaraan gerelateerde grondrechten voor uiters, bronnen en ontvangers een recht volgt om anoniem te zijn. Direct daarmee verbonden is de vraag in hoeverre de overheid de anonieme openbaarmaking, verspreiding en ontvangst van informatie mag reguleren en verbieden en in hoeverre zij zich dient te onthouden van het stellen van registratie- en identificatieverplichtingen. Tot de materiële vraagstukken wordt hier ook de vraag gerekend hoe het recht om anoniem te communiceren in abstracto moet worden afgebakend.

Procedurele vragen doemen op wanneer een aanspraak op anonimiteit in concrete gevallen moet worden afgewogen tegen andere belangen. Relevant is allereerst wie deze afweging dient te maken en op basis van welke criteria hij dat dient te doen. Bekijkt men de zaak vanuit de anonymus dan is het de vraag hoe hij in staat kan worden gesteld zijn grondrechtelijke aanspraken en belangen te verdedigen. Heeft de anonymus het recht om op de hoogte te worden gebracht van een poging om zijn anonimiteit te doorbreken? Dient hij in dat verband in de gelegenheid te worden gesteld zijn stem te laten horen en, zo ja, op welke wijze dient dit dan te geschieden? Voor de tussenpersoon is de vraag van belang of, en zo ja wanneer, hij kan worden gedwongen om mee te werken aan identificatie.

Bij het beantwoorden van de bovengenoemde materiële en procedurele vraagstukken is het nuttig een blik te werpen over de grenzen van het eigen rechtssysteem. Om een aantal redenen is ervoor gekozen het Amerikaanse recht te bestuderen. In de eerste plaats werd in de Verenigde Staten eerder dan in andere landen een diepgaand inzicht verworven in het verband tussen anonimiteit en uitingsvrijheid. De Verenigde Staten kent een lange traditie van anonieme politieke geschriften en het Amerikaanse Supreme Court heeft in verschillende uitspraken constitutionele bescherming toegekend aan anonieme uitingen op basis van het First Amendment. Het anonimiteitsvraagstuk wordt daarnaast ook in de juridische literatuur uitgebreid geanalyseerd. In de lagere rechtspraak is tenslotte een speciale procedure ontwikkeld, ook wel bekend als de 'John Doe procedure', waarin door de rechter wordt beoordeeld of aan een internetprovider kan worden bevolen de identificerende gegevens van een anonieme internetgebruiker te verstrekken aan een derde partij. Bij zijn afweging betrekt de rechter ook de grondrechtelijke aanspraken van de anonymus. Om de genoemde aspecten als voorbeeld te kunnen nemen bij de bespreking van het eigen recht wordt hierna eerst het Amerikaanse en dan het Nederlandse recht besproken.

Probleemstelling
Vanuit het hierboven geschetste perspectief wordt in dit onderzoek allereerst getracht te komen tot een beter begrip van de betekenis van anonimiteit en tot een analyse van het verband tussen de bescherming van anonimiteit en de uitoefening van grondrechten. Daarnaast neemt de beschrijving en analyse van het geldende recht een belangrijke plaats in. Tenslotte is het de bedoeling om de constitutionele grondslagen van een mogelijk recht om anoniem te communiceren in kaart te brengen. In dit onderzoek wordt getracht een antwoord te formuleren op de volgende drie onderzoeksvragen:

- *Hoe is anonieme communicatie in het Nederlandse recht gereguleerd?*
- *Wat zijn de constitutionele grondslagen voor de bescherming van anonieme openbare communicatie?*
- *Dient in Nederland bij openbare communicatie een recht op anonimiteit te worden erkend?*

Begripsbepaling
Enkele van de in dit onderzoek gebruikte begrippen behoeven nadere toelichting. Allereerst moet het onderscheid tussen de *uitingsvrijheid* of de vrijheid van meningsuiting en de *communicatievrijheid* worden verduidelijkt. De uitingsvrijheid, beschermd in artikel 7 van de Nederlandse Grondwet (Gw) en artikel 10 van het Europees Verdrag voor de Rechten van de Mens (EVRM), omvat het recht om ideeën en meningen te openbaren en te verspreiden. Dit recht brengt voor de overheid een plicht mee om zich te onthouden van bemoeienis met de inhoud van uitingen. In ruimere zin omvat de uitingsvrijheid het hele scala van uiten, verspreiden en ontvangen van informatie. De communicatievrijheid omvat deze elementen eveneens, maar heeft daarnaast betrekking op de vrije uitwisseling van informatie in een ruimere zin. Tot de communicatiegrondrechten behoort niet alleen de uitingsvrijheid, maar ook het communicatiegeheim, zoals vastgelegd in artikel 13 Gw. De communicatievrijheid omvat daarnaast het recht op vrije toegang tot communicatiemiddelen. Daaronder kan ook het recht op toegang tot informatie en tot informatie- en communicatienetwerken worden gerekend.

Het recht op eerbiediging van de persoonlijke levenssfeer, ook wel aangeduid als het recht op privacy, is vastgelegd in artikel 10 Gw en artikel 8 EVRM. In literatuur en rechtspraak worden doorgaans een onderscheid gemaakt tussen *relationele* en *informationele privacy*. De *relationele privacy* geeft het individu het recht om in sociale relaties met anderen, bijvoorbeeld binnen het gezin of de vriendenkring, met rust gelaten te worden.[5] Deze vorm van privacy beschermt naast de fysieke privé-sfeer een niet aan een bepaalde plaats gebonden privé-sfeer die zich nog wel rond de persoon bevindt, maar niet beperkt

5. Zie voor een uitgebreide behandeling van het begrip relationele privacy Holvast 1986, p. 20 e.v.

is tot privé-ruimten of de fysieke grens van het eigen lichaam.[6] De *informationele privacy* geeft het individu zeggenschap over informatie en gegevens die tot hem herleidbaar zijn en stelt normen met betrekking tot de opslag en verwerking van deze gegevens.

Dit onderzoek richt zich voor een belangrijk deel op vraagstukken rondom anonimiteit in de *informatiesamenleving*. De informatiesamenleving is een samenleving waarin informatie een van de belangrijkste productiefactoren is en waarin complexe informatievoorzieningsprocessen plaatsvinden. Als belangrijke kenmerken van de informatiesamenleving kunnen in het kader van dit onderzoek worden genoemd: de ontwikkeling van nieuwe communicatietechnieken, de samenvloeiing of 'convergentie' van deze technieken, de toename van informatie- en communicatiestromen, het grensoverschrijdende karakter van de informatieverwerking, de toegenomen opslag en verwerking van persoonsgegevens door overheid en bedrijfsleven en de registratie van het communicatiegedrag van de burger.[7]

Plan van behandeling

De betekenis van het begrip anonimiteit is sterk afhankelijk van de historische, technische of juridische context waarin het wordt gebruikt. In het eerste hoofdstuk van dit onderzoek wordt daarom begonnen met de verklaring van de functie en de inhoud van dit begrip. In hoofdstuk 2 wordt vervolgens meer specifiek ingegaan op de functie van anonimiteit in het publieke debat. Dit onderwerp was zowel in het Amerikaanse als het Nederlandse recht reeds vroeg een belangrijk thema en wordt daarom, voorafgaand aan de behandeling van de relevante rechtsregels in beide rechtssystemen, afzonderlijk behandeld. Hoofdstuk 3 bevat een korte uiteenzetting over de betekenis van anonieme geschriften in de Amerikaanse geschiedenis, gevolgd door een uitgebreide beschrijving van de jurisprudentie van het Supreme Court inzake de bescherming van anonimiteit onder het First Amendment, zowel in de fysieke wereld als in de digitale omgeving. Hoofdstuk 4 behandelt in het verlengde daarvan de positie van de anonieme gedaagde in het Amerikaanse recht. Hier wordt met name aandacht besteed aan de bescherming van anonieme internetgebruikers in wetgeving en rechtspraak. In hoofdstuk 9 zal de Amerikaanse aanpak op dit punt worden vergeleken met wetgeving en rechtspraak in Nederland en Europa.

Bij de bespreking van het Nederlandse recht in de hoofdstukken 5 tot en met 7 is een chronologische lijn gevolgd. In hoofdstuk 5 komen verschillende episodes uit de Nederlandse geschiedenis aan de orde. Lange tijd golden in Nederland, ter ondersteuning van censuurbepalingen, verboden op de publicatie en verspreiding van anonieme geschriften. De achtergrond en ontwikkeling van deze verboden worden aan een nader onderzoek onderworpen. Hoofdstuk 6 beschrijft het geldende recht inzake de positie van drukkers,

6. Dommering e.a. 2000, p. 49.
7. Idem, p. 21-25.

uitgevers en journalisten. Vervolgens komen wij toe aan de regulering van anonimiteit bij elektronische communicatiemiddelen. Hoofdstuk 7 zet uiteen hoe de betekenis van anonimiteit na de informatierevolutie veranderd is. Dit hoofdstuk bespreekt met name de nieuwe vragen die zich bij elektronische communicatie voordoen en behandelt daarnaast het verband tussen anonimiteit en informationele privacy. In de hoofdstukken 8 en 9 wordt de bescherming en doorbreking van anonimiteit bij elektronische communicatie in kaart gebracht. De bescherming van anonimiteit is grotendeels gereguleerd in de Europese privacyrichtlijnen en de implementatie daarvan. Dit onderwerp komt aan de orde in hoofdstuk 8. Wettelijke mogelijkheden voor de doorbreking van anonimiteit zijn verdeeld over uiteenlopende regelingen. Deze worden in hoofdstuk 9 tegen het licht gehouden. Hoofdstuk 10 bevat de conclusie van dit onderzoek alsmede enige aanbevelingen.

Beschouwd vanuit constitutioneel perspectief valt dit onderzoek uiteen in twee delen. In de hoofdstukken 2 tot en met 6 ligt de nadruk op het verband tussen anonimiteit en uitingsvrijheid. In het Amerikaanse recht heeft de uitingsvrijheid als grondslag voor de bescherming van anonimiteit altijd een grotere rol gespeeld dan het recht op privacy. Ook in Nederland heeft het recht op privacy pas later betekenis gekregen. Men kan zodoende onderscheid maken tussen het tijdperk van de drukpers en de traditionele media waarin anonimiteitsvraagstukken met name raakten aan de uitingsvrijheid en de informatiesamenleving waarin daarnaast de bescherming van de informationele privacy een steeds groter gewicht in de schaal legt. De overgang tussen deze twee tijdperken wordt in hoofdstuk 7 beschreven. Ook het verband tussen anonimiteit en informationele privacy wordt daar behandeld omdat dit belang met name actueel is in de sfeer van elektronische communicatie.

1 Het begrip anonimiteit

1.1 Inleiding

Een samenhangende analyse van de regulering van anonieme openbare communicatie is alleen mogelijk wanneer duidelijk is wat het begrip anonimiteit precies inhoudt. Daarom zullen hier verschillende betekenissen en verschijningsvormen van anonimiteit aan een nader onderzoek worden onderworpen. Ook komt aan de orde hoe anonimiteit en machtsuitoefening zich tot elkaar verhouden en hoe het oordeel over anonimiteit historisch samenhangt met opvattingen over vrijheid en de scheiding tussen het publieke en het private.

1.2 Drie betekenissen

Anonimiteit betekent letterlijk 'naamloosheid'. Het Nederlandse woord anoniem is via het Franse *anonyme* en het middeleeuws Latijnse *anonymus* ontleend aan het Griekse woord *anonumos*. Dit woord is samengesteld uit de elementen *a(n)* (ontkennend) en *onuma* (naam), en betekent 'zonder naam'.[1] Het Groot Woordenboek der Nederlandse Taal vermeldt ook andere betekenissen: 'zonder bekendmaking van de naam van de schrijver of spreker', 'zonder ondertekening', 'waaraan men geen naam kan toekennen', 'niet met een naam te onderscheiden.'[2] Daarnaast wordt het woord *anonymus* vermeld. Dit verwijst naar een ongenoemde of naamloze persoon.

Wie zijn ware naam voor anderen wil verbergen kan ook besluiten om gebruik te maken van een pseudoniem. Dit is 'een aangenomen naam die iemand voert bij zijn optreden in het openbaar, met name als schrijver, met het doel onbekend te blijven' of, korter gezegd, een 'schuilnaam'.[3] Ook dit woord is afkomstig uit het Grieks: *pseudos* (onwaarheid) + *onoma* (naam). Het woord pseudoniem kan, in een minder vaak voorkomende betekenis, ook betrekking hebben op een geschrift dat onder een schuilnaam is geschreven of op de schrijver die onder een aangenomen naam publiceert. Als bijvoeglijk naamwoord heeft het de betekenis 'een schuilnaam dragend': een *pseudonieme* uitgever. Anonimiteit en pseudonimiteit hebben dus gemeenschappelijk dat zij de ware naam van een persoon voor anderen verhullen.

1. Van Veen & Van der Sijs 1989.
2. Van Dale 1995.
3. Idem.

In het dagelijkse spraakgebruik gebruikt men het begrip anonimiteit niet alleen in de betekenis van naamloosheid. Wanneer iemand bijvoorbeeld zegt dat hij het prettig vindt om op te gaan in 'de anonimiteit van de grote massa' dan doelt hij op anonimiteit in een ruimere betekenis. Deze tweede benadering van het begrip anonimiteit is treffend onder woorden gebracht door Westin, die anonimiteit opvat als één van de basisvormen van individuele privacy. Hij onderscheidt 'solitude' als eerste en meest vergaande basisvorm van privacy. Dit is de situatie waarin het individu gescheiden is van de groep en gevrijwaard blijft van observatie door andere personen. De tweede vorm is 'intimacy'. Hier maakt het individu deel uit van een hecht sociaal verband, zoals een liefdesrelatie, een vriendschap tussen twee of meer personen, de familie of de werkomgeving. De derde vorm van privacy is 'anonimity'. Volgens Westin is sprake van anonimiteit wanneer het individu zich in de openbare ruimte begeeft of handelingen verricht in de publieke sfeer, maar gevrijwaard blijft van identificatie en controle. Onder identificatie verstaat Westin iedere handeling die inbreuk maakt op de anonimiteit van een persoon en waardoor een persoon het privilege verliest om niet gehouden te zijn aan de sociale regels en rollenpatronen die zouden gelden indien hij bekend zou zijn bij degenen die hem observeren:

> "The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behavior and role that would operate if he were known to those observing him. In this state the individual is able to merge into the 'situational landscape.' Knowledge or fear that one is under systematic observation in public spaces destroys the sense of relaxation and freedom that men seek in open spaces and public arenas."[4]

Deze definitie van anonimiteit is een uitbreiding van het taalkundige begrip, die begrepen moet worden binnen de opvattingen van Westin over privacy als belangrijk middel om bepaalde aspecten van menselijke vrijheid te beschermen. De beschrijving koppelt anonimiteit los van zijn etymologische betekenis. Nieuwe elementen zijn het ontbreken van identificatie in de publieke sfeer en de associatie met persoonlijke vrijheid. Daarnaast bevat de geciteerde passage een sociologisch element: Westin beschrijft de anonimiteit van de grote stad waar persoonlijke banden tussen individuen ontbreken en men in mindere mate is gehouden aan sociale regels.

De derde en meest abstracte betekenis van anonimiteit die ik hier onderscheid stelt het verschijnsel centraal dat personen, gegevens en handelingen niet, of slechts met

4. Als vierde vorm van privacy noemt Westin 'reserve'. Hiervan is sprake als er een psychologische barrière tegen ongewenste inmenging bestaat die in stand wordt gehouden door de bereidheid van anderen om discreet te zijn. Westin 1970, p. 31-32. Zie voor een nadere bespreking van Westins ideeën over privacy Holvast 1986, p. 19 e.v.

onevenredig veel inspanning, met elkaar in verband kunnen worden gebracht. Dit verschijnsel wordt afwisselend aangeduid met begrippen als 'onidentificeerbaarheid', 'ontraceerbaarheid' en 'niet-herleidbaarheid'. Deze begrippen hebben grofweg dezelfde betekenis. Wel kan men stellen dat het begrip onidentificeerbaarheid doorgaans voornamelijk wordt gebruikt om een eigenschap van personen aan te duiden, terwijl de begrippen ontraceerbaarheid en niet-herleidbaarheid ook betrekking hebben op gegevens en handelingen, met name in een technische context.

De Amerikaanse filosofe Wallace geeft een grondige analyse van anonimiteit als onidentificeerbaarheid. Zij formuleert een abstracte definitie: anonimiteit is een vorm van onidentificeerbaarheid die kan worden gedefinieerd als de niet-herleidbaarheid van persoonlijke eigenschappen.[5] Hiermee wordt bedoeld dat in de relatie tussen een anonieme persoon en anderen van de eerste slechts één of enkele eigenschappen bekend zijn die niet op een zodanige manier in verband kunnen worden gebracht met andere eigenschappen, dat deze persoon in zijn geheel kan worden geïdentificeerd. Een voorbeeld is de anonieme auteur van een boek. Hoewel het lezerspubliek zijn werkelijke naam niet kent, is het mogelijk wel op de hoogte van een aantal andere persoonlijke eigenschappen. Zo kan men uit het boek misschien opmaken welke politieke ideeën de auteur er op nahoudt en biedt de stijl waarin het boek geschreven is wellicht aanwijzingen omtrent leeftijd, geslacht en nationaliteit. Zolang men echter niet over genoeg persoonlijke eigenschappen beschikt om de auteur te onderscheiden van alle andere personen, blijft hij anoniem. De anonimiteit wordt pas doorbroken als de eigenschap 'auteur van het boek X' door het lezerspubliek in verband gebracht kan worden met de persoon van de auteur.[6]

Wallace benadrukt dat anonimiteit moet worden onderscheiden van loutere sociale onbekendheid of isolatie, zoals die van een kluizenaar. Een kluizenaar is ten opzichte van anderen misschien naamloos of onbekend, maar in het algemeen zal men hem niet als 'anoniem' bestempelen. Hij is eerder een "unrelated, socially disconnected agent whose life does not and whose actions do not, for the most part affect or are not affected by the lives of others in a social environment".[7] Anonimiteit houdt in dat de eigenschap dankzij welke men van het bestaan van de persoon op de hoogte is niet in verband kan worden gebracht met andere eigenschappen. Volledige onbekendheid, zoals die van de kluizenaar, houdt daarentegen in dat bij anderen geen enkele eigenschap van een persoon bekend is; men weet niet eens dat de persoon bestaat. Met andere woorden: de notie van anonimiteit veronderstelt de deelname van de anonieme persoon in sociale relaties. Wetenschap over iemands identiteit, of het gebrek daaraan, is relevant en beïnvloedt

5. Wallace spreekt van 'noncoordinability of traits in a given respect.' Het woord 'trait' vertaal ik hier als een 'persoonlijke eigenschap' van een persoon. Een 'trait' is altijd een eigenschap waarmee een persoon kan worden onderscheiden van anderen. Wallace 1999b, p. 25.
6. Wallace 1999b, p. 23-24.
7. Idem, p. 25.

anderen wanneer men handelt in een sociale context. Deze constatering van Wallace sluit precies aan bij het onderwerp van dit onderzoek. Communicatie is immers per definitie een sociale activiteit.

De sociale dimensie van anonimiteit impliceert dat de sociale verbanden waarin personen functioneren voor een goed begrip van anonimiteit bepalend zijn. Sociale verbanden zijn immers netwerken van persoonlijke eigenschappen en relaties.[8] Wallace gebruikt als algemene term voor dergelijke netwerken het woord 'orde'. Anonimiteit is de niet-herleidbaarheid van persoonlijke eigenschappen in een bepaalde sociale orde. Ieder persoon bevindt zich in een veelheid van dergelijke sociale, economische of culturele ordes. De auteur van een boek bevindt zich als zoon (of als broer, oom, neef enz.) in de orde van zijn familie. Als schrijver bevindt hij zich in een wat men een literaire orde zou kunnen noemen.

Anonimiteit kan worden bereikt omdat een persoon een 'pluraliteit van eigenschappen' is *en* omdat iedere afzonderlijke eigenschap niet aan alle andere eigenschappen van een persoon gerelateerd is: "Traits must be interrelated, that is, related to some other traits, if they are traits of the same person. But they need not be related to every other in order for a person to be a unitary whole."[9] Of een eigenschap andere eigenschappen toegankelijk maakt en daarmee verdere identificatie mogelijk maakt hangt af van de relatie van die eigenschap met andere eigenschappen en de mate waarin degene die de anonimiteit tracht te doorbreken beschikt over de praktische middelen en de bekwaamheid om toegang te verkrijgen tot die eigenschappen en hun onderlinge samenhang. Methoden om anonimiteit te bereiken, beogen altijd het contact met andere gerelateerde eigenschappen te verbreken.[10]

Wallace onderscheidt verschillende functies van anonimiteit. Van *agent anonymity* is sprake wanneer anonimiteit een bepaald handelen van een persoon mogelijk maakt. Het kan gaan om goede, slechte of ethisch neutrale handelingen. Voorbeelden zijn anonieme auteurs, anonieme bronnen in de media, anonieme donoren, maar ook anonieme bieders bij veilingen. *Recipient anonymity* is aanwezig wanneer de anonieme persoon wordt beschermd tegen de handelingen van anderen. *Process anonymity* verzekert ten slotte de

8. Wallace licht dit alsvolgt toe: "As far as anonymity is concerned, the pertinent beings are societies and persons. Societies and persons are networks of traits or relations. (…) Every society is an interrelation of locations, for example, of economic, political, geographical, climatic, cultural, linguistic and so on locations. These may also be related to or located in other locations or orders an economic order, a political order, a geographical order and so on. Conversely, each such location that constitutes a society is also an order in which individual members or groups of individuals can be located. Each person is a combination of interrelated traits; each trait is a position in a network of relations or equivalently, the location of the person in an order. Every person *is* a combination of traits, *is* located in multiple orders." Wallace 1999b, p. 26.
9. Wallace 1999b, p. 27.
10. Idem, p. 28.

betrouwbare, onpartijdige of geldige uitkomsten van een proces waarin beslissingen over personen worden genomen. Voorbeelden zijn het afnemen van examens, het doen van statistisch wetenschappelijk onderzoek en besluitvorming bij wetgeving en rechtspraak. Anonimiteit kan in ieder afzonderlijk geval meerdere van de genoemde doelen dienen.[11]

De betekenis en functie van anonimiteit wordt pas echt goed duidelijk op het moment dat aan de anonimiteit, gewild of ongewild, een einde komt. Het is daarom van belang stil te staan bij de vraag wat men precies bedoelt met 'doorbreking' of 'opheffing' van anonimiteit. Uitgaande van hetgeen hierboven werd besproken, kan doorbreking op verschillende wijzen geschieden. Vat men anonimiteit, in zijn meest beperkte betekenis, op als naamloosheid, dan is met het bekend worden van de naam de anonimiteit doorbroken. Legt men de nadruk op anonimiteit als onidentificeerbaarheid dan zijn daarentegen vele verschillende situaties denkbaar, waarin voor doorbreking telkens verschillende handelingen vereist zijn. De doorbreking staat dan logischerwijs gelijk aan het vaststellen van identiteit of aan identificatie. Het begrip identiteit zou men in dat verband kunnen definiëren als 'een set eigenschappen van een persoon'. Identificatie is dan het relateren van reeds bekende eigenschappen van een persoon aan andere eigenschappen totdat één persoon overblijft die met een bepaalde mate van waarschijnlijkheid als enige aan deze eigenschappen voldoet. Het Amerikaanse Computer Science and Telecommunication Board definieert beide begrippen alsvolgt:

> Identity: The identity of X is the set of information about an indiviual X, which is associated with that individual in a particular identity system Y.
>
> Identification: Identification is the process of using claimed or observed attributes of an individual to infer who the individual is.[12]

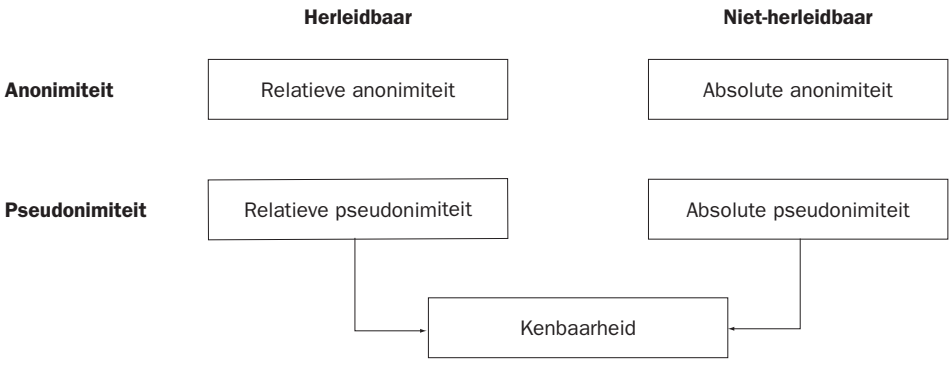
Vaak geschiedt identificatie op basis van fysieke kenmerken. Verhult de anonymus zijn identiteit bijvoorbeeld door een masker te dragen, dan staat doorbreking van anonimiteit gelijk aan ontmaskering in de letterlijke zin van het woord. Ook bij een paspoortcontrole wordt het gelaat, door middel van een pasfoto, gebruikt als aanknopingspunt. Modernere biometrische identificatietechnologieën, zoals de irisscan of een DNA-test, maken daarnaast gebruik van verschillende andere fysieke kenmerken. Er zijn echter ook gevallen waarin de identiteit, bij gebrek aan fysieke kenmerken, op andere wijze moet worden achterhaald. Dit is bijvoorbeeld het geval in het digitale communicatieproces. Wanneer men een e-mailbericht ontvangt dat is verzonden met gebruikmaking van een e-mailadres dat geen aanwijzingen bevat omtrent de identiteit van de verzender, dan is identificatie slechts mogelijk door verschillende categorieën van digitale gegevens aan elkaar te koppelen. In feite gaat het hier om het doorbreken van anonimiteit in de bete-

11. Idem, p. 29.
12. Kent & Linette 2003, p. 19-20.

kenis van 'ontraceerbaarheid': door het e-mailadres in verband te brengen met verkeers- en adresseringsgegevens, het IP-adres van de computer van de verzender, en naam-, adres en woonplaatsgegevens kan men vaak, maar lang niet altijd, een fysieke persoon aanwijzen als verzender of ontvanger van bepaalde informatie. Daarbij is in de praktijk van groot belang in hoeverre de benodigde identificerende gegevens met behulp van providers en andere digitale tussenpersonen verkregen kunnen worden en in hoeverre er juridische mogelijkheden bestaan om de verstrekking hiervan af te dwingen. Op de juridische betekenis van het begrip identificerend gegevens en op de verstrekking hiervan wordt nog nader ingegaan in hoofdstuk 9.

Bij de afhandeling van communicatie is doorgaans een tussenpersoon betrokken. In veel gevallen is hij in staat om met behulp van bij hem berustende informatie anonimiteit op te heffen. Dit leidt er toe dat men in het communicatieproces een onderscheid kan maken tussen *relatieve* en *absolute* vormen van anonimiteit en pseudonimiteit.[13] Van absolute anonimiteit of pseudonimiteit is sprake wanneer een boodschap of een handeling op geen enkele manier tot de verantwoordelijke persoon herleidbaar is. Relatieve anonimiteit of pseudonimiteit bestaat wanneer het praktisch gezien nog mogelijk is om de identiteit van de verantwoordelijke persoon te achterhalen. Dit kan bijvoorbeeld het geval zijn wanneer een drukker, uitgever of internetprovider, beschikt over naam-, adres en woonplaatsgegevens. De kwalificatie 'relatief' heeft in dat geval twee betekenissen: (1) de anonimiteit geldt ten opzichte van iedereen behalve de tussenpersoon en (2) de anonimiteit kan met behulp van die tussenpersoon ook ten opzichte van al die anderen worden opgeheven.

Uit het bovenstaande volgt dat men in het communicatieproces vier gradaties van anonimiteit kan onderscheiden.



13. Zie voor juridische literatuur over dit onderscheid Froomkin 1996; Prins 2000a; Prins 2000b; Du Pont 2001.

I Relatieve pseudonimiteit
Bij relatieve pseudonimiteit zijn er bepaalde instanties of tussenpersonen die de verantwoordelijke persoon kunnen identificeren:

> *A heeft een boek geschreven onder een pseudoniem. Bij het publiek is niet bekend wie er achter het pseudoniem schuilgaat maar de drukker van het boek beschikt over de naam en het adres van A.*

II Absolute pseudonimiteit
Bij absolute pseudonimiteit zijn er voor de tussenpersoon, ondanks het gebruik van een pseudoniem, geen aanknopingspunten waarmee de identiteit van de verantwoordelijke persoon kan worden achterhaald:

> *A stuurt vanaf het e-mailadres 'repelsteeltje@gmail.com' een e-mail aan een collega. Daarbij maakt hij gebruik van een zogenaamde 'anonymizer'. De anonymizer wist alle sporen van A's surfgedrag onmiddellijk zodat zijn provider de verstuurde boodschap niet tot hem kan herleiden.*[14]

III Relatieve anonimiteit
Wanneer geen gebruik is gemaakt van een echte naam of een pseudoniem kan de verantwoordelijke persoon aan de hand van andere identificerende informatie soms toch achterhaald kan worden. In een dergelijk geval is sprake van relatieve anonimiteit:

> *A stuurt opnieuw een e-mail naar zijn collega. Ditmaal maakt hij gebruik van een anonieme remailer.*[15] *Deze remailer bewaart het IP-adres van A's computer gedurende drie maanden. Derden kunnen gedurende die periode A's identiteit met behulp van de remailer achterhalen.*[16]

14. Bij e-mail moet voor het '@'-teken natuurlijk altijd een naam worden vermeld. Wanneer hiervoor een andere naam wordt gebruikt dan de echte naam van de afzender is dit mijns inziens alleen een pseudoniem wanneer deze onechte naam structureel door dezelfde persoon wordt gebruikt zodat sprake is van kenbaarheid. Sommige anonymous remailers geven iedere doorgestuurde e-mail dezelfde gebruikersnaam (bijvoorbeeld 'nobody@anonymizer.com'). De onechte naam 'nobody' is in dat geval geen pseudoniem aangezien hij verwijst naar iedere willekeurige gebruiker van de remaildienst.
15. Een anonieme remailer is een programma dat het emailadres en andere identificerende informatie verwijdert alvorens de boodschap door te sturen.
16. Om te voorkomen dat de identificerende informatie op deze wijze alsnog kan worden achterhaald wordt vaak gebruik gemaakt van 'chained remailing'. Wanneer een bericht door een keten van remailers wordt gestuurd wordt de kans steeds kleiner dat de identificerende gegevens nog beschikbaar zijn. Op een bepaald moment kan men dan spreken van absolute anonimiteit.

IV Absolute anonimiteit
Indien geen pseudoniem werd gebruikt en de verantwoordelijke persoon ook niet op andere wijze achterhaald kan worden, is sprake van absolute anonimiteit:

> *De periode van drie maanden is verstreken. A's IP-adres wordt gewist.*

Er dient hier nog te worden gewezen op een belangrijk verschil tussen anonimiteit en pseudonimiteit. Het gebruik van pseudoniemen leidt tot een bepaalde mate van 'kenbaarheid': de ontvanger kan verschillende boodschappen met elkaar in verband brengen omdat zij zijn ondertekend met dezelfde schuilnaam. De boodschappen krijgen daardoor een samenhang die de afzender een bepaalde identiteit verleent. De auteur is niet te identificeren, maar hij is wel 'individualiseerbaar'. Dit kan een reden zijn om te kiezen voor het gebruik van een pseudoniem. De uit het gebruik van een pseudoniem voortvloeiende kenbaarheid biedt in sommige gevallen overigens wel mogelijkheden voor het achterhalen van de identiteit van de verzender, met name bij elektronische communicatie. Wanneer bekend is dat meerdere boodschappen van een en dezelfde persoon afkomstig zijn kan aan de hand van gegevens over tijdstip en plaats van verschillende verzonden boodschappen soms worden bepaald vanaf welk e-mailadres of telefoonnummer een boodschap is verstuurd.

1.3 Anonimiteit, communicatie en macht

Anonimiteit verbreekt niet alleen de band tussen de bron en zijn boodschap. Wie zijn ware naam in nevelen hult kan minder makkelijk, of helemaal niet, verantwoordelijk worden gehouden voor zijn handelen. Dit verschijnsel zal hierna worden aangeduid als 'ontoerekenbaarheid'.

Een vroege verhandeling over ontoerekenbaarheid vinden wij bij Plato. In de *Politeia* beschrijft hij een discussie tussen zijn leermeester Socrates en diens leerling Glaukon.[17] Het gaat over de aard en oorsprong van de moraal. Glaukon is van mening dat de mens zich niet uit eigen verkiezing aan wetten en normen houdt, maar alleen omdat hij dat beschouwt als een noodzakelijk kwaad. Om zijn standpunt kracht bij te zetten vertelt Glaukon de parabel van Gyges. Gyges, een schaapherder in dienst van de koning van Lydië, vindt op een dag een ring die hem de magische kracht verleent om onzichtbaar te worden.[18] Wanneer hij als boodschapper naar het hof wordt gezonden om de koning ver-

17. Een Nederlandse vertaling vindt men bij Koolschijn 1997, p. 36-40.
18. Gyges vindt de ring bij toeval wanneer er tijdens het hoeden van zijn schapen een hevige aardbeving plaatsvindt die een opening maakt in de aarde. Hij gaat door de opening naar binnen en stuit na een lange ondergrondse wandeling op een enorm beeld van een koperen paard met vensters in zijn buik. In de buikholte van het paard vindt hij het lijk van een gebalsemde reus. De reus draagt een gouden ring om zijn pink. Gyges neemt de ring mee en keert terug. Wanneer hij zich weer voegt bij de andere herders ontdekt hij dat hij voor anderen onzichtbaar wordt wanneer hij de ring zo draait dat de steen zich aan de binnenkant van zijn hand bevindt. De anderen beginnen dan over hem te spreken alsof hij niet langer aanwezig is. Zie Koolschijn 1997, p. 38-39.

slag te doen van het reilen en zeilen van de veestapel, weet hij de kracht van de ring op sluwe wijze uit te buiten. Hij verleidt de koningin, doodt met haar hulp de koning en maakt zich meester van de troon.

De parabel brengt volgens Glaukon een wezenlijke eigenschap van de mens aan het licht: geen enkel mens is zo rechtschapen dat hij, wanneer hij de ring van Gyges zou bezitten, onder alle omstandigheden zou blijven handelen volgens de regels van rechtvaardigheid en fatsoen. Onzichtbaarheid biedt immers mogelijkheden die de menselijke fantasie prikkelen.[19] Het is de perfecte dekmantel voor het begaan van misdrijven: men kan ongestraft een moord plegen of een vriend redden uit de gevangenis en ook dieven en insluipers kunnen ongestoord hun gang gaan. Glaukon tracht aan te tonen dat het handelen van de mens in hoge mate wordt bepaald door de wetenschap dat hij wordt gadegeslagen. Het is in de eerste plaats die wetenschap, en niet het besef dat bepaalde handelingen goed of slecht zijn, die ons weerhoudt van onrechtvaardig of strafbaar gedrag. Wie de volledige vrijheid heeft om te doen en laten wat hij wil, zal zich in hogere mate laten leiden door zijn eigen belang en minder door de regels van rechtvaardigheid. De mens houdt zich dus niet uit eigen verkiezing aan wetten en normen maar alleen omdat hij daartoe wordt gedwongen.

Anonimiteit vertoont belangrijke overeenkomsten met onzichtbaarheid. Het probleem van de ontoerekenbaarheid doet zich bij anoniem gedrag dan ook voor op de wijze die Glaukon beschrijft: degene die achter een bepaalde handeling schuilgaat is niet bekend en kan dus ook niet verantwoordelijk worden gehouden voor zijn gedrag. Vanuit juridische perspectief leidt deze omstandigheid tot een dilemma. Enerzijds tast ontoerekenbaarheid de handhaafbaarheid van rechtsregels aan. Wanneer men onzichtbaar of anoniem is, ontbreekt de sociale dwang die uitgaat van het persoonlijk contact met anderen, zoals Westin beschrijft, en wordt ook het afschrikwekkend effect van juridische sancties op maatschappelijk onwenselijk gedrag weggenomen. Anderzijds is volstrekte ontoerekenbaarheid in zekere zin de perfecte verwerkelijking van persoonlijke vrijheid. Een private en staatsvrije sfeer voor het individu kan niet bestaan zonder een zekere mate van anonimiteit en ontoerekenbaarheid. De spanning tussen de tegengestelde belangen van rechtshandhaving en individuele vrijheid manifesteert zich op vele gebieden van het recht, met name in de sfeer van grondrechten.

19. Er bestaan vele voorbeelden van verhalen waarin onzichtbaarheid een rol speelt. Het verhaal van Gyges is door de schrijver Tolkien verwerkt in het boek *Lord of the Rings*. Bekend is ook het kinderboek over Bram Vingerling die op zijn zolderkamer een magische vloeistof brouwt waarmee hij zichzelf onzichtbaar kan maken. Zie Roggeveen 1933. Ten slotte noem ik hier het sciencefictionverhaal *The invisible man* van H.G. Wells.

Het verband tussen ontoerekenbaarheid en de gelding van (rechts)regels brengt een fundamentele relatie aan het licht tussen anonimiteit en machtsuitoefening in brede zin. Het anoniem zijn is een verdedigingslinie voor de staatsvrije sfeer waar een verwoed gevecht plaatsvindt tussen overheid en burger. Door zich te onttrekken aan identificatie, registratie en controle onttrekt het individu zich ook aan overheidsbemoeienis. Anderzijds spannen instanties die met macht bekleed zijn zich onophoudelijk in om de anonimiteit van hun subjecten zoveel mogelijk uit te bannen. De mate waarin het individu beschikt over juridische en andere middelen om zijn anonimiteit te verdedigen is daarom bepalend voor zijn positie in de geldende maatschappelijke machtsverhoudingen.

Verschillende politieke denkers en filosofen hebben zich bezig gehouden met de relatie tussen anonimiteit en macht. Zo komen in het boek *Discipline, toezicht en straf* van de Franse filosoof Foucault, waarin deze de historische ontwikkeling van de strafvoltrekking en het strafproces schetst, controle en identificatie duidelijk naar voren als een middel om burgers in een ijzeren greep te houden. Foucault beschrijft hoe zich in de achttiende en negentiende eeuw een systeem van discipline en toezicht ontwikkelde dat uiteindelijk zou leiden tot de afschaffing van lijfstraffen en de opkomst van de moderne gevangenis. Een vroeg voorbeeld van 'disciplinerend toezicht' is de bestrijding van pestepidemieën in de zeventiende eeuw. Om verspreiding van de ziekte tegen te gaan werden hele steden afgegrendeld en opgedeeld in wijken die onder het gezag van een intendant werden geplaatst. Alle burgers werden nauwgezet geregistreerd en in quarantaine gezet. Het was hen op straffe van de dood verboden hun huizen te verlaten:

> "In deze afgegrendelde, opgedeelde en tot in alle uithoeken bewaakte ruimte worden de individuen op een vaste plaats ingesloten, worden de geringste bewegingen gecontroleerd en alle voorvallen geregistreerd, verbindt een ononderbroken beschrijving centrum en periferie, wordt de macht onderverdeeld uitgeoefend volgens een continu hiërarchisch patroon en wordt ieder individu permanent gelokaliseerd, onderzocht en ingedeeld bij de levenden, de zieken of de doden – en dit alles vormt een compact model van het disciplinerende systeem."[20]

De peststad is volledig in de greep van hiërarchie, toezicht, controle en registratie. Foucault beschrijft hoe het disciplinerende schema dat uit de bestrijding van de pest voortvloeit vanaf het begin van de negentiende eeuw wordt toegepast in openbare instellingen van individuele controle, zoals de psychiatrische inrichting, het tuchthuis, het huis van correctie, het opvoedingsgesticht, en hospitalen.[21]

De opperste verbeelding van disciplinerend toezicht is het *Panopticon* van Jeremy Bentham: een ontwerp van een ringvormig gebouw met in het midden een toren van waaruit één bewaker alle krankzinnigen, zieken, veroordeelden, arbeiders of scholieren kan observeren. Iedere cel heeft twee ramen. Het binnenraam geeft de bewaker zicht op

20. Foucault 1989, p. 270-273.
21. Idem, p. 275.

het doen en laten van de gedetineerde, het buitenraam zorgt dat iedere cel tot in alle hoeken is verlicht. Deze constructie heeft als belangrijkste effect dat de gedetineerde zich bewust wordt van zijn permanente zichtbaarheid. De machtsuitoefening is voor hem zichtbaar maar tegelijkertijd ondoorzichtig; hij weet niet of er daadwerkelijk naar hem gekeken wordt maar wel dat dit te allen tijde mogelijk is. Het toezicht is discontinu maar heeft continu effect. De uitoefening van macht wordt daardoor geperfectioneerd, geautomatiseerd en ontindividualiseert.

Bij de vormgeving van de maatschappij dienden volgens Bentham niet de natuurlijke rechten en de individuele vrijheid centraal te staan, maar het principe van *utiliteit*: de overheid moet streven naar een evenwichtssituatie waarin een zo groot mogelijk geluk voor allen wordt bereikt. De moreel juiste handeling in een bepaalde situatie is de handeling die deze situatie dichterbij brengt. Het proces van wetgeving moet daarom volledig gericht zijn op het bepalen van wat goed is voor de samenleving en het bedenken van middelen om de gewenste uitkomsten te realiseren. Het belangrijkste doel is daarbij het garanderen van veiligheid voor iedereen. In de visie van Bentham zijn alle andere rechten, zoals persoonlijke en politieke vrijheid, van dit belang afgeleid.[22] Het Panopticon is voor Bentham dan ook niet alleen een architectonisch en optisch systeem maar een blauwdruk voor de hele maatschappij. Het panoptisme is een methode om de samenleving vorm te geven volgens de principes van het utilitarisme. Telkens wanneer een groep individuen tot specifiek gedrag moet worden gedwongen, kan dit machtsmechanisme als politiek-technologische constructie worden toegepast.[23]

Bentham was geobsedeerd door het gebruik van sociale controle om het gedrag van individuen te beïnvloeden en een effectieve handhaving van het strafrecht mogelijk te maken. Hij was eveneens een voorstander van het gebruik van alle mogelijke sancties en van alle mogelijke bronnen van overheidsmacht. Een vergaande aantasting van privacy en anonimiteit of zelfs de volledige vernietiging daarvan, was een prijs die hij bereid was te betalen. Om het mechanisme van sociale controle te verbeteren opperde hij onder andere de invoering van een verplichting voor alle burgers om hun naam op hun pols te laten tatoeëren.[24]

Het ideaal van de panoptische samenleving wordt door George Orwell beschreven als een angstvisioen. In zijn boek *1984* is de praktische uitwerking van het panoptische principe volledig geperfectioneerd. Een alomtegenwoordig 'telescreen' stuurt elk woord en elke gedraging direct door aan een alleswetende Thought Police:

> "Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being

22. De Hert 2003, p. 75-78.
23. Foucault 1989, p. 283-284.
24. De Hert 2003, p. 82-83.

> watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time."[25]

Identificatie en sociale controle, discipline en hiërarchisch toezicht, bewaking en permanente zichtbaarheid – het zijn alle begrippen die machtsuitoefening weerspiegelen. Waar machtsuitoefening geperfectioneerd moet worden om bepaalde maatschappelijke of politieke doelen te bereiken, zoals de bestrijding van de pest of het utilitarisme van Bentham, is uitbanning van anonimiteit een noodzakelijkheid. Geredeneerd vanuit het belang van de persoonlijke vrijheid in ruime zin is deze machtsuitoefening echter een bedreiging en een verschijnsel met een negatieve normatieve lading.

Het machtsprobleem tekent zich ook zeer duidelijk af in de context van klassieke grondrechten zoals de uitingsvrijheid, het kiesrecht en de vrijheid van vereniging, vergadering en betoging. Deze grondrechten hebben immers als doel overheidsmacht in te perken en de staatsvrije sfeer van het individu te beschermen. Zij kunnen in veel situaties niet ongehinderd worden uitgeoefend indien de mogelijkheid om anoniem te zijn, als 'filter' voor overheidsbemoeienis, ontbreekt. In de verhouding tussen overheid en burger heeft anonimiteit voor de laatste met andere woorden een belangrijke 'afweerfunctie' als schild tegen willekeur en machtsmisbruik. Op verschillende gebieden van het recht bestaan daarom tot de overheid gerichte verboden om te vragen naar de identiteit van burgers, verboden om bepaalde gegevens te registreren of rechten van de burger om zijn identiteit verborgen te houden.

Ik geef hier twee voorbeelden waaruit de functie van anonimiteit als schild tegen machtsuitoefening naar voren komt. Als eerste noem ik de beginselen van vrije en geheime stemming die tot uitdrukking zijn gebracht in artikel 53 lid 2 van de Grondwet en de Kieswet.[26] De geheime stemming houdt in dat niemand, in welke verhouding dan ook, verplicht kan worden te kennen te geven op wie hij heeft gestemd.[27] De wettelijke procedure voor de gang van zaken op het stembureau dient te waarborgen dat een stem kan worden uitgebracht zonder dat iemand anders daarvan kennis kan nemen. Artikel J 15 van de Kieswet bepaalt daarom dat het stemlokaal zodanig is ingericht dat het stemgeheim wordt beschermd. Hieruit kan bijvoorbeeld worden afgeleid dat een kiezer bij het uitbrengen van zijn stem niet mag worden vergezeld door een overheidsfunctionaris.[28] Zodoende wordt onder andere voorkomen dat de kiezer door middel van bedreigingen of beloningen zou kunnen worden beïnvloed.

Als tweede voorbeeld noem ik het verbod op de verwerking van 'bijzondere persoonsgegevens' in de Wet bescherming persoonsgegevens. Artikel 16 van deze wet verbiedt de

25. Orwell 1951, p. 6.
26. Wet van 28 september 1989 houdende nieuwe bepalingen inzake het kiesrecht en de verkiezingen, *Stb.* 1989, 423.
27. *Kamerstukken II* 1978/79, 14 233, nr. 6, p. 4-5.
28. In artikel J 28 Kieswet is een uitzondering gemaakt voor lichamelijk gehandicapten.

verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Ook de verwerking van strafrechtelijke persoonsgegevens is verboden. Het verbod dient in de eerste plaats de bescherming van de persoonlijke levenssfeer. Aan de bepaling ligt echter ook de gedachte ten grondslag dat men politieke grondrechten niet ongehinderd uit kan oefenen wanneer gegevens over godsdienst en levensovertuiging, politieke gezindheid en het lidmaatschap van een vakvereniging bij de overheid bekend zijn of op eenvoudige wijze verkregen kunnen worden. Daarnaast is beoogd discriminatie te voorkomen door verwerking van bepaalde categorieën van gegevens, met name die betreffende ras, gezondheid en het seksuele leven, te verbieden. Het verbod op gegevensverwerking is zodoende mede een uitwerking van het in artikel 1 Grondwet opgenomen non-discriminatie beginsel.

Wij begonnen deze paragraaf met de constatering dat anonimiteit leidt tot ontoerekenbaarheid. De betekenis van dat laatste begrip werd toegelicht aan de hand van de parabel van Gyges, die beschrijft hoe mensen zich zouden gedragen als zij onzichtbaar zouden kunnen zijn. Vervolgens werd vastgesteld dat ontoerekenbaarheid een dilemma creëert tussen individuele vrijheid en rechtshandhaving. Ten slotte werd de relatie tussen anonimiteit en macht zowel in brede zin als in de context van grondrechten met enkele voorbeelden nader geïllustreerd.

Betrekt men het bovenstaande op het communicatieproces, dan volgt daaruit een aantal zaken. In de eerste plaats gaat de vergelijking tussen anonimiteit en onzichtbaarheid ook op in de context van openbare communicatie. Een anonieme auteur is in overdrachtelijke zin onzichtbaar voor zijn lezerspubliek en voor instanties die toezicht willen uitoefenen op de inhoud van zijn geschrift. De uit anonimiteit voortvloeiende ontoerekenbaarheid houdt hier in dat een uiter niet verantwoordelijk gehouden kan worden voor de inhoud van zijn uiting of voor de gevolgen daarvan. Ook het dilemma tussen individuele vrijheid en rechtshandhaving manifesteert zich. De vrijheid van de auteur en andere actoren, zoals drukkers, uitgevers en andere tussenpersonen staat tegenover het maatschappelijke belang dat opruiende, beledigende en onrechtmatige uitingen kunnen worden tegengegaan.

De relatie tussen anonimiteit en machtsuitoefening komt bij openbare communicatie tot uitdrukking in het kat-en-muis-spel tussen de overheid als censor en de burger als uiter, zender en ontvanger van informatie. Uitbanning van anonimiteit is ook hier een middel om machtsuitoefening mogelijk te maken. Zoals in het hiernavolgende nog zal blijken hebben overheden altijd getracht om preventieve en repressieve controle op de inhoud van boeken en geschriften te ondersteunen door de anonieme publicatie en verspreiding daarvan strafbaar te stellen. Soms gingen de maatregelen om auteurs tot ondertekening te dwingen zo ver dat men in feite zou kunnen spreken van pogingen om een panoptische publieke sfeer te creëren, met dien verstande dat de suggestie van Bentham om iedere burger zijn naam op zijn pols te laten tatoeëren ten uitvoer werd gebracht voor geschriften. Auteurs trachtten zich op hun beurt aan toezicht op de inhoud te ontworste-

len door naamsvermelding achterwege te laten. Voor hen was anonimiteit een middel om zich tegen overheidsinmenging te wapenen.

Ook bij andere communicatiemiddelen dan de drukpers komt de verhouding tussen anonimiteit en macht telkens terug. In het vervolg van dit onderzoek zal nog uiteen worden gezet hoe digitalisering en de opkomst van elektronische gegevensverwerking het machtsprobleem in enigszins gewijzigde vorm opnieuw tot een actueel onderwerp maken: gegevensverwerking leidt tot kennis over (communicerende) burgers en deze kennis leidt op zijn beurt tot een machtspositie van de gegevensverwerker. Deze 'informatiemacht' ligt, voornamelijk als gevolg van de liberalisering van de telecommunicatiesector, meer dan vroeger bij private elektronische tussenpersonen. Zij verwerken op grote schaal gegevens over elektronisch communicatiegedrag, bijvoorbeeld via (mobiele) telefonie en het internet. Daarmee wordt niet alleen relevant aan welke normen de tussenpersoon zich bij de verwerking dient te houden en hoe de eindgebruiker in zijn verhouding met de tussenpersoon beschermd wordt, maar ook onder welke omstandigheden de tussenpersoon bevoegd is, of verplicht kan worden, om gegevens te verstrekken aan derde partijen. In het verlengde hiervan speelt de vraag hoe de machtspositie van de verwerker in het virtuele publieke domein wordt ingedamd met behulp van het recht op (informationele) privacy en de uitingsvrijheid.

1.4 Anonimiteit en opvattingen over individuele vrijheid

De samenhang tussen anonimiteit en persoonlijke vrijheid lijkt vanuit hedendaags perspectief vanzelfsprekend. Bekijkt men deze samenhang echter vanuit een historische invalshoek, dan blijkt het maatschappelijke oordeel over anonimiteit sterk afhankelijk te zijn van het in een samenleving geldende vrijheidsideaal. De 'klassieke' opvatting van vrijheid biedt aanmerkelijk minder steun voor bescherming van anonimiteit. Hoe dit komt, kan worden verduidelijkt aan de hand van het onderscheid dat de Zwitsers-Franse filosoof Benjamin Constant maakte tussen de 'liberté des anciens' en de 'liberté des modernes'.[29]

De liberté des anciens, het vrijheidsideaal van de oude Grieken en Romeinen, stelde de positie van de burger in de publieke sfeer centraal. Vrijheid bestond uit het direct en collectief uitoefenen van souvereiniteit en werd zodoende allereerst geassocieerd met burgerschap en een actieve deelname aan het publieke leven. Dit ideaal was volgens Constant direct te herleiden tot de sociale organisatie van de stadstaat. In deze kleinschalige samenleving was iedere burger bekleed met daadwerkelijke macht en direct betrokken bij collectieve beslissingen over publieke aangelegenheden, zoals het voeren van oorlog, de rechtspraak en het bestuur van de magistraten. Als gevolg hiervan ontstond een contrast

29. Constant besprak het verschil tussen de twee vrijheden in het jaar 1819 in een lezing met de titel 'De la Liberté des Anciens Comparée à celle des Modernes'. Deze lezing werd later ook als essay uitgegeven. Zie Constant 1980. Zie over de opvattingen van Constant ook De Hert 2003 en Holmes 1984.

tussen het publieke en het private, waar bij het eerste als positief en het laatste als negatief, als een bedreiging van het publieke, werd ervaren. Private handelingen waren onderworpen aan strikte controle. De private sfeer van de burger was zeer beperkt en zijn private belangen waren aan het publieke ondergeschikt. Individuele vrijheid en onafhankelijkheid in de moderne zin van het woord bestonden niet.

Tegenover het klassieke vrijheidsideaal plaatst Constant de 'liberté des modernes', de opvatting van individuele vrijheid zoals die sinds de Verlichting bestaat in de moderne westerse samenleving. Constant verklaart de opkomst van deze moderne opvatting door er op te wijzen dat de directe uitoefening van burgerlijke en politieke rechten, onder andere als gevolg van de toegenomen bevolkingsomvang, niet langer mogelijk is. Deze rechten zijn welhaast symbolisch geworden en geven minder voldoening. Het moderne individu is als gevolg hiervan meer verknocht aan de bescherming van zijn private sfeer en aan zijn onafhankelijkheid ten opzichte van het collectief. Het genot van de private sfeer wordt niet langer als iets negatiefs ervaren en evenmin als een bedreiging van het publieke.

Het onderscheid tussen de liberté des anciens en de liberté des modernes is ook wel verwoord als een tegenstelling tussen 'positieve' en 'negatieve' vrijheid. De Britse filosoof Isaiah Berlin werkte dit onderscheid verder uit, daarbij voortbouwend op het werk van Constant. Positieve vrijheid omschrijft hij als "not freedom from, but freedom to – to lead one prescribed form of life".[30] Deze vorm maakt deel uit van de politieke stroming van het republikanisme en correspondeert met het klassieke vrijheidsideaal. Van negatieve vrijheid is daarentegen sprake wanneer een individu kan handelen zonder daarbij door anderen te worden gehinderd.[31] Negatieve vrijheid omvat het recht van het individu op een staatsvrije sfeer en op bescherming tegen schending daarvan. Deze vorm maakt deel uit van de liberale politieke filosofie en wordt ondersteund door moderne grondrechten.[32]

Het is duidelijk dat de wens om anoniem te blijven vanuit beide benaderingen verschillend wordt beoordeeld. Het klassieke vrijheidsideaal biedt geen ruimte voor anonimiteit. In de publieke sfeer heeft de burger niets te verbergen en voorzover er een private sfeer bestaat is deze ondergeschikt aan het publieke belang. Wie anoniem wil zijn is dus per definitie verdacht. In de moderne visie heeft de burger echter wel aanspraak op bescherming van zijn private sfeer tegen het collectief. Anonimiteit kan een legitiem middel zijn om deze sfeer af te bakenen.

De Hert wijst erop dat het zuivere republikanistisch denken zijn invloed in de loop der tijd grotendeels heeft verloren.[33] De overgang naar een liberale visie op vrijheid gaat gepaard met een toename van het politieke en filosofische denken over anonimiteit.

30. Berlin 1969, p. 131.
31. Zie uitgebreider over negatieve vrijheid Berlin 1969, p. 122-131.
32. Berlin 1969, p. 165.
33. De Hert 2003, p. 53.

Constant stelde als eerste vast dat de klassieke nadruk op het onderscheid tussen het publieke en het private in de moderne samenleving aan betekenis had verloren. Volgens hem was de verwerping van het private en de daarmee gepaarde afkeuring van iedere vorm van anonimiteit achterhaald. Hij ontkende dan ook het conflict tussen de publieke en de private sfeer. De mogelijkheid tot het dragen van een masker was naar zijn oordeel niet een bedreiging van de publieke sfeer, maar een essentiële voorwaarde voor de ontwikkeling daarvan en voor de bescherming van vrijheid. Ook andere moderne denkers, zoals Arendt en Habermas, betogen dat het individu juist een private sfeer nodig heeft waarin hij zijn identiteit en zijn opvattingen kan ontwikkelen, alvorens aan het publieke leven deel te nemen.[34] In de literatuur over het internet als publieke sfeer gaat men nog een stap verder. Het republikeinse argument wordt hier als het ware omgedraaid door te stellen dat het publieke debat niet kan bestaan zonder anonimiteit.[35] Ook Berlin maakte de republikeinse nadruk op burgerschap en publieke participatie verdacht.[36]

Door de opkomst van het liberalisme is de waardering van de private sfeer toegenomen en kan ook de bescherming van het private een valide argument zijn om anoniem te blijven. Voor de grondrechtelijke analyse van anonimiteitsvraagstukken blijft het onderscheid tussen het publieke en het private echter van cruciaal belang. In de literatuur zijn verschillende analyses te vinden van deze tegenstelling, die wordt beschouwd als een 'grote dichotomie' in het Westerse denken.[37] Ik onderscheid hier drie relevante aspecten. In de eerste plaats is het publieke, zoals wij reeds zagen, sterk verweven met politieke participatie en burgerschap. Daarnaast kan dit predikaat verwijzen naar datgene wat openbaar is en toegankelijk voor iedereen. In die betekenis contrasteert het met zaken die worden gezegd en gedaan in beperkte kring of in het geheim. Ten slotte kan het publieke betrekking hebben op dat wat collectief is en op het collectieve belang van een groep individuen of van de samenleving als geheel. Daar tegenover staat dan dat wat behoort tot het individu respectievelijk het individuele belang.

Voor de mate van bescherming die onder de uitingsvrijheid aan anonieme uitingen moet worden toegekend is het zeer relevant in hoeverre de wens om zijn identiteit af te schermen ten goede komt aan het publieke. Een beroep op het collectieve belang van het vrije publieke debat is in het algemeen immers sterker dan een beroep op het private. Een romanschrijver die onder een pseudoniem publiceert om niet lastig gevallen te worden door zijn bewonderaars beschermt eigenlijk alleen zijn private belang. De auteur van een anoniem politiek pamflet over een maatschappelijk relevant onderwerp doet iets fundamenteel anders. Zijn anonimiteit is direct verbonden met elk van de drie genoemde aspecten van het publieke. Hij neemt als burger actief deel aan een openbare politieke

34. Idem, p. 72.
35. Idem, p. 73.
36. Idem, p. 54-55.
37. Bobbio 1989; Wientraub 1997; Blok 2002, p. 279-284 en p. 287-289.

discussie die betrekking heeft op een collectief belang. Anonimiteit ondersteunt deze verschillende aspecten doordat het de auteur beschermt tegen represailles.

1.5 Conclusie

In dit hoofdstuk werden allereerst drie verschillende betekenissen van anonimiteit behandeld. De meest enge betekenis was die van anonimiteit als naamloosheid. In een ruimere betekenis, zoals geformuleerd door Westin, kan het begrip verwijzen naar de notie van individuele privacy, het ontbreken van sociale controle en het gevrijwaard zijn van identificatie. Volgens de meest ruime en abstracte omschrijving wordt de kern van anonimiteit gevormd door de onidentificeerbaarheid van de anonieme persoon, welke bestaat uit de 'niet-herleidbaarheid' van persoonlijke eigenschappen. In dat verband kan men een onderscheid maken tussen absolute vormen van anonimiteit, waarbij identificatie van een verantwoordelijke persoon onmogelijk is en relatieve vormen, waarbij de tussenpersoon beschikt over identificerende informatie die de doorbreking van anonimiteit mogelijk maakt. De drie genoemde omschrijvingen van anonimiteit overlappen elkaar. Zij sluiten elkaar niet uit maar benadrukken slechts verschillende aspecten.

In het vervolg werd uiteengezet hoe de bescherming en doorbreking van anonimiteit gerelateerd is aan machtsuitoefening en hoe dit verband zich manifesteert in het communicatieproces. Vanuit constitutioneel oogpunt is de functie van anonimiteit als middel om individuele vrijheid te beschermen van bijzonder belang. Doordat het individu zich kan onttrekken aan machtsuitoefening kan hij zowel in feitelijke als in juridische zin niet langer verantwoordelijk worden gehouden voor zijn gedrag. Hoewel de hieruit voortvloeiende ontoerekenbaarheid onmiskenbaar negatieve effecten heeft, moet worden geconstateerd dat een zekere mate van anonimiteit in een democratische samenleving ook waardevolle kanten heeft omdat het de ongehinderde uitoefening van constitutionele rechten stimuleert.

Tot slot bespraken wij de historische ontwikkeling van het denken over individuele vrijheid. Daarbij kwam een verband aan het licht tussen opvattingen over de publieke sfeer en de bescherming van anonimiteit. De moderne liberale visie op vrijheid bleek anonimiteit in hogere mate te ondersteunen dan de klassieke benadering. Hoewel de tegenstelling tussen de private en de publieke sfeer daar is verdwenen, dient nog steeds een onderscheid te worden gemaakt tussen anonimiteit als waarborg voor het private en anonimiteit als voorwaarde voor de uitoefening van publieke vrijheden. Op het laatste aspect wordt in het volgende hoofdstuk nader ingegaan.

2 Anonimiteit en het publieke debat

2.1 Inleiding

Een democratie kan niet functioneren zonder een vrije en voor iedereen toegankelijke discussie over politieke en maatschappelijke aangelegenheden. Aan het democratische systeem ligt immers het idee ten grondslag dat na een uitwisseling van meningen uiteindelijk een meerderheidsstandpunt kan worden bereikt. De stimulering van het 'publieke debat' wordt in de westerse wereld daarom algemeen beschouwd als een zwaarwegend maatschappelijk belang en als een sterk argument voor een ruime uitingsvrijheid. In het vervolg van dit onderzoek zal blijken dat het belang van het publieke debat, zowel in de Verenigde Staten als in Nederland, telkens terugkomt als argument voor de bescherming van anonieme uitingen. In dit hoofdstuk wordt daarom, voorafgaand aan de bespreking van het Amerikaanse en het Nederlandse recht, op dit onderwerp afzonderlijk ingegaan. Het is de bedoeling de betekenis en de functie van anonimiteit in de democratische discussie en in het publieke debat te analyseren. Meer in het bijzonder zal worden getracht de positieve en negatieve effecten van anonimiteit in kaart te brengen.

2.2 Discussie als democratisch beginsel

In de zeventiende en de achttiende eeuw werden de beginselen van de moderne representatieve democratie voor het eerst geformuleerd en in de praktijk gebracht. Het meest bepalende element van dit politieke systeem was de gekozen volksvertegenwoordiging en haar taak om te vergaderen. Politieke discussie werd hierdoor eveneens een centraal element. Manin noemt 'trial by discussion' als een van de vier centrale principes van de representatieve democratie. Dit principe houdt in dat geen enkel voorstel de kracht van een publieke beslissing kan verkrijgen, tenzij het de steun van de meerderheid heeft gekregen na onderwerp te zijn geweest van discussie.[1] Manin constateert dat de notie van politieke discussie lange tijd vrij ongrijpbaar bleef. Voor de vraag hoe die discussie precies gevoerd moest worden was niet veel aandacht.[2] Politieke discussie werd aanvankelijk slechts beschouwd als middel voor het bereiken van overeenstemming in het parlement en als een manier om te bepalen wat de meerderheid van het volk wilde. Omdat de func-

1. De andere drie principes zijn: 'election of representatives at regular intervals', 'the partial independence of representatives' en 'freedom of public opinion'. Manin 1997, p. 197-198.
2. Manin 1997, p. 184.

tie van discussie adequaat te kunnen beschrijven formuleert Manin zelf een ideaaltypische definitie binnen de context van politieke besluitvorming:

> "a type of communication in which at least one of the party (a) seeks to bring about a change in the other party's position, and (b) does so using propositions that are impersonal or relate to the long-term future".

Het element van overreding (persuasion) onderscheidt politieke discussie van andere vormen van verbale communicatie.[3] Het tweede kenmerk (the use of impersonal or long-term propositions) correspondeert met het rationele, argumentatieve. Dit kenmerk onderscheidt politieke discussie van politieke koehandel, waarbij men anderen probeert over te halen door geld, goederen of gunsten aan te bieden.

Rationaliteit speelt ook in latere theorieën over het voeren van discussies een belangrijke rol. Invloedrijk is het werk van Habermas over de publieke sfeer en het publieke debat.[4] Hierin beschrijft hij het publieke debat als historisch-sociologisch verschijnsel. De belangrijkste periode in de ontwikkeling van de publieke sfeer is volgens Habermas de achttiende eeuw. Habermas beschrijft hoe burgers uit verschillende sociale lagen van de bevolking in salons en koffiehuizen bijeen kwamen om te discussiëren. De bijeenkomsten hadden een open karakter en de discussies kenmerkten zich, in de geest van de Verlichting, door rationaliteit. Burgers waren vrij om op een open wijze, zonder interventie van de staat, met medeburgers van gedachten te wisselen over problemen van maatschappelijk belang. Deze discussie, gericht op pragmatische consensus en gezuiverd van vooringenomenheid en eigenbelang, zou een belangrijke bijdrage leveren aan de democratie en het democratisch bewustzijn.

De publieke sfeer van de achttiende eeuw vormt de basis van het ideaalbeeld dat uit het denken van Habermas naar voren komt: een vrije en voor iedereen toegankelijke discussie over publieke aangelegenheden. In deze ideaaltypische discussie wordt op basis van rationele argumenten en op communicatieve wijze een consensus bereikt. Om de discussie op de gewenste manier te laten verlopen dient aan een aantal voorwaarden te zijn voldaan: de deelnemers zijn rationeel, zij zijn gericht op wederzijds begrip in plaats van op hun eigen belang en zij nemen op een gelijkwaardige basis deel. Het debat is gediend bij de afwezigheid van economische en politieke machtsuitoefening.

Om de door Habermas nagestreefde 'ideale gesprekssituatie' te bereiken, dienen de deelnemers aan de discussie gemeenschappelijke ideeën hebben over de manier waarop wordt gecommuniceerd. Om dit mogelijk te maken stelt Habermas een aantal 'etiquetteregels' op, ook wel bekend als de 'discourse ethics'. Hij onderscheidt regels op drie

3. Idem, p. 197-198.
4. Habermas 1989.

niveaus. De eerste twee niveaus omvatten logische regels die noodzakelijk zijn voor het goede verloop van een discussie:

"1.1) No speaker may contradict himself;
1.2) Every speaker who applies predicate F to object A must be prepared to apply F to all other objects resembling A in all relevant aspects;
1.3) Different speakers may not use the same expression with different meanings.

2.1) Every speaker may assert only what he really believes;
2.2) A person who disputes a proposition or norm not under discussion must provide a reason for wanting to do so."

Kort gezegd komen deze regels er op neer dat sprekers zich zelf niet tegen mogen spreken en dat zij oprecht en consequent moeten zijn. Als iedereen zich aan deze regels houdt, zal de discussie zonder fricties verlopen en het meest productief zijn.[5] In het derde niveau komt de 'ethiek' van de discourse ethics naar voren. Pas wanneer ook deze regels in acht worden genomen, kan het debat echt democratisch worden genoemd en levert het een constructieve bijdrage aan de democratische besluitvorming:

"3.1) Every subject with the competence to speak and act is allowed to take part in a discourse;
3.2) A) Everyone is allowed to question any assertion whatever;
B) Everyone is allowed to introduce any assertion whatever into the discourse;
C) Everyone is allowed to express his attitudes, desires and needs;
3.3) No speaker may be prevented, by internal or external coercion, from exercising his rights as laid down in (3.1) and (3.2)."[6]

Het werk van Habermas bevat geen nadere uitgewerkte denkbeelden of opmerkingen over de rol van anonimiteit. Op basis van de discourse ethics kan men hierover echter wel het een en ander zeggen. Enerzijds lijkt anonieme deelname strijdig met de door Habermas geformuleerde voorwaarden omdat het een bedreiging vormt voor het open karakter van de ideale gesprekssituatie. Onbekendheid met de identiteit van de spreker geeft andere deelnemers minder zicht op zijn motieven, leidt tot minder toerekenbaarheid en maakt machtsverhoudingen minder doorzichtig. Anonimiteit maakt de discussie kortom minder transparant. Anderzijds zou men, gezien regel 3.1 en 3.3, kunnen stellen dat anonimiteit de toegankelijkheid van het debat verhoogt. Men zou de eis om zijn identiteit bekend te maken kunnen zien als een vorm van 'internal or external coercion' in de zin van regel 3.3. Daarnaast valt te betogen dat veronderstellingen, argumenten en behoeftes van de spreker objectiever worden ontvangen wanneer zij alleen op hun inhoud kunnen worden beoordeeld.

5. Habermas 1990, p. 84.
6. Idem, p. 84.

In de modernere politieke theorie bestaat sinds de jaren tachtig en negentig van de twintigste eeuw opnieuw veel aandacht voor de plaats van discussie binnen de moderne samenleving als middel voor het oplossen van morele conflicten. Ontevredenheid met de alledaagse praktijk van de liberale democratie heeft geleid tot nieuwe theorieën, die doorgaans worden geschaard onder de noemer 'deliberative democracy'.[7] De voorstanders van dit concept wensen terug te keren naar het oorspronkelijke democratische ideaal van een overheid als belichaming van de wil van het volk. Openbare gedachtenwisseling tussen vrije en gelijke burgers is volgens hen de kern van legitieme politieke besluitvorming. De politicologen Fennema en Maussen onderscheiden een aantal democratische principes die bij het voeren van discussie leidinggevend dienen te zijn. Zij baseren zich onder andere op het werk van de Amerikaanse politicologen Gutmann en Thompson.[8] Allereerst dienen burgers in de publieke sfeer te worden beschouwd als *moreel gelijkwaardig* en dienen alle belangen en meningen bij het publieke besluitvormingsproces op basis van gelijkheid te worden meegewogen. Zodoende wordt voldaan aan twee kenmerken van democratie: *equality* en *inclusion*. In de tweede plaats dienen maatschappelijke conflicten, voortvloeiende uit verschillen in morele standpunten, belangen of meningen *openbaar* (public) te zijn. Dit kan bijdragen aan een vreedzame oplossing van conflicten en maakt diversiteit en oppositie mogelijk. Op lange termijn versterkt dit het democratische systeem. Vanuit dit perspectief beïnvloedt een taboe op bepaalde onderwerpen of standpunten de discussie negatief. Tenslotte onderscheidt men het principe dat deelnemers aan een discussie *verantwoording* moeten afleggen, ook wel aangeduid als *democratic accountability*. Dit principe speelt allereerst een rol bij 'public deliberation', dat wil zeggen: binnen organen waar collectieve beslissingen worden genomen. Het gaat hier om toerekenbaarheid van politieke actoren in het democratische, procedurele besluitvormingsproces: de volksvertegenwoordiger heeft van de kiezer een politiek mandaat gekregen om zijn belangen te vertegenwoordigen en politieke beslissingen te nemen en moet zich dus verantwoorden. Ook bij 'public discussion' in ruimere zin speelt dit principe een rol. Deelnemers moeten ten opzichte van elkaar openheid betrachten en inzicht geven in hun motieven.

Op basis van de genoemde principes formuleren Fennema en Maussen, evenals Habermas, een aantal regels voor het debat. Zij maken een onderscheid tussen juridisch afdwingbare toegangsregels en suggestieve gedragsregels of 'deliberatieregels'.[9] In die laatste categorie is voor het vraagstuk van de anonimiteit met name de regel van *wederzijds respect* van belang. Fennema werkt deze 'gouden' deliberatieregel verder uit:

> "Wederzijds respect heeft te maken met de erkenning van de integriteit en intellectuele autonomie van politieke tegenstanders. Wederzijds respect vereist van de deelnemers aan het publieke debat dat

7. Bohman 1998.
8. Fennema & Maussen 2000, p. 379.
9. Fennema & Maussen 2000, p. 382-383.

> zij elkaar als discussiepartner accepteren. Dat betekent dat iedereen moet proberen opinies zo te formuleren dat zij voor anderen begrijpelijk en optimaal aanvaardbaar zijn, en al doende zoekt naar een gemeenschappelijke grondslag voor debat."[10]

Het voorschrift dat deelnemers aan een discussie respect voor elkaar moeten hebben is bedoeld om de 'horizontale loyaliteit' van deelnemers te optimaliseren.[11] Daarnaast dient het om een scheiding van het private en het publieke domein tot stand te brengen. De persoonlijke levenssfeer van burgers dient buiten het publieke domein te worden gehouden. In de publieke ruimte respecteert men de ander door hem op afstand te houden. Het publieke domein veronderstelt een sociale afstand tussen de deelnemers die voorkomt dat de druk om zich aan de gemeenschappelijke identiteit te conformeren te groot wordt. Daar "hoort iedereen maskers te dragen en rollen te spelen die relatief losstaan van de identiteiten die de persoonlijke levenssfeer bepalen", aldus Fennema.[12] Hij verwijst hier naar het werk van Richard Sennett over het publieke domein. Sennett stelt dat beleefdheid en voorkomendheid, door hem aangeduid als 'civility', van oudsher zijn verbonden met de verplichtingen voortvloeiend uit burgerschap. In het openbare leven creëert civility de door Fennema bedoelde sociale afstand:

> "(…) it is the activity which protects people from each other and yet allows them to enjoy each other's company. Wearing a mask is the essence of civility. Masks permit pure sociability, detached from the circumstances of power, malaise, and private feeling of those who wear them. Civility has as its aim the shielding of others form being burdened with oneself. (…) Civility is treating others as though they were strangers and forging a social bond upon that social distance."[13]

Uit de eis van wederzijds respect vloeit als tweede gedragsregel voort dat men de motieven van de tegenstander moet respecteren. In een democratisch debat moet iedereen er van uit (kunnen) gaan dat de ander oprecht meent wat hij zegt. Complottheorieën of de veronderstelling dat de tegenstander een dubbele agenda heeft, hebben op het verloop van het debat een desastreus effect.

Confronteert men de anonieme uiting met de hierboven genoemde principes en gedragsregels, dan lijkt daaruit een aantal zaken te volgen. Een sterk argument voor het toelaten danwel bevorderen van anonieme uitingen is de omstandigheid dat hiermee tegemoet kan worden gekomen aan de principes van *equality* en *inclusion* en aan het vereiste dat meningen en belangen zoveel mogelijk openbaar zijn. Anonimiteit verlaagt toegangsdrempels tot het debat en maakt het onmogelijk te discrimineren op basis van per-

10. Fennema 2003, p. 33.
11. De tweede regel gouden regel, het afleggen van verantwoording, betreft de verhouding tussen politieke vertegenwoordigers en de achterban en optimaliseert de 'verticale loyaliteit'. In een democratisch debat dienen met name politieke elites zich aan deze tweede gouden regel te houden. Zie Fennema 2003, p. 32.
12. Fennema 2003, p. 34.
13. Sennett 1977, p. 264.

soonlijke eigenschappen. Men kan daarnaast betogen dat anonieme deelname onder omstandigheden de gewenste 'sociale afstand' tot stand brengt. Daar staat tegenover dat anonimiteit het moeilijker maakt om de motieven van de tegenstander te respecteren. Al snel kan immers de indruk ontstaan dat men voor anonimiteit heeft gekozen om bepaalde motieven of belangen te verhullen. De eis van wederzijds respect is eveneens problematisch. Deze eis betreft in de eerste plaats de formulering van het standpunt maar zou ook meer in zijn algemeenheid kunnen worden toegepast op het zich al dan niet anoniem presenteren. In sommige gevallen zal het prijsgeven van zijn identiteit een persoonlijk standpunt voor anderen eerder optimaal aanvaardbaar maken. Maar dit is lang niet altijd het geval. Daarnaast is het moeilijker de motieven van de tegenstander te respecteren wanneer deze motieven niet of in mindere mate kenbaar zijn. Anonimiteit kan het vertrouwen dat de ander oprecht is op het spel zetten en de beschuldiging dat iemand een dubbele agenda heeft in de hand werken.

2.3 Het publieke debat als grondslag voor een ruime uitingsvrijheid

Het juridische domein kent zijn eigen theorieën over het publieke debat. Met name in de Amerikaanse jurisprudentie over de bescherming en afbakening van de uitingsvrijheid is aan dit belang veel aandacht besteed. Justice Holmes, rechter bij het Supreme Court, introduceerde in *Abrams* v. *United States* de bekende metafoor van de 'marketplace of ideas':

> "When men have realized that time has upset many fighting faiths, they may come to believe (…) that the ultimate good desired is better reached by a free trade in ideas – that the best test of truth is the power of the thought to get itself accepted in the competition of the market (…)"[14]

De marketplace of ideas werd geboren uit een huwelijk tussen het rationalistische vooruitgangsgeloof van de Verlichting en de economische laissez faire-theorie. De gedachte is dat een ruime uitingsvrijheid voor het individu via het publieke debat leidt tot een democratische discussie over maatschappelijke belangen en tot maatschappelijke vooruitgang. Er zijn optimistische en sceptische varianten van de marketplace-gedachte. Optimisten zien uit de concurrentie van meningen en ideeën op een ongereguleerde 'markt' van uitingen door toedoen van 'een onzichtbare hand' als vanzelf de waarheid naar voren komen.[15] Deze verwachting getuigt van een zeer groot vertrouwen in het zelfregulerende karakter van het maatschappelijk communicatieproces en lijkt te zijn gebaseerd op het geloof dat het goede het kwade uiteindelijk zal overwinnen.[16] Veelgehoorde

14. *Abrams* v. *United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).
15. Zie over de verschillende varianten van de marketplace of ideas Nieuwenhuis 1997, p. 20-25; De Meij e.a. 2000, p. 32 en 33.
16. "The marketplace metaphor appeals to our optimism that good will finally conquer evil. (…) Our hope that truth will prevail should be combined with pragmatic measures to give it its best fighting chance." Smolla 1992, p. 7.

kritiek is dan ook dat de marketplace of ideas, evenals de theorie van de zuivere mededinging, weinig realistisch is. Het economische laissez faire-denken leidt in zijn meest zuivere vorm vaak tot maatschappelijk ongewenste resultaten zoals scheefgroeiende machtsverhoudingen en sociaal onrecht.[17] Overheden moeten daarom ingrijpen in de economische werkelijkheid. Ook op de markt van meningen bestaan grote machtsongelijkheden. Sceptici gaan er bovendien van uit dat een objectieve waarheid niet bestaat en dat overeenstemming lang niet altijd bereikt kan worden. Zij hebben dan ook geen hooggespannen verwachtingen van de uitkomsten die het debat zal hebben, maar benadrukken de intrinsieke waarde van het debat zelf. Justice Holmes moet worden gerekend tot de gematigde stroming:

> "For him the benefit of the marketplace was not the end but the quest, not the marketplace's capacity to arrive at final and ultimate truth but rather the integrity of the process."[18]

In de jurisprudentie van het Supreme Court komt het belang van het publieke debat naar voren doordat aan 'public speech' een hogere bescherming wordt toegekend dan aan 'private speech'. Beperkingen op public speech worden middels een 'strict scrutiny test' onderworpen aan extra kritisch onderzoek. Zij kunnen slechts worden gerechtvaardigd door een 'substantial state interest'.[19] Wanneer in de media kritiek wordt geuit op 'public officials', kan smaad bovendien alleen worden aangetoond als sprake is van 'actual malice'. Ook het Europese Hof voor de Rechten van de Mens kent bijzondere bescherming toe aan het publieke debat. Het Hof heeft zich daarbij door de Amerikaanse benadering laten beïnvloeden.[20] De bescherming van artikel 10 lid 2 EVRM is blijkens vaste jurisprudentie niet alleen toepasselijk op informatie en ideeën die gunstig worden ontvangen of die als onschadelijk worden beschouwd, maar ook op "those that offend, shock or disturb the State or any sector of the population". Dit vloeit voort uit de eisen van pluralisme, tolerantie en ruimdenkendheid, zonder welke een democratische samenleving niet kan bestaan.[21] Lidstaten hebben een 'margin of appreciation' bij het vaststellen of sprake is van een 'pressing social need'. De ruimte voor een eigen afweging is echter minder groot wanneer sprake is van een 'political speech or debate on questions of public

17. "The marketplace image is grounded in laissez-faire economic theory. Even if we are to accept the apparent lesson of *perestroika* that on the whole, free economic markets perform more efficiently than controlled economies, almost all governments utilize some controls on markets to correct for excesses an imperfections that lead to violent economic swings. (…) The marketplace does not seem to produce truth, not at least with any consistency, and so we are left with the nagging suspicion that good ideas have precious little capacity to drive out bad ones." Smolla 1992, p. 6.
18. Smolla 1992, p. 8.
19. *New York Times Co.* v. *Sullivan* 376 US 254 (1964).
20. Peters 2003.
21. EHRM 7 december 1976, *NJ* 1987, 236 (*Handyside*).

interest'.[22] Dan kan het Hof de door partijen naar voren gebrachte argumenten volledig toetsen.

Ook bij de beantwoording van de vraag of beperkingen kunnen worden aangemerkt als 'necessary in a democratic society', zoals vereist door artikel 10 lid 2 EVRM, worden belemmeringen van het publieke debat extra kritisch beschouwd.[23] De media kunnen rekenen op extra bescherming omdat zij als 'public watchdog' een essentiële rol vervullen bij het informeren van het publiek.[24] Een ruime persvrijheid verzekert dat burgers kennis kunnen nemen en een oordeel kunnen vormen over de ideeën en standpunten van politieke leiders. De grenzen van acceptabele kritiek zijn ook in de Europese rechtspraak ruimer wanneer het een politicus betreft. Kritiek op de regering komt de meeste bescherming toe. In een democratisch systeem moet haar doen en laten aan nauwkeurig onderzoek kunnen worden onderworpen, niet alleen door de rechterlijke en de wetgevende macht, maar ook door de media en de publieke opinie.[25]

Bij de totstandkoming van de constitutionele bescherming voor anonieme uitingen in de Amerikaanse rechtspraak heeft de marketplace-gedachte een belangrijke rol gespeeld. Dit blijkt onder andere in *McIntyre* v. *Ohio* en *ACLU* v. *Reno* (zie par. 3.4 en 3.5). In de rechtspraak van het Europese Hof is de relatie tussen anonimiteit en het publieke debat daarentegen nooit diepgaand behandeld. In *Goodwin* werd weliswaar bescherming toegekend aan het recht van de journalist om de anonimiteit van zijn bronnen te beschermen, maar in deze uitspraak is geen algemene beschouwing te vinden over de positieve en negatieve effecten van anonimiteit bij de verspreiding van informatie. Het journalistieke verschoningsrecht werd meer in zijn algemeenheid gebaseerd op de rol van de media in de democratische samenleving (zie par. 6.4).

22. Zie onder andere EHRM 25 augustus 1998 (*Hertel*) *Mediaforum* 1998-10, p. 290-297 (m. nt. J.J.C. Kabel), overweging 47; EHRM 25 maart 1985 (*Barthold*) overweging 58; EHRM 28 september 2001 (*VGT Verein gegen Tierfabriken* v. *Switzerland*), overweging 57, 70 en 71. Volgens Nieuwenhuis kunnen alle uitlatingen die vanwege hun verband met het publieke debat in de jurisprudentie van het Europese Hof extra bescherming krijgen, onder deze noemer worden gebracht. Zie Hins & Nieuwenhuis 2003, p. 259 e.v.
23. EHRM 10 juli 2003, *Mediaforum* 2003 (10), p. 332 (*Murphy* v. *Ireland*), overweging 67. Artikel 10 lid 2 EVRM betreft beperkingen op de uitingsvrijheid. Dit artikellid luidt: "Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen."
24. EHRM 26 april 1979, *NJ* 1980, 146 (*Sunday Times*); EHRM 27 maart 1996, *NJ* 1996, 577 (*Goodwin*). Zie ook par. 6.4.
25. EHRM 23 april 1992, *NJ* 1994, 102 (*Castells*), overweging 46.

Indien het Europese Hof in de toekomst een oordeel moet vellen over identificatieverplichtingen of verboden op anonimiteit bij het ontvangen of verspreiden van inlichtingen en denkbeelden, dan zou hij deze kunnen aanmerken als 'formaliteiten, voorwaarden, beperkingen of sancties' in de zin van het artikel 10 lid 2 EVRM. Dergelijke verplichtingen of verboden zouden dan aan de in dat lid gestelde voorwaarden moeten voldoen. De eis dat beperkingen in een *democratische* samenleving noodzakelijk zijn voor de bescherming van de daar genoemde belangen en het grote gewicht van het publieke debat in de jurisprudentie van het Europese Hof zou kunnen leiden tot de conclusie dat te ruime of te vaag geformuleerde verboden of verplichtingen in strijd komen met de uitingsvrijheid.

2.4 Anonimiteit en publiek debat in de digitale omgeving

De komst van elektronische communicatiemiddelen confronteert juristen en politicologen met nieuwe vragen. Verloopt het publieke debat in de digitale omgeving op dezelfde wijze als offline of is de dynamiek hier, als gevolg van de architectuur van elektronische media, fundamenteel anders? Wat is online het effect van anonimiteit op de participanten aan de discussie? Voldoen de gevestigde ideeën over het publieke debat online nog wel?

Het antwoord op bovengenoemde vragen hangt sterk samen met vooronderstellingen over de aard van nieuwe communicatiemedia. Theorieën over de dynamiek van het virtuele publieke debat zijn vaak gebaseerd op aannames omtrent de mate waarin moderne communicatietechnieken gereguleerd kunnen worden. In literatuur en rechtspraak vindt men verschillende opvattingen. Zo brengt de typering van het internet als een 'information superhighway' het idee tot uitdrukking dat het internet als communicatiemedium zeer geschikt is voor overheidsbemoeienis en regulering en dat deze technologie slechts in beperkte mate afwijkt van de klassieke technologieën.[26] In deze benadering lijkt een virtuele publieke sfeer weinig nieuwe vragen op te roepen. De metafoor van het internet als 'Cyberspace' daarentegen, verwerpt vergelijkingen met post en telefonie en benadrukt de anarchistische notie van het internet als een fysiek onbegrensde ruimte waarin territoriale machthebbers geen gezag meer hebben. De architectuur van het internet zou Cyberspace immuun maken voor traditionele overheidsbemoeienis. Er is zelfs betoogd dat regulering geheel zou moeten worden overgelaten aan haar virtuele bewoners.[27] Ook het chaotische karakter van internetcommunicatie zou aan regulering in de weg staan, althans vragen om een andere benadering. Op het internet is de omloopsnelheid van

26. Deze vergelijking werd begin jaren negentig geïntroduceerd door de Amerikaanse regering. Die plaatste de stimulering van het internet als een overheidsproject op de politieke agenda. De Nederlandse wetgever nam de vergelijking over in de nota 'Wetgeving voor de Elektronische Snelweg', waarin onder andere het 'online-offline adagium' werd gepresenteerd: wat offline geldt dient ook online te gelden. *Kamerstukken II* 1997/98, 25 880, nrs. 1-2.
27. Blavin & Cohen 2002.

informatie hoog en het onmiddellijke en informele karakter van online discussiefora brengt waarden als nauwkeurigheid en waarheidsgetrouwheid in de verdrukking.

Iedere nieuwe communicatietechnologie voedt de hoop op democratisering.[28] Velen zien in het internet dan ook de belofte van een machtsvrije publieke sfeer waarin democratische idealen volledig tot hun recht komen. Ook hier speelt de architectuur van het internet een belangrijke rol. Het idee is dat het internet machtsconcentraties onmogelijk maakt en dat dit medium laagdrempelige toegangsmogelijkheden biedt tot maximale en gelijkwaardige participatie.[29] Waar het publieke debat offline wordt gedomineerd door een relatief klein aantal mensen en de meeste burgers nog van betekenisvolle deelname zijn uitgesloten, zou het internet ongelijkheden tussen burgers wegnemen en het debat meer toegankelijk maken. Het feit dat het internet ruime mogelijkheden biedt tot anoniem handelen is daarbij een belangrijke factor. Een ander aspect van deze optimistische visie is de verwachting dat ook de kwaliteit van het politieke debat en de democratische besluitvorming kunnen worden vergroot. Elektronische communicatie tussen overheid en burger zou de afspiegeling van belangen binnen de representatieve democratie ten goede komen. Pessimisten menen daarentegen dat al te directe vormen van democratie burgers doen bezwijken onder een informatieovervloed en dat zij achter hun computers vluchtige en onbezonnen keuzes maken over toevallige issues en incidenten. Bovens trekt de voorlopige conclusie dat het gebruik van internet vooralsnog niet lijkt te leiden tot een verbreding van de politieke participatie. Het internet lijkt juist bestaande patronen te bestendigen. Deelnemers aan digitale debatten zijn dezelfde hoogopgeleide middelbare mannen die ook al langs andere kanalen politiek actief waren. Aan dit 'digitaal onderonsje' wordt door nieuwe groepen volgens Bovens nauwelijks deelgenomen.[30]

Wetenschappelijke onderzoeken waarin specifiek wordt ingegaan op de effecten van anonimiteit op het kritisch-rationele karakter van online deliberatie zijn schaars. Zij leveren bovendien geen duidelijk beeld op. Stromer-Galley concludeert dat de negatieve effecten van anonimiteit worden gecompenseerd door de ruimere mogelijkheden tot deelname.[31] Zij constateert dat politieke discussie voor veel mensen in het algemeen een oncomfortabele aangelegenheid is omdat het meningsverschillen oproept. Deze meningsverschillen verstoren het geheel van beleefdheidsnormen die het sociaal verkeer tussen onbekenden reguleren. Politieke conversatie onthult bovendien zeer persoonlijke overtuigingen die in het verkeer tussen onbekenden gewoonlijk niet naar voren worden gebracht. Online worden deze sociale belemmeringen gedeeltelijk weggenomen. Door het tekstuele karakter van de communicatie vallen subtiele sociale signalen waarmee men

28. Dahlberg 2000, p. 31.
29. Deze visie komt duidelijk naar voren in de zaak *ACLU* v. *Reno* (zie par. 3.5). De rechter paste hier het marketplace model toe in een zaak over de regulering van pornografie op het internet. *Reno* v. *American Civil Liberties Union*, 521 U.S. 844 (1997). Zie Asscher 2002, p. 189.
30. Bovens 2003, p. 30-35.
31. Stromer-Galley 2002.

elkaars reacties kan peilen gedeeltelijk weg. In de discussie heeft men daardoor een groter gevoel van anonimiteit, onpersoonlijkheid en sociale afstandelijkheid.[32] Dit maakt het makkelijker om voor de ware mening uit te komen. Dahlberg komt tot een andere conclusie. Hij heeft op basis van Habermas' discourse ethics voorwaarden geformuleerd op basis waarvan uitspraken kunnen worden gedaan over het rationeel-kritische karakter van online discussie.[33] Zijn analyse van anonimiteit schenkt met name aandacht aan de reeds genoemd voorwaarden van *sincerity*, *discursive inclusion* en *equality*:

> "For a position to be rationally judged within deliberation, participants must make a sincere effort to make known all relevant information and their true intentions, interests, needs, and desires. Intentionally misleading others about aspects of one's identity relevant to the discourse, or falsifying information about one's claims, undermines the process of reaching understanding. It is important to carefully examine the extent to which such falsification may be a threat to rational deliberation in cyberspace, particularly given the degree of control over the presentation of self and information made possible by CMC" [Computer-Mediated Communication, AE].[34]

Dahlberg waardeert anonimiteit negatief vanwege de moeilijkheid om beweringen en identiteitsaanspraken te verifiëren. De mogelijkheid om een andere identiteit aan te nemen stelt deelnemers in staat anderen te misleiden over hun werkelijke motieven. Dergelijk 'bedrog' belemmert zijns inziens een rationele discussie en moet daarom zoveel mogelijk worden tegengegaan, bijvoorbeeld door middel van 'netiquette' en forum management.[35]

2.5 Conclusie

De genoemde visies op het publieke debat zijn niet geheel eenduidig en bovendien vatbaar voor kritiek. Het maatschappelijk belang van het publieke debat wordt echter breed onderschreven. In grote lijnen kan men een aantal voor- en nadelen van anonimiteit onderscheiden. Mijns inziens kan anonimiteit op twee manieren een belangrijke positieve bijdrage leveren. In de eerste plaats is er een *kwantitatief* voordeel. Door de afwezigheid van identificatie en sociale controle zullen meer mensen hun stem laten horen. Deelnemers worden niet gehinderd door het idee dat zij na het uiten van hun mening lastig gevallen zouden kunnen worden door overheden of instanties die niet gesteld zijn op kritiek. Wanneer men denkt vanuit een economisch perspectief kan men het blokkeren van identificatieverplichtingen beschouwen als het wegnemen van een toetredingsbelemmering tot de markt van meningen. Beschouwt men het vraagstuk vanuit de discours ethics van Habermas of aan de hand van de deliberatieregels van Fennema en Maussen, dan komt men uit op dezelfde constatering.

32. Idem, p. 134-142.
33. Dahlberg 2000, p. 56 e.v.
34. Idem, p. 192.
35. Idem, p. 204.

Het tweede voordeel is *kwalitatief*: bij onbekendheid van de spreker kan een argument alleen op zijn inhoud worden beoordeeld. De persoonlijke eigenschappen van de afzender, zoals geslacht, nationaliteit, leeftijd, of etnische en religieuze achtergrond zijn niet bekend en kunnen dus ook geen rol spelen bij de beoordeling van de boodschap. Anonimiteit is in die zin een schild tegen discriminatie. Een mening zal alleen op basis van rationele argumenten worden beoordeeld. Dit brengt de ideale gesprekssituatie dichterbij. Wie niet geremd wordt door de angst voor represailles zal daarnaast eerder geneigd zijn tot het ongegeneerd naar buiten brengen van zijn mening. Hierdoor zal in de discussie een grotere verscheidenheid aan meningen en belangen aan bod komen. Aanhangers van de marketplace-gedachte zullen dit toejuichen. Als het achterhalen van de waarheid door middel van de vrije concurrentie van ideeën het enige doel is, is iedere mening immers welkom, hoe extreem of kwetsend ook.

Er zijn echter ook negatieve consequenties. Wie het accent legt op de toerekenbaarheid van uitingen zal er op wijzen dat anonieme uitspraken kunnen leiden tot vervuiling van het debat. Wanneer er geen sanctie staat op het ventileren van meningen die maatschappelijk onacceptabel zijn, zullen ook verwerpelijke of krenkende ideeën doordringen in de discussie. Het aanmoedigen van een brede publieke discussie zonder verantwoording als remmende factor kan leiden tot de waarheid maar ook tot een toren van Babel. Anonimiteit leidt met andere woorden tot oncontroleerbaarheid van het communicatieproces.

Tegen de stelling dat anonimiteit de kwaliteit van het debat zou bevorderen kan men daarnaast inbrengen dat anonieme uitingen minder waarde hebben voor de discussie vanwege de betekenis die de identiteit van de afzender heeft voor het effect van een boodschap. Toerekenbaarheid heeft een duidelijk effect op het prestige van de afzender. Wie niet bang is verantwoordelijk te worden gehouden voor zijn ideeën zou geloofwaardiger zijn. Iemand die echt voor zijn ideeën staat, zal strijden met open vizier in plaats van zich lafhartig te verschuilen achter het schild van de schuilnaam, zo is de gedachte. Identiteit is relevant omdat het veel zegt over de achtergrond en de motieven van de spreker. Eigenbelang en vooringenomenheid worden door anonimiteit aan de waarneming onttrokken.

Al met al lijkt het moeilijk om algemene uitspraken te doen over de effecten van anonimiteit. Wanneer men de voordelen van anonimiteit serieus neemt kan men wel stellen dat de maatschappelijke nadelen in abstracto niet reeds bij voorbaat zwaarder dienen te wegen. In een democratische samenleving moeten deze nadelen wellicht worden beschouwd als negatieve bijwerkingen van een ruime uitingsvrijheid. Zij zijn als het ware de prijs die men betaalt voor een open uitwisseling van ideeën. De waarde van anonimiteit lijkt het minst buiten kijf te staan wanneer anonimiteit een voorwaarde is voor het ontstaan van een maatschappelijke discussie en voor de toegang daartoe. De voor- en nadelen van anonimiteit als factor in het debat zelf kunnen echter niet in abstracto tegen elkaar worden afgewogen. Zoals in de komende hoofdstukken zal blijken heeft de discussie over deze voor- en nadelen zowel in de Nederlandse als in de Amerikaanse geschiedenis haar sporen nagelaten en blijft zij tot op de dag van vandaag voortbestaan.

3 Bescherming van anonimiteit onder het First Amendment

3.1 Inleiding

De jurisprudentie en de theorievorming over de uitingsvrijheid zijn nergens omvangrijker dan in de Verenigde Staten. Ook over het verband tussen anonimiteit en uitingsvrijheid is in de Verenigde staten veel nagedacht en geschreven. Bovendien heeft het Supreme Court, het Amerikaanse Hooggerechtshof, het recht om anoniem te zijn in een lange reeks uitspraken beschermd als onderdeel van de uitingsvrijheid en de andere in het First Amendment genoemde rechten. Een beschrijving van het Amerikaanse recht mag in dit onderzoek dan ook niet ontbreken.

In dit hoofdstuk zal eerst het historische belang van anonieme geschriften en de discussie over de toelaatbaarheid daarvan worden besproken. Vervolgens komt de jurisprudentie over anonimiteit en het First Amendment aan de orde. Hierin komen de grondslagen van het recht om anoniem te communiceren en de grenzen aan de uitoefening van dat recht naar voren. In hoofdstuk 4 zal vervolgens specifiek aandacht worden besteed aan de regulering van anonimiteit op het internet en de bescherming van anonieme internetgebruikers. De twee hoofdstukken vormen tezamen een leidraad voor de bespreking van het eigen recht.

3.2 Anonieme politieke geschriften

De geschiedenis van de Verenigde Staten kent vele invloedrijke anonieme en pseudonieme geschriften. Zo wordt 'Cato's Letters', de meest gezaghebbende verhandeling over vrijheid van meningsuiting en politieke vrijheden in de achttiende eeuw, in 1720 door John Trenchard en Thomas Gordon gepubliceerd onder het pseudoniem 'Cato'. 'Common Sense', van Thomas Paine betwist het gezag van de Engelsen en is het eerste openbare pleidooi voor onafhankelijkheid. Het boek verschijnt in 1776, het jaar van de Onafhankelijkheidsverklaring, onder het pseudonym 'an Englishman'. Benjamin Franklin, een van de opstellers van de Declaration of Independence, publiceerde verschillende invloedrijke anonieme pamfletten en anonieme artikelen, onder andere in de 'New England Courant' van zijn broer James, een van de eerste kranten van de Verenigde Staten.[1] Het meest genoemde voorbeeld is echter het anoniem verschijnen van de 'Federalist

1. Wilson & Fiske 1999.

Papers'. Deze serie van 85 essays wordt in de jaren 1787 en 1788 door James Madison, Alexander Hamilton en John Jay, onder het pseudoniem 'Publius' gepubliceerd in verschillende kranten in de staat New York. De New Yorkers worden hierin aangespoord om het voorstel voor de Constitutie te ratificeren. In de essays worden de verschillende bepalingen in detail uitgelegd. De Anti-Federalisten geven door middel van gelijksoortige essays repliek, daarbij eveneens gebruik makend van pseudoniemen. De drie auteurs van de Federalist Papers zouden later als 'Founding Fathers' betrokken zijn bij de totstandkoming van de Amerikaanse Constitutie.[2]

Ook nadat George Washington in 1789 president wordt, verschijnen nog vele anonieme publicaties. In de periode tot 1810 zijn er ten minste 600 bekend.[3] In deze periode publiceerden ten minste zes Presidenten, vijftien leden van het kabinet, twintig Senatoren en vierendertig leden van het Congres anonieme of pseudonieme politieke geschriften.[4]

Anonieme publicaties zijn in de Amerikaanse geschiedenis niet alleen reeds vroeg een veelvoorkomend verschijnsel; zij zijn ook vanaf het begin onderwerp van discussie. Al in de periode rond de onafhankelijkheid komen de opvattingen van de Framers van de Constitutie over de relatie tussen anonimiteit en drukpersvrijheid naar voren.[5] In 1779 verschijnt een anoniem artikel waarin leden van het Congres verantwoordelijk worden gehouden voor de heersende inflatie en waarin zij worden beschuldigd van fraude. Een aantal leden van het Congres slaagt er met een beroep op de drukpersvrijheid in te voorkomen dat de drukker gedwongen wordt de identiteit van de auteur vrij te geven. Een vergelijkbaar geval doet zich voor in het Hogerhuis van New Jersey, waar pogingen om een kritische auteur te achterhalen worden gedwarsboomd door de State Assembly.[6]

Onder redacteuren bestaat intussen geen overeenstemming over de publicatie van anonieme artikelen en pamfletten. In 1787 roept een Federalist alle drukkers op om geen geschriften te drukken waarvan de auteur onbekend wenst te blijven. Hij is bang dat de kranten gevuld zullen worden met bezwaren tegen de ratificatie van de Constitutie. Voor Benjamin Russell, redacteur van de vooraanstaande Federalistische krant 'the Massachusetts Centinel', is de oproep aanleiding om geen Anti-Federalistische stukken meer te plaatsen tenzij de auteur zijn identiteit aan hem bekend maakt, opdat deze, indien nodig, aan het publiek bekend kan worden gemaakt. Medestanders van Russell betogen

2. Zij zouden ook na de onafhankelijkheid een belangrijke rol blijven spelen. James Madison werd in 1809 de vierde president van de Verenigde Staten, Alexander Hamilton werd Secretary of the Treasury en John Jay werd de eerste Supreme Court Justice.
3. Gaines 1972.
4. Westin 1970, p. 331.
5. Supreme Court Justice Thomas gaat hierop uitgebreid in in zijn concurring opinion bij *McIntyre* v. *Ohio*. *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 334 (1995).
6. William Livingston, de gouverneur van New Jersey, publiceerde in 1784 vier artikelen waarin hij het recht om anoniem te publiceren verdedigde met een beroep op de drukpersvrijheid. Idem.

dat het redelijk is en in overeenstemming met de drukpersvrijheid om een dergelijke eis te stellen. De Anti-Federalisten gaan tegen het beleid van Russell echter fel tekeer. Onder het pseudoniem Philadelphiensis schrijft een van hen dat de Federalisten door de praktijken van Russell te ondersteunen uiteindelijk naar het laatste redmiddel gegrepen hebben, te weten: afschaffing van de drukpersvrijheid. De poging om de Anti-Federalistische meningen te onderdrukken is in zijn ogen een voorbode van de onderdrukking die onder de nieuwe Constitutie plaats zal vinden.[7]

Het recht om anoniem te spreken is in de 18e en de 19e eeuw ook in de rechtszaal een belangrijk en terugkerend thema als fundament voor de bescherming van onpopulaire sprekers. Dit recht speelt onder andere een rol in het vroegste en meest bekende Amerikaanse proces over de drukpersvrijheid: het in 1735 gevoerde proces tegen de drukker John Peter Zenger. De laatste weigert de namen bekend te maken van een aantal anonieme auteurs die kritiek hebben geuit op William Cosby, de gouverneur van New York. Cosby spant daarop een procedure aan tegen Zenger zelf wegens 'seditious libel', maar verliest. Het oordeel wordt algemeen beschouwd als een overwinning voor de principes van anonimiteit en drukpersvrijheid en illustreert dat deze reeds op een vroeg moment in de Amerikaanse geschiedenis met elkaar verweven en in het rechtsbewustzijn verankerd waren.[8]

Hoewel over de verspreiding van anonieme pamfletten en artikelen van het begin af aan onenigheid bestond, moet men constateren dat het anoniem publiceren in de Verenigde Staten nooit streng is bestreden. De tolerantie ten aanzien van anonieme bijdragen aan de publieke discussie heeft achtergestelde of van deelname uitgesloten groeperingen in verschillende episodes van de Amerikaanse geschiedenis in staat gesteld toch hun stem te laten horen. Zo brachten vrouwelijke en zwarte auteurs in de negentiende eeuw met gebruikmaking van pseudoniemen hun mening over de afschaffing van de slavernij naar voren. Tijdens de Koude Oorlog bleven communistische auteurs publiceren ondanks het feit dat zij stonden vermeld op de zwarte lijst van McCarthy.[9]

3.3 Het First Amendment

De uitingsvrijheid neemt in het Amerikaanse constitutionele recht een zeer belangrijke plaats in. Dit recht is, tezamen met enkele daaraan verwante rechten, opgenomen in het First Amendment:

7. "Here we see pretty plainly through [the Federalists'] excellent regulation of the press, how things are to be carried on after the adoption of the new constitution." Idem.
8. Een uitgebreide beschrijving van dit proces vindt men bij Alexander. Zie Alexander 1963.
9. Wallace 1999a, p. 3.

> "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

Voorschriften van de federale of de statelijke wetgever die een beperking van de uitingsvrijheid met zich meebrengen worden door het Supreme Court getoetst aan vier fundamentele principes:

1. Regulering van uitingen moet 'content-neutral' zijn. Censuur mag niet worden uitgeoefend enkel en alleen omdat de overheid het niet eens is met het standpunt van de spreker;
2. Gezien de gewichtige positie die de uitingsvrijheid inneemt in de hiërarchie van constitutionele waarden moet de overheid om censuur te kunnen uitoefenen een belang aannemelijk maken dat uitstijgt boven gewone alledaagse belangen. Onder de 'balancing doctrine' worden de door de overheid naar voren gebrachte belangen bij het uitoefenen van censuur afgewogen tegen het zwaarwegende maatschappelijk belang van een onbelemmerde uitingsvrijheid;
3. De overheid dient een zeer direct causaal verband aan te tonen tussen bestreden uitingen en het gevreesde of beweerdelijk negatieve effect van die uitingen voordat zij die uiting kan onderdrukken;[10]
4. De overheid moet bij de regulering van de uitingsvrijheid altijd kiezen voor het middel dat de uitingsvrijheid het minst beperkt.[11]

Deze moderne free speech doctrine werd ontwikkeld in het tijdperk van de befaamde Supreme Court Justices Holmes en Brandeis. Later werd nog een vijfde principe toegevoegd. Deze bepaalt het aan een uiting toe te kennen beschermingsniveau door middel van 'labeling'. In plaats van de 'clear and present danger test' of de 'balancing test' toe te passen wordt de uiting ingedeeld in een categorie van uitingen. 'Political speech' wordt beschouwd als het hart van het First Amendment en maakt daarom aanspraak op de

10. In *Schenk* v. *United States* werd voor het eerst de 'clear and present danger test' aanvaard die dit principe tot uitdrukking brengt. Justice Holmes formuleerde de ratio voor deze test in deze uitspraak als volgt: "The most stringent protection of free speech would not protect a man in falsely shouting fire in a theater and causing panic. (…) The question in every case is whether the words are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent." Zie *Schenk* v. *United States*, 249 U.S. 47 (1919). In *Brandenburg* v. *Ohio* werd de clear and present danger test verlaten en vervangen door een andere twee-stappen toets. Sindsdien geldt als uitgangspunt dat de overheid een uiting, een oproep tot geweld of een wetsovertreding slechts mag verbieden "where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action". Zie *Brandenburg* v. *Ohio*, 395 U.S. 444 (1969).
11. Morrison 1996, p. 92-93.

meeste bescherming. Commerciële uitingen zijn minder beschermenswaardig en obscene uitingen worden beschouwd als 'non-speech' zodat het First Amendment daarvoor niet kan worden ingeroepen. Labeling wordt ook toegepast om te bepalen of sprake is van smaad. Wanneer een uitlating betrekking heeft op 'public figures or public issues' is de bescherming hoger dan wanneer sprake is van 'private figure' libel.[12]

Om de wetgever bij de regulering van uitingen te dwingen tot het tot stand brengen van nauw omschreven en duidelijk bepalingen, heeft het Supreme Court strenge sancties gesteld op 'overbreadth' en 'vagueness'. Bepalingen die te ruim of te vaag zijn geformuleerd of die tot doel of tot gevolg hebben dat zowel beschermde als onbeschermde uitingen aan banden worden gelegd, worden als in strijd met het First Amendment en derhalve als nietig beschouwd. Ten slotte volgt uit het First Amendment een verbod op 'prior restraints'.

3.4 Bescherming van anonimiteit

Sinds de jaren vijftig van de vorige eeuw heeft het Supreme Court het recht om anoniem te zijn in verschillende contexten erkend als een essentiële waarborg voor de uitoefening van de door het First Amendment beschermde rechten. De godsdienstvrijheid, de vrijheid van vereniging en de uitingsvrijheid komen in zijn jurisprudentie samen als nauw met elkaar verweven grondslagen. In de eerste zaken betreft het telkens federale of statelijke regelgeving die de mogelijkheid om anoniem te zijn beknot, doordat als voorwaarde voor de oprichting en instandhouding van politieke of religieuze organisaties, danwel voor uiteenlopende door het First Amendment beschermde activiteiten, zoals 'canvassing', 'pamphleteering' en 'speeching', een verplichting tot naamsvermelding of een registratieplicht wordt opgelegd.[13]

Bescherming door het First Amendment wordt voor het eerst toegekend in *NAACP* v. *Alabama*.[14] De National Association for the Advancement of Colored People (NAACP) zet zich in voor het welzijn en de emancipatie van de zwarte bevolking. In de zuidelijke staten Arkansas en Alabama tracht men het functioneren van de organisatie onmogelijk te maken. Van overheidswege wordt onder andere verlangd dat zij alle namen en adressen van haar leden en vertegenwoordigers prijsgeeft. De NAACP weigert, ondanks een boete van honderdduizend dollar, aan deze eis te voldoen. Zij is bevreesd dat onthulling van de

12. Heeft de uitlating betrekking op 'public figures or public issues' dan moet door de eiser worden aangetoond dat 'the speech is consciously false or delivered with reckless disregard for the truth'. Is sprake van 'private libel' dan hoeft slechts te worden 'negligence' te worden aangetoond.
13. Het woord 'canvassing' verwijst naar het verspreiden van politieke en religieuze meningen in ruime zin. Hieronder kan vallen het voeren van (politieke) campagne, het (huis aan huis) uitdelen van blaadjes, het verzamelen van stemmen, het doen van opinieonderzoek, maar ook colportage.
14. *NAACP* v. *Alabama,* 357 U.S. 449 (1958). Zie ook *Bates* v. *Little Rock,* 361 U.S. 516 (1960).

namen zal leiden tot pesterijen, economische represailles en fysieke mishandeling. Bovendien is zij van mening dat de eis in strijd is met de Amerikaanse Constitutie.

Het Supreme Court komt unaniem tot het oordeel dat gedwongen afgifte van de ledenlijsten in strijd is met het recht tot vereniging en met de Due Process Clause in het Fourteenth Amendment, dat de Amerikaanse burgers beschermt tegen een schending van constitutionele rechten door statelijke overheden. Het recht tot vereniging omvat het recht van een organisatie om een vertrouwelijke ledenlijst bij te houden alsmede het recht van de leden om hun lidmaatschap geheim te houden:

> "It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective (…) restraint on freedom of association. (…) This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. (…) Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[15]

Korte tijd later komt de relatie tussen anonimiteit en de vrijheid van meningsuiting aan de orde in *Talley* v. *California*.[16] Het betreft een wettelijk verbod op het verspreiden van anonieme pamfletten in de staat Californië. De bepaling verbiedt de verspreiding van "any hand-bill in any place under any circumstances" zonder vermelding van de namen van de afzender en de verspreider.[17] Deze algemene verplichting tot identificatie is naar het oordeel van het Supreme Court te ruim geformuleerd en vormt daardoor een te vergaande beperking van de vrijheid om informatie te verspreiden, die een essentieel onderdeel is van de uitingsvrijheid. Het Supreme Court plaatst de verspreiding van anonieme pamfletten in een historische context:

> "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."

15. *NAACP* v. *Alabama,* 357 U.S. 449 (1958), at 462. Enigszins vergelijkbaar is de Nederlandse uitspraak in de zaak *Ravage* vs. *de Staat* waarin de President van de Rechtbank Den Haag oordeelde dat het in beslag nemen van een abonneebestand en aanmeldingsbronnen van de linkse organisatie Ravage een inbreuk was op het recht om in vrijheid ideeën en informatie te verspreiden. Pres. Rb. Den Haag, 4 december 1997, *Mediaforum* 1997/2, p. 33 (*Ravage* vs. *de Staat*).
16. *Talley* v. *California*, 362 U.S. 60 (1960).
17. Het betrof een verbodsbepaling in de gemeente Los Angeles die luidde: "No person shall distribute any hand-bill in any place under any circumstances, which does not have printed on the cover, or the face thereof, the name and address of the following: (a) The person who printed, wrote, compiled or manufactured the same; (b) The person who caused the same to be distributed; provided, however, that in the case of a fictitious person or club, in addition to such fictitious name, the true names and addresses of the owners, managers or agents of the person sponsoring said hand-bill shall also appear thereon."

De angst voor represailles kan een vreedzame discussie over publieke aangelegenheden in de weg staan. Justice Black roept de onrechtvaardige Engelse perswetten in herinnering die voor de onafhankelijkheid in de Verenigde Staten golden.[18]

Drie decennia later gaat het in *McIntyre* v. *Ohio* opnieuw om een verbod op de verspreiding van anonieme pamfletten.[19] Ook deze bepaling, die overigens uitsluitend betrekking heeft op *politieke* pamfletten, wordt in strijd met het First Amendment bevonden.[20] Hoewel lezers vaak nieuwsgierig zullen zijn naar de identiteit van een auteur en het publiek er in het algemeen belang bij heeft de maker van een kunstwerk te identificeren, mag een auteur in principe zelf beslissen of hij zijn identiteit al dan niet onthult. De beslissing om anoniem te blijven is, net als andere beslissingen omtrent de inhoud van een publicatie, een onderdeel van de uitingsvrijheid. De keuze voor anonimiteit kan zijn ingegeven door angst voor economische vergelding of vergelding door overheidsinstanties, door de vrees voor sociale verbanning of louter door het verlangen om zoveel mogelijk van zijn privacy te bewaren. Daarnaast kan de afzender van mening zijn dat zijn ideeën meer overtuigingskracht hebben wanneer lezers zijn identiteit niet kennen. Anonimiteit voorkomt dat de boodschap van een onpopulaire auteur puur op persoonlijke gronden terzijde wordt geschoven.

De omstandigheid dat anonimiteit belemmeringen uit de weg neemt voor de uitoefening van de uitingsvrijheid weegt zeer zwaar:

> "Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry."

Het Supreme Court betrekt in zijn overwegingen de omstandigheid dat vele grote literaire werken zijn uitgegeven onder een pseudoniem. Ook buiten de literaire sfeer is men

18. Ook een algemeen vergunningsvereiste voor de verspreiding van literatuur was door het Supreme Court reeds nietig bevonden met een verwijzing naar de geschiedenis: 'Pamphlets and leaflets have been historic weapons in the defense of liberty.' *Lovell* v. *City of Griffin*, 303 U.S. 444 (1938).
19. *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 334 (1995).
20. Ohio Rev. Code Ann. par.3599.09(A) (1988) luidde: "No person shall write, print, post, or distribute, or cause to be written, printed, posted, or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to promote the nomination or election or defeat of a candidate, or to promote the adoption or defeat of any issue, or to influence the voters in any election, or make an expenditure for the purpose of financing political communications through newspapers, magazines, outdoor advertising facilities, direct mailings, or other similar types of general public political advertising, or through flyers, handbills, or other nonperiodical printed matter, unless there appears on such form of publication in a conspicuous place or is contained within said statement the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefor. (…)".

echter vrij om anoniem te publiceren. Een beperking van dat recht moet door zwaarwegende belangen worden gerechtvaardigd. De staat Ohio heeft de voorkoming van frauduleuze en smadelijke uitlatingen en de juiste voorlichting van het electoraat als dergelijke belangen naar voren gebracht. Het Supreme Court wijst deze motivering van de hand. Het belang van de voorlichting van het electoraat kan niet leiden tot een verplichting om informatie te vermelden die de afzender anders zou weglaten. Bij de verspreiding van pamfletten door een bij de lezers onbekende particulier draagt vermelding van naam en adres immers weinig bij aan de mogelijkheden van de lezer om de inhoud van de boodschap te beoordelen. De bestrijding van fraude en smaad is evenmin een voldoende rechtvaardiging. Het bestreden verbod, dat in Ohio fungeert als een hulpmiddel bij de handhaving van meer algemene bepalingen die het doen van onjuiste uitlatingen in verkiezingstijd verbieden, is in een aantal opzichten te ruim geformuleerd. In de eerste plaats is de bepaling ook van toepassing op documenten die niet onjuist of misleidend zijn. In de tweede plaats vallen niet alleen de grootschalige activiteiten van verkiezingskandidaten en hun politieke organisaties maar ook de bescheiden bijdragen van onafhankelijke individuen binnen de reikwijdte. Ten derde heeft het verbod niet alleen betrekking op de verkiezing van politici, maar ook op verkiezingsonderwerpen waar geen enkel risico voor smaad bestaat. Ten vierde is het verbod niet beperkt in de tijd: het geldt ook voor pamfletten die niet aan de vooravond van de verkiezingen maar maanden van te voren worden verspreid.[21] Ten slotte is het verbod toepasselijk ongeacht de aard of het gewicht van het belang van de auteur bij zijn anonimiteit.

Belangrijk is dat de vermelding van naam en adres door het Supreme Court wordt aangemerkt als een onderdeel van de *inhoud* van het document:

> "Insofar as the interest in informing the electorate means nothing more than the provision of additional information that may either buttress or undermine the argument in a document, we think the identity of the speaker is no different form other components of the document's content that the author is free to include or exclude."

Het Supreme Court eindigt zijn oordeel alsvolgt:

21. Door het Illinois Supreme Court waren soortgelijke argumenten al eerder naar voren gebracht: "Implicit in the State's (…) justification is the concern that the public could be misinformed and an election swayed on the strength of an eleventh hour anonymous smear campaign to which the candidate could not meaningfully respond. The statute cannot be upheld on this ground, however, because it sweeps within its net a great deal of anonymous speech completely unrelated to this concern. In the first place, the statute has no time limit and applies to literature circulated two months prior to an election as well as that distributed two days before. The statute also prohibits anonymous literature supporting or opposing not only candidates, but also referenda. A public question clearly cannot be the victim of character assassination." Zie *People* v. *White*, 116 Ill. 2d 171, 180, 506 NE 2d 1284, 1288 (Ill. 1987).

> "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."

De laatste volzin is een verwijzing naar de ideeën van John Stuart Mill: onpopulaire individuen moeten worden beschermd tegen vergelding in een onverdraagzame maatschappij en hun ideeën moeten worden beschermd tegen onderdrukking. Het recht om anoniem te zijn kan worden misbruikt als dekmantel voor onheus gedrag. De bescherming van politieke uitingen heeft echter in het algemeen onvermijdelijk onplezierige consequenties. Uiteindelijk kent de Amerikaanse samenleving meer waarde toe aan de voordelen van de uitingsvrijheid dan aan de nadelen van het misbruik daarvan.

Justice Thomas en Justice Scalia leveren beiden kritiek op de meerderheidsbeslissing. In hun 'opinions' komt een fundamenteel verschil van inzicht naar voren over de juiste methode van constitutionele interpretatie en over de wijze waarop de Amerikaanse geschiedenis moet worden geanalyseerd. Justice Thomas onderschrijft het resultaat van de meerderheidsbeslissing maar is het niet eens met de motivering. In zijn concurring opinion betoogt hij dat een andere methode had moeten worden toegepast om tot het oordeel te komen. In plaats van aan te knopen bij de Amerikaanse traditie van anonieme meningsuiting had volgens hem moeten worden vastgesteld of het First Amendment, zoals dit oorspronkelijk door de opstellers van de Constitutie werd begrepen, ook anonieme politieke pamfletten beschermde. Aangezien er geen verslagen bestaan van discussies over de bescherming van anonieme politieke uitlatingen door het First Amendment ten tijde van de totstandkoming daarvan, is de oorspronkelijke betekenis van het First Amendment op dit punt echter onduidelijk. Bij gebreke van directe historische bronnen moet daarom op andere wijze uit de geschiedenis worden afgeleid wat de geldende praktijken en opvattingen waren van de opstellers van de Constitutie. De anonieme publicatie van de Federalist Papers tijdens de ratificatie van de Constitutie laat weinig twijfel dat zij zich zelf ook bezighielden met de verspreiding van anonieme politieke geschriften. Het kan dus worden aangenomen dat de Anti-Federalisten, die de stuwende kracht waren achter de totstandkoming van de Bill of Rights, meenden dat de drukpersvrijheid het recht omvatte om anoniem politieke geschriften te publiceren. Er zijn volgens Thomas eveneens duidelijke historische aanwijzingen dat de Amerikanen die leefden tijdens de revolutie de gedwongen onthulling van auteurs afkeurden omdat zij van mening waren dat dit in strijd was met de persvrijheid.

Justice Scalia hanteert een andere methode om de constitutie te interpreteren. Hij is het niet eens met de meerderheidsbeslissing. De ideeën van John Stuart Mill worden zijns inziens ten onrechte gesteld boven het weloverwogen oordeel van de wetgever. Bepalingen zoals die in Ohio bestaan in verschillende vormen in iedere staat behalve Californië en gaan terug tot het einde van de 19e eeuw. Hoewel aannemelijk kan worden gemaakt dat het verspreiden van anonieme pamfletten ten tijde van de totstandkoming van de Constitutie gebruikelijk was, volgt hieruit volgens hem nog niet dat dit ook een

constitutioneel recht is. De door het Supreme Court gehanteerde interpretatie is naar zijn oordeel niet die van het huidige Amerikaanse volk. Bovendien zijn er onvoldoende aanwijzingen dat deze interpretatie in de Amerikaanse samenleving ten tijde van de totstandkoming van het First Amendment werd aangehangen. Voor Scalia lijkt het gebrek aan toerekenbaarheid dat uit de constitutionele bescherming van anonimiteit zou kunnen voortvloeien echter het doorslaggevende argument te zijn:

> "I do not know where the Court derives its perception that 'anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.' (…) I can imagine no reason why an anonymous leaflet is any more honorable, as a general matter, than an anonymous phone call or an anonymous letter. It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity. There are of course exceptions, and where anonymity is needed to avoid 'threats, harassment, or reprisals' the First Amendment will require an exemption from the Ohio law. But to strike down the Ohio law in its general application – and similar laws of 48 other States and the Federal Government – on the ground that all anonymous communication is in our society traditionally sacrosanct, seems to me a distortion of the past that will lead to a coarsening of the future."

Na *McIntyre* v. *Ohio* staat vast dat het recht op anonimiteit in ieder geval van toepassing is op de oprichting en instandhouding van religieuze en politieke organisaties, op de publicatie van boeken en geschriften en op de verspreiding van politieke en andersoortige pamfletten. Deze handelingen en activiteiten moeten worden beschouwd als de kern van het First Amendment. De reikwijdte van het recht op anonimiteit is in een aantal recente zaken vervolgens geleidelijk aan uitgebreid. In *Buckley* v. *American Constitutional Law Foundation, Inc*, vernietigt het Supreme Court een bepaling in de staat Colorado aangaande het verzamelen van handtekeningen voor een wetgevend volksreferendum. Burgers die voor dat doel petities uitdelen dienen een badge te dragen met daarop hun naam en hun status als vrijwilliger of als betaalde kracht.[22] Indien zij voor het uitdelen van de petities worden betaald, moeten daarnaast de naam en het telefoonnummer van de betalende instantie worden vermeld. Doorslaggevend is het door eisers naar voren gebrachte argument dat de verplichting om een badge te dragen mensen weerhoudt van deelname aan het uitdelen van petities.

In *Watchtower Bible* v. *Stratton Ohio* komt vervolgens de vraag aan de orde of bescherming ook moet worden toegekend aan het verkondigen van politieke en religieuze ideeën van deur tot deur.[23] Aanleiding is een gemeentelijke regeling in de gemeente Stratton die 'canvassing' alleen toestaat indien daarvoor een 'solicitation permit' is verkregen. Deze vergunning, waarop de naam van de houder is vermeld, moet op verzoek van de politie of op verzoek van de persoon bij wie men langsgaat, worden getoond. Het doel van de

22. *Buckley* v. *American Constitutional Law Foundation*. Inc., 525 U.S. 182 (1999).
23. *Watchtower Bible & Tract Soc. of N.Y., Inc.* v. *Village of Stratton*, 536 U.S. 150 (2002).

regeling is de voorkoming van fraude en de bescherming van de privacy van Strattons inwoners. De vergunning kan kosteloos worden verkregen. Wel moeten op een registratieformulier gegevens van de aanvrager worden ingevuld zoals onder andere zijn naam en adres, een korte beschrijving van de goederen, diensten of ideeën die aan de man worden gebracht, naam en adres van de werkgever of organisatie waarvoor men optreedt, alsmede referenties van die werkgever of organisatie en het adres van iedere woning waar men voornemens is langs te gaan. De Jehova's getuigen weigeren een vergunning aan te vragen omdat zij van mening zijn dat hun plicht om het geloof te verspreiden en de bevoegdheid daartoe, voortvloeien uit de bijbel.[24] Zij betogen dat de gemeentelijke regeling, die het tot een overtreding maakt om zonder vergunning langs de deur te gaan, in strijd is met het First Amendment.[25] Deze regeling zou te ruim zijn, onder andere omdat afbreuk wordt gedaan aan het recht om anonieme pamfletten te verspreiden, zoals erkend in *McIntyre* v. *Ohio*.

Het Supreme Court erkent dat een gemeentelijke overheid een gerechtvaardigd belang kan hebben bij de regulering van canvassing, met name wanneer geld wordt ingezameld. In *Cantwell* v. *Connecticut* oordeelde het reeds:

> "(…) a State may protect its citizens from fraudulent solicitation by requiring a stranger in the community, before permitting him publicly to solicit funds for any purpose, to establish his identity and his authority to act for the cause which he purports to represent."[26]

Ook de voorkoming van andere strafbare feiten kan een gerechtvaardigd belang zijn. Een vergunningsvereiste met een daaraan gekoppelde registratieplicht kan bijvoorbeeld nuttig zijn om te voorkomen dat inbrekers zich voordoen als canvassers om er achter te komen of een huis bewoond is. Er moet echter een evenwicht bestaan tussen deze belangen en de beperking van de rechten van First Amendment. In dat verband weegt zeer zwaar dat de bestreden verordening niet slechts van toepassing is op commerciële activiteiten en het inzamelen van geld, maar ook op het uitdragen van religieuze en politieke meningen:

---

24. De jehovagetuigen geloven dat hun plicht en de bevoegdheid om te prediken volgt uit Matteus 28, vers 19 en 20: "Ga er daarom op uit om alle volken tot mijn discipelen te maken." De verplichting om een vergunning aan te vragen staat in hun ogen daarom gelijk aan godslastering.
25. Section 116.01 van de bestreden regeling luidde: "The practice of going in and upon private property and/or the private residence of Village residents in the Village by canvassers, solicitors, peddlers, hawkers, itinerant merchants or transient vendors of merchandise or services, not having been invited to do so by the owners or occupants of such private property or residences, and not having first obtained a permit pursuant to Section 116.03 of this Chapter, for the purpose of advertising, promoting, selling and/or explaining any product, service, organization or cause, or for the purpose of soliciting orders for the sale of goods, wares, merchandise or services, is hereby declared to be a nuisance and is prohibited."
26. *Cantwell* v. *Connecticut*, 310 U.S. 296 (1940).

> "The mere fact that the ordinance covers so much speech raises constitutional concerns. It is offensive – not only to the values protected by the First Amendment, but to the very notion of a free society – that in the context of everyday public discourse a citizen must inform the government of her desire to speak to her neighbors and than obtain a permit to do so. Even if the issuance of permits by the mayor's office is a ministerial task that is performed promptly and at no cost to the applicant, a law requiring a permit to engage in such speech constitutes a dramatic departure from our national heritage and constitutional tradition."[27]

Een vergunningsvereiste kan op verschillende manieren een belemmering vormen, aldus het hoogste rechtscollege. In *Talley* v. *California* en *McIntyre* v. *Ohio* werd reeds vastgesteld dat de keuze om anoniem te blijven kan zijn ingegeven door de angst voor represailles en sociale uitsluiting of door de wens om de individuele privacy te beschermen. Daarnaast is er een aanzienlijke hoeveelheid personen die om religieuze of principiële redenen weigert om een vergunning aan te vragen. Tenslotte wordt 'spontaneous speech' door de verordening feitelijk onmogelijk gemaakt. Wie tijdens een vakantieperiode of in het weekend besluit om deel te nemen aan een politieke campagne zal moeten wachten totdat hij een vergunning heeft verkregen.

Voor het Supreme Court weegt zwaar dat het huis-aan-huis campagne voeren een van de meest effectieve manieren is om ideeën te verspreiden en steun te vergaren. Canvassing is essentieel voor 'the poorly financed causes of little people'. Het historische belang van dit traditionele verspreidingsmiddel wordt uitgebreid besproken.[28] Voor vele gevestigde religieuze en politieke organisaties en vakbonden is canvassing daarnaast een effectief middel om leden te werven.[29]

Dat bepalingen zoals die in Ohio ook een beperking kunnen zijn voor 'non-religious speech' was reeds gebleken in *Thomas* v. *Collins,* waarin aan de orde kwam of van een vakbondsleider kan worden verlangd dat hij een vergunning verkrijgt alvorens een toespraak te mogen houden voor een groep van potentiële vakbondsleden. Het Supreme Court oordeelde dat een registratieplicht voor het houden van een openbare toespraak zich in het algemeen niet verdraagt met de uitingsvrijheid en het recht tot vereniging:

> "Lawful public assemblies, involving no element of grave and immediate danger to an interest the State is entitled to protect, are not instruments of harm which require previous identification of the speakers. (…) If the exercise of the rights of free speech and free assembly cannot be made a crime, we do not think this can be accomplished by the device of requiring previous registration as a condition for exercising them and making such a condition the foundation for restraining in advance their exercise and for imposing a penalty for violating such a restraining order. So long as no more is involved than exercise of the rights of free speech and free assembly, it is immune to such a restric-

27. *Watchtower Bible & Tract Soc. of N.Y., Inc.* v. *Village of Stratton*, 536 U.S. 150 (2002).
28. Zie ook *Murdock* v. *Pennsylvania*, 319 U.S. 105 (1943); *Schneider* v. *State (Town of Irvington)*, 308 U.S. 147 (1939).
29. *Martin* v. *City of Struthers*, 319 U.S. 141 (1943).

> tion. (…) We think a requirement that one must register before he undertakes to make a public speech to enlist support for a lawful movement is quite incompatible with the requirements of the First Amendment."[30]

De hierboven besproken zaken hebben telkens betrekking op vergunningsvereisten en verplichtingen tot registratie of naamsvermelding. In *Church of American Knights* wordt aan het Court of Appeals van de staat New York echter de vraag voorgelegd of het First Amendment ook bescherming biedt aan maatregelen die bedoeld zijn om identificatie op grond van fysieke kenmerken tegen te gaan. De Church of American Knights, een splintergroepering van de Ku Klux Klan, brengt in deze zaak naar voren dat uit het First Amendment onder bepaalde omstandigheden een recht voort zou vloeien om in het openbaar zijn gelaat te verbergen.[31] Aanleiding is de weigering van een vergunning om te demonstreren wegens het voornemen om tijdens de demonstratie maskers te dragen. Dit zou in strijd komen met een bepaling in de New York Penal Code, een overblijfsel van een in 1845 ingevoerde 'anti-mask law', die bedoeld was om geweld tegen te gaan en de arrestatie van wetsovertreders te vergemakkelijken.[32] Het Court of Appeals verwerpt het beroep van de American Knights op de jurisprudentie van het Supreme Court sinds *NAACP* v. *Alabama*:

> "These Supreme Court decisions establish that the First Amendment is implicated by government efforts to compel disclosure of names in numerous speech-related settings, whether the names of an organization's members, the names of campaign contributors, the names of producers of political leaflets, or the names of persons who circulate petitions. In contrast, the Supreme Court has never held that freedom of association or the right to engage in anonymous speech entails a right to conceal one's appearance in a public demonstration. Nor has any Circuit found such a right. We decline

30. *Thomas* v. *Collins.* 323 U.S. 516 (1945).
31. *Church of the American Knights of the Ku Klux Klan* v. *Kerik*, 356 F.3d 197, 203 (2d Cir. 2004). Maskers hebben altijd deel uitgemaakt van de tradities van de Ku Klux Klan. Vanaf 1867 werden de maskers gedragen tijdens 'night riding', waarbij African Americans werden geïntimideerd, mishandeld en vermoord. Na 1915 richtte het geweld zich daarnaast tegen joden en katholieken. In 1949 viel de beweging uiteen in een aantal splintergroeperingen, waaronder de American Knights. Veel van deze splintergroeperingen dragen de maskers ook bij demonstraties.
32. Par. 240.35(4) New York Penal Law luidde: "A person is guilty of loitering when he (…) being masked or in any manner disguised by unusual or unnatural attire or facial alteration, loiters, remains or congregates in a public place with other persons so masked or disguised, or knowingly permits or aids persons so masked or disguised to congregate in a public place; except that such conduct is not unlawful when it occurs in connection with a masquerade party or like entertainment if, when such entertainment is held in a city which has promulgated regulations in connection with such affairs, permission is first obtained from the police or other appropriate authorities." Gemaskerde groepen werden in de oorspronkelijke regeling van 1845 extra zwaar bestraft. Concrete aanleiding voor de verboden was een hoogoplopend conflict tussen boeren en grootgrondbezitters waarbij de laatsten werden bedreigd en besmeurd met pek en veren. Ook vielen er enkele doden. De verantwoordelijken konden niet worden achterhaald omdat zij zich hadden vermomd als indianen.

> the American Knights' request to extend the holdings of NAACP v. Alabama and its progeny and to hold that the concealment of one's face while demonstrating is constitutionally protected."

De stelling dat het dragen van een masker als door het First Amendment beschermde 'expressive conduct' zou moeten worden aangemerkt wordt eveneens afgewezen. Dat met het uniform, zoals met ieder uniform, een boodschap werd overgebracht staat niet ter discussie. Door het uniform te dragen identificeren de eisers zich immers met de American Knights en met de ideologie van deze beweging. In casu is bovendien aannemelijk dat deze boodschap door het publiek wordt begrepen. De bestreden regeling verbiedt echter alleen het masker en niet het hele uniform en de zeggingskracht van het masker is redundant; het masker voegt niets toe aan de boodschap die reeds wordt overgedragen door de rest van het uniform, in het bijzonder de witte mantel en de puntmuts.[33]

Het gaat in *American Knights* niet om gedwongen afgifte van namen maar om een verbod op het verbergen van het gelaat en dus om anonimiteit in een ruimere betekenis. Niettemin zou het bestreden verbod op dezelfde wijze een chilling effect kunnen hebben op de uitoefening van de rechten van het First Amendment. Het Court of Appeals lijkt van oordeel te zijn dat het verbergen van het gelaat een stap verder gaat dan de geheimhouding van een naam. Het valt echter niet uit te sluiten dat de onpopulaire boodschap van de American Knights en het gewelddadige imago van deze organisatie hier een rol hebben gespeeld. Het is de vraag of het beroep op het First Amendment ook geweigerd zou zijn indien de maskers werden gedragen door leden van de National Association for the Advancement of Colored People.

De jurisprudentie van het Supreme Court beschermt anonimiteit blijkens het voorgaande bij uiteenlopende wijzen van verspreiding. De uitingsvrijheid beschermt naast het recht om te verspreiden echter ook het recht om informatie te ontvangen. De vraag dringt zich dan ook op in hoeverre ook aan de kant van de ontvanger een recht bestaat om anoniem te blijven. Dit is temeer het geval nu elektronische communicatietechnieken het in toenemende mate mogelijk maken om het communicatiegedrag van zenders én ontvangers van informatie te controleren en te registreren. Het Supreme Court heeft zich over dit onderwerp nog niet uitgesproken. Op statelijk niveau is het vraagstuk wel aan de orde gekomen. In *Tattered Cover, Inc.* v. *City of Thornton* speelde de opvraging van gegevens over de aanschaf van boeken in het kader van strafrechtelijk onderzoek.[34] In deze uitspraak leidde het Colorado Supreme Court zowel uit de federale als uit de statelijke constitutie een 'right to read anonymously' af, inhoudende dat men het recht heeft om op anonieme wijze en zonder inmenging van de overheid boeken aan te schaffen.[35]

33. De American Knights brachten in dit verband nog tevergeefs het argument naar voren dat de maskers symbool stonden voor de gelijkheid van de leden van de organisatie en voor nederigheid ten overstaan van God.
34. *Tattered Cover, Inc.* v. *City of Thornton*, 44 P.3d 1044,1047 (Col., 2002).
35. Zie over het recht om anoniem te lezen, met name in de context van Digital Rights Management-systemen, Cohen 1996 en 2003.

Het kopen van een boek is als uitoefening van het recht om te lezen en het recht om ideeën en informatie te ontvangen een door het First Amendment beschermde activiteit. Iedere inmenging van de overheid die een 'chilling effect' heeft op de bereidheid van burgers om boeken aan te schaffen, raakt dus de door het First Amendment beschermde belangen.[36] Het Colorado Supreme Court oordeelde daarom dat de verstrekking van 'search warrants', waarmee opsporingsinstanties het koopgedrag van consumenten kunnen achterhalen, met verzwaarde procedurele waarborgen moet zijn omgeven. Een te ruime mogelijkheid om de gewoonten van lezers in kaart te brengen, creëert bij hen immers het gevoel dat de overheid over hun schouder meekijkt.

3.5 Bescherming van anonimiteit op het internet

Het maatschappelijke communicatieproces is heden ten dage grotendeels gedigitaliseerd. De hierboven besproken elementen van het recht om anoniem te communiceren moeten dientengevolge in een nieuwe omgeving worden toegepast. Met name op het internet levert de anonimiteit van zenders en ontvangers enkele nieuwe vraagstukken op.

Het recht om op het internet anoniem te communiceren is, althans op statelijk niveau, voor het eerst expliciet erkend in *ACLU* v. *Miller*.[37] In deze uitspraak vernietigt een District Court in Georgia twee bepalingen die het strafbaar stellen om op het internet informatie te verzenden met gebruikmaking van een pseudoniem danwel met gebruikmaking van een handelsnaam of een (auteursrechtelijk beschermd) logo of symbool, zonder toestemming.[38] Doel van de regeling is het tegengaan van 'fraudulent transmissions or the appropriation of the identity of another person or entity for some improper purpose'.[39] Het District Court oordeelt conform de jurisprudentie van het Supreme Court dat sprake is van regulering naar de inhoud. Blijkens *McIntyre* v. *Ohio* is de identiteit van de spreker immers 'no different from other components of [a] document's contents that the author is free to include or exclude'. De bepalingen zijn daarnaast te ruim geformuleerd en bestrijken daardoor ook onschuldige en beschermde handelingen en

36. *Tattered Cover, Inc.* v. *City of Thornton*, 44 P.3d 1044,1047 (Col., 2002), at 1052.
37. *American Civil Liberties Union of Georgia* v. *Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997).
38. De bepalingen stellen het voor eenieder strafbaar: "knowingly to transmit any data through a computer network (…) for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name (…) to falsely identify the person (…), and for (…) any person (…) knowingly to transmit any data through a computer network (…) if such data uses any (…) trade name, registered trademark, logo, legal or official seal, or copyrighted symbol (…) which would falsely state or imply that such person (…) has permission or is legally authorized to use [it] for such purpose when such permission or authorization has not been obtained." Zie Act No. 1029, GA. Laws 1996, p. 1505, codified at O.C.G.A. par. 16-9-93.1.
39. Ten tijde van de uitspraak waren in tenminste 13 andere staten soortgelijke wetsvoorstellen aanhangig.

uitingen. Ook het verhullen van identiteit met het doel om sociale uitsluiting, discriminatie en pesterijen te voorkomen of ter bescherming van de persoonlijke privacy is verboden. Ten slotte zijn de bepalingen *void for vagueness*: het is niet duidelijk welke handelingen precies verboden zijn. De bepaling creëert daardoor het risico van willekeurige wetstoepassing en maakt een inbreuk op de uitingsvrijheid van de klagers doordat het zelfcensuur oproept.

Een week na *ACLU* v. *Miller* wijst het Supreme Court vonnis in de zaak *ACLU* v. *Reno*.[40] Het twistpunt in deze zaak is de grondwettelijkheid van de in 1996 door de federale wetgever tot stand gebrachte Communications Decency Act (CDA), die minderjarigen middels een aanpassing van de Communications Act beoogt te beschermen tegen schadelijke informatie op het internet. Aanleiding voor de CDA is bezorgdheid over de grote aanbod van pornografie.[41] Afdeling 223(a) van de gewijzigde Communications Act stelt het strafbaar om bewust obscene en onfatsoenlijke informatie te verzenden aan personen onder de achttien jaar.[42] Afdeling 223(d) verbiedt het bewust verzenden of tonen aan personen van onder de achttien jaar van iedere boodschap die 'in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs'.[43] In afdeling 223(e) is wel voorzien in

40. *Reno* v. *American Civil Liberties Union*, 521 U.S. 844 (1997).
41. Directe aanleiding voor de CDA was de publicatie van een onderzoek in het *Georgetown Law Journal* waarin werd geconcludeerd dat 83.5% van al het beeldmateriaal op het internet bestond uit pornografie. Hoewel deze resultaten later onjuist bleken, creëerden zij bij de wetgever het idee dat er een dringende maatschappelijke behoefte bestond aan regulering van online pornografie. Zie Rosen 2001, p. 183 e.v.
42. Section 223(a) van de Communications Act (47 U.S.C. 223) zou, voor zover van belang, komen te luiden: "Whoever (1) in interstate or foreign communications (A) by means of a telecommunications device knowingly (i) makes, creates, or solicits, and (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person; (B) by means of a telecommunications device knowingly (i) makes, creates, or solicits, and (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication; (…) shall be fined under title 18, United States Code, or imprisoned not more than two years, or both."
43. Section 223(d) van de Communications Act (47 U.S.C. 223) zou, voor zover van belang, komen te luiden: "Whoever (1) in interstate or foreign communications knowingly (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; (…) shall be fined under title 18, United States Code, or imprisoned not more than two years, or both."

een strafuitsluitingsgrond voor personen die alleen toegang tot het netwerk verschaffen zonder betrokken te zijn bij de vervaardiging van obscene informatie.

Ook de bepalingen in de CDA worden op grond van *overbreadth* en *vagueness* vernietigd. De voornaamste bezwaren zijn dat de bepalingen geen duidelijke definitie bevatten van de begrippen 'indecent' en 'patently offensive' en dat regulering plaatsvindt op basis van de inhoud. Daarnaast laten de bepalingen het bijvoorbeeld niet toe dat kinderen met toestemming van hun ouders kennis nemen van de bestreden informatie. *ACLU* v. *Reno* is ook om andere redenen een mijlpaal in de jurisprudentie over het First Amendment. Het Supreme Court erkent in een unanieme beslissing dat de uitingsvrijheid op het internet dezelfde bescherming verdient als offline. De expressieve kracht van het internet is ongeëvenaard:

> "(…) through the use of internet chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox".[44]

De CDA confronteert het Supreme Court met een nieuw probleem. Deze wet is de eerste fundamentele poging van de federale wetgever om de toegang tot informatie op het internet te reguleren door middel van 'zonering'. Het doel is pornografie af te zonderen van andere informatie en alleen toegankelijk te maken voor volwassenen. De CDA bevat daarom een bepaling die strafrechtelijke aansprakelijkheid uitsluit indien te goeder trouw redelijke en effectieve maatregelen zijn genomen om toegang voor minderjarigen te verhinderen of te beperken.[45] Aansprakelijkheid kan dus worden voorkomen door middel van volwassenidentificatie.[46]

Aan volwassenenidentificatie kleeft echter een aantal bezwaren. In 1997 was er nog geen effectieve manier om de identiteit of de leeftijd van een internetgebruiker te bepalen. Zelfs indien het technisch mogelijk zou zijn om voor minderjarigen de toegang te blokkeren tot newsgroups en chatrooms waarin zich informatie bevindt die potentieel 'indecent' of 'patently offensive' is, dan zouden deze maatregelen er waarschijnlijk toe

44. *Reno* v. *American Civil Liberties Union*, 521 U.S. 844 (1997), finding 35.
45. Section 223(e)(5) en onder (A) Communications Act zou komen te luiden: "It is a defense to a prosecution under subsection (a)(1)(B) or (d) (…) that a person (A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology."
46. Section 223(e)(5) en onder (B) Communications Act zou komen te luiden: "It is a defense to a prosecution under subsection (a)(1)(B) or (d) (…) that a person (B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number." Een andere vorm van zonering is kinderidentificatie. Hierbij heeft iedere gebruiker toegang tot bepaald materiaal, tenzij een signaal wordt verzonden waaruit blijkt dat de desbetreffende gebruiker minderjarig is. Zie Lessig 1999, p. 176.

leiden dat ook een grote hoeveelheid ander materiaal wordt geblokkeerd.[47] Het Supreme Court sluit zich daarom aan bij de overwegingen van het District Court, dat overwoog:

> "Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers."[48]

Een tweede bezwaar is dat het gebruik van een credit card om de leeftijd van de gebruiker te bepalen alleen mogelijk is tijdens de afhandeling van een commerciële transactie waarbij de credit card wordt gebruikt of wanneer, tegen betaling, gebruik wordt gemaakt van een 'verification agency'. Het gebruik van credit cards als een middel om leeftijd aan te tonen zou voor vele niet-commerciële websites onoverkomelijke kosten met zich meebrengen. Voor een substantieel aantal content providers is credit card verification dus geen optie. De verplichting om een dergelijk systeem in stand te houden zou voor volwassenen zonder credit card de toegang tot afgeschermd materiaal bovendien onmogelijk maken. Volwassenen die zich niet kunnen of willen identificeren worden zo verstoken van materiaal waar zij recht op hebben. Men dient daarbij te bedenken dat ook pornografie door het First Amendment wordt beschermd.

3.6 Conclusie

Het uitdragen van een mening in anonieme geschriften is vanaf het begin van de Amerikaanse geschiedenis een veel voorkomende praktijk geweest. Deze praktijk is door het Supreme Court gebillijkt en zelfs verheven tot een 'honorable tradition of advocacy and dissent'. De bescherming van deze traditie is gegrondvest op diepgaande beschouwingen omtrent het verband tussen anonimiteit en de rechten in het First Amendment. Kenmerkend voor de Amerikaanse jurisprudentie zijn zeer uitgebreide motiveringen en verwijzingen naar de geschiedenis en de literatuur. Het Supreme Court behandelt de vragen rondom anonimiteit bovendien in een breed constitutioneel kader. Het erkent het anoniem openbaren van ideeën en informatie allereerst als een uit de uitingsvrijheid voortvloeiend recht. De bescherming strekt zich uit tot verschillende wijzen van verspreiding. Een ieder heeft het recht om politieke of religieuze ideeën op anonieme wijze wereldkundig te maken met behulp van fysieke dragers, zoals pamfletten, artikelen en boeken. Ook de verspreiding van ideeën door middel van het gesproken woord is beschermd. Voorafgaande identificatieverplichtingen bij het houden van openbare toespraken en 'canvassing' worden als een ongeoorloofde beperking van het First Amendment beschouwd, tenzij een zwaarwegend belang aannemelijk kan worden gemaakt. In ruimere zin wordt

47. *Reno* v. *American Civil Liberties Union*, 521 U.S. 844 (1997), finding 20-21.
48. Zie 929 F. Supp. 824 (ED Pa. 1996), finding 107.

het recht om anoniem te zijn beschermd door een geheel van met de uitingsvrijheid samenhangende en in het First Amendment genoemde constitutionele rechten. Herhaaldelijk komt het verband met het vrijheid van vereniging, de godsdienstvrijheid en het recht op privacy naar voren.

Verboden op anonimiteit worden door het Supreme Court aangemerkt als regulering van de *inhoud* van een uiting. Zij worden daarom extra kritisch getoetst aan de principes van de free speech doctrine. Met name het verbod op 'overbreadth' en 'vagueness' heeft vele wettelijke regelingen doen sneuvelen. Zo wordt het bestreden verbod in *McIntyre* v. *Ohio* op maar liefst vijf punten te ruim bevonden. Restricties op anonimiteit dienen door de wetgever dus zeer zorgvuldig te worden geformuleerd. Deze strenge houding is onder andere ingegeven door de wens om zoveel mogelijk uitingen te laten doordringen tot de 'marketplace of ideas'.

ACLU v. *Miller* en *ACLU* v. *Reno* moeten worden beschouwd als de voorbode van een lange zoektocht naar de grenzen van het recht op anonimiteit in de digitale omgeving. De oprukkende registratie van gegevens over het communicatiegedrag van burgers door aanbieders van elektronische communicatienetwerken en -diensten creëert vele nieuwe juridische problemen. Zo heeft het Supreme Court zich nog niet gebogen over de vraag in hoeverre de ontvangstvrijheid en het in *Tattered Cover* erkende 'right to read anonymously', ook op het internet anoniem uitgeoefend kunnen worden. Het lijkt echter logisch te veronderstellen dat identificatieverplichtingen met een te ruim toepassingsbereik ook daar in strijd komen met het First Amendment, indien zij de toegang tot informatie te veel belemmeren. Een ander actueel vraagstuk is de verstrekking van identificerende gegevens door elektronische tussenpersonen, zoals telefonieaanbieders en internetproviders. In de praktijk blijkt dat private partijen steeds vaker willen weten wie verantwoordelijk is voor de anonieme verspeiding van informatie op het internet. Op dit probleem wordt in het volgende hoofdstuk nader ingegaan.

4 De anonieme gedaagde in het Amerikaanse recht

4.1 Inleiding

Het recht op anonimiteit werd reeds in de jaren vijftig van de vorige eeuw door het Supreme Court aanvaard en vervolgens gaandeweg toepasselijk verklaard op verschillende klassieke wijzen van informatieverspreiding. Amerikaanse burgers werden in de jurisprudentie over het First Amendment met name beschermd tegen van overheidswege uitgevaardigde registratieverplichtingen en anonimiteitsverboden.

Met de opkomst van elektronische communicatiemiddelen dient de bescherming van anonieme communicatie nu in een nieuwe context gestalte te krijgen. Zeer actueel zijn civiele procedures waarin wordt getracht internetgebruikers te identificeren om hen aansprakelijk te kunnen stellen voor beweerdelijk beledigende of anderszins onrechtmatige informatie. Hier doet zich telkens de procedurele vraag voor onder welke voorwaarden elektronische tussenpersonen verplicht kunnen worden tot het verstrekken van identificerende gegevens van internetgebruikers. Om deze vraag te kunnen beantwoorden dient onder andere te worden vastgesteld hoe de belangen van de eiser bij de handhaving van zijn rechten moeten worden afgewogen tegen het recht van de gedaagde om anoniem te blijven. Daarnaast rijst de vraag hoe de anonymus op de hoogte kan worden gesteld van de poging zijn anonimiteit te doorbreken en hoe hij in staat kan worden gesteld zijn belangen te verdedigen. De genoemde vragen raken alle direct aan het de belangen van het First Amendment en het publieke debat. Onbeperkte mogelijkheden tot identificatie zouden het recht om ongehinderd informatie te verspreiden en te ontvangen immers illusoir maken.

Bij de behandeling van de genoemde aspecten zal voornamelijk statelijk procesrecht worden behandeld. Het Californische recht krijgt bijzondere aandacht omdat het voorziet in een vergaande bescherming van anonieme uitlatingen op het internet.

4.2 Ontmaskering in pre-trial discovery

'Pre-trial discovery' is een fase van de civiele procedure waarin, voorafgaand aan de eigenlijke behandeling van de zaak, door partijen bewijs wordt verzameld. Om te garanderen dat beide partijen bij aanvang van de procedure een zo groot mogelijke kennis van de feiten hebben, beschikken zij over ruime bevoegdheden om benodigde informatie te bemachtigen. Door middel van een zogenaamde 'subpoena' kunnen personen worden opgeroepen om te getuigen. Ook kan van hen worden verlangd dat zij bepaalde documenten of andere zaken overleggen. Om bewijsmiddelen voor de rechter te brengen kan

gebruik worden gemaakt van een 'subpoena duces tecum'.[1] Een subpoena wordt in de meeste gevallen uitgevaardigd door de griffier van het gerecht waar de procedure aanhangig is gemaakt.[2] Daarnaast is het mogelijk dat een advocaat zelfstandig een subpoena uitvaardigt.[3] Een kenmerk van het Amerikaanse procesrecht is dat subpoenas in de beginfase van de procedure in het algemeen sneller worden uitgereikt dan in andere common law jurisdicties en dat zij worden uitgereikt zonder rechterlijke toetsing.[4]

Discovery proceedings vinden normaalgesproken pas plaats nadat aan de gedaagde een dagvaarding is uitgebracht. In procedures tegen anonieme internetgebruikers levert dit een probleem op omdat de naam van de gedaagde in de dagvaarding dient te worden vermeld.[5] Om de eiser in staat te stellen de voor de dagvaarding noodzakelijke identificerende informatie te verkrijgen wordt daarom 'limited discovery' toegestaan. Zolang de identiteit van de gedaagde nog niet bekend is, wordt hij of zij aangeduid als 'John' of 'Jane Doe'. Aan de persoon of instantie die mogelijk beschikt over identificerende gegevens van de gedaagde, doorgaans is dit een internetprovider, wordt vervolgens een zogenaamde 'John Doe subpoena' uitgereikt. John Doe subpoenas wijken af van de meeste andere subpoenas doordat zij niet zijn gericht op het achterhalen van feiten maar enkel en alleen op het achterhalen van de identiteit van de gedaagde. Het geschil concentreert zich gedurende pre-trial discovery vervolgens volledig op de vraag of de provider aan de John Doe subpoena dient te voldoen.

De provider en de anonieme gedaagde kunnen zich beiden verzetten tegen de subpoena door middel van een 'motion to quash'.[6] Hierin wordt de rechter gevraagd om de

1. Par. 1985.(b) California Code of Civil Procedure (C.C.P).
2. Par. 1986.(a) C.C.P.
3. Par. 1985.(c) C.C.P. en Rule 45(A)(3) van de Federal Rules of Civil Procedure. De laatste bepaling beschouwt de advocaat voor het uitbrengen van een subpoena als een 'officer of the court'.
4. De Verenigde Staten wijken in dit opzicht af van andere common law stelsels. Van oudsher kenden zij de mogelijkheid om in zeer uitzonderlijke omstandigheden door middel van een zogenaamde 'bill of discovery' de identiteit te achterhalen van een persoon die geen partij was in het geding. In het Verenigd Koninkrijk, Australië Nieuw Zeeland en Canada raakte dit procedurele middel echter in ongebruik. In het Verenigd Koninkrijk is de bill of discovery slechts één keer gebruikt in een John Doe zaak. Zie *Totalise plc v. The Motley Fool Ltd* [2002] EMLR 20 (CA). Zie Sims 2003, p. 271.
5. Par. 412.20.(a)(2) C.C.P. en rule 4(a) van de Federal Rules of Civil Procedure.
6. Par. 1987.1. C.C.P. luidt: "When a subpoena requires the attendance of a witness or the production of books, documents or other things before a court, or at the trial of an issue therein, or at the taking of a deposition, the court, upon motion reasonably made by the party, the witness, or any consumer described in Section 1985.3, or upon the court's own motion after giving counsel notice and an opportunity to be heard, may make an order quashing the subpoena entirely, modifying it, or directing compliance with it upon such terms or conditions as the court shall declare, including protective orders. In addition, the court may make any other order as may be appropriate to protect the parties, the witness, or the consumer from unreasonable or oppressive demands including unreasonable violations of a witness's or consumer's right of privacy. Nothing herein shall require any witness or party to move to quash, modify, or condition any subpoena duces tecum of personal records of any consumer served under paragraph (1) of subdivision (b) of Section 1985.3."

subpoena te vernietigen. De rechter kan daarnaast op basis van par. 2017(c) California Code of Civil Procedure (C.C.P.) de reikwijdte van het discovery process beperken indien hij van oordeel is dat 'the burden, expense, or intrusiveness of that discovery clearly outweighs the likelihood that the information sought will lead to the discovery of admissible evidence.'[7] De toepassing van deze bepaling kan leiden tot het oordeel dat verstrekking van identificerende gegevens niet op zijn plaats is zodat de John Doe subpoena moet worden vernietigd.

Indien een motion to quash is ingediend is het de eisende partij niet toegestaan om het bewuste materiaal te inspecteren of te kopiëren, tenzij hiertoe een rechterlijk bevel is verkregen. De ontvanger van de subpoena is op zijn beurt verplicht om het gezochte bewijsmateriaal beschikbaar te houden. Providers zijn na het ontvangen van de subpoena dus verplicht om te verzekeren dat de gewenste informatie beschikbaar blijft. Ook het automatisch wissen van informatie kan worden aangemerkt als vernietiging van bewijs.[8]

In de begindagen van het internet vond de verstrekking van identificerende informatie door providers aan private partijen veelal plaats buiten het discovery proces om. De meeste providers waren kleine 'message board operators' zonder privacy policy en zonder juridische expertise. Zij verstrekten identificerende en andere informatie doorgaans zonder protest, ook wanneer aan hen geen subpoena was uitgereikt. Anonieme internetgebruikers werden in veel gevallen door de provider niet op de hoogte gesteld van de poging om hun identiteit te achterhalen. Dientengevolge waren zij vaak niet in de gelegenheid om zich tegen de onthulling van identificerende informatie te verzetten. Rechterlijke toetsing van John Doe subpoenas vond in de eerste John Doe lawsuits slechts plaats wanneer de anonieme gedaagde via andere wegen, bijvoorbeeld via de media, er achter was gekomen dat een procedure was aangespannen om zijn identiteit te achterhalen.

4.3 Wettelijke bescherming van identificerende gegevens

Op federaal niveau ontbreekt tot op heden een adequate wettelijke bescherming voor identificerende gegevens. De Electronic Communications Privacy Act (ECPA) biedt ruime mogelijkheden voor afgifte. par. 2703(c)(5) ECPA bepaalt dat een provider, dat wil zeggen "a person or entity providing an electronic communication service to the public" (par. 2702(a)(1) ECPA), "may divulge a record or information pertaining to a subscriber to or customer of such service (…) to any person other than a governmental entity." Voor de afgifte van identificerende informatie is alleen een rechterlijk bevel vereist indien het verzoek afkomstig is van een overheidsinstantie. In alle andere gevallen

7. Par. 2017.(c) C.C.P.
8. *Federal Rules of Civil Procedure*, rule 45(c)(2)(B).

eist de ECPA noch rechterlijke toetsing, noch de uitreiking van een subpoena.[9] Evenmin is voorzien in een verplichting om de anonieme gedaagde te notificeren. Het grote aantal verzoeken om identificerende gegevens heeft sommige providers er inmiddels toe gebracht een 'civil subpoena policy' op te stellen, niet alleen om de privacy van hun klanten te beschermen, maar ook om te voorkomen dat zij aansprakelijk worden gesteld voor ongeoorloofde verstrekking. Het gebrek aan waarborgen op federaal niveau heeft zich hierdoor in de praktijk voor een deel opgelost. Providers zullen identificerende gegevens doorgaans niet afgeven wanneer geen geldige subpoena is ontvangen en veel van hen hanteren een notificatieprocedure.

Zoals Sobel reeds in 2000 betoogde zou de bescherming van anonieme internetgebruikers, gezien het feit dat John Doe procedures veelal over de grenzen van verschillende staten worden gevoerd, aanmerkelijk worden versterkt wanneer op federaal niveau voor de verstrekking van identificerende informatie een subpoena zou worden vereist en wanneer deze subpoena vervolgens door de rechter zou worden getoetst. Ook in een notificatieverplichting zou naar zijn mening op federaal niveau moeten worden voorzien.[10] Zodoende zou kunnen worden voorkomen dat de anonieme gedaagde het slachtoffer wordt van een lager beschermingsniveau in de staat waar de procedure werd aangespannen.

In Californië werd in 2003 een wetsvoorstel ingediend om het gebrek aan bescherming te verhelpen. Assembly Bill 1143 voegt service providers toe aan par. 1985.3 van de California Code of Civil Procedure.[11] Deze bepaling regelt de verstrekking van 'personal records' door personen of organisaties die als getuige in pre-trial discovery geconfronteerd kunnen worden met een subpoena duces tecum, zoals artsen, ziekenhuizen, financiële instellingen, advocaten en telefoonbedrijven. Het initiatief, ondersteund door enkele grote belangenorganisaties, zoals de Electronic Frontier Foundation (EFF) en het California Anti-SLAPP project, is een directe reactie op het grote aantal John Doe subpoenas dat door providers wordt ontvangen en het misbruik van de discovery procedure in de verhevigde juridische strijd tegen auteursrechtinbreuk en spamming. In de toelichting bij het voorstel wordt geconstateerd dat anonieme gedaagden in de praktijk slechts

9. Voor afgifte van gegevens die moeten worden gerekend tot de inhoud van de communicatie gelden strengere regels. Zie par. 2702 ECPA.
10. Sobel 2000.
11. Het voorstel spreekt van 'an interactive computer service'. Hieronder zou moeten worden verstaan: "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer service, including, but not limited to, a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions". Zie par. 1985.3(a)(2) van het voorstel.

zelden kunnen opkomen tegen een subpoena duces tecum gezien het gebrek aan notificatie en de korte termijn waarbinnen aan de subpoena voldaan moet worden.[12]

De voorgestelde wijziging introduceert een afzonderlijke procedure voor het opvragen van identificerende gegevens bij een provider.[13] De regeling verlangt van de partij die de subpoena duces tecum uitvaardigt (hierna: de 'subpoenaing party') dat hij aan de consument wiens gegevens het betreft, kopieën doet toekomen van een aantal documenten, waaronder de subpoena. Zo dient aan de betrokkene een kennisgeving te worden verzonden waarin hij van de subpoena op de hoogte wordt gesteld en waarin wordt aangegeven hoe hij zich hiertegen kan verzetten.[14] In de meeste gevallen zal de subpoenaing party niet beschikken over het postadres van de betrokkene. Daarom is voorzien in de mogelijkheid om de documenten per e-mail aan de betrokkene te verzenden. Dit dient tenminste 20 dagen voor de dag waarop de gegevens moeten worden verstrekt te geschieden (subsection (b)(4)(A)). Als de subpoenaing party noch over een postadres, noch over een e-mail adres beschikt, kunnen de documenten ook worden verstrekt aan de provider, ten minste 34 dagen voorafgaand aan de dag waarop de gegevens moeten worden verstrekt (subsection (b)(4)(B)). In het laatste geval dient de provider de betrokkene binnen veertien dagen te notificeren. Indien ook de provider niet over een postadres van de betrokkene beschikt, maar wel over zijn e-mailadres, kunnen de bescheiden worden verstuurd naar dat e-mailadres, danwel naar het e-mailadres dat door de betrokkene voor dat doel is opgegeven. Als de provider niet over een e-mailadres beschikt wordt van hem geen nadere actie verlangd. Evenmin rust op hem een verdergaande verplichting om te zorgen dat de kennisgeving de betrokkene bereikt.

Gewone subpoenas moeten worden vergezeld van een beëdigde verklaring (affidavit) waarin slechts enige relevantie hoeft te worden gesteld. Assembly Bill 1143 stelt echter strengere eisen. Blijkens subdivision (b)(6) van het voorstel dient de subpoena vergezeld

12. Bill Analysis 2004, p. 5.
13. Onder 'personal records' worden in dat verband verstaan: "a first and last name, pseudonym, home or other physical address, including the name of a city, town, or street, e-mail address, telephone number, social security number, Internet protocol (IP) address, or any other identifier or combination of information that allows for the identification of a consumer." Zie par. 1985.3(a)(1) van het voorstel. Het voorstel is overigens niet van toepassing op gevallen waarin een auteursrechthebbende de identiteit van een inbreukmaker probeert te achterhalen. Hiervoor bestaat immers een specifieke regeling in de Digital Millenium Copyright Act (DMCA) (zie par. 4.6).
14. Subdivision (e) bepaalt: "Every copy of the subpoena duces tecum and affidavit, if any, (…) shall be accompanied by a notice, in a typeface designed to call attention to the notice, indicating that records about the consumer are being sought from the witness named on the subpoena; if the consumer objects to the witness furnishing the records to the party seeking the records, the consumer must file papers with the court or serve a written objection as provided in subdivision (g) prior to the date specified for production on the subpoena; and if the party who is seeking the records will not agree in writing to cancel or limit the subpoena, an attorney should be consulted about the consumer's interest in protecting his or her rights of privacy. If a notice of taking of deposition is also served, that other notice may be set forth in a single document with the notice required by this subdivision."

te gaan van *'a declaration, without attachments or exhibits in a plain text electronic file',* welke de volgende informatie dient te bevatten:

> "A) A statement of the cause of action, and, if the action relates to communications, the communications that are the subject of the action, the subpoena, or both;
> B) A statement explaining how, or in what manner, the personal records are directly relevant to a claim or defense;
> C) A statement that other reasonable efforts to serve the consumer have not been effective, that the subpoena is issued in good faith and not for an improper purpose, and that the interactive computer service to which the subpoena is addressed is likely to have responsive personal records;
> D) The name of all courts in which complaints or motions relating to this subpoena have been filed, and all corresponding case numbers;
> E) The date of production;
> F) A statement that the subpoenaing party attests to the accuracy of the foregoing information."

De persoon wiens gegevens het betreft kan zich kan zich vóór de datum van de productie, tegen de subpoena duces tecum verzetten door een 'motion' in te dienen.[15] Iedere andere persoon kan eveneens schriftelijk bezwaar indienen. Indien de eiser belang heeft bij een spoedige afwikkeling, kan hij een bevel verkrijgen dat de genoemde termijnen verkort. De provider mag redelijke kosten die voortvloeien uit het voldoen aan de aan hem gestelde eisen, in rekening brengen aan de eiser (subdivision (l)).

4.4 Balancing tests

Wanneer een John Doe subpoena in rechte wordt aangevochten, dient de rechter de belangen van de eiser af te wegen tegen de belangen van de anonieme gedaagde. Er zijn reeds verschillende procedures gevoerd waarin een dergelijke afweging aan de orde kwam.[16] In *Seescandy* overwoog het District Court in the Northern District of California:

> "(…) the need to provide injured parties with a 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."

De mogelijkheid om anoniem of onder een pseudoniem een mening naar voren te brengen wordt ook hier uitdrukkelijk erkend als een stimulans voor open communicatie en een robuust debat. Misbruik van procedurele middelen dient te worden voorkomen:

15. Par. 1985.3(g).
16. Veel van de hier behandelde zaken kunnen worden gevonden op <http://www.cyberslapp.org>.

> "People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity. Thus some limiting principles should apply to the determination of whether discovery to uncover the identity of a defendant is warranted."[17]

John Doe subpoenas roepen de vraag op wat een privacy partij precies moet aantonen om afgifte van identificerende informatie te kunnen afdwingen. *2theMart* is een van de eerste John Doe zaken waarin een stappentoets wordt geformuleerd die aan de eisende partij een welomschreven bewijsplicht oplegt.[18] De stappentoets is bedoeld als een flexibel mechanisme dat misbruik van de discovery procedure dient te voorkomen en dat voorziet in criteria waarmee het uit het First Amendment voor de gedaagde voortvloeiende recht op anonimiteit kan worden afgewogen tegen het belang van de eiser om de anonieme persoon in het geding te betrekken:

> "The court will consider four factors in determining whether the subpoena should issue. These are whether: (1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim of defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source."[19]

Het betrof in *2theMart* overigens niet de onthulling van een anonieme gedaagde, maar van andere anonieme sprekers wier uitlatingen niettemin van belang waren voor de beoordeling van de vordering van de eiser. In *Seescandy* en *America Online* is de onthulling bedoeld om de anonieme spreker zelf in het geding te betrekken. In *Seescandy* wordt een stappentoets geformuleerd die enigszins afwijkt van de toets in *2TheMart*:

> "First, the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court. This requirement is necessary to ensure that federal requirements of jurisdiction and justiciability can be satisfied (…);
>
> Second, the party should identify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a food faith effort to comply with the requirements of service of process and specifically identifying defendants (…);
>
> Third, plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss;

17. *Columbia Ins. Co.* v. *Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999). Zie over de hier geformuleerde standaard Wein 2002.
18. Het betreft in deze procedure overigens de onthulling van anonieme sprekers die niet als partij betrokken zijn in het geding maar wier uitlatingen niettemin van belang zijn voor de vordering van de eiser.
19. *Doe* v. *2TheMart.com, Inc.*, 140 F. Supp.2d 1088. U.S. District Court, Western District of Washington.

> Lastly, the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible."[20]

Het eerste element van de stappentoets is bedoeld om te verzekeren dat de rechter bevoegd is. Het tweede element bevat een subsidiariteitstoets: de eisende partij dient aan te tonen dat hij te goeder trouw pogingen heeft gedaan om de gedaagde te identificeren en te dagvaarden. Onthulling van identificerende gegevens kan in pre-trial discovery slechts worden toegestaan wanneer de eiser te goeder trouw alle traditionele mogelijkheden om de gedaagde te identificeren heeft benut. Het derde element is bedoeld om misbruik van procedurele middelen te voorkomen. Onthulling van identiteit in pre-trial discovery is in wezen verwant aan de procedure voor het verkrijgen van een 'warrant' ten behoeve van strafrechtelijk onderzoek. Het vereiste dat de overheid voorafgaand hieraan een 'probable cause' aannemelijk maakt, dient ongeoorloofde privacyinbreuken tegen onschuldige burgers te voorkomen. Een vergelijkbare eis is ook in civiele procedures nodig. Daarom wordt als voorwaarde gesteld dat de vorderingen van de eiser een zogenaamde 'motion to dismiss' moeten kunnen weerstaan. In een motion to dismiss verzoekt de gedaagde de rechter om vast te stellen dat de eiser zijn stellingen niet kan bewijzen. In dat geval zal de eiser een 'prima facie case' aannemelijk moeten maken. Van een prima facie case is sprake wanneer de stellingen van de eiser 'op het eerste gezicht' door de gepresenteerde bewijsmiddelen kunnen worden bewezen, tenzij tijdens de zitting door de gedaagde bewijs van het tegendeel wordt overlegd. De strengheid waarmee het vereiste van een prima facie case wordt toegepast varieert van staat tot staat.[21]

In *Dendrite* formuleert het Appellate Court van New Jersey een balancing test die in vergelijking met de reeds genoemde een aantal extra waarborgen bevat. In de eerste plaats wordt van de eiser verlangd dat hij zich inspant om de anonieme gedaagden op de hoogte te stellen van het feit dat aan de provider een John Doe subpoena is uitgereikt. Aan de eiser wordt zelfs opgedragen dat hij daartoe een notificatiebericht plaatst op het message board waar de bestreden uitlatingen zijn gedaan.[22] Vervolgens dienen de gedaagden gedurende een redelijke termijn in de gelegenheid te worden gesteld om zich tegen

20. Va. S. Ct. Rule 4:9(c) luidt, voor zover van belang: "Upon written request therefore filed with the clerk of the court in which the action or suit is pending by counsel of record for any party (…) the clerk shall (…) issue to a person not a party therein a subpoena duces tecum which shall command the person to whom it is directed (…) to produce the documents and tangible things (…) designated and described in said request (…) but, *the court, upon written motion promptly made by the person so required to produce,* or by the party against whom such production is sought, *may quash or modify the subpoena if it is unreasonable and oppressive*" [curs. AE].
21. Sims 2003, p. 277.
22. *Dendrite International, Inc.* v. *Doe*, 342 N.J. Super. 134 (App. Div. 2001).

de subpoena te verzetten. Ten slotte wordt de motion-to-dismiss standaard door het appellate court verzwaard met de eis dat de gedaagde daadwerkelijke schade aan moet tonen, terwijl dit normaal gesproken geen eis is om een motion to dismiss te overleven.

In *NAACP* v. *Alabama* oordeelde het Supreme Court reeds dat de National Association of Colored People het recht op anonimiteit van haar leden mocht inroepen om zich te verzetten tegen gedwongen verstrekking van ledenlijsten (zie par. 3.4).[23] De omstandigheid dat de NAACP zelf ook schade zou ondervinden van de onthulling van de identiteit van haar leden doordat financiële steun en lidmaatschap zou teruglopen, speelde daarbij een rol. In *America Online* wordt wederom ingegaan op de vraag of het recht op anonimiteit ook kan worden ingeroepen door een derde partij, in casu provider America Online (AOL).[24] De eiser voert aan dat een John Doe subpoena alleen kan worden aangevochten door de anonieme gedaagde zelf, aangezien hij door de goedkeuring daarvan direct in zijn belangen wordt geraakt. Het Circuit Court van Virginia verwerpt dit standpunt en oordeelt dat ook de provider bevoegd is om het recht op anonimiteit van haar klanten te verdedigen. Hiervoor zijn twee redenen. In de eerste plaats mag worden aangenomen dat gebruikers van chat rooms en message boards uitgaan van de verwachting dat de anonimiteit van hun communicatie wordt beschermd, mede gezien het feit dat AOL hiertoe contractueel verplicht is. Als AOL aan deze verwachting niet tegemoet komt, is het aannemelijk dat sommige gebruikers overstappen naar een concurrent. De bestreden subpoena heeft dus ook een potentieel schadelijk effect voor AOL zelf. In de tweede plaats zijn de abonnees van AOL vaak niet op de hoogte van de aanhangige procedures en hebben zij evenmin de financiële draagkracht om zich tegen de subpoena te verzetten.[25]

23. *NAACP* v. *Alabama*, 357 U.S. at 459.
24. *In re Subpoena Duces Tecum to America Online, Inc.*, Misc. Law No. 40570, 2000 WL 1210372, (Va.Cir.Ct.2000). Opmerkelijk in deze zaak was het feit dat niet alleen de gedaagde, maar ook de eiser anoniem wenste te blijven. De laatste trad daarom op onder het pseudoniem 'Anonymous Publicly Traded Company' ('APTC'). Het United States Court of Appeals for the Fifth Circuit ging naar aanleiding hiervan kort in op de vraag hoe de anonimiteit van partijen zich verhoudt tot het recht van het publiek op openbare rechtspraak en oordeelde dat "the public's right to scrutinize governmental functioning is not so completely impaired by a grant of anonymity to a party as it is by closure of the trial itself. Party anonymity does not obstruct the public's view of the issues joined or the court's performance in resolving them. The assurance of fairness preserved by public presence at a trial is not lost when one party's cause is pursued under a fictitious name. These crucial interests served by open trials are not inevitably compromise by allowing a party to proceed anonymously". *Doe v. Stegall*, 653 F. 2d 180, 185 (1985).
25. In *Melvin* v. *Doe* diende America Online (AOL) een 'brief amicus curiae' in waarin zij stelde in drie opzichten belang te hebben bij duidelijke juridische criteria voor de uitreiking en handhaving van John Doe subpoenas: (1) als internetprovider is AOL verplicht om de privacy en free speech-belangen van haar klanten te beschermen, (2) het ontbreken van duidelijke criteria leidt tot hoge kosten bij de afhandeling van subpoenas en vergt inzet van personeel en (3) de mogelijkheid om anoniem of onder een pseudoniem te handelen is een essentiële voorwaarde voor de ontwikkeling van het internet. Het ontbreken van deze mogelijkheid is dus indirect ook een bedreiging voor AOL. Zie Brief America Online 2000.

4.5 Anti-SLAPP statutes

In de voorgaande paragrafen werd beschreven hoe anonieme gedaagden worden beschermd door de procedurele regels van het discovery proces en de California Code of Civil Procedure. In deze paragraaf komt een andere vorm van wettelijke bescherming aan de orde. In veel staten van de VS gelden zogenaamde 'anti-SLAPP statutes'. Deze regelingen zijn bedoeld om een halt toe te roepen aan civiele procedures die het publieke debat belemmeren, ook wel aangeduid als 'Strategic Lawsuits Against Public Participation', of kortweg 'SLAPPs'. Wanneer een John Doe procedure is aangespannen wegens anonieme uitlatingen die de bescherming van het First Amendment verdienen, kan de gedaagde een anti-SLAPP statute aanwenden om de onthulling van zijn identiteit tegen te gaan.[26] Anti-SLAPP statutes zijn in de regel ook van toepassing op online uitlatingen en kunnen dus ook worden ingeroepen door anonieme internetgebruikers.

Het effect van SLAPPs op het publieke debat verdient enige toelichting. Kenmerkend voor deze procedures is dat de eiser niet in de eerste plaats uit is op het verhalen van schade. Zijn voornaamste doel is het tot zwijgen brengen van critici. SLAPPs hebben dus een 'strategisch' karakter. Zoals Lidsky beschrijft komen strategische doelen zeer duidelijk naar voren in het grote aantal SLAPPs dat door bedrijven wordt aangespannen wegens 'corporate defamation' op het internet.[27] Laatstgenoemd verschijnsel staat inmiddels bekend als 'cybersmearing'. Napels en Maher omschrijven cybersmearing als "the act of communicating a false, disparaging, or defamatory remark about a company, its management or stock".[28] In veel gevallen is de gedaagde anoniem, zodat ook sprake is van een John Doe lawsuit.

De hierboven reeds aangehaalde zaak *Dendrite* is een typische voorbeeld van anonieme cybersmearing. Het farmaceutische bedrijf Dendrite International dagvaardde in deze procedure 4 anonieme internetgebruikers wegens uitlatingen op een message board van Yahoo!. De gedaagden, waarvan 2 blijkens de internetberichten huidige of voormalige werknemers van Dendrite zijn, werden onder andere beschuldigd van 'breach of contract', 'breach of fiduciary duty', 'defamation' en 'misappropriation of trade secrets'. Zij zouden het management van Dendrite valselijk hebben beschuldigd van frauduleuze praktijken. Zo beweerde John Doe 3 dat het management heimelijk geprobeerd had het bedrijf te verkopen en had John Doe 4 zich schuldig gemaakt aan de verspreiding van

26. Begin 2005 hadden minstens 23 staten een anti-SLAPP statute. Zie voor een overzicht <http://www.casp.net/menstate.html>. Zie voor een uitgebreide behandeling van de problematiek rond SLAPPs Pring & Canan 1996.
27. Lidsky 2000, 877-883.
28. Naples & Maher 2002. Het tegenovergestelde van 'cybersmearing', in het Nederlands vrij te vertalen als 'digitaal moddergooien', is het minder vaak voorkomende 'cyberhyping', waarbij de aandelenkoersen van het becommentarieerde bedrijf de hoogte in gaan: "(…) in few hours a company's reputation can be damaged, its trade secrets revealed, its stock price slammed ('cybersmearing') or sent through the ceiling ('cyberhyping') by a few anonymous comments posted on an Internet bulletin board." Zie Brown & Raysman 2001.

vertrouwelijke bedrijfsinformatie. Illustratief voor de toonzetting van de berichten was de boodschap van 'Sonofthethunder', een van de anonieme gedaagden:

> "Anybody else notice that since May, Dendrite's world class upper management team has been exercising their options and unloading their stock? Doesn't show much confidence, gang, now does it? On the other hand, maybe a Porsche dealer was running a really good sale… Now how does that saying go … something like 'Rats deserting a sinking ship."[29]

Opmerkingen over de financiële situatie van een bedrijf, beschuldigingen van fraude of beledigingen aan het adres van directieleden kunnen resulteren in koersdalingen en een dalend vertrouwen van aandeelhouders. Ook Dendrite stelde dat de koers van haar aandelen telkens na het verschijnen van de bestreden berichten sterk gedaald was.

De daadwerkelijke of potentiële financiële schade als gevolg van de bestreden uitlatingen is zeer groot. De kans dat de verantwoordelijke internetgebruiker deze schade zal kunnen vergoeden is in de typische SLAPP daarentegen verwaarloosbaar klein. Voor het getroffen bedrijf is dit echter geen reden om van procederen af te zien. Er is immers een dringende economische noodzaak om negatieve uitlatingen te weerspreken en de geschonden reputatie te beschermen. Aankondigingen in de media van de beslissing om de juridische strijd aan te gaan met anonieme internetgebruikers maken soms deel uit een public relations campagne waarin een alternatieve versie van de feiten wordt geboden en waarin de boodschap wordt overgebracht dat de onderneming sterk en stabiel is.[30] Ook wanneer de claim van de eiser geen enkele kans van slagen heeft kan dergelijk handelen de schadelijke effecten beperken.

Het 'chilling effect' dat uitgaat van SLAPPs speelt een belangrijke rol in de discussie over de dynamiek van het publieke debat in de online omgeving en de regulering van anonieme uitingen. Het risico bestaat dat procedurele middelen misbruikt worden om ongewenste maar legitieme kritiek de mond te snoeren. In een SLAPP wordt aan de gedaagde en aan andere potentiële critici een duidelijk signaal gegeven dat kritische uitlatingen niet zonder gevolg zullen blijven. Kenmerkend in de typische SLAPP is in dit verband het verschil in macht en financiële draagkracht tussen eiser en gedaagde. De eiser beschikt over voldoende financiële middelen om louter op basis van strategische redenen door te procederen, ook als zijn vordering geen reële kans van slagen heeft, terwijl de kosten van een procedure voor de gedaagde een onoverkomelijk probleem kunnen zijn. In een 'John Doe/CyberSLAPP'-geval is het potentiële chilling effect nog groter

29. Sonofthethunder 2001.
30. In sommige gevallen lijkt het erop dat de procedure louter om pr-redenen werd aangespannen. De beslissing om te procederen kan door aandeelhouders worden gezien als een signaal dat de onderneming sterk en slagvaardig is en dat men negatieve geruchten niet moet geloven. Zie hierover Lidsky 2000, p. 878-880: "By announcing its decision to file suit, the company appears to respond aggressively to the Internet rumor-mongers who revel in reports of its demise."

dan in gevallen waarin de identiteit van de gedaagde al bekend is. De gedaagde wordt immers niet alleen geconfronteerd met een procedure, maar loopt eveneens het risico dat zijn identiteit wordt onthuld.[31] Volgens velen vormen John Doe-procedures en SLAPPs daarom een bedreiging voor de open discussie op het internet dat, door de mogelijkheden die het biedt om met beperkte financiële middelen een groot publiek te bereiken, een krachtig instrument kan zijn voor het gelijktrekken van machtsongelijkheden en het wegnemen van toegangsdrempels tot het publieke debat. Deze belofte wordt teniet gedaan wanneer machtige ondernemingen internetgebruikers dwingen tot overdreven zelfcensuur.

Ook de Californische wetgever meende dat het aantal SLAPPs noopte tot wettelijke maatregelen. Belemmering van het publieke debat met behulp van procedurele middelen moest worden tegengegaan.[32] In par. 425.16. van de California Code of Civil Procedure is daarom een anti-SLAPP statute opgenomen. Een SLAPP wordt hierin gedefinieerd als "a cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States or California Constitution in connection with a public issue". Indien de gedaagde in een civiele procedure van mening is dat sprake is van een SLAPP kan hij reeds aan het begin van de procedure een 'special motion to strike' indienen.[33] Het proces van pre-trial discovery wordt dan opgeschort.[34] Voor de anonieme gedaagde betekent dit dat de onthulling van zijn identi-

31. John Doe lawsuits en SLAPPs hebben aanleiding gegeven tot uitgebreide beschouwingen over de juridisch-dogmatische problemen die zijn verbonden aan de toepassing van het First Amendment in de context van het internet. Verschillende Amerikaanse juristen betogen dat de traditionele theorie omtrent de bescherming van het First Amendment online niet onverkort toegepast zou kunnen worden. Zo zou het traditionele onderscheid in beschermingsniveau tussen 'media defendants' (omroepen, kranten, uitgevers e.d.) en 'non media defendants' door de komst van het internet achterhaald zijn. Ook de 'actual malice standard', die bedoeld is om te voorkomen dat onpopulaire gedaagden voor ondergeschikte feitelijke onjuistheden worden gestraft met een verlammende aansprakelijkheid, is toegespitst op traditioneel journalistiek speurwerk en verslaggeving en zou daardoor niet geschikt zijn om de uitlatingen van anonieme internetgebruikers te beoordelen. De gemiddelde internetgebruiker heeft immers niet de opleiding en ervaring van een journalist en beschikt evenmin over een kritische redactie of bijstand van een advocaat. Hij baseert zijn uitlatingen in veel gevallen op secundaire bronnen en wordt niet door een professionele ethiek aangespoord om zijn mening nauwkeurig naar voren te brengen. De internetcultuur in het algemeen, en de informele cultuur van 'message boards' in het bijzonder, zou internetgebruikers juist aansporen tot het doen van roekeloze uitlatingen. Zie Lidsky 2000; Wein 2002 en O'Brien 2002. Lidsky constateert in 2000 dat het First Amendment geen adequate bescherming biedt. Zie in haar artikel de paragraaf over John Doe and First Amendment Doctrine en noot 256. Zie ook p. 905 en verder.
32. Zie de overweging in par. 425.16.(a) C.C.P.
33. Een special motion to strike, uitgevaardigd op basis van het anti-SLAPP statute, verschilt van een motion to quash in het discovery proces doordat een motion to quash alleen bedoeld is om de subpoena te vernietigen, terwijl de motion to strike beoogt om de hele procedure niet-ontvankelijk te laten verklaren.
34. Par. 425.16.(g) C.C.P.

teit in ieder geval is verhinderd totdat de rechter heeft beoordeeld of de vordering van de eiser kans van slagen heeft.[35] Indien dit niet het geval is wordt de motion to strike toegewezen en de vordering niet-ontvankelijk verklaard.[36]

De bescherming onder de Californische anti-SLAPP statute is, in vergelijking met anti-SLAPP statutes in andere staten, om drie redenen zeer sterk. In de eerste plaats beschermt de regeling bijna alle uitingen die betrekking hebben op publieke aangelegenheden, in tegenstelling tot andere anti-SLAPP statutes waarvan de reikwijdte bijvoorbeeld beperkt is tot bepaalde vormen van political speech of klokkeluiden. Als een door de regeling beschermde uitlating wordt aangemerkt:

> "(1)any written or oral statement or writing made before a legislative, executive, or judicial proceeding, or any other official proceeding authorized by law;
> (2) any written or oral statement or writing made in connection with an issue under consideration or review by a legislative, executive, or judicial body, or any other official proceeding authorized by law;
> (3) any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest;
> (4) or any other conduct in furtherance of the exercise of the constitutional right of petition or the constitutional right of free speech in connection with a public issue or an issue of public interest."[37]

In de tweede plaats rust de bewijslast op de eiser. Hij dient aan te tonen dat zijn vordering kans van slagen heeft. De motion to strike wordt toegewezen tenzij de rechter vaststelt "that the plaintiff has established that there is a probability that the plaintiff will prevail on the claim".[38] Tenslotte kan de gedaagde, wanneer is vastgesteld dat inderdaad sprake is van een SLAPP, zijn proceskosten volledig verhalen op de eiser.[39] Deze omstandigheid maakt het voor hem aanzienlijk eenvoudiger om juridische bijstand te vinden. De eiser wordt zodoende gestraft voor zijn poging om het publieke debat te belemmeren.

35. Par. 425.16.(c) C.C.P. voorziet in een sanctie op misbruik van de motion to strike. Indien aan de kant van de gedaagde dergelijk misbruik wordt vastgesteld is hij op zijn beurt verplicht 'costs and reasonable [sic] attorney's fees' te vergoeden. In de praktijk bleek de Californische anti-SLAPP regeling overigens ook vaak te worden misbruikt. Om dit misbruik te gaan werd per 1 januari 2004 een nieuwe bepaling aan de regeling toegevoegd die de werking van de SLAPP-regeling beperkt. Krachtens par. 425.17 C.C.P. kunnen anti-SLAPP motions nu niet langer worden ingediend (1) tegen vordering die zijn worden ingediend in het algemeen belang of namens 'the general public', of (2) wanneer sprake is een vordering tegen commerciële uitlatingen of tegen onrechtmatig gedrag van een onderneming.
36. Par. 425.16.(b)(1) C.C.P.
37. Par. 425.16.(e) C.C.P.
38. Par. 425.16.(b)(1) C.C.P.
39. Par. 424.16.(c) C.C.P.

4.6 Identificatie van peer-to-peergebruikers

In deze paragraaf komt een categorie van procedures aan de orde die recentelijk veel aandacht heeft getrokken. Het gaat om zaken waarin organisaties van auteursrechthebbenden pogingen doen om de identiteit te achterhalen van internetgebruikers die zich bezighouden met de verspreiding van auteursrechtelijk beschermde film- en muziekbestanden.

De genoemde procedures onderscheiden zich van andere John Doe procedures en SLAPPs doordat zowel bij de eiser als bij de gedaagde andersoortige belangen een rol spelen. De eiser is niet in de eerste plaats uit op het voorkomen van imagoschade, zoals in de meeste SLAPPs, maar wenst een ander, commercieel belang te beschermen, namelijk: de exploitatie van zijn auteursrechten. Pogingen om uitwisselaars van bestanden te ontmaskeren zijn in wezen bedoeld om de ontwikkeling van een voor het business model van de muziek- en filmindustrie zeer bedreigende technologie zo veel mogelijk tegen te gaan.

Ook aan de kant van de gedaagde liggen de zaken enigszins anders omdat doorgaans geen sprake is van werkelijke 'uitingen' maar van digitale bestanden die als zodanig geen individuele boodschap van de verspreider in zich dragen. Waar de gedaagde in een SLAPP een beroep doet op het maatschappelijke belang van het publieke debat, gaat een dergelijk beroep bij de verspreiding van de genoemde bestanden in het algemeen niet op. Dit neemt niet weg dat pogingen tot identificatie in strijd kunnen komen met het recht om ongehinderd en anoniem informatie te verspreiden en te ontvangen.

Peer-to-peer-systemen kwamen eind jaren negentig in zwang.[40] Het programma 'Napster' was in 1999 het eerste programma dat het grote publiek bereikte. Nog in datzelfde jaar werd het gelijknamige bedrijf dat het programma exploiteerde aangeklaagd wegens auteursrechtinbreuk door de Recording Industry Association of America (RIAA). Toen na verschillende procedures tegen Napster en andere aanbieders van filesharingsoftware bleek dat daarmee de verspreiding van muziekbestanden niet adequaat kon worden tegengehouden, besloot men ook individuele gebruikers aan te pakken. Er werden grootschalige mediacampagnes opgezet waarbij werd aangekondigd dat peer-to-peergebruikers zouden worden opgespoord en beboet.

De RIAA meende haar vorderingen tot identificatie van filesharers te kunnen baseren op een aantal bepalingen in de Amerikaanse Copyright Act, die in 1998, nog voor de opkomst van peer-to-peer-technologie, door het Amerikaanse Congres middels de Digital Millenium Copyright Act (DMCA) was aangepast aan het digitale tijdperk. De DMCA reguleerde onder andere de aansprakelijkheid van providers voor auteursrechtinbreuken. Het 'safe harbor'-systeem in par. 512 sluit providers uit van aansprakelijkheid

40. Zie voor een uiteenzetting van de technische en juridische aspecten van peer-to-peer software en filesharing Alberdingk Thijm 2003; Van Daalen & Ekker 2003. Zie voor een internationaal overzicht van juridische procedures tegen aanbieders en gebruikers van file-sharingsoftware OECD 2005, p. 98-104.

zolang zij voldoen aan de daar genoemde voorwaarden. Op aandringen van de film- en muziekindustrie is in deze afdeling ook een bepaling opgenomen die het mogelijk maakt om anonieme inbreukmakers op te sporen met behulp van een subpoena. par. 512(h) van de Copyright Act luidt:

> "(1) Request. – A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.
> (2) Contents of request – The request may be made by filing with the clerk –
> (A) a copy of a notification described in subsection (c)(3)(A);
> (B) a proposed subpoena; and
> (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.
> (3) Contents of subpoena. – The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider."

De schriftelijke notification of claimed infringement die aan de provider wordt verstrekt, moet worden ondertekend door of namens de auteursrechthebbende en dient onder andere aan te geven op welk auteursrechtelijk beschermd werk de inbreuk betrekking heeft en waar het inbreukmakende materiaal zich precies bevindt.[41] Wanneer de notificatie aan de gestelde eisen voldoet en aan subsection (2)(B) en (2)(C) is voldaan, wordt de voorgestelde subpoena door de griffier van het District Court onverwijld uitgereikt en ondertekend. Vervolgens kan deze door de aanvrager worden overhandigd aan de service provider.[42] Na ontvangst van de subpoena en de notificatie dient de service provider de identificerende informatie onverwijld aan de auteursrechthebbende ter beschikking te stellen. De uitreiking en de handhaving van de subpoena en de sancties op het niet voldoen daaraan worden beheerst door de Federal Rules of Civil Procedure.[43]

De toepassing van par. 512(h) door de RIAA leidde tot een felle juridische strijd. Provider Verizon weigerde na ontvangst van een subpoena to identify infringer de namen van de vermeende inbreukmakers prijs te geven. In *Verizon* v. *RIAA* werd door het Court of Appeals for the District of Columbia vastgesteld dat de tekst en strekking van par. 512 van de Copyright Act het gebruik van de subpoena to identify infringer alleen toestaan indien de inbreukmakende bestanden zich bevinden op de systemen van de provider.[44]

41. 17 U.S.C. par. 512(h)(2)(A) Jo. par. 512(c)(3)(A)(i) e.v.
42. 17 U.S.C. par. 512(h)(4).
43. 17 U.S.C. par. 512(h)(6).
44. *Recording Industry Association of America, Inc.* v. *Verizon Internet Services, Inc.*, Case No. 03-7015 (D.C. Cir., December 19, 2003).

Dit volgde onder andere uit het feit dat de voor de subpoena vereiste notification of claimed infringement deel uitmaakt van de bepalingen inzake het zogenaamde 'notice-and-take-down'-systeem, dat de provider verplicht om beweerdelijk inbreukmakend materiaal dat zich bevindt op haar systemen terstond te verwijderen of ontoegankelijk te maken zodra zij van de inbreuk op de hoogte is gesteld. Voorzover de rol van de provider zich bij het uitwisselen van bestanden via peer-to-peer systemen beperkt tot de enkele doorgifte van informatie van eindgebruiker naar eindgebruiker kon de subpoena to identify infringer in de strijd tegen filesharing niet worden gebruikt.[45]

Nu het Court of Appeals reeds op basis van een tekstuele interpretatie van de Copyright Act concludeerde dat par. 512(h) niet kon worden toegepast op gevallen van filesharing, kwam zij niet toe aan de behandeling van de constitutionele bezwaren die door Verizon c.s. naar voren worden gebracht tegen deze bepaling. Volgens Verizon is par. 512(h) in strijd met het First Amendment omdat niet is voorzien in afdoende waarborgen voor de bescherming van het recht op anonimiteit van internetgebruikers. De Electronic Frontier Foundation (EFF) diende een amicus brief in die werd gesteund door 47 Amerikaanse belangenorganisaties van providers en consumenten. Centraal daarin stond de vraag of het uit het First Amendment voortvloeiende recht op anonimiteit en het recht op privacy kunnen worden geschonden middels een subpoena die vaak het resultaat is van haastig papierwerk en die enkel is gebaseerd op een 'good faith allegation' dat sprake is van auteursrechtinbreuk.[46] De inhoud van de subpoena en de waarheidsgetrouwheid van de bewering dat sprake is van auteursrechtinbreuk worden noch door de griffier, noch door de rechter beoordeeld. Als aan de formele eisen van par. 512(h) is voldaan wordt de subpoena zonder verdere toetsing uitgereikt. Hierdoor komt de taak om internetgebruikers te beschermen tegen ongerechtvaardigde inbreuken in feite te liggen bij de service provider.

Het District Court had overwogen dat het First Amendment i.c. slechts minimale bescherming bood omdat par. 512(h) zich richt op beweerdelijke auteursrechtinbreuk.[47] Dit standpunt miskende volgens EFF c.s. het feit dat op het moment dat de subpoena wordt uitgereikt nog niet onomstotelijk vaststaat dat daadwerkelijk sprake is van een inbreuk. Een bewezen inbreuk op het auteursrecht wordt weliswaar niet beschermd door het First Amendment, maar de enkele beschuldiging daarvan kan een inbreuk op de uit het First Amendment voortvloeiende rechten niet rechtvaardigen.[48] Dat dit leidt tot mis-

45. Voor zover de activiteiten van de provider zich beperken tot de enkele doorgifte van informatie, vallen zij onder de bepalingen van par. 512(a) van de Copyright Act. Deze bepalingen zijn vergelijkbaar met de artikelen 12 t/m 14 van de richtlijn elektronische handel. Zie par. 9.4.1.
46. Alliance for Public Technology 2003.
47. *Second Subpoena Op.*, 2003 WL 1946489, at 12.
48. "A selfinterested declaration of a 'good faith' belief that speech or association is unprotected is not sufficient to shift the burden to the speaker to defend his or her presumptively protected activities on the Internet." Zie Brief Verizon 2003.

bruik is in de praktijk reeds gebleken. De RIAA heeft de plank herhaaldelijk volledig misgeslagen. Zo bleek in enkele gevallen dat op de verspreide informatie in het geheel geen auteursrecht rustte.

De bepalingen in de Copyright Act zijn volgens Verizon eveneens in strijd met het Fifth Amendment, dat adequate procedurele waarborgen verlangt voordat vrijheidsrechten kunnen worden ontnomen.[49] De omstandigheid dat rechten enkel op basis van een verklaring van een van de partijen worden beperkt zonder dat daarbij zwaarwegende redenen hoeven te worden aangetoond en zonder dat degene die in zijn belangen wordt geraakt op de hoogte wordt gesteld en de gelegenheid krijgt om zich te verweren is in de rechtspraak reeds eerder aanleiding geweest om strijd met het Fifth Amendment vast te stellen.[50] Een laatste bezwaar is het feit dat de DMCA niet voorziet in effectieve santies voor auteursrechthebbenden die de subpoena to identify infringer misbruiken. par. 512(f) schept weliswaar een schadevergoedingsactie voor degene die schade heeft geleden als gevolg van een ongegronde kennisgeving van auteursrechtinbreuk en de daaruit voortvloeiende verstrekking van identificerende gegevens, maar dit lijkt onvoldoende om de muziekindustrie te dwingen tot een zorgvuldig gebruik van de subpoena.

Na *Verizon* kan de subpoena to identify infringer kan niet langer worden gebruikt in de strijd tegen filesharing. De RIAA moet de identiteit van inbreukmakers nu via de normale John Doe procedure zien te achterhalen. Het is echter niet uitgesloten dat de Amerikaanse wetgever dit gat in de bescherming van het auteursrecht met wettelijke maatregelen zal dichten.

4.7 Conclusie

In het vorige hoofdstuk bleek dat mogelijkheden om anoniem te communiceren naar het oordeel van het Supreme Court ook op het internet bescherming verdienen. Maatregelen ter identificatie van internetgebruikers kunnen onder omstandigheden in strijd komen met het First Amendment. In dit hoofdstuk kwam naar voren dat Amerikaanse internetgebruikers daarnaast beschikken over een zelfstandig en afdwingbaar constitutioneel recht om anoniem informatie te verspreiden en te communiceren. Met dit recht kunnen zij de doorbreking van hun anonimiteit aanvechten.

Ook in de lagere rechtspraak is grote aandacht voor de constitutionele waarden die met de onthulling gemoeid zijn. Met name het 'chilling effect' dat onthulling van anonieme internetgebruikers kan hebben op het publieke debat wordt zeer serieus genomen. In de praktijk blijkt dat regulering van het publieke debat online niet kan worden overgelaten aan de 'invisible hand' waarop optimistische aanhangers van de marketplace of ideas vertrouwen. De machtsongelijkheden zijn daarvoor te groot. Grote spelers duwen

49. Het Fifth Amendment luidt, voor zover hier van belang: "No person shall be (…) deprived of life, liberty, or property, without due process of law; (…)."
50. *Connecticut* v. *Doehr*, 501 U.S. 1, 10 (1991).

de kleintjes uit de publieke arena door eerst hun masker af te rukken en hen vervolgens te belagen met schadevergoedingsacties. Een aanzienlijk aantal statelijke wetgevers is tot de conclusie gekomen dat het publieke debat online door middel van overheidsingrijpen moet worden beschermd tegen misbruik van procedurele middelen.

De constitutionele bescherming van anonimiteit roept de vraag op hoe het recht van een internetgebruiker om anoniem te blijven in een concreet geval moet worden afgewogen tegen het belang van de eiser in een John Doe procedure bij de handhaving van zijn rechten. De hierboven besproken balancing tests voorzien in criteria voor een dergelijke afweging. Zoals nog zal blijken vertonen zij grote gelijkenissen met de in het Nederlandse recht geldende criteria. De wettelijke regels rondom pre-trial discovery en de regelgeving omtrent SLAPPs creëren daarentegen een systeem dat op verschillende punten afwijkt van het Nederlandse. In de eerste plaats kan de John Doe procedure worden aangespannen tegen de anonieme internetgebruiker zelf. De onthulling van identiteit van de gedaagde en de vordering van de eiser jegens hem kunnen hierdoor in één en dezelfde procedure aan de orde komen. In de tweede plaats zijn, om effectieve bescherming van de anonymus te garanderen, verschillende waarborgen voorgesteld die in Nederland nog niet bestaan, zoals een verplichting van de provider om de anonymus te notificeren en een mogelijkheid van de laatste om zich via de provider tegen verstrekking te verzetten.

Waar het de bescherming van het auteursrecht betreft heeft de principiële benadering van het Supreme Court en statelijke wetgevers moeten wijken voor commerciële belangen. Het gemak waarmee identificerende gegevens onder de Amerikaanse Copyright Act kunnen worden verkregen, staat in schril contrast tot de afweging van belangen in andere John Doe procedures. Alle waarborgen lijken te vervallen zodra er een vermoeden is van auteursrechtinbreuk. Plotseling komt er aan de beoordeling van de verstrekking dan geen rechter meer te pas en hoeft er geen 'prima facie case' aannemelijk te worden gemaakt.

5 Anonieme geschriften in Nederland

5.1 Inleiding

De hiernavolgende hoofdstukken gaan in op de regulering van anonieme communicatie in het geldende Nederlandse recht. Voordat wij hieraan toekomen dient echter enige aandacht te worden besteed aan de Nederlandse geschiedenis. Dit is nuttig omdat identificatie- en registratieverplichtingen ook in ons land van oudsher een rol hebben gespeeld als ondersteuning van toezicht op de inhoud en de verspreiding van informatie. De Nederlandse situatie wijkt op bepaalde punten echter enigszins af van de Amerikaanse. Ons land kende door de eeuwen heen verschillende periodes van vijandige bezetting waarin strenge verboden op anonieme publicaties golden. Bovendien speelde de verspreiding van anonieme geschriften al een rol van maatschappelijke betekenis in de zestiende eeuw, toen het Amerikaanse continent nog nauwelijks gekoloniseerd was.

Een andere belangrijke reden om de historie in ogenschouw te nemen is dat zich bij de drukpers reeds enkele lijnen aftekenen die bij andere communicatiemiddelen telkens terugkomen. Het gaat daarbij met name om het verband tussen anonimiteit en machtsuitoefening en om de verhouding tussen verschillende actoren in het communicatieproces. Rondom het anonieme geschrift ontvouwt zich een onophoudelijk machtsspel tussen enerzijds overheden die de verspreiding van politieke en religieuze ideeën willen beteugelen en anderzijds auteurs die zich aan verboden op anonimiteit weinig gelegen laten liggen. Daarbij nemen drukkers en uitgevers een spilfunctie in als verspreiders van de bestreden geschriften en als subjecten van regulering. In het juridische domein komt als gevolg van de felle bestrijding van anonieme geschriften langzamerhand de vraag op in hoeverre uit de uitingsvrijheid een recht volgt om anoniem te publiceren. Ook het verband met de bescherming van het publieke debat wordt gaandeweg duidelijk.

5.2 De Spaanse overheersing

Door de geweldige expansie van de boekdrukkunst wordt West-Europa in het begin van de zestiende eeuw overspoeld met voornamelijk godsdienstige boeken.[1] De maatschappelijke impact van deze ontwikkeling is enorm, temeer nu deze samenvalt met de opkomst van de Hervorming. Kerkelijke en wereldlijke autoriteiten zijn verontrust. Zij vrezen het propagandistische potentieel van de bijbel als bron van kennis en geloof en als middel voor de verspreiding van nieuwe ideeën.[2] Zelfbewuste bijbellezers zouden maar al te snel van de rechte leer af kunnen dwalen. Al snel voelt de Spaanse overheerser zich gedwongen de controle op de verspreiding van informatie te intensiveren. Luther en zijn aanhangers worden in de periode 1520 tot 1540 bestookt met een reeks van pauselijke bullen, keizerlijke decreten en plaatselijke verboden waarin de verspreiding van ketterse geschriften steeds strenger wordt veroordeeld en strafbaar gesteld.[3]

In 1521 verbiedt Karel V het verkopen en in bezit hebben van de boeken van Luther en zijn aanhangers. Als aanvulling hierop wordt het verboden om anoniem te publiceren. Het eerste expliciete verbod op het anoniem uitgeven van geschriften vindt men in het derde keizerlijke plakkaat tegen de verboden boeken van 24 september 1525. Dit plakkaat vermeldt de boeken van Luther en aanhang, maar ook die van "andere inden heyliger scriften mit Luther gevoelende, mitsgaders alle die boucken die sonder tytel geprent zijn".[4] Het keizerlijke plakkaat van 18 januari 1527 stelt voor het eerst de eis dat drukkers in alle uitgaven hun naam en merk moeten plaatsen.[5] In 1559 verbiedt de eerste pauselijke Index alle boeken door ketters geschreven, over welk onderwerp ook, alle anonieme publicaties vanaf 1519 gedrukt of nog te drukken, alle boeken die zonder naam van de drukker of plaats van herkomst verschijnen en alle werken, die niet eerst door de bisschop of de inquisiteur van een 'imprimatur' zijn voorzien.[6]

1. De godsdienstige geschriften beslaan in de periode tot 1540 tweederde van de totale boekproductie. Tussen 1522 en 1545 verschijnen er in totaal ongeveer tachtig Nederlandstalige bijbeldrukken. In de periode 1520-1566 werden alleen al van Nederlandstalige bijbels in de Noordelijke en Zuidelijke Nederlanden ongeveer 200.000 exemplaren verspreid, op een bevolking van circa vijf miljoen mensen. Den Hollander 2003, p. 5-7.
2. Het Keizerlijk plakkaat van 24 september 1525 stelt dat allerlei dwalingen zijn ontstaan doordat "die leecke ende ongeleerde persoenen die Duytsche evangelien ende andere geestelicke scriften dagelicx lesen naer hueren verstande (…)". Den Hollander 2003, p. 8 en 22.
3. Zie Duke & Tamse 1987, p. 30 e.v.
4. Kronenberg veronderstelt dat waar het plakkaat spreekt van "alle die boucken die sonder tytel geprent zijn" waarschijnlijk de anoniem verschenen boeken bedoeld worden. Het gaat dus niet om boeken die in het geheel geen titel hadden maar om boeken zonder auteursnaam. Boeken zonder titel zijn wel bekend maar deze kwamen voornamelijk voor in de 15e eeuw. Kronenberg 1947, p. 16-17.
5. Vermoedelijk kwam dit bevel reeds voor in een eerdere missive: "Tenminste één plaatselijke Antwerpse verordening – en dat zijn gewoonlijk de echo's der keizerlijke plakkaten – van 14 Febr. 1524/1525 schrijft uitdrukkelijk voor naam van auteur, van drukker en tevens diens merk, en jaar en plaats der uitgave te vermelden." Kronenberg 1947, p. 18 en p. 118-119.
6. Van Gelder 1947, p. 13-14.

Auteurs en drukkers trekken zich van de verboden maar weinig aan. In de Nederlandse edities van de traktaten van Luther tussen 1529 en 1540 wordt slechts bij uitzondering een naam vermeld.[7] Anderzijds blijven sommige auteurs en drukkers, ook nadat hun uitgaven in plakkaten reeds als verboden boeken zijn vermeld, naam en adres juist wel vermelden. Zodoende riskeren zij gevangenschap, geldboetes, verbeurdverklaring van goederen, verbanning of zelfs de doodstraf.[8] Het geringe effect van de strenge verboden blijkt uit de herhaaldelijke afkondiging ervan en uit de toenemende wreedheid van de straffen. De handhaving van de wetgeving werd onder andere bemoeilijkt doordat lokale magistraten vaak geen medewerking verleenden.[9]

5.3 De Republiek der Verenigde Nederlanden

Met de afzwering van Filips II in 1581 breekt een nieuwe periode aan. In de Republiek der Verenigde Nederlanden wordt de vrijheid van geweten afgekondigd en artikel 13 van de Unie van Utrecht waarborgt voor een ieder de vrije uitoefening van de eredienst. De Protestanten worden van knellende banden bevrijd doordat het niet langer mogelijk is boeken te verbieden op grond van ketterij. Er blijft nog wel censuur bestaan. Een plakkaat van 20 december 1581 verbiedt lasterschriften tegen de overheid en de provinciën en de publicatie van anonieme geschriften.[10] De censuur richt zich niet langer alleen op geschriften die godsdienstige zaken of de bijbel aanvallen. De aandacht verschuift enigszins naar staatkundige en politieke geschriften.[11] Elke provincie van de Vereenigde Nederlanden heeft op dit gebied haar eigen wetgeving zodat afhankelijk van de omstandigheden in de verschillende gebiedsdelen verschillende plakkaten worden uitgevaardigd. Vooral in Holland, waar de meeste boeken werden gedrukt, gelden vele bepalingen die de uitgave van 'fameuse libellen' en andere schadelijke en oproerige geschriften verbieden of waarin de wijze van verspreiding van kerkelijke boeken wordt gereguleerd.[12] De verbo-

7. Alleen al van de werken van Luther zijn in het tijdvak tot 1540 minstens een twintigtal drukken bekend die zonder naam werden gepubliceerd. Een voorbeeld is de Nederlandse vertaling van Luther's 'Betbüchlein' van 1523, zonder naam van plaats en drukker of jaartal verschenen, die werd uitgegeven onder de onschuldig klinkende titel 'Een deuoet ende zeer schoon bedeboxken uyt die heylighe schrifftuer ghetrocken daer int corte begrepen is wat een kersten mensch schuldich is te weten'. Kronenberg 1947, p. 17. Zie voor meer voorbeelden Kronenberg 1947, p. 54 en p. 118-119.
8. De straffen op het bezit van verboden boeken worden in 1530 te Leiden voor het eerst gelijkgesteld aan die voor ketterij: de dood en verbeurdverklaring van alle goederen. Zie Den Hollander 2003, p. 10 alsmede de daar opgenomen verwijzingen. Zie ook Diemer over het plakkaat van 20 augustus 1556 tegen de boeken van Luther en andere ketters. "Voor het geval de schuldigen hun dwaling toegeven, moeten de mannen met het zwaard worden omgebracht en de vrouwen levend begraven. In het andere geval wordt men gevierendeeld." Diemer 1937, p. 40. Zie voor andere voorbeelden Kronenberg 1947, p. 92, 128 en 133.
9. Duke & Tamse 1987, p. 32 e.v.
10. Zei Duke & Tamse 1987, p. 110. Zie over dit placaat ook Van Gelder 1947, p. 104-105.
11. Bodel Nyenhuis 1892, p. 96-97.
12. Idem, p. 209.

den zijn meestal gericht op specifieke publicaties of specifieke onderwerpen waarvoor preventieve censuur en een verbod van anonimiteit geldt.[13] Zo worden bijvoorbeeld talloze plakkaten uitgevaardigd om smaadschriften tegen Willem van Oranje tegen te gaan. Tijdens de onderhandelingen over het sluiten van een wapenstilstand met Spanje wordt een verbod afgekondigd tegen de vele paskwillen[14] en naamloze geschriften waarin men tracht aan te tonen dat deze slechts noodlottige gevolgen zal hebben.[15]

Ondanks de vele verboden en strafbepalingen is er een ruime vrijheid om godsdienstige en politieke meningen, mits op gematigde toon, te openbaren. Door het ontbreken van een centraal gezag en centrale wetgeving worden de plakkaten niet erg streng gehandhaafd. Vervolgingen komen dan ook relatief weinig voor en van een algemene preventieve censuur is evenmin sprake.[16] In de Republiek der Verenigde Nederlanden worden daardoor beduidend meer pamfletten en spotprenten uitgegeven dan elders in West-Europa. Een relatief groot deel van deze geschriften verschijnt anoniem.[17]

13. Toch zijn er in de 17e en de 18e eeuw waarschijnlijk nog vele algemene verboden op anonimiteit uitgevaardigd. Buyn vermeldt een placaat van de Staten-Generaal van 27 augustus 1608 waarin aanzienlijke premies worden uitgeloofd om de schrijver, de drukker en zelfs de zetter van verboden geschriften in handen te krijgen. Zie Buyn 1867, p. 56. In 1726 verbiedt het Hof van Holland "het drucken en publiceren van geschriften over saken van staet en religie, die dezelve in eenighe respecten zouden konnen chocqueeren, hinderlijk of nadeeligh zijn, dat niemand wie het ook zij, sig sal hebben te verstouten eenige geschriften van wat natuur dezelve ook mogen zijn, uit te geven ofte doen drucken, tenzij dat het origineel door den autheur of uitgever, die ook bekent moet zijn, is geteekent, en voor soo veel die geschriften saeken van religie of van staet en regeeringe betreffen, daarenboven gemunieert met de permissie of authoriteit daaromtrent na de ordre van den lande vereischt". Zie Schimmel 1882, p. 3.
14. Paskwil is een ander woord voor smaadschrift.
15. Zie voor een uitgebreid chronologisch overzicht Bodel Nyenhuis 1892, p. 95-184.
16. Groenveld gaat uitgebreid in op de vraag in hoeverre in de zeventiende eeuw sprake was van een onbelemmerde drukpersvrijheid. Hij schat dat tussen 1580 en 1700 in totaal niet meer dan tweehonderd publicaties werden verboden. Het systematisch toezicht op de inhoud van geschriften had echter wel zijn weerslag op het gevoel van vrijheid dat schrijvers en drukkers ervaarden. Groenveld komt tot de conclusie dat preventieve en repressieve censuur in die periode in de praktijk minder streng was dan in de rest van Europa en dat deze bovendien beperkt was tot geschriften met politieke of religieuze inhoud. Zie Groenveld 1987, m.n. p. 80 e.v.
17. In de periode 1607-1648 verschijnt zestig procent van het totaal aantal pamfletten over binnenlandse aangelegenheden zonder naam van drukker, auteur of plaats van uitgave. "Doorgaans werden eenmaal gedrukte geschriften in pakketjes van tussen tien en de vijfentwintig exemplaren in een gesloten couvert en volledig anoniem aan diverse boekverkopers toegezonden. Een tussenpersoon of winkelbedienden droegen naderhand zorg voor het incasseren van de opbrengsten. In de censuurplakkaten was het boekverkopers verplicht gesteld dergelijke anonieme zendingen direct te melden aan de magistraat of aan de schout; de verhoren van het Hof maken echter duidelijk dat zij zich aan deze verplichting niet of nauwelijks hielden. Vaak probeerde een boekverkoper wanneer het misliep het anonieme karakter van een zending aan te wenden als bewijs voor het feit dat hij de afzender eenvoudigweg niet kon kennen." Weekhout 1998, p. 108-109.

Aan het eind van de achttiende eeuw doen de opkomende verlichtingsdenkbeelden de discussie over de rechten van het volk hevig oplaaien. Ter bestrijding van de geldende plakkaten pleit men voor een praktisch onbelemmerde drukpersvrijheid.[18] Dit is ook de tijd van het ontstaan van de publieke opiniepers. De ontwikkelde laag van de bevolking wordt voor het eerst politiek bewust. De staatkundige polemiek wordt een essentieel element van de inhoud en doet nieuwe bladen ontstaan.[19] Voor het eerst zijn sporen te vinden van een maatschappelijke discussie over de wenselijkheid van naamloze geschriften. Het is goed mogelijk dat het anoniem verschijnen van het democratisch manifest 'Aan het Volk van Nederland' aan deze discussie een belangrijke impuls heeft gegeven. Joan Derk Baron van der Capellen tot den Pol, door veel historici beschouwd als de leider van de democratische tak van de patriottenbeweging, richt zich in dit pamflet tegen het bewind van Stadhouder Willem V en tegen de zich steeds uitbreidende macht van het Huis van Oranje. Hij publiceert de brochure anoniem omdat hij bevreesd is voor de militaire en politieke macht van de Stadhouder en van zijn aartsvijand Van Heiden Hompesch, de drost van Twente.[20] De angst voor politieke terreur klinkt ook door in zijn pamflet:

> "Hebt gij, o Willem, niet door ons hele land Uw spionnen, aanbrengers en verklikkers, die zich in alle gezelschappen weten in te dringen en ons van de genoegens van een gulle openhartige samenleving beroven? Zijt gij 't niet, die onze hele natie daardoor vreesachtig, achterhoudend en geveinsd gemaakt hebt en haar rondborstig, eenvoudig en oud-Hollands karakter en bestaan hebt bedorven? Door wiens toedoen, o vorst, zijn zelfs de briefwisselingen niet meer heilig?"[21]

Van der Capellen houdt Willem V verantwoordelijk voor de politieke en economische problemen waar ons land mee te kampen heeft. Hij roept om maatschappelijke hervorming en democratisering. Ook bepleit hij het vormen van democratisch verkozen comités van burgers en boeren en een burgerbewapening op democratische basis naar Zwitsers of Amerikaans model. De vrijheid van drukpers moet de basis worden van een nationale vrijheid.

---

18. Diemer 1937, p. 61.
19. Goedhart 1943, p. 15.
20. Aan het begin van zijn betoog verzekert Van der Capellen de lezer dat zijn keuze voor anonimiteit door nobele motieven is ingegeven: "Waarde medeburgers! Indien gij mij, schrijver dezes, in mijn persoon, denkwijzen en particuliere omstandigheden kende, zou ik U niet behoeven te verzekeren, dat ik geen fortuinzoeker ben; dat ik niet alleen nooit enig ambt heb bekleed, maar dat ik er zelfs nooit een bekleden noch begeren kan; dat ik derhalve volkomen belangeloos en daarom geloofwaardig ben, wanneer ik U betuig, gelijk ik voor den Alwetenden God doe, dat niets dan verontwaardiging over de goddeloze wijze, waarop ge verkocht en verraden wordt, mij dringt om mij tot U te wenden; en daarnaast met een vurige begeerte om, eer het voor altijd te laat is, nog een poging tot *Uw*, tot *ons aller* redding te doen." Wertheim & Wertheim-Gijse Weenink 1981, p. 63. Dit pamflet is ook te vinden bij Knuttel 1987 onder nr. 19864.
21. Wertheim & Wertheim-Gijse Weenink 1981, p. 124.

Het democratisch manifest tast het moreel en politiek gezag van de Stadhouder ernstig aan en het is de aanzet voor de patriotse revolutie. Daarom markeert het een belangrijk moment in de geschiedenis van het Nederlandse democratische bestel. Het democratisch manifest wordt dan ook algemeen beschouwd als een van de belangrijkste Nederlandse staatkundige geschriften. Ondanks strenge verboden op het bezit en de verkoop van het boekje verschijnen kort naar de eerste verspreiding ervan vier nieuwe drukken alsmede Franse, Duitse en Engelse vertalingen.

Reeds bij het schrijven van het pamflet beseft Van der Capellen dat het waarschijnlijk als opruiend zal worden gebrandmerkt:

> "Ik heb – voor zover de beperkte ruimte van deze brief mij toeliet – getracht tot zelfs de eenvoudigste mens te verlichten; maar juist daardoor zal ik de woede van de Prins en zijn groten, die de gemene man niet al te wijs willen zien maken, tegen dit mijn geschrift, en zo ze mij kenden of in hun macht hadden, tegen mijn persoon niet weinig doen ontbranden. Dus als ge plakkaten of publikaties ziet verschijnen, waarin deze brief wordt verklaard te zijn een vuilaardig, oproerig, schandelijk, eerrovend, berucht lasterschrift en een premie wordt beloofd aan wie er de schrijver of drukker van weet aan te wijzen, bedenkt dan, dat zulke plakkaten en premies de gewone toevlucht zijn van lieden die de macht in handen, en de waarheid niet gezegd hebben willen; van lieden wier gedrag geen onderzoek kan velen.
> Het is veel makkelijker een schrijver die de waarheid aan het licht brengt, te mishandelen dan te bewijzen dat hij leugens vertelt."[22]

Over de vrijheid van drukpers zegt hij:

> "Zij is de enige steun van Uw nationale vrijheid. Als men niet vrij tot zijn medeburgers kan spreken, en hen niet bijtijds kan waarschuwen, dan valt het de onderdrukkers van het volk al zeer gemakkelijk hun rol te spelen. Daarom is het dat zij wier gedrag geen onderzoek kan velen, altijd zo tegen de vrijheid van schrijven en drukken ageren en wel graag zouden zien dat er niet gedrukt of verkocht zou worden zonder toestemming."[23]

Een maand later verschijnt van het Genootschap 'Amore Patriæ' te Groningen een boekje met de titel 'Consideratiën in hoeverre het verbieden van naamloze geschriften dienstig is, en welke daaronder moeten begrepen worden'. De auteurs stellen de vraag aan de orde of het "dienstiger voor het algemeen belang zijn zoude, de vrijheid van schrijven en drukken te beteugelen, dan, dezelve in haar geheel te laaten" en zij "tragten aan te toonen, omtrent welke Geschriften, en in hoe verre, deeze Beteugeling diende te geschieden, om met de Vrijheid bestaanbaar te blijven". Zij maken onderscheid tussen drie verschillende categorieën van geschriften te weten: (1) wat wij nu 'overheidsdocumenten' zouden

22. Idem, p. 140.
23. Idem, p. 143.

noemen,[24] (2) geschriften, "welke geschikt zijn, om, ware het moogelijk, het Gedrag en Denkwijze der beide partijen in hun waar daglicht voor te stellen, om daar door de onkundigen te onderrigten, en door gegronde bewijzen te overtuigen der zaak van de Partij die zij verhandelen (…)"[25], en (3) 'opruiende' geschriften.[26] Onder de laatste categorie valt volgens de auteurs ook het manifest van Van der Capellen.

Alleen de eerste twee categorieën zouden volgens de auteurs moeten worden toegestaan. Publicatie mag ook anoniem geschieden, tenzij sprake is van geschriften die "geen ander oogmerk hebben dan de Twisten aan te stooken, de Gemoederen teegen elkander meer en meer te verbitteren, regeeringen verdacht te doen voorkomen, eminente Personadien veragtelijk te maaken, te lasteren; en wat dies meer strekken kan tot nadeel van de Maatschappij of van eenige Leeden van dezelve".[27]

Ter onderbouwing van hun standpunt brengen de auteurs enkele argumenten naar voren, die wij in de discussie over anonimiteit nog vaker tegen zullen komen:

> "(…) men kan zulke Geschriften, als wij onder de tweede soort gebracht hebben, ofschoon zonder Naam des Auteurs, niet als Libellen aanmerken. Wat nut zoude het te weeg brengen, indien men zig maar binnen de paalen door ons gesteld houd, of men den naam al of niet van zoodanig eenen Schrijver wist? Het voordeel dat 'er de Maatschappij uit trekken zou, kan de nadeelen, die het den Schrijver zoude kunnen berokkenen, niet evenaaren. (…) En wat ligt er in den grond eenen onpartijdigen Leezer aan geleegen, door wien hem de waarheid wordt voorgesteld? De Geschriften van eenen onbekenden hebben zeeker het voordeel, van eenig en alleen beoordeeld te worden naar hunnen

24. "Extracten van de Resolutiën. Petitiën, Advisen, Aanspraaken, Brieven, Advisen en Protesten, bij Hun Hoog Mogende, den Raad van Staaten, de bijzondere Gewesten, Steeden en Leeden, genoomen of gedaan." Genootschap Amore Patriæ 1781, p. 6.
25. Onder de tweede categorie vallen geschriften die "alleen geschikt zijn, om de Dwaaling van een der beide Partijen voor te stellen, door onloochenbaare Bewijzen of gezonder Reedeneeringen bekragtigt, zonder zig in te laaten om deezen of geenen verdagt te maaken, en voor al, zonder hen, die in Hoogheid boven ons gestelt zijn, aan te roeren". Genootschap Amore Patriæ 1781, p. 10. Dit boekje vindt men ook bij Knuttel 1987 onder nr. 19876.
26. "(…) fameuze Libellen, schandelyke Lasterschriften, seditieuse Bedenkingen; in een woord: Alle zulke die ingerigt zyn, om de Gemeenten tegens eenige Leeden of tegens eene geheel Party aan te hitsen en op te stooken". Genootschap Amore Patriæ 1781, p. 12.
27. "Deeze Boeken en Geschriften, zijn niet alleen schandelijk en injurieus voor hen, die er in behandelt worden, maar zijn daar en boven nog strijdig met het waar Belang van eenen Staat, en moeten daarom op het sterkst verboden worden: ja, zoodanige Schrijveren ontdekt wordende, moesten als Vijanden van den Staat behandeld worden, en de eige straffe ondergaan, die men den Landverraderen aandoet. Want wat onderscheid is er tusschen eenen Landverrader en zulk een die de Ingezeetenen tot Oproer aanstookt, de Overigheid bij hun verdagt maakt, en eene Verandering in den Staat zoekt te bewerken? De opentlijke Vijanden van een Land zijn minder te dugten dan deeze; om dat zij, in de boezem zelve, het vuur van Tweedragt ontvonken." Genootschap Amore Patriæ 1781, p. 6, p. 12-13.

> inhoud: daar dikwijls anders, het een of ander dat men tegens de Schrijver weet, de partijdigheid doet ontwaaken, en zyne Schriften dus, met vooringenoomenheid teegens hem, geleezen worden."[28]

Een jaar na het verschijnen van de 'Consideratiën' verschijnt als reactie een werkje getiteld 'De vryheid der drukpers, onafscheidelyk verknogt aan de vryheid der Republiek'.[29] De schrijver laat naamsvermelding achterwege. Evenals het Genootschap keert hij zich tegen de Paskwilschrijvers, "een volk bijkans zo nadelig voor de waarheid als de stremming van den vrijen loop der drukpers zelve is".[30] Als voorstander van een zeer ruime drukpersvrijheid weigert hij echter een onderscheid te maken tussen anonieme en andere geschriften "dewijl toch de beste, de cordaatste man, niet alles kan zeggen, zoo hij niet onbekend kan zijn, 't geen hij wel zeggen wilde, en ook zeggen moest, indien hij, ten nutte des menschdoms, de naakte waarheid voor de oogen des volks zou openleggen".[31] Het door het Genootschap 'Amore Patriæ' voorgestane verbod op (anonieme) opruiende geschriften wijst hij van de hand.[32] Het belang van de vrije drukpers weegt zijns inziens zwaarder dan de dreiging van anonieme laster.[33] Bovendien laat een dergelijk verbod aan de machthebber de mogelijkheid om ongewenste anonieme geschriften te bestrijden door ze als opruiend te bestempelen.

28. Genootschap Amore Patriæ 1781, p. 16. Schimmel zegt een eeuw later precies hetzelfde: "Wanneer het gebeurt dat een artikel van een onbekende schrijver instemming vindt dan zal dit geheel en al te wijten zijn aan het stuk zelf, geen bijkomende gedachten aan den schrijver, geen haat of vrienschap, geen blinde waardeering van opgevijzelde talenten of kleingeestige minachting voor zekere standen en richtingen in de maatschappij zullen vooraf het oordeel wijzigen of over het al of niet gelezen worden beslissen, en moge al in vele gevallen de naam van den schrijver een waarborg zijn voor zijn goede trouw en eerlijke bedoelingen, diezelfde naam zou ook een dekmantel kunnen zijn voor leugen en bedrog." Schimmel 1882, p. 73.
29. Bodel Nyenhuis vermoedt dat de Friese jurist Simon Stijl de auteur is. Het betreft drie brieven, opgedragen aan 'de jonge Regenten van het Vaderland'. Zie Bodel Nyenhuis 1892, p. 84. Het geschrift wordt ook geciteerd door Diemer. Zie Diemer 1937, p. 61. Men kan dit boekje ook vinden bij Knuttel 1987 onder nr. 20348.
30. De auteur steekt zijn minachting voor de schrijvers van paskwillen niet onder stoelen of banken: "Dat ze beven zulke monsters! Daar ze toch eenmaal de snerpende geessels van een knagend Gewisse voor hun lasterziek gewoel zullen omdragen." Vryheid der Drukpers 1782, p. 24.
31. Vryheid der Drukpers 1782, p. 6.
32. De auteur is van mening dat het tegengaan van lasterschriften "met de waare Vrijheid geheel onbestaanbaar is, [en] dat dit een gevaarlijke stap tot eene langzaam inkruipende slavernij kan worden". Vryheid der Drukpers 1782, p. 23.
33. "Doch indien wij dit misbruik, hoe haatelijk, hoe ongelukkig voor hem, die onschuldig wordt aangevallen, tegen een ander misbruik, dat uit de minste beteugeling der Drukpers voort kan vloeijen, vergelijken, dan behoeven wij, mijn Vriend! niet lang stil te staan (…) wie (zal) beslissen (…) of dit geschrift tot de zulken behoore, die hij onder de *derde* Klasse plaatste (…) dan of het onder de *tweede* Klasse plaats verdiene, de Regenten zelve, zulken die aan het hoofd van den Staat zitten, of wie dezen hier toe mogten stellen." Vryheid der Drukpers 1782, p. 24.

5.4 Onder Franse invloed

Nadat het Franse revolutieleger in 1795 de Bataafse omwenteling tot stand brengt, geldt gedurende enige jaren een vrijwel onbeperkte drukpersvrijheid, die onder andere inhoudt dat schotschriften en naamloze geschriften niet worden onderdrukt.[34] In mei 1789 wordt door de Nationale Vergadering echter een nieuwe Staatsregeling goedgekeurd. Artikel 16 van de Burgerlijke en Staatkundige Grondregels bepaalt:

> "Ieder burger mag zijne gevoelens uiten en verspreiden, op zoodanige wijze, als hij goedvindt; des niet strijdig met het oogmerk der Maatschappij. De vrijheid der drukpers is heilig; mits de geschriften met den naam van uitgever, drukker of schrijver voorzien zijn. Deze allen zijn ten allen tijden, aansprakelijk voor alle zoodanige bedrijven, door middel der drukpers, ten aanzien van afzonderlijke personen, of der gansche Maatschappij, begaan, die door de wet als misdadig zijn erkend."[35]

De publicatie en verspreiding van naamloze geschriften is dus wederom vogelvrij. Als Napoleon zijn broer Lodewijk Bonaparte in 1806 koning van Holland maakt, komt ook aan de korte periode van drukpersvrijheid abrupt weer een einde. Vrijwel meteen nadat Lodewijk Bonaparte zijn ambt aanvaardt, worden uitgevers van kranten gelast zich in hun berichtgeving te onthouden van politieke oordelen over de daden van de regering. Enige tijd later wordt bij Keizerlijk decreet een strenge censuur geïntroduceerd.[36] In dit decreet wordt een Directeur-Generaal voor de boekdrukkerijen en de boekhandel ingesteld en voor iedere stad wordt een beperkt aantal boekdrukkers aangewezen. De titel en de naam van de schrijver van elk nieuw werk worden in registers bijgehouden. Daarnaast wordt bepaald dat boekdrukkers en boekhandelaars hun vak slechts mogen uitoefenen na een beëdigde aanstelling door de regering. Op 1 maart 1811 wordt in het gehele Franse keizerrijk, waar ons land sinds 1810 ook deel van uitmaakt, de Franse wetgeving, waaronder de Code Pénal, het Franse Wetboek van Strafrecht, van kracht.[37] Om ontduiking van de censuur tegen te gaan verbieden de artikelen 283 tot en met 286 de uitgave en verspreiding van alle anonieme geschriften, ongeacht de inhoud. Artikel 283 Code Pénal luidt:

34. Bodel Nyenhuis 1892, p. 209.
35. Zie ook De Meij 2000, p. 10.
36. Geen boekdrukker werd aangesteld, *qu'après avoir justifié de son attachement à la patrie et au souverain* (art. 7). Zie Décret Impérial contenant Réglement sur l'Imprimerie et la Librairie du 5 Février 1810, *Bulletin des Lois* N°. 264. Rondonneau, T. II, p. 531. Zie ook De Sitter 1869, p. 118-119 en De Bosch Kemper 1865, p. 137.
37. Zie ook Bodel Nijenhuis 1892, p. 228.

> "Alle uitgaaf of verspreiding van gedrukte werken, geschriften, bekendmakingen, berigten, aanplak- of uithangbiljetten, waarin de ware naam, beroep en woning van den schrijver of drukker niet uitgedrukt is, zal te dier zake alleen, met eene gevangenzetting van zes dagen tot zes maanden gestraft worden; en zulks ten aanzien van ieder, die met zijn weten tot de uitgave of verspreiding medegewerkt zal hebben."[38]

De zwaarte van de straf is afhankelijk van de inhoud van het geschrift. Als wordt aangezet tot het plegen van misdrijven, worden zij die het geschrift verspreiden aangemerkt als medeplegers, tenzij zij bekend maken van wie het geschrift afkomstig is. In het laatste geval kan ten hoogste drie maanden celstraf worden opgelegd.[39] Ook in andere gevallen kunnen verkopers en verspreiders worden gestraft, met dien verstande dat de straf verminderd wordt indien men de uitgever bekend maakt. De uitgever kan op zijn beurt rekenen op strafvermindering als hij de naam van de schrijver prijsgeeft.[40] De schrijver tenslotte, krijgt altijd de maximum straf.[41] Dit mechanisme, ook wel bekend als het stelsel van de 'successieve verantwoordelijkheid' of de 'responsabilité par cascades', tracht via de verkopers en verspreiders van een geschrift de drukker en uitgever van een geschrift te achterhalen, om vervolgens via hen de schrijver, de eigenlijke bron van de strafbare uiting, op te sporen.[42] Onverschillig de schuld van de anderen wordt slechts één persoon

38. De Nederlandse vertaling van deze artikelen is ontleend aan Van Deinse 1867, p. 98 e.v. De oorspronkelijke Franse tekst van artikel 283 Code Pénal luidt: "Toute publication ou distribution d'ouvrages, écrits, avis, bulletins, affiches, journaux, feuilles périodiques ou autres imprimés, dans lesquels ne se trouvera pas l'indication vraie des noms, profession et demeure de l'auteur ou de l'imprimeur, sera, pour ce seul fait, puni d'un emprisonnement de 6 jours á 6 mois, contre toute personne, qui aura sciemment contribué à la publication ou distribution."
39. Art. 285 Code Pénal: "In gevalle het gedrukte stuk eenige opzetting tot misdaden of wanbedrijven behelst, zullen de omroepers, aanplakkers, verkoopers en verspreiders als medepligtigen van den opzetter gestraft worden, tenzij zij diegenen bekend gemaakt hebben waarvan zij het stuk, dat de opzetting behelst, bekomen hebben. In geval van ontdekking zullen zij slechts in een gevangenzetting van zes dagen tot zes maanden vervallen, en de straf van medepligtigheid zal niet toepasselijk blijven dan op diegenen, die de personen, van wie zij het gedrukte stuk ontvangen hebben, niet bekend gemaakt zullen hebben, en op de drukker, indien hij bekend is."
40. Art. 284 Code Pénal: "Deze bepaling zal tot bloote policiestraffen gebragt worden, 1°. Ten aanzien van de omroepers, aanplakkers, verkoopers of verspreiders, die den persoon van wien zij het gedrukte stuk hebben, bekend gemaakt zullen hebben; 2°. Ten aanzien van al wie den drukker zal hebben bekend gemaakt, 3°. Ten aanzien zelfs van den drukker, die den schrijver zal hebben bekend gemaakt."
41. Art. 289 Code Pénal: "In alle gevallen bij deze afdeeling uitgedrukt, en waarin de auteur bekend zal zijn, zal hij het hoogste der straf ondergaan, aan de soort van het wanbedrijf verknocht."
42. Hetzelfde systeem geldt ten aanzien van geschriften die strijdig zijn met de goede zeden (zie art. 287 en 288 Code Pénal). Ook België en Zwitserland kenden een stelsel van successieve verantwoordelijkheid.

gestraft, ook al waren die anderen bekend met de strafbare inhoud. De publicatie van het drukwerk geldt als het misdadige feit.[43]

5.5 Het Koninkrijk der Nederlanden

Na de aftocht van Napoleon schaft koning Willem I bij Souverein besluit van 24 Januari 1814 de meeste Franse censuurbepalingen weer af.[44] De verspreiding van anonieme geschriften is echter nog steeds aan banden gelegd. De artikelen 1, 4 en 5 van dit besluit luiden:

> *"Artikel 1*
> De Fransche wetten en reglementen, betrekkelijk de boekdrukkerij en den boekhandel, daaronder begrepen die, welke de nieuwspapieren betreffen, zijn, van dato dezes, geheel en al afgeschaft.
>
> *Artikel 4*
> Een ieder is verantwoordelijk voor hetgeen hij schrijft, drukt of uitgeeft; indien de Schrijver niet bekend is, of aangewezen kan worden, is de Drukker alleen aansprakelijk.
>
> *Artikel 5*
> Elk stuk, dat zonder naam van den Schrijver of Drukker, en zonder aanwijzing van den tijd en de plaats der uitgave, in het licht komt, zal als een Libel beschouwd, en de Uitgever of Verspreider daarvan als Paskwilschrijver vervolgd kunnen worden."[45]

43. In Engeland werd de publicatie en de verspreiding als het strafbare feit beschouwd, zonder dat de verantwoordelijkheid van een der medewerkers (dat wil zeggen schrijver, drukker, uitgever en verspreider) die van anderen uitsloot. In Duitsland gold het stelsel van de gewone verantwoordelijkheid met bijkomende straffen voor nalatigheid. Als strafbaar feit werd hier beschouwd de publicatie van de misdadige gedachte met het opzet om deze te publiceren. Slechts de personen die met dat opzet aan publicatie en verspreiding meewerkten werden verantwoordelijk gehouden. Wanneer sprake was van een strafbare inhoud, was voorzien in bijzondere straffen voor diegenen die aan publicatie en verspreiding hadden meegewerkt. Onbekendheid met de inhoud werd dus mogelijk geacht, maar in geval van strafbare inhoud als nalatigheid gestraft. Schimmel 1882, p. 76-100.
44. Souverein besluit van 24 Januari 1814, *Stb.* no. 17. In het besluit werd overwogen dat "de Wetten en Regelementen, aangaande de Boekdrukkerij en den Boekhandel, door het Fransch Bestuur in deze gewesten ingevoerd, niet alleen in den Boekhandel eene zeer nadeelige stremming veroorzaakten, maar ook eene strekking hadden, om de vrijheid der drukpers volkomen te onderdrukken, den voortgang van de verlichting te beletten, en alles te onderwerpen een eene willekeurige censuur, ten eenemale strijdig met de liberale denkwijze, waarop elk regtgeaard Nederlander den hoogstens prijs stelt, en die steeds het Gouvernement dezer Landen heeft gekenschetst". Zie De Bosch Kemper 1865, p. 137 en Bodel Nyenhuis 1892, p. 245.
45. Daarnaast vermeld ik hier de Wet van 28 September 1816 tot vaststelling van straffen, voor hen, die vreemde mogendheden beledigen, *Stb.* 1816, 51. Deze wet verklaart drukkers, uitgevers, uitventers en boekverkopers van dergelijke beledigende geschriften strafbaar "voor zooverre dezelve den schrijver niet zullen kunnen aanwijzen, met zoodanig gevolg, dat de laatstgemelden niet alleen in handen der justitie geraken, maar van het gepleegde misdrijf in rechten kunnen worden overtuigd, en alzoo bestraft". Zie Asscher & Simons 1886, p. 51-52.

In 1847 beslist de Hoge Raad dat de artikelen 283 en 284 van de Code Pénal niet zijn afgeschaft of vervangen door het bovengenoemde besluit.[46] Deze bepalingen blijven daarom gelden totdat in 1886 het nieuwe Wetboek van Strafrecht van kracht wordt. Van Hasselt, raadsheer in het Provinciaal Gerechtshof van Noord-Holland, publiceert in 1861 zijn bedenkingen tegen deze uitspraak.[47] Een groot bezwaar tegen de bepalingen is zijns inziens dat zij niet de inhoud van het geschrift, maar de enkele uitgave en verspreiding daarvan bestraffen. Er wordt geen uitzondering gemaakt voor geschriften met een onschuldige inhoud.[48] Van Hasselt spoort de wetgever daarom aan de bepalingen van de Code Pénal zo spoedig mogelijk door een mildere wetgeving te doen vervangen.

Ook andere juristen verzetten zich tegen de strafbaarstelling van anonieme geschriften.[49] De theoloog, wijsgeer en jurist Opzoomer, die in zijn studententijd zelf nog anoniem publiceerde, schrijft:[50]

> "Waar door een geschrift tegen de wetten van den staat is gezondigd, daar is altijd iemand verantwoordelijk, en wordt het regt dus bevredigd; waar niets misdreven is, daar is er geen reden, waarom men op de openbaring van den naam des schrijvers zou aandringen. Men spreekt wel van ridderlijken kamp, van open vizier, en dergelijken, en noemt een nameloozen aanval een sluipmoord, maar zeer ten onregte. Waar er inderdaad een wonde is toegebragt, die door de wet als zoodanig wordt beschouwd, waar dus vervolging voor den regter mogelijk is, daar houdt de geheimhouding op. Menig licht zal in het geheel niet ontstoken worden, wanneer degeen, die het ontsteekt, zich altijd bekend moet maken. Zeer dikwijls zijn er omstandigheden, waarin heilige plichten het verzwijgen van den naam des schrijvers vorderen, en niet zelden zijn zij, die hun naam moeten verbergen, de eenigen, die in staat zijn de nuttige waarheid aan het licht te brengen."[51]

De Amsterdamse strafrechtjurist Buyn beschouwt het Franse stelsel van aansprakelijkstelling als een vorm van 'plaatsvervangend straflijden', die als een laatste overblijfsel uit

46. H.R. 30 November 1847. Zie J. van den Honert Thz., 'Verzameling van Arresten van den H.R. der Nederlanden', *Strafregt en Strafvordering* 1847, IIe Deel, p. 345; *Ned. Regtspr.* Deel XXIX, p. 144 en *Weekblad van het Regt*, N°. 870.
47. Van Hasselt 1861.
48. De Hoge Raad had reeds beslist dat artikel 283 Code Pénal van toepassing was op alle soorten van geschriften, onverschillig de omvang of gedaante daarvan: "Eene prent, waarop slechts eenige woorden gedrukt zijn ter verduidelijking of opheldering der voorstelling, is in de zin van dit Art. als écrit imprimé te beschouwen." Zie H.R. 25 november 1845, Ned. Regtspr. XXIII. 4, 26. W. 658.
49. De Meij noemt Evertsen de Jonge, Buys en de Bosch Kemper. Zie De Meij 1980, p. 124.
50. Cornelis Willem Opzoomer (1821-1892) was in zijn tijd al legendarisch. Van 1854 tot 1890 was hij hoogleraar in de wijsbegeerte te Utrecht. In 1843 publiceerde hij te Leiden anoniem een artikel waarin hij reageerde op kritische uitlatingen van de jurist Da Costa over de theologen van de 'Groninger richting'. Later verscheen van zijn hand een enorm aantal geschriften over theologie, wijsbegeerte, het recht en over politiek en literatuur. Opzoomer was ook politiek actief. Naar huidige maatstaven was hij links liberaal. In 1871 sloeg hij een aanbod om Minister van Justitie te worden af. Zie Veen & Kop 1987, p. 218-224.
51. Opzoomer 1854, p. 132-133.

de folterkamer moet worden aangemerkt.[52] De ervaring leert dat het gezag dikwijls stuit op "een idioot, die naauwelijks lezen en schrijven kan, doch die zich voor een geringe belooning als *autheur* aanmeldt, en als *homme de paille* zich slachten laat op het altaar der geregtigheid". Opvallend is dat hij spreekt van een 'recht op anonimiteit'.[53] De Leidse jurist Bodel Nyenhuis komt het niet billijk voor dat de boekdrukker en de boekverkoper ook worden gestraft als de auteur nog te bereiken is. Men kan hen immers niet verwijten dat zij het boek niet gelezen hebben.[54] De strafrechtjurist Simons, eveneens afkomstig uit Leiden, keert zich om soortgelijke redenen tegen de Franse bepalingen.[55] Simons was van mening dat het principe 'geen straf zonder schuld' in het gehele strafrecht diende te worden aanvaard. Het is aannemelijk dat de regeling in de Code Pénal hem om die reden tegen de borst stuitte. In zijn dissertatie wijst hij op de maatschappelijke rol van de zich ontwikkelende dagbladen en het belang van de vrije verspreiding van denkbeelden en meningen:

> "Wanneer de periodieke pers in werkelijkheid worden wil wat zij zijn moet, de leidster maar tevens en vooral de uiting van de publieke mening, dan is het nodig (…) dat zeer vele personen van de dagbladen gebruik maken, om hunne denkbeelden en meeningen over aanhangige onderwerpen in wijden kring bekend te maken. Dit zal echter slechts dan mogelijk zijn, wanneer geen verplichte onderteekening iedereen dwingt hetgeen hij schrijft door de verantwoordelijkheid van zijn naam te dekken; want de gevallen kunnen zich voordoen en doen zich dagelijks voor, dat iemand buiten staat zou zijn, zijn gedachten in 't publiek te ontwikkelen wanneer hij zich daarbij bekend moest maken. Wil men dat de periodieke pers het nut verschaffe dat zij verschaffen kan, en wil men niet dat eene schijnonderteekening toch de bepalingen van de wet illusior make, dan moet men er van afzien om van elkeen te vorderen dat hij strijde met open vizier."[56]

52. "Immers in haren wezenlijken en naakten vorm, ontdaan van hare moderne inkleeding, vertoont zij zich als een stelsel van pijniging en marteling des drukkers, *opdat* en *totdat* hij den schuldige aanwijze. Mogen deze overblijfselen uit barbaarsche tijden, spoedig uit ons strafregt verwijderd worden!" Buyn 1867, p. 57.
53. Buyn 1867, p. 56-57.
54. Bodel Nyenhuis 1892, p. 264.
55. David Simons (1860-1930) wordt beschouwd als een van de belangrijkste strafrechtjuristen van zijn tijd. In 1883 voltooide hij te Leiden een dissertatie getiteld 'De vrijheid van drukpers in verband met het Wetboek van Strafrecht'. In 1897 werd hij te Utrecht hoogleraar in het strafrecht en de strafvordering. Simons staat bekend als een groot voorvechter van de rechten van de verdachte in het strafproces. Hij streed onder andere voor de positie van de verdachte in het voorbereidend onderzoek en voor het vrije verkeer tussen verdachte en raadsman. Ook was hij was lid van de staatscommissie die in 1913 een ontwerp voor een nieuw Wetboek van Strafvordering presenteerde. Zie Veen & Kop 1987, p. 340-344 en Stolwijk 2003.
56. Simons 1883, p. 202-203. Ook Schimmel is van oordeel dat ten aanzien van de verantwoordelijkheid voor drukpersmisdrijven de gewone regels van strafrechtelijke verantwoordelijkheid dienen te gelden. Schimmel 1882, p. 62 e.v.

Bij de totstandkoming van het nieuwe Wetboek van Strafrecht van 1886 komt de wetgever aan de kritiek tegemoet. Er wordt nadrukkelijk afstand genomen van de regeling in de Code Pénal.[57] In de toelichting bij het wetsvoorstel overweegt de regering dat

> "er een zeer overwegende grond van staatsbelang [moet] bestaan om de op zich zelve volkomen geoorloofde handeling der verspreiding van een geschrift, dat niet onder het bereik der strafwet valt, strafbaar te verklaren, alleen omdat het den naam van den drukker, uitgever of schrijver niet draagt. Zoodanige grond nu bestaat niet wanneer de wet verspreiding van strafbare geschriften genoegzaam beteugelt".[58]

De wetgever wenst te voorkomen dat uitgevers en drukkers uit angst voor strafrechtelijke aansprakelijkheid eigenhandig censuur uitoefenen op de inhoud van uit te geven of te drukken geschriften:

> "De grondwet wil geen censuur van het staatsgezag, maar er bestaat gevaar voor eene andere censuur, nog wel zoo belemmerend als die door of van wege den staat uitgeoefend, wanneer uitgevers en drukkers in het belang van hunne eigene veiligheid gedwongen zijn, een streng toezigt te houden over alle werken tot welker openbaarmaking zij hunne tusschenkomst of hunne pers lenen."[59]

Daarom wordt in artikel 53 en 54 van het nieuwe Wetboek van Strafrecht een nieuwe regeling opgenomen, ook wel aangeduid als 'het drukkers- en uitgeversprivilege'. Deze regeling introduceert als nieuwe hoofdregel dat men vrij is om anoniem geschriften te verspreiden. Drukkers en uitgevers zijn in principe niet aansprakelijk. Slechts indien achteraf komt vast te staan dat sprake is van een geschrift met strafbare inhoud, kunnen zij worden gedwongen om mee te werken aan het opsporen van de dader. In het volgende hoofdstuk wordt op het drukkers- en uitgeversprivilege verder ingegaan.

5.6 De Duitse bezetting

Het systeem van het drukkers- en uitgeversprivilege maakt een eind aan het gebruik van verplichte naamsvermelding als machtsinstrument. Gedurende de Tweede Wereldoorlog wordt deze stap vooruit echter teruggedraaid door maatregelen van de bezetter. Deze kondigt aanvankelijk aan dat geen voorafgaande censuur zal worden uitgeoefend. Men wenst een wederzijds vertrouwen te vestigen. Wel wordt van uitgevers en redacteurs een absoluut loyale houding verwacht.[60] Naarmate de oorlog vordert neemt de bemoeienis met de inhoud van publicaties echter toe. Het hele perswezen wordt tussen 1941 en 1943 grondig gereorganiseerd. Kritische geluiden worden gesmoord. Het vereiste van toestemming wordt gepresenteerd als een maatregel die in verband met de papier-

57. De Meij 1980, p. 123.
58. Smidt 1881, p. 423-424.
59. Smidt 1881, p. 422.
60. Vos 1987, p. 181 e.v.

schaarste nodig zou zijn om het aantal publicaties te beperken. In werkelijkheid wordt wel degelijk een inhoudelijke beoordeling toegepast.[61]

In november 1941 wordt de Kultuurkamer opgericht. Dit is een beroepsvereniging onder leiding van de NSB waarvan alle toneelspelers, musici, dansers, schrijvers, beeldend kunstenaars, filmers, fotografen, journalisten en zelfs boekhandelaren lid moeten worden. Wie weigert mag zijn beroep niet langer uitoefenen. De beroepsgroep van journalisten wordt aan een speciaal regime onderworpen. Het Duitse *Schriftleitergesetz* uit 1933 wordt daartoe in het Nederlands vertaald en afgekondigd als het *Journalistenbesluit*. Dit besluit regelt nauwkeurig aan welke eisen een journalist moet voldoen en het bevat allerlei gedetailleerde registratieverplichtingen voor een ieder die in het perswezen werkzaam is.[62] Lidmaatschap van het Verbond van Nederlandsche Journalisten en inschrijving in het beroepsregister is verplicht (art. 1 lid 3 en art. 7 lid 1 Journalistenbesluit). Inschrijving is alleen mogelijk voor Nederlanders die de eigenschappen bezitten "welke noodig zijn om de taak van het voorlichten der openbare meening te vervullen". Op basis van de laatste zinsnede worden joden systematisch geweerd.[63] De registratieplicht is dus enerzijds bedoeld om via de uitbanning van anonimiteit het toezicht op de inhoud te ondersteunen en anderzijds om bepaalde bevolkingsgroepen van deelname aan het publieke debat uit te sluiten.

Niet alleen in het beroepsregister worden de journalisten geregistreerd, ook op elk exemplaar van krant of tijdschrift moeten naam en woonplaats van de hoofdredacteur en andere verantwoordelijke journalisten worden vermeld. Eenieder die bij de totstandkoming van een nieuwsblad betrokken is moet bij het Verbond van Nederlandse Journalisten met naam en toenaam bekend zijn en op elk exemplaar van een nieuwsblad moeten de naam en de woonplaats van de hoofdredacteur en van zijn plaatsvervanger, alsmede van elke journalist die de leiding heeft van een bepaald onderdeel van het nieuwsblad, worden vermeld (art. 18 lid 2 Journalistenbesluit). Wanneer voor een bepaalde afdeling van een blad geen verantwoordelijke is aangewezen draagt de hoofdredacteur de gehele verantwoordelijkheid.[64] Een uitgever die de werkzaamheden van een journalist toevertrouwt aan een persoon die niet in het beroepsregister is ingeschreven of die nalaat de naam van een hoofdredacteur door te geven kan worden gestraft met hechtenis van zes maanden of een geldboete van maximaal duizend gulden (art. 33 Journalistenbesluit). Toestemming voor de uitgave van een drukwerk moet worden verkregen bij de rijkscom-

61. Duke & Tamse 1987, p 189.
62. Besluit van den Secretaris-Generaal van het Departement van Volksvoorlichting en Kunsten betreffende het beroep van Journalist van 14 mei 1941. De integrale tekst van dit besluit vindt men bij Goedhart 1943, p. 261-266. Het journalistenbesluit en aanverwante regelingen worden bij Goedhart eveneens nader besproken vanuit het perspectief van de bezetter. Zie De Ranitz 1943.
63. De Ranitz 1943, p. 244-245.
64. Zie artikel 6 van het Derde Uitvoeringsbesluit van den Secretaris-Generaal van het Departement van Volksvoorlichting en Kunsten van 13 Juni 1941 betreffende het Journalistenbesluit, eveneens te vinden bij Goedhart 1943, p. 269.

missaris voor het bezette Nederlandse gebied en wordt alleen verleend wanneer nauwkeurige gegevens worden verstrekt over schrijvers, drukkers, uitgevers en de eigenaars en bestuurders van de uitgeverij (art. 1 jo. art. 2 lid 2 Journalistenbesluit).

Ten slotte wordt ook het gebruik van schuilnamen aan banden gelegd. Journalisten die hun artikelen met een pseudoniem ondertekenen, moeten hiervan aan het secretariaat van het Verbond van Nederlandsche Journalisten mededeling doen.[65] Persfoto's en perstekeningen mogen alleen worden gepubliceerd met vermelding van de volledige naam van de maker of het persbureau.[66]

De pogingen om de verspreiding van informatie te beheersen moeten worden gezien als onderdeel van een breder geheel van maatregelen dat bedoeld is om via de nauwgezette registratie van burgers iedere kritiek te smoren, het verzet de kop in te drukken en de jodenvervolging mogelijk te maken.[67] Men kan de voorschriften in het Journalistenbesluit in dat opzicht vergelijken met de voor alle Nederlanders vanaf veertien jaar geldende verplichting tot het dragen van een persoonsbewijs en de voor joden geldende verplichting tot het dragen van een davidsster.[68]

65. Goedhart 1943, p. 271.
66. Beschikkingen van den Verbondsvoorzitter. Bepalingen betreffende de bronvermelding bij persfoto's en persteekeningen. Zie Goedhart 1943, p. 279.
67. De identiteitsregistratie is tijdens de Tweede Wereldoorlog in geen enkel Europees land zo volmaakt als in Nederland. Dit komt doordat het persoonsbewijs voor de oorlog al was ontwikkeld door het ministerie van Binnenlandse Zaken. De bezetter maakt van de klaarliggende plannen dankbaar gebruik. Technisch is het persoonsbewijs lastig na te maken. Het wordt namelijk beschreven met paarse inkt die onder een kwartslamp onzichtbaar wordt. Pas in 1944 weten de Landelijke Knokploegen een vat van deze inkt te bemachtigen. Ook administratief is het systeem zeer solide. Van ieder persoonsbewijs bestaat een kopie die wordt bewaard in een zwaarbewaakte centrale cartotheek in Den Haag. Valse persoonsbewijzen voor onderduikers en leden van het verzet bieden minder bescherming wanneer de gegevens niet overeenkomen met die in het bevolkingsregister. Mede daarom worden op verschillende plaatsen acties ondernomen om het bevolkingsregister te vernietigen. Zeer bekend is de aanslag op het Amsterdamse bevolkingsregister aan de Plantage Kerklaan op 27 maart 1943. Deze aanslag was een reactie op de wegvoering van mannen voor de arbeidsinzet. Vanaf augustus 1943 worden door het netwerk Landelijke Knokploegen (LKP) ook op andere plaatsen bevolkingsregisters in brand gestoken. Ook pleegt men gewapende overvallen om blanco persoonsbewijzen te verkrijgen.
68. Het boek 'Soldaat van Oranje' bevat in dat licht een interessante passage, waarin de auteur beschrijft hoe aan de Universiteit van Leiden de numerus clausus wordt afgekondigd. De bezetter had laten weten dat de universiteit weer geopend zou worden als men de registratie van joodse studenten zou accepteren. Roelfzema, de schrijver van het boek, verspreidt een pamflet dat hij ondertekent met 'de Leidsche Studenten'. Hierin protesteert hij onder andere fel tegen de numerus clausus. De universiteit blijft hierdoor gesloten. Een week later wordt de drukker van het pamflet door de Gestapo gearresteerd. Hij krijgt te horen dat hij op vrije voeten wordt gesteld als hij zijn opdrachtgever aanwijst. De drukker weigert. Hij voert het klassieke verweer: "ik heb ze gezegd dat ik van dat hele pamflet geen woord begrijp. Ik ben alleen maar de drukker, ik moet m'n brood verdienen". Enige maanden later wordt hij vrijgelaten. Zie Hazelhoff Roelfzema 1971, p. 78-80.

5.7 Conclusie

De huidige juridische vraagstukken rondom anonimiteit worden maar al te vaak beschouwd als uniek voor deze tijd. Uit het voorgaande blijkt dat deze gedachte herziening behoeft. De anonieme verspreiding van informatie heeft door de tijden heen maatschappelijke betekenis gehad en er is een direct historisch verband tussen verboden op anonimiteit en de uitoefening van censuur. Anonimiteit maakt censuur immers onmogelijk. Streng voorafgaand toezicht op de inhoud van geschriften dient dus te worden ondersteund door verboden op anonimiteit. Alleen dan kunnen ongewenste politieke en religieuze uitingen effectief worden bestraft en bestreden. Het is geen toeval dat de maatregelen tegen anonieme publicaties strenger en de straffen op overtreding van de verboden wreder werden in tijden van overheersing door vreemde mogendheden. Met wisselend succes trachtten zowel de Spaanse, de Franse als de Duitse bezetter kritiek de mond te snoeren. Juist de anonieme geschriften vormden een bedreiging omdat men alleen daarin zijn gedachten vrijelijk naar voren kon brengen.

De maatregelen tegen anonimiteit richtten zich in de eerste plaats tegen tussenpersonen zoals de drukker, de uitgever, de boekverkoper en de journalist. Zij waren immers degenen die de geschriften verveelvoudigden en verspreidden. Reeds vroeg was het gezag erop bedacht een middel uit te denken om tot de oorsprong van de misdadige gedachte te kunnen opklimmen teneinde de verdere verspreiding van gevaarlijke ideeën te beletten. Door drukkers en uitgevers streng te straffen maar hen straffeloosheid of strafvermindering in het vooruitzicht te stellen wanneer zij de schrijver bekend maakten, werd getracht om de verantwoordelijke op te sporen. Het systeem van de successieve verantwoordelijkheid in de Code Pénal is hiervan het duidelijkste voorbeeld. Via een ingenieus mechanisme van strafbepalingen werden drukkers en uitgevers tot medewerking gedwongen.

Toch moet worden geconcludeerd dat men er nooit in is geslaagd de verspreiding van anonieme geschriften geheel te stoppen. Er zijn eenvoudigweg te veel manieren om regulering en registratie te ontduiken. De invoering van censuurbepalingen leidde vaak tot een enorme toename van het aantal anonieme pamfletten, illegale boeken en ondergrondse bladen. Om de aanval van de censuur te pareren bedienden drukkers en uitgevers zich massaal van schijnadressen, schuilnamen en antedateringen.[69] Sommigen verplaatsten zelfs hun hele bedrijf naar gebieden met een gunstiger politiek klimaat. De vele voorbeelden in ogenschouw nemend, zou men kunnen spreken van een historische 'traditie' van anoniem verzet. Menig auteur van verzetsliteratuur in de Tweede Wereldoorlog was zich van de historie bewust. Men vindt dan ook vaak vergelijkingen met de Geuzenliederen uit de 16e eeuw.[70]

69. Kronenberg 1947, p. 111-126.
70. Een voorbeeld is het gedicht 'Het jaar 1572' van Martinus Nijhoff. De titel van dit gedicht verwijst naar het jaar waarin de opstand tegen de Spanjaarden begon. Een verzameling van illegaal uitgegeven 'nieuwe Geuzenliederen' werd na de Tweede Wereldoorlog gebundeld in het Geuzenliedboek 1940-1945. Zie Schenk 1945.

Een diepgaande discussie over de wenselijkheid van een verbod op anonieme geschriften treffen wij voor het eerst aan in de tweede helft van de achttiende eeuw. In die tijd werden de voor- en nadelen van anonimiteit voor het eerst geplaatst in het bredere kader van de drukpersvrijheid en werd ook het maatschappelijk belang van wat wij nu het 'publieke debat' noemen expliciet meegewogen bij de oordeelvorming over de wenselijkheid van strafbaarstelling. Dat dezelfde discussie in de Verenigde Staten ongeveer gelijktijdig ontstond, lijkt geen toeval. De Verlichtingsidealen maakten de drukpersvrijheid in die tijd aan beide kanten van de oceaan tot een veelbesproken thema. In Nederland was men nog opgescheept met het stelsel van de successieve verantwoordelijkheid, terwijl men zich in de Verenigde Staten na de onafhankelijkheid bezon op de grenzen van de drukpersvrijheid.

De Nederlandse juristen die zich aan het einde van de negentiende eeuw uitspraken over het systeem van de Code Pénal, lieten hun oordeel zonder uitzondering uitvallen in het voordeel van de uitingsvrijheid. Bij de invoering van het huidige Wetboek van Strafrecht in 1886 werd de heersende mening voor het eerst ook in de wet tot uitdrukking gebracht. Als hoofdregel geldt sindsdien dat drukkers en uitgevers bij de verspreiding van niet-anonieme geschriften met strafbare inhoud in principe vrijuit gaan. Bij anonieme geschriften moeten zij echter voorzichtiger zijn. Daar dienen zij zich te vergewissen of het niet gaat om inhoudelijk strafbare publicaties. Het publiceren van geschriften zonder de naam van de auteur of de anderszins voor de inhoud verantwoordelijke persoon is daarentegen op zichzelf niet verboden en het verspreiden van die geschriften is dat evenmin. Ook de wetgever lijkt uit de geschiedenis een belangrijke conclusie te hebben getrokken: als het verbod op anonimiteit een middel is om de inhoud van informatie preventief te controleren en te sanctioneren, dan volgt daaruit dat werkelijke uitingsvrijheid niet kan bestaan wanneer men te allen tijde verplicht is om op een geschrift zijn naam te vermelden.

6 Regulering van anonimiteit bij traditionele communicatie

6.1 Inleiding

De inwerkingtreding van het nieuwe Wetboek van Strafrecht maakte in 1886 een einde aan pogingen van kerkelijke en wereldlijke wetgevers om het drukken en verspreiden van anonieme geschriften door middel van verboden tegen te gaan. Het drukkers- en uitgeversprivilege bracht een aanvaardbaar maatschappelijk compromis tot stand tussen enerzijds een zo ruim mogelijke uitingsvrijheid en anderzijds het maatschappelijk belang van een effectieve rechtshandhaving bij drukpersdelicten. In de loop der tijd ontstonden rondom de anonieme verspreiding echter enige nieuwe vraagstukken. In het Muurkrantenarrest kwam de vraag aan de orde of een gemeentelijke regeling die het verbiedt om anonieme muurkranten te verspreiden, verenigbaar was met artikel 7 Gw. Daarnaast was een eventueel te aanvaarden recht van de journalist om zijn bronnen geheim te houden onderwerp van discussie. Voordat wij aan deze onderwerpen toekomen, wordt hieronder eerst dieper ingegaan op het drukkers- en uitgeverprivilege.

6.2 Het drukkers- en uitgeversprivilege

Het drukkers- en uitgeversprivilege is in de eerste plaats bedoeld om drukkers en uitgevers te beschermen tegen strafrechtelijke vervolging wegens het in omloop brengen van geschriften met een strafbare inhoud (zie par. 5.5). Door de dreiging van strafrechtelijke vervolging zouden zij zich immers gedwongen kunnen voelen tot het uitoefenen van censuur. In de artikelen 53 en 54 van het nieuwe Wetboek van Strafrecht (Sr) is daarom een vervolgingsuitsluitingsgrond opgenomen, die drukkers en uitgevers vrijwaart van vervolging in het geval dat zij, door geschriften van strafbare aard te drukken of uit te geven, als medepleger of medeplichtige hebben meegewerkt aan een drukpersdelict. Het privilege geldt alleen voor drukkers en uitgevers 'als zodanig'; zij mogen het strafbare geschrift dus niet zelf hebben geschreven of het schrijven daarvan hebben uitgelokt. De bepalingen zijn daarnaast alleen van toepassing op het meewerken aan misdrijven 'door middel van de drukpers gepleegd'.[1] Hierbij moet men onder andere denken aan beledi-

1. Cleiren & Nijboer 2002, p. 355-356.

ging, opruiing, het aanzetten tot discriminatie, godslastering, smaadschrift en laster. De artikelen luiden in de huidige redactie:

> *"Artikel 53*
> 1. Bij misdrijven door middel van de drukpers gepleegd wordt de uitgever als zodanig niet vervolgd, indien het gedrukte stuk zijn naam en woonplaats vermeldt en de dader bekend is of op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door de uitgever is bekendgemaakt.
> 2. Deze bepaling is niet toepasselijk, indien de dader op het tijdstip van de uitgave strafrechtelijk niet vervolgbaar of buiten het Rijk in Europa gevestigd was.
>
> *Artikel 54*
> 1. Bij misdrijven door middel van de drukpers gepleegd wordt de drukker als zodanig niet vervolgd, indien het gedrukte stuk zijn naam en woonplaats vermeldt en de persoon op wiens last het stuk is gedrukt, bekend is of op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door de drukker is bekendgemaakt.
> 2. Deze bepaling is niet toepasselijk, indien de persoon, op wiens last het stuk is gedrukt, op het tijdstip van het drukken strafrechtelijk niet vervolgbaar of buiten het Rijk in Europa gevestigd was."

Voor politie en justitie moest het mogelijk blijven om de dader of degene op wiens last een strafbaar geschrift gedrukt is, op te sporen. De vervolgingsuitsluitingsgrond is daarom alleen van toepassing wanneer aan een aantal voorwaarden is voldaan. In de eerste plaats moeten drukker en uitgever hun naam en woonplaats op het gedrukte stuk vermelden. Belangrijker is echter dat de in artikel 53 Sr genoemde dader of de in artikel 54 Sr genoemde lastgever bekend is of op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door drukker of uitgever aan de politie of aan het Openbaar Ministerie bekend wordt gemaakt. Geeft de uitgever of drukker aan de aanmaning gehoor dan zal krachtens de artikelen 243 en 244 Wetboek van Strafvordering een kennisgeving van niet verdere vervolging moeten uitgaan.[2] Tenslotte moet de dader of de lastgever krachtens het tweede lid van beide artikelen vervolgbaar zijn en in Europa gevestigd.

In de Tweede Kamer kon men het niet eens worden over de vraag in hoeverre uitgevers en drukkers voor de inhoud van een stuk konden worden gestraft indien de voorwaarden van artikel 53 en 54 niet waren vervuld. Volgens sommigen konden zij alleen volgens de normale regels als medeplichtige of medepleger worden gestraft. Dit betekende dat bewezen zou moeten worden dat zij kennis hadden gehad van de inhoud van het geschrift omdat anders niet voldaan zou zijn aan het bestanddeel 'opzettelijk' zoals dit bij medeplichtigheid en de meeste uitingsdelicten voorkomt. Anderen waren van mening dat dit zou neerkomen op een vrijbrief voor uitgevers en drukkers om alles uit te geven of te drukken, mits zij er maar geen kennis van namen. In de artikelen 418 en

2. Cleiren & Nijboer 2002, p. 358.

419 Sr is uiteindelijk een compromis geformuleerd. Deze artikelen stellen het strafbaar om enig geschrift of enige afbeelding van strafbare aard uit te geven of te drukken wanneer niet aan de voorwaarden van artikel 53 of 54 Sr is voldaan.[3] De strafrechtelijke aansprakelijkheid is in dat geval, als een aansprakelijkheid sui generis, gegrond op onvoldoende voorzichtigheid bij het uitgeven of drukken.[4]

Uit het voorgaande volgt een aantal belangrijke constateringen. In de eerste plaats is het drukken, uitgeven en verspreiden van anonieme geschriften als zodanig niet strafbaar. Dat dit een bewuste keuze is van de wetgever komt uit de Memorie van Toelichting bij het wetsvoorstel ter invoering van de artikelen 53 en 54 Sr duidelijk naar voren (zie par. 5.5). Voor de schrijver van een naamloos geschrift bewerkstelligt het drukkers- en uitgeversprivilege een vorm van relatieve anonimiteit. Hij kan ervan uitgaan dat de drukker en de uitgever strafrechtelijk niet kunnen worden gedwongen om de anonimiteit op te heffen zolang het geschrift geen strafbare uitlatingen bevat. Bestaat echter een verdenking van een drukpersdelict en is naar aanleiding daarvan een gerechtelijk vooronderzoek begonnen, dan staat op het niet noemen van de dader de sanctie van strafrechtelijke aansprakelijkheid. Drukkers en uitgever kunnen immers slechts een beroep doen op het privilege wanneer zij de dader of de lastgever van het anonieme geschrift bekend maken. Indien zij dat weigeren kunnen zij op basis van de artikelen 418 en 419 Sr strafrechtelijk verantwoordelijk worden gehouden.

Door de technische ontwikkeling zijn de artikelen 53 en 54 Sr niet meer geheel bij de tijd: de klassieke drukpers is al lang niet meer het enige middel voor de openbaarmaking en verspreiding van uitingen.[5] Met de opkomst van nieuwe communicatietechnieken zijn nieuwe tussenpersonen ontstaan, zoals telecombedrijven en internetproviders, die in

3. Artikel 418 Sr luidt: "Hij die enig geschrift of enige afbeelding uitgeeft van strafbare aard, wordt gestraft met gevangenisstraf of hechtenis van ten hoogste een jaar of geldboete van de derde categorie, indien:
1° de dader noch bekend is, noch op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, is bekendgemaakt; 2° de uitgever wist of moest verwachten dat de dader op het tijdstip van de uitgave strafrechtelijk niet vervolgbaar of buiten het Rijk in Europa gevestigd zou zijn. Artikel 419 Sr luidt: Hij die enig geschrift of enige afbeelding drukt van strafbare aard, wordt gestraft met gevangenisstraf of hechtenis van ten hoogste een jaar of geldboete van de derde categorie, indien: 1° de persoon op wiens last het stuk gedrukt is noch bekend is, noch op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, is bekendgemaakt; 2° de drukker wist of moest verwachten dat de persoon op wiens last het stuk gedrukt is, op het tijdstip van de uitgave strafrechtelijk niet vervolgbaar of buiten het Rijk in Europa gevestigd zou zijn."
4. *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 8.
5. Eind jaren negentig was het ministerie van Justitie voornemens het drukkers- en uitgeversprivilege aan te passen aan de technologische ontwikkelingen. In het wetsvoorstel Computercriminaliteit II zou het begrip 'uitgever' in artikel 53 Sr worden vervangen door 'tussenpersoon' en zou het begrip 'misdrijven door middel van de drukpers gepleegd' worden uitgebreid tot 'uitingen in gesproken woord, beeld of geschrift'. Door de komst van de richtlijn elektronische handel, die wordt behandeld in hoofstuk 9, kwam het voorstel echter te vervallen. Het wetsvoorstel Computercriminaliteit II wordt besproken door Schuijt. Zie Schuijt 1998.

de informatiemaatschappij een vergelijkbare functie hebben. Daarnaast is de reikwijdte van het drukkers- en uitgeversprivilege beperkt tot de primaire openbaarmakingshandeling. De verdere verspreiding van de uiting, bijvoorbeeld door een boekhandel, valt hier niet onder. Naarmate het onderscheid tussen drukken, uitgeven en verspreiden vervaagt, is de systematiek van het drukkers- en uitgeversprivilege steeds minder houdbaar.[6]

6.3 Het Muurkrantenarrest

Na de afschaffing van het verbod op anonieme geschriften krijgt de anonieme verspreiding van informatie gedurende lange tijd weinig aandacht. Pas in de jaren zeventig van de twintigste eeuw komt het vraagstuk weer bovendrijven. Aanleiding is de verspreiding van anonieme muurkranten in de gemeente Utrecht. Deze worden wekelijks op een groot aantal plaatsen in de stad aangeplakt. De berichtgeving heeft voornamelijk betrekking op plaatselijke aangelegenheden zoals het bestuur van de stad en de universiteit. Er wordt felle en soms beledigende kritiek geuit op gemeentelijke instellingen en vooraanstaande personen.

De gemeenteraad van Utrecht reageert op de muurkranten door in artikel 69 lid 1 van de Algemene Politie Verordening Utrecht (APVU) een algeheel verbod op te nemen om zonder voorafgaand verlof van burgemeesters en wethouders op of tegen een onroerend goed, gelegen in het niet-landelijk gedeelte van de gemeente, afbeeldingen, letters, cijfers of andere tekens dan wel illuminatie aan te brengen of te hebben, welke van de openbare weg af zichtbaar zijn. In het tweede en derde lid worden uitzonderingen gemaakt voor achter het raam aangebrachte biljetten en voor "het aanbrengen van meningsuitingen of bekendmakingen, geen betrekking hebbende op commerciële reclame, indien dit geschiedt: a) op door B&W bij openbare kennisgeving daartoe aangewezen plaatsen en b) overeenkomstig de bij die kennisgeving gestelde voorschriften, welke geen betrekking mogen hebben op de inhoud van de meningsuitingen of bekendmakingen".

In het bij de bepalingen behorende uitvoeringsbesluit worden als 'aangewezen plaatsen' de door de gemeente geplaatste publicatieborden voor ideële meningsuitingen aangemerkt. Daarnaast wordt bepaald dat meningsuitingen en bekendmakingen die op deze borden worden aangebracht, moeten zijn voorzien van de naam en het adres van de voor de publicaties verantwoordelijke persoon of instantie. Een meerderheid van de gemeenteraad ondersteunt de voorgeschreven vermelding van naam en adres omdat op deze wijze de voor de aangeplakte tekst of afbeelding verantwoordelijke persoon kan worden achterhaald. Men is van mening dat gestreden moet worden met open vizier. De burgemeester is bevreesd dat zonder vermelding van naam en adres het gemeentebestuur moreel medeverantwoordelijk zou worden gehouden, gezien de beschikbaarstelling van de aanplakborden.[7]

6. *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 9.
7. Zie De Meij 1980, p. 121-122.

Het verbod blijkt weinig effect te hebben. Tegen een van de plakkers wordt daarom proces-verbaal opgemaakt wegens het aanbrengen van een muurkrant zonder vergunning van burgemeester en wethouders en zonder vermelding van zijn adres. De plakker heeft slechts de aanduidingen 'Muurkrant 408' en 'Adres: Postbus p/a Oudegracht 36' vermeld en de kopijbus bevindt zich op een andere plaats dan zijn woonadres. De kantonrechter komt tot vrijspraak omdat hij van oordeel is dat niet uitputtend is onderzocht of de verantwoordelijke persoon via de kopijbus te bereiken was. Tegen deze uitspraak wordt hoger beroep aangetekend. Voor de rechtbank voert de verdachte het verweer dat de genoemde aanduidingen op de muurkrant de naam en het adres vormen van de voor de publicatie verantwoordelijke persoon of instantie. De rechtbank acht deze vermelding voor de benadering van natuurlijke en andere personen in een strafrechtelijk kader echter onvoldoende. Uit de totstandkomingsgeschiedenis van het uitvoeringsbesluit en de van gemeentewege gegeven toelichting blijkt immers dat de strekking van het voorschrift is om te verzekeren dat de voor de publicatie verantwoordelijke persoon of instantie ook inderdaad ter verantwoording kan worden geroepen. Deze strekking zou worden miskend indien als aanduiding van een adres de vermelding van een kopijbus, die zich bevindt op een andere plaats dan de plaats waar de persoon woont of verblijft, voldoende zou zijn. Het past volgens de rechtbank niet in het door het Wetboek van Strafvordering voorgeschreven systeem van benadering van natuurlijke en andere personen dat slechts door middel van een kopijbus communicatie mogelijk is (r.o. 8). Elke andere opvatting zou leiden tot de

> "naar huidige opvattingen volstrekt onaanvaardbare consequentie (…) dat een persoon of groepering, die pretendeert een bijdrage aan de publieke meningsvorming te leveren en aldus aan het maatschappelijk verkeer deelneemt, het geheel in eigen hand zou hebben of hij/zij, na door middel van een eenzijdig communicatiemiddel als een kopijbus benaderd te zijn, al dan niet reageert en voor het voetlicht treedt teneinde verantwoording af te leggen voor zijn/haar handelen".[8]

Het belang van toerekenbaarheid weegt naar het oordeel van de rechtbank dus zwaar. De rechtbank vernietigt het vonnis van de kantonrechter en veroordeelt de verdachte tot een geldboete van vijftig gulden.

In cassatie komt de vraag aan de orde of de Utrechtse regeling verenigbaar is met het recht op vrijheid van meningsuiting.[9] De verdachte stelt dat artikel 69 APVU in strijd is met artikel 7 Gw en artikel 10 EVRM. Het aanbrengen tegen een onroerend goed van afbeeldingen en teksten waarin gedachten en gevoelens zijn geopenbaard moet naar zijn

8. Dit oordeel wordt door de Hoge Raad bevestigd met de overweging dat de verplichte vermelding van naam en adres ertoe strekt te voorkomen dat de van gemeentewege aangewezen aanplakborden worden gebruikt tot het anoniem beledigen van anderen zonder daarvoor achteraf ter verantwoording te kunnen worden geroepen.
9. HR 24 juni 1980, *NJ* 1981, 659.

mening worden aangemerkt als een middel van bekendmaking dat naast andere middelen zelfstandige betekenis heeft en dat met het oog op die bekendmaking in een behoefte kan voorzien, zodat het gebruik van dat middel niet in het algemeen mag worden verboden of van een voorafgaand verlof van de overheid afhankelijk mag worden gesteld. De gevallen waarin het genoemde verbod niet van toepassing is, zijn volgens de verdachte niet van zodanige betekenis dat zij daaraan een algemeen karakter zouden kunnen ontnemen.[10] Het belangrijkste bezwaar van de verdachte betreft echter de poging van de gemeentelijke wetgever om te bewerkstelligen dat iedere op of tegen een onroerend goed aangebrachte meningsuiting of bekendmaking is voorzien van naam en adres van de voor publicatie verantwoordelijke persoon of instantie. Hierdoor is er zijns inziens getreden op het terrein van de formele wetgever, die blijkens de Memorie van Toelichting bij de artikelen 53 en 54 Sr en het Wetboek van Strafvordering ten aanzien van drukpersdelicten een uitputtende en sobere regeling heeft willen geven.[11]

De bezwaren van de verdachte worden verworpen. De Hoge Raad erkent dat de muurkranten een verspreidingsmiddel met zelfstandige betekenis vormen maar is van oordeel dat het uitvoeringsbesluit van de APVU voldoende ruimte laat aangezien het daarin opgenomen verbod niet geldt voor mededelingen of bekendmakingen op de bij dat besluit aangewezen, aan de openbare weg geplaatste, borden. Op artikel 7 Gw zou slechts inbreuk worden gemaakt indien de gemeentelijke wetgever bij de beperkingen zo ver zou gaan dat het gebruik van de muurkranten als verspreidingsmiddel in het algemeen zou worden verboden of van voorafgaand verlof afhankelijk zou worden gesteld. Het beroep op artikel 10 EVRM wordt om die reden eveneens afgewezen (r.o. 12 en 13). Ten slotte wordt ook het betoog dat de rijkswetgever de bevoegdheid tot strafbaarstelling van het verspreiden van anonieme geschriften aan de gemeentelijke wetgever heeft onttrokken, van de hand gewezen. De overwegingen van de wetgever kunnen naar het oordeel van de Hoge Raad niet de gevolgtrekking dragen dat de gemeentelijke wetgever – die bij het geven van zijn voorschriften dient uit te gaan van plaatselijke omstandigheden – de bevoegdheid zou missen om het op onroerende goederen aanbrengen van anonieme, van de openbare weg af zichtbare, meningsuitingen of bekendmakingen, in het belang van de openbare orde te verbieden (r.o. 14).

Een mogelijk punt van kritiek op de uitspraak van de Hoge Raad is dat de relatie tussen anonimiteit en uitingsvrijheid onvoldoende wordt onderkend. Afgezet tegen de Amerikaanse jurisprudentie komt de motivering van de Hoge Raad in dat opzicht nogal mager over. Het verbod op anonimiteit wordt noch als een beperking van de verspreidingsvrijheid, noch als een regulering van de inhoud aangemerkt zodat naar het oordeel van de Hoge Raad geen sprake is van een beperking van de uitingsvrijheid. De Utrechtse

10. Zie het zesde en het zevende middel. Blijkens de jurisprudentie mag de verspreidingsvrijheid niet in het algemeen verboden of van een voorafgaand verlof afhankelijk gesteld worden. De Meij 2000, p. 111-120.
11. Zie het negende middel.

regeling wordt getoetst aan de verspreidingsjurisprudentie zonder dat het verbod op anonimiteit wordt meegewogen. Overwogen wordt slechts dat de gemeentelijke wetgever de bevoegdheid heeft om anonieme meningsuitingen in het belang van de openbare orde te verbieden en dat hij door dat te doen niet treedt op het terrein van de formele wetgever. Met deze benadering verwerpt de Hoge Raad het door De Meij ingenomen en door de Advocaat-generaal onderschreven standpunt dat het vereiste van vermelding van naam en adres een verspreidingsregeling is die aanknoopt bij de inhoud van de publicaties. Volgens De Meij kan de beperking die de Utrechtse regeling bevat moeilijk worden aangemerkt als in het belang van de openbare orde, gezien het feit dat het begrip openbare orde in de context van de verspreidingsvrijheid een beperkte strekking heeft en gezien het Tilburgse drukpersarrest, dat de toegestane mogelijkheid om de verspreidingsvrijheid ter bescherming van de openbare orde te reguleren beperkt tot tijd, plaats of wijze van verspreiding.[12] Het voorschrift is bedoeld om te verzekeren dat de verantwoordelijke persoon of instantie voor een bepaald drukpersdelict door justitie ter verantwoording kan worden geroepen en alleen op grond van de inhoud kan van een drukpersdelict worden gesproken, aldus De Meij.[13]

Door het verbod op anonimiteit niet aan te merken als een regulering van de inhoud, slaat de Hoge Raad een fundamenteel andere weg in dan het Amerikaanse Supreme Court. Het lijkt waarschijnlijk dat de Hoge Raad het standpunt van De Meij niet heeft willen overnemen vanwege zijn praktische consequenties. Wanneer een verbod op anonimiteit zou worden aangemerkt als regulering van de inhoud, dan zou dit er toe leiden dat de gemeentelijke wetgever anonimiteit niet mag verbieden. Bemoeienis met de inhoud van gedrukte stukken is in het systeem van de Nederlandse verspreidingsjurisprudentie immers voorbehouden aan de formele wetgever. In de Verenigde Staten speelt dit probleem niet. Daar mag de locale wetgever de inhoud wel reguleren, mits sprake is van een 'compelling state interest' en voldaan is aan de eisen van proportionaliteit en subsidiariteit (zie par. 3.4).

De Hoge Raad gaat eveneens geheel voorbij aan het 'chilling effect' dat een algemeen verbod op anonimiteit kan hebben op niet-strafbare anonieme geschriften. Criminalisering van anonieme uitingen leidt er immers toe dat ook de onschuldige burger met een legale boodschap te allen tijde zijn naam moet vermelden. Dit kan onder omstandigheden leiden tot zelfcensuur. Dat de Hoge Raad hierop niet ingaat is temeer opmerkelijk aangezien het voorkomen van zelfcensuur voor de formele wetgever een belangrijke reden was om ten behoeve van drukkers en uitgevers in het Wetboek van Strafrecht een vervolgingsuitsluitingsgrond in het leven te roepen.

12. HR 28 november 1950, *NJ* 1951, 137 (*Tilburg*).
13. De Meij 1980, p. 125; De Meij 2000, p. 121. In zijn annotatie bij het Muurkranten-arrest merkt Peters op dat men anonieme geschriften zou kunnen rekenen tot de categorie 'alternatieve verspreidingsmiddelen'. *NJCM-Bulletin* (5) 1980, p. 300-301.

Hoe verhoudt de benadering van de Hoge Raad zich nu met het door de formele wetgever ingenomen standpunt ten aanzien van anonieme geschriften? In de Memorie van Toelichting bij het drukkers- en uitgeversprivilege van artikel 53 en 54 Sr overwoog de wetgever dat

> "er een zeer overwegende grond van staatsbelang [moet] bestaan om de op zich zelve volkomen geoorloofde handeling der verspreiding van een geschrift, dat niet onder het bereik der strafwet valt, strafbaar te verklaren, alleen omdat het den naam van den drukker, uitgever of schrijver niet draagt' én dat 'zoodanige grond [niet] bestaat wanneer de wet verspreiding van strafbare geschriften genoegzaam beteugelt".[14]

De Hoge Raad oordeelt, zonder nadere motivering, dat hieruit niet kan worden afgeleid dat de gemeentelijke wetgever de bevoegdheid zou missen om anonieme uitingen in het belang van de openbare orde te verbieden. Ook dit oordeel lijkt vatbaar voor kritiek. Men kan hieraan immers tegenwerpen dat een gemeentelijk verbod op anonimiteit, hoewel staatsrechtelijk misschien in overeenstemming met de regelgevende competentie van de gemeentelijke wetgever, toch tenminste in strijd is met de bedoeling van de formele wetgever. De bestrijding van strafbare geschriften werd door de formele wetgever niet aangemerkt als een 'zeer overwegende grond van staatsbelang' die een algemeen verbod op anonimiteit in het Wetboek van Strafrecht rechtvaardigde. Waarom zou het door de gemeente Utrecht naar voren gebrachte belang – het ter verantwoording kunnen roepen van de voor de publicatie verantwoordelijke persoon of instantie – dan wel als zodanig kunnen worden aangemerkt? Bij gebreke van een nadere motivering valt, gezien het oordeel van de formele wetgever dat een algemeen verbod op anonieme geschriften in het Wetboek van Strafrecht niet gewenst is, moeilijk in te zien waarom een dergelijk verbod op gemeentelijke niveau wel wenselijk zou zijn.

Mijns inziens had de Hoge Raad zijn oordeel overtuigender kunnen motiveren door er op te wijzen dat de verspreiding van anonieme muurkranten waarop de gemeentelijke regeling betrekking had in één belangrijk opzicht verschilde van de verspreiding van gedrukte stukken in de zin van de artikelen 53 en 54 Sr. Bij de verspreiding van de muurkranten was, naar mag worden aangenomen, geen drukker of uitgever betrokken. Daarmee ontbrak eveneens de mogelijkheid om de verantwoordelijke persoon met hulp van de tussenpersoon te achterhalen. Er was bij de muurkranten zodoende sprake van absolute anonimiteit. Waar de bescherming van de bron bij relatieve vormen van anonimiteit slechts wordt opgeheven als daarvoor zwaarwegende redenen zijn, moest de gemeente Utrecht kiezen tussen twee kwaden: óf de anonieme verspreiding van informatie werd vooraf verboden met als risico een 'chilling effect' op onschuldige uitingen óf strafbaarstelling werd achterwege gelaten met als nadeel dat de afzender in de meeste

14. Smidt 1881, p. 423-424.

gevallen niet kan worden opgespoord. Deze omstandigheid had een voorafgaand verbod op anonimiteit op een meer geloofwaardige manier kunnen rechtvaardigen.

6.4 Het journalistieke verschoningsrecht

Met de totstandkoming van de artikelen 53 en 54 Sr was de positie van drukkers en uitgevers bij de verspreiding van anonieme geschriften geregeld. Over de positie van een andere belangrijke tussenpersoon in het communicatieproces, de journalist, bleef in Nederland echter lange tijd verschil van mening bestaan.[15] Met name vanuit de perswereld werd gepleit voor de aanvaarding van een journalistiek verschoningsrecht, inhoudende dat journalisten niet verplicht zouden zijn de identiteit van hun bronnen te onthullen. De Hoge Raad wees principiële erkenning echter af. In 1977 erkende zij in het arrest *Hoogendijk/KGB* wel dat

> "het algemene belang van de nieuwsgaring ermee kan zijn gediend dat de journalist een verschoningsrecht wordt toegekend, omdat daardoor de door informanten gewenste geheimhouding, in het bijzonder m.b.t. hun identiteit, beter is verzekerd en zodoende informanten niet van het geven van inlichtingen worden weerhouden".

Dit belang werd echter resoluut achtergesteld bij het belang van de rechtshandhaving. Toekenning van een verschoningsrecht aan de journalist zou voor degenen die door een perspublicatie worden geschaad een ernstige belemmering in de handhaving van hun rechten opleveren. De onaanvaardbaarheid van deze consequentie moest zwaarder wegen dan de nadelen voor de nieuwsgaring, die in bepaalde gevallen verbonden kunnen zijn aan het ontbreken van een verschoningsrecht. De stelling dat de journalist een verschoningsrecht toekomt kon daarom in haar algemeenheid niet worden aanvaard.[16] Ook in een uitspraak over bronbescherming door gemeenteraadsleden toonde de Hoge Raad zich zeer terughoudend. Wel werd het belang van de nieuwsgaring nogmaals nadrukkelijk bevestigd. De Hoge Raad spreekt van het hoogwaardige maatschappelijke belang

> "dat niet, door gebrek aan bekendheid bij het grote publiek, misstanden die de samenleving raken kunnen voortbestaan dankzij het onvermogen van de verantwoordelijke overheidsorganen om, in een gecompliceerde maatschappij als die waarin wij leven aandacht te geven aan alle zaken die deze aandacht verdienen".[17]

15. Een overzicht van de ontwikkelingen in het Nederlandse recht kan men vinden in het proefschrift van Korthals Altes. Korthals Altes 1989.
16. HR 11 november 1977, *NJ* 1978, 399 (*Hogendijk/KGB*). Zie ook Korthals Altes 1989, p. 10 e.v.
17. HR 24 juni 1983, *NJ* 1984, 801 (*Gemeenteraadslid*).

Het standpunt van de Hoge Raad wordt onderuitgehaald wanneer het Europese Hof voor de Rechten van de Mens uitspraak doet in de zaak *Goodwin*.[18] Goodwin, een Britse journalist, wordt telefonisch ingelicht over de labiele financiële situatie van de vennootschap Tetra Ltd. (hierna: Tetra). Wanneer hij tracht om bij Tetra een bevestiging van die informatie te verkrijgen, blijkt deze informatie afkomstig te zijn uit een gestolen exemplaar van Tetra's vertrouwelijke bedrijfsplan. Tetra is bang dat het bekend worden van de informatie zal leiden tot volledig vertrouwensverlies bij haar schuldeisers en slaagt er in om via de rechter een publicatieverbod te verkrijgen. De rechter beveelt Goodwin om de notities van zijn telefoongesprek te overleggen en de identiteit van de bron vrij te geven.[19] Goodwin weigert aan deze bevelen te voldoen. Na afwijzing van zijn bezwaren in hoger beroep wordt aan hem een boete van vijfduizend Britse ponden opgelegd. Voor het Europese Hof betoogt Goodwin dat het rechterlijk bevel om de identiteit van de bron te openbaren en de boete op weigering dat te doen, in strijd zijn met artikel 10 EVRM. Hij stelt dat een verplichting om zijn bron te onthullen slechts kan worden aangenomen in uitzonderlijke omstandigheden, wanneer vitale algemene of individuele belangen op het spel staan.

Het Hof constateert dat sprake is van een beperking op de vrijheid van meningsuiting en gaat in op de vraag of de geconstateerde beperking noodzakelijk is in een democratische samenleving. Het kent een bijzonder belang toe aan de omstandigheid dat journalistieke bronbescherming een van de basisvoorwaarden is voor persvrijheid:

> "Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected."

Gezien het mogelijke 'chilling effect' dat een rechterlijk bevel tot onthulling van een bron kan hebben op de uitoefening van de persvrijheid, is een dergelijke maatregel onverenigbaar met artikel 10 EVRM tenzij zij wordt gerechtvaardigd door een "overriding requirement in the public interest" (r.o. 39).[20]

Het doel van het bevel tot onthulling was naar het oordeel van het Hof al grotendeels bereikt doordat aan Goodwin reeds een verspreidingsverbod was opgelegd dat aan alle

18. EHRM 27 maart 1996, *NJ* 1996, 577 (*Goodwin*).
19. Het bevel wordt gegeven op basis van sectie 10 van de Contempt of Court Act 1981, dat luidt: "No court may require a person to disclose, nor is a person guilty of contempt of court for refusing to disclose the source of information contained in the publication for which he is responsible, unless it be established to the satisfaction of the court that disclosure is necessary in the interests of justice or national security or for the prevention of disorder or crime."
20. Het Europese Hof heeft zijn uitgangspunt in latere uitspraken enkele malen bevestigd. Zie onder andere EHRM 23 september 1994, *NJ* 1995, 387 (*Jersild*) en EHRM 21 januari 1999, *NJ* 1999, 713 (*Fressoz & Roire*).

nationale kranten en weekbladen ter kennisgeving was gebracht. Dat met dit verbod de verspreiding van de informatie door de pers effectief kon worden voorkomen was in rechte reeds komen vast te staan. Voor zover het bevel tot onthulling van de bron louter bedoeld was om handhaving van het verspreidingsverbod mogelijk te maken werd het daarom niet ondersteund door voldoende redenen in de zin van artikel 10 lid 2 EVRM (r.o. 42). Tetra had echter nog andere belangen bij de onthulling van de bron. In de eerste plaats kon het aan Goodwin gerichte verspreidingsverbod niet voorkomen dat de bron zelf de informatie zou verspreiden onder klanten of concurrenten van Tetra. Verspreiding door de bron zelf kon door Tetra alleen worden tegengegaan wanneer zij op de hoogte zou zijn van zijn identiteit. Alleen dan zouden immers gerechtelijke stappen kunnen worden ondernomen om het vermiste document terug te krijgen. In de tweede plaats had Tetra als commerciële onderneming een gerechtvaardigd belang om de werknemer te ontmaskeren die voor het uitlekken van het document verantwoordelijk was (r.o. 44). Tetra's belang bij het wegnemen van de resterende dreiging van de verspreiding van de vertrouwelijke informatie anders dan door de pers, bij het verkrijgen van schadevergoeding en bij het ontmaskeren van een ontrouwe werknemer, wogen zelfs in onderlinge samenhang beschouwd, echter onvoldoende zwaar om het essentiële belang van Goodwin bij de bescherming van zijn bron opzij te zetten. Het Hof overweegt:

> "(…) as also recognised by the national courts, it will not be sufficient, per se, for a party seeking disclosure of a source to show merely that he or she will be unable without disclosure to exercise the legal right or avert the threatened legal wrong on which he or she bases his or her claim in order to establish the necessity of disclosure".

Enige tijd later neemt de Hoge Raad in de zaak *Van den Biggelaar* de zienswijze van het Europese Hof over.[21] Het betreft publicaties van de journalisten Dohmen en Langenberg in het dagblad 'De Limburger' over gerechtelijke vooronderzoeken tegen een aantal Limburgse bestuurders, waaronder Van den Biggelaar, wegens verdenking van omkoping. Van den Biggelaar c.s. vorderen schadevergoeding wegens schending van hun privacy en wensen door middel van een voorlopig getuigenverhoor de bronnen van de betreffende publicaties en de door die bronnen verstrekte informatie te weten te komen. Het beroep van de twee journalisten op het journalistiek verschoningsrecht wordt aanvankelijk afgewezen. De Hoge Raad oordeelt echter dat uit het Goodwin arrest volgt:

> "dat moet worden aanvaard dat uit het eerste lid van art. 10 EVRM voor een journalist in beginsel het recht voortvloeit zich te verschonen van het beantwoorden van een hem gestelde vraag indien hij daardoor het bekend worden van zijn bron zou riskeren, maar dat de rechter een beroep op dit recht niet behoeft te honoreren wanneer hij van oordeel is dat in de bijzondere omstandigheden van het gegeven geval openbaring van die bron in een democratische samenleving noodzakelijk is met het

21. HR 10 mei 1996, *NJ* 1996, 578 (*Van den Biggelaar*).

> oog op een of meer van de in het tweede lid van voormelde verdragsbepaling bedoelde, door degene die de journalist als getuige doet horen, te stellen en, zonodig, aannemelijk te maken belangen".

Advocaat-generaal Koopmans wijst in zijn conclusie op drie ontwikkelingen die zich sinds de uitspraak van de Hoge Raad in de zaak *Hoogendijk/KGB* in 1977 hebben voorgedaan. Het belang van de nieuwsgaring is, onder andere in het arrest *Gemeenteraadslid* verder uitgewerkt. In de tweede plaats is er in de samenleving in toenemende mate sprake van mafiose praktijken zoals de 'omkopingscultuur' in Limburg waar het in casu om ging. Bij corruptie, drugscriminaliteit en georganiseerde afpersing plegen zowel daders als slachtoffers te zwijgen, hetzij omdat zij zelf medeplichtig zijn, hetzij uit angst voor represailles. Hoe beter anonimiteit wordt beschermd, hoe groter de kans dat dergelijke misstanden toch aan het licht komen. In de derde plaats wordt in het burgerlijk procesrecht van partijen steeds meer verlangd dat zij meewerken aan de waarheidsvinding. Sinds 1989 kan de rechter op basis van artikel 19a Rv aan partijen bevelen dat zij bescheiden overleggen en inlichtingen verschaffen. Daarnaast is de partij-getuige geïntroduceerd en zijn de eisen inzake de stelplicht verzwaard. De genoemde ontwikkelingen brengen met zich mee dat aan de waarheidsvinding tegengestelde belangen, zoals de bescherming van een anonieme bron, eerder in het gedrang komen (r.o. 5). Koopmans voegt hier nog de sociologische observatie aan toe dat de politieke en sociale rol van de media steeds belangrijker wordt in een samenleving waarin georganiseerde verbanden met bureaucratische structuren steeds meer zeggenschap en invloed verwerven. Wanneer binnen zulke organisaties misstanden bestaan is de publieke opinie eigenlijk het enige mogelijke tegenwicht. Het publiek kan echter slechts in actie komen als het op de hoogte is.

De erkenning van het journalistieke verschoningsrecht in het *Goodwin*-arrest is voor het Comité van Ministers van de Raad van Europa aanleiding geweest om een aanbeveling tot stand te brengen.[22] Hierin worden de lidstaten opgeroepen het beroepsgeheim van de journalist wettelijk te regelen. Om te bevorderen dat het bronnengeheim in alle lidstaten dezelfde bescherming krijgt is daarnaast een aantal principes geformuleerd. De werkingssfeer van het verschoningsrecht is ruim omschreven. In de appendix bij de aanbeveling wordt als journalist aangemerkt "any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication". Onder het begrip 'information' valt 'any statement of fact, opinion or idea in the form of text, sound and/or picture'. De aanbeveling bevat zeven basisprincipes waarvan de eerste en belangrijkste het recht is van de journalist om zijn bron niet te onthullen. Dit recht kan krachtens slechts onder nauw omschreven voorwaarden worden beperkt (zie principle 3b):

22. Zie Recommendation R (2000) 7. Zie over deze aanbeveling ook Voorhoof 2000.

"The disclosure of information identifying a source should not be deemed necessary unless it can be convincingly established that:
- reasonable alternative measures to the disclosure do not exist or have been exhausted by the persons or public authorities that seek the disclosure, and
- the legitimate interest in the disclosure clearly outweighs the public interest in the non-disclosure, bearing in mind that:
  - an overriding requirement of the need for disclosure is proved,
  - the circumstances are of a sufficiently vital and serious nature,
  - the necessity of the disclosure is identified as responding to a pressing social need, and
  - member states enjoy a certain margin of appreciation in assessing this need, but this margin goes hand in hand with the supervision by the European Court of Human Rights."

Als 'information identifying a source' moet, voor zover het aannemelijk is dat deze zal kunnen leiden tot identificatie van de bron, in ieder geval worden aangemerkt:

"– the name and personal data as well as voice and image of a source,
- the factual circumstances of acquiring information from a source by a journalist,
- the unpublished content of the information provided by a source to a journalist, and
- personal data of journalists and their employers related to their professional work".[23]

In Nederland is aan het advies om te voorzien in een wettelijke regeling geen gevolg gegeven. De Minister van Justitie was van oordeel dat de rechter de nadere invulling van de belangenafweging, zoals uitgewerkt in de aanbevelingen, direct kan betrekken in zijn beoordeling en dat in de aanbevelingen geen ruimere betekenis wordt toegekend aan het recht op bronbescherming dan voortvloeit uit de rechtspraak van het EHRM.[24]

Wie precies als journalist kan worden aangemerkt, is het onderwerp van een eeuwige discussie. Ook de aanbeveling van de Raad van Europa geeft hierover geen duidelijkheid, nu het begrip journalist daarin zeer ruim is omschreven. Een actuele ontwikkeling is in dit verband het steeds toenemende aantal zogenaamde 'weblogs' op het internet. In hoeverre de schrijvers hiervan ook bescherming kunnen ontlenen aan het journalistieke verschoningsrecht komt in het volgende hoofdstuk nog aan de orde (zie par. 7.1.3).

6.5 Conclusie

Het drukkers- en uitgeversprivilege en het journalistieke verschoningsrecht regelen de anonieme verspreiding van informatie door middel van de drukpers en via de institutionele media zoals kranten en tijdschriften. Daarmee wordt in grote lijnen het hele scala

23. Zie de 'definitions' sub d in de appendix bij de Aanbeveling. De Nederlandse rechter heeft conform de aanbeveling ook een zipschijf met identificerende informatie onder de bescherming van het brongeheim gebracht. HR 8 april 2003, *Mediaforum 2003-6,* p. 209-210 m.nt. Schuijt (*Bronbescherming voor zipschijf*).
24. *Kamerstukken II* 2000/01, 27 400 VI, nr. 7; *Handelingen II* 2000/01, 26 september 2000, p. 174-176. Zie ook Schuijt 2001.

van traditionele communicatiemiddelen bestreken. Het journalistieke verschoningsrecht reikt zelfs nog verder doordat het van toepassing is op de verspreiding van informatie 'via any means of mass communication'. Beide rechtsinstituten betreffen de positie van de tussenpersoon en zij creëren een systeem van relatieve anonimiteit. Het bekendmaken van de dader of de lastgever geldt, wanneer wegens verdenking van een drukpersdelict tot een gerechtelijk vooronderzoek is overgegaan, ten aanzien van drukkers en uitgevers als voorwaarde om een beroep te kunnen doen op de vervolgingsuitsluitingsgrond in het Wetboek van Strafrecht. Een weigering om de dader of de lastgever bekend te maken wordt zodoende gesanctioneerd met strafrechtelijke aansprakelijkheid voor de inhoud van het gedrukte. Het journalistieke privilege is in de rechtspraak nadrukkelijk geformuleerd als een aan de journalist toekomend recht. Hij kan door de rechter slechts worden gedwongen tot afgifte van identificerende informatie nadat het belang van de eisende partij getoetst is aan artikel 10 lid 2 EVRM. Waar de lagere rechter en de Hoge Raad het belang van de toerekenbaarheid aanvankelijk zwaar lieten wegen, kent het Europese Hof meer bescherming toe aan de essentiële positie van de journalist in de democratische samenleving.

Wetgever en rechter hebben bij de totstandkoming van zowel het drukkers- en uitgeversprivilege als het journalistieke verschoningsrecht veel waarde gehecht aan het belang van de 'free flow of information'. De positie van drukkers, uitgevers en journalisten, als onmisbare schakels in het maatschappelijke communicatieproces, zou ernstig worden bedreigd indien zij te allen tijde zouden kunnen worden ingeschakeld bij de opsporing van de anonymus. De vervolgingsuitsluitingsgrond voor drukkers en uitgevers werd tot stand gebracht om te voorkomen dat zij zouden overgaan tot het eigenhandig uitoefenen van censuur uit angst voor strafrechtelijke vervolging. Bij de journalist speelt, naast de voorkoming van censuur, in het bijzonder het belang van de vrije nieuwsgaring, de rol van de media als 'public watchdog' en het risico dat bronnen 'opdrogen' wanneer hun anonimiteit niet voldoende gewaarborgd is.

Waar algemene maatschappelijke belangen en de bescherming van de tussenpersoon veel aandacht krijgen, lijkt het individuele belang van de anonieme bron zelf een minder grote rol te hebben gespeeld. Hij kan uit de aard der zaak moeilijk op de voorgrond treden om zijn stem te laten horen en is in procedures als partij niet betrokken. De vraag of de anonieme auteur van een gedrukt stuk en de anonieme journalistieke bron een zelfstandig recht op anonimiteit zouden hebben met een eventueel daaruit voortvloeiende aanspraak op bescherming door de tussenpersoon, is dan ook nog niet aan de orde gekomen. In de volgende hoofdstukken zal blijken dat deze vraag in de informatiesamenleving aanzienlijk aan belang heeft gewonnen. Daarnaast is nergens in de overwegingen van wetgever en rechter een diepgaande theoretische beschouwing te vinden over het precieze verband tussen anonimiteit en uitingsvrijheid.

Vergelijkt men het Nederlandse Muurkrantenarrest met de jurisprudentie van het Amerikaanse Supreme Court, dan ontstaat de indruk dat de Hoge Raad een uitgelezen mogelijkheid voorbij heeft laten gaan om de relatie tussen anonimiteit en uitingsvrijheid

en de daarmee samenhangende noodzaak tot bescherming van anonimiteit te erkennen. Het gebrek aan aandacht voor de grondrechtelijke aspecten van het Utrechtse anonimiteitsverbod staat in schril contrast met de benadering van het Supreme Court, dat de grondrechtelijke aspecten van identificatie en registratie juist herhaaldelijk heeft benadrukt. Doordat de Hoge Raad het anonimiteitsverbod niet aanmerkte als een beperking van de uitingsvrijheid, kwam hij aan een inhoudelijke toetsing daarvan niet toe. Zodoende negeerde hij de Nederlandse geschiedenis, waarin het verband tussen verboden op anonimiteit en de uitoefening van censuur, zoals wij zagen in het vorige hoofdstuk, meer dan in de Amerikaanse geschiedenis al vroeg aanwezig is.

7 Anonimiteit in de informatiesamenleving

7.1 Inleiding

Na de uitvinding van de drukpers stonden vraagstukken rondom de regulering van anonieme communicatie lange tijd voornamelijk in het teken van de uitingsvrijheid. Dit kwam in de voorgaande hoofdstukken duidelijk naar voren. In de tweede helft van de negentiende eeuw kreeg de drukpers echter concurrentie. De telegraaf en de telefoon werden uitgevonden en men begon met de aanleg van telecommunicatienetwerken. Informatie werd nu niet langer alleen verspreid via fysieke dragers en het gesproken woord, maar ook met behulp van elektromagnetische signalen, via telefoon- en telegraafkabels. In de twintigste eeuw zouden deze nieuwe technologieën zich geleidelijk ontwikkelen tot de elektronische communicatiemiddelen die wij vandaag de dag kennen. Dit hoofdstuk beschrijft hoe de betekenis van anonimiteit als gevolg van digitalisering, de opkomst van elektronische gegevensverwerking en de samenvloeiing van communicatiemiddelen langzamerhand veranderde. Daarbij komt onder andere aan de orde hoe het recht op privacy aan betekenis won en hoe dit recht in de digitale omgeving een ondersteuning vormt voor anonieme openbare communicatie. Aldus wordt een inleiding gegeven voor de hiernavolgende hoofdstukken waarin de bescherming en doorbreking van anonimiteit bij elektronische communicatie aan de orde zullen komen.

7.1.1 Telecommunicatie

Voor de wetgever leidde de opkomst van telecommunicatie, anders dan die van de drukpers, niet onmiddellijk tot radicaal nieuwe handhavingsproblemen. In de begindagen van de telegrafie en de telefonie was het anonieme gebruik van telecommunicatienetwerken en -diensten nog niet aan de orde. Aanvragen voor een telefoongesprek werden afgehandeld door een telefoniste en telegrammen werden doorgaans persoonlijk aan het loket gedicteerd.[1] De telegraaf en de telefoon werden bovendien voornamelijk gebruikt voor besloten communicatie en niet voor de verspreiding van openbare informatie. Een duidelijke relatie met de uitingsvrijheid tekende zich daarom nog niet af. Ook de relatie met het recht op privacy zou later pas werkelijk van belang worden. Het denken over privacy kwam aan het einde van de 19e eeuw weliswaar sterk op, maar werd nog niet in ver-

1. Een gedetailleerde historische beschrijving van het telefoon- en telegraafverkeer in Nederland kan men vinden bij Schuilenga e.a. 1981.

band gebracht met de verwerking van persoonsgebonden informatie en de daaruit voortvloeiende herleidbaarheid van communicatiehandelingen.[2] Het communicatiegeheim speelde al wel een rol. Dit grondrecht bood echter geen bescherming voor de identiteit van gebruikers.

In de twintigste eeuw werd de telecommunicatie-infrastructuur gestaag uitgebreid. Ook de technische ontwikkeling schreed voort. Men stapte over van handmatige naar automatische schakelcentrales en in de jaren zeventig begon een overgang van analoge naar digitale communicatie.[3] Het samengaan van computertechnologie en telecommunicatie leidde tot ingrijpende veranderingen. Begin jaren tachtig werd het openbare telefoonnet met behulp van de ISDN-standaard (Integrated Services Digital Network) omgebouwd tot een digitaal netwerk. Op een ISDN-toegang konden acht verschillende randapparaten worden aangesloten (telefoon, fax, modem etc.). Bovendien konden nieuwe diensten worden aangeboden, zoals gelijktijdige verzending van beeld en spraak, videoconferenties, automatische nummerherkenning, het doorschakelen van oproepen en telefonische wekdiensten.

De introductie van de ISDN-standaard luidde een belangrijke nieuwe fase in omdat de digitalisering van het telefoonnet het communicatieproces doorzichtig maakte. Bij de afhandeling van telecommunicatieverkeer via digitale telefooncentrales worden immers zogenaamde 'call records' aangemaakt met gegevens die benodigd zijn voor het tot stand brengen van de verbinding. Sommige van deze 'verkeersgegevens', zoals het telefoonnummer van de oproepende en de opgeroepen gebruiker, zijn privacygevoelig. Netwerkbeheerders en leveranciers van diensten zijn met behulp van deze gegevens in staat om individuele communicatiehandelingen te registreren, bijvoorbeeld voor factureringsdoeleinden. Maar de gegevens kunnen ook voor andere doeleinden worden gebruikt. Ook de nieuwe diensten die over het digitale netwerk worden geleverd roepen privacyvraagstukken op. Gespecificeerde rekeningen stellen de gebruiker enerzijds in staat om zijn rekening te controleren maar zeggen anderzijds veel over zijn gedrag. Eenzelfde dilemma speelt bij nummeridentificatie. Nummeridentificatie kan preventief werken bij ongewenste telefoontjes en nuttig zijn voor hulpdiensten. Anderzijds wordt de anonimiteit van de oproepende beller doorbroken.[4]

2. Dommering e.a. 2000, p. 49-50. In de Verenigde Staten, waar het denken over privacy het eerst opkwam, is de constitutionele bescherming van het recht op privacy onder andere gebaseerd op het in het Fourth Amendment geformuleerde recht van burgers "to be secure in their persons, their houses, papers and effects against unreasonable searches and seizures". Historisch is het privacyrecht dus sterk verbonden met de bescherming van de fysieke privé-sfeer door het eigendomsrecht en het huisrecht. Asscher 2002, p. 196-204; Blok 2002, p. 20-25, 43-48 en 157-158.
3. Sciarone-Gorgels 1994; Dommering e.a. 1999, p. 37 e.v.
4. Privacyaspecten van ISDN komen aan de orde bij Holvast 1994; Van Hoogstraten & Berkvens 1992.

De invoering van ISDN ging gepaard met heftige discussies, die uitmondden in initiatieven tot regelgeving.[5] Als aanvulling op de algemene privacyrichtlijn werd de 'ISDN-richtlijn' tot stand gebracht waarin de regelgeving over verwerking van gegevens in de telecommunicatiesector werd geharmoniseerd.[6] Deze richtlijn bevatte onder andere voorschriften over de anonimisering en verwijdering van verkeersgegevens, blokkering van nummeridentificatie, afscherming van nummers op gespecificeerde nota's en vermelding van persoonsgegevens in abonneelijsten (zie hierover het volgende hoofdstuk).[7] De aandacht voor de bescherming van privacy in de telecommunicatiesector stond overigens niet op zichzelf. Zij was uitvloeisel van een bredere maatschappelijke beweging waarin de gestage opmars van (elektronische) gegevensverwerking leidde tot een sterke opkomst van de informationele privacy en de ontwikkeling van het gegevensbeschermingsrecht.[8] Gegevensverwerking over communicatiegedrag kan bovendien in strijd komen met de bescherming van het communicatiegeheim. Dit kwam onder andere tot uitdrukking in de rechtspraak van het Europese Hof voor de Rechten van de Mens, die elektronische communicatie onder de bescherming van artikel 8 EVRM bracht en ook de verwerking van verkeersgegevens beschouwde als rakend aan het recht op respect voor correspondentie.[9]

De verwerking en opslag van gegevens in de telecommunicatiesector neemt nog steeds toe. Oorzaken hiervoor zijn onder andere de toegenomen hoeveelheid communicatieverkeer en een toegenomen verwerkings- en opslagcapaciteit. Met de komst van nieuwe communicatietechnologieën worden ook nieuwe soorten gegevens verwerkt en opgeslagen. Zo worden in mobiele communicatienetwerken gegevens gegenereerd over de locatie van mobiele randapparatuur (de zgn. locatiegegevens) waarmee vrij nauwkeurig kan worden vastgesteld waar de gebruiker van bijvoorbeeld een mobiele telefoon zich op een bepaald moment bevindt. Op het internet ontstaan verkeersgegevens over surfgedrag. De

5. Met name vanuit Duitsland klonken sterke bezwaren. Daar werd, met de Duitse geschiedenis in het achterhoofd, sterk aangedrongen op bescherming van burgerlijke vrijheden. Bovendien pleitte men voor technische maatregelen om de opslag en verwerking van gegevens zoveel mogelijk te beperken. Zie Garnham & Aksoy 1989, m.n. p. 65 e.v.
6. Richtlijn 97/66/EG van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *PbEG* 1998 L 24/1.
7. Sciarone Gorgels 1994.
8. Een ander goed voorbeeld van een maatschappelijke discussie omtrent gegevensverwerking is die rond de volkstellingen van 1971 en 1981, uitgebreid behandeld door Holvast. Holvast 1986, p. 147 e.v.
9. De belangrijkste uitspraken zijn *Klass, Malone, Kruslin en Huvig* en *Kopp*. Zie EHRM 6 september 1978 (*Klass*), Series A, nr. 28, *AA* 1979, jrg. 28, p. 327-334, m.nt. EAA, Lawson & Schermers 1997, p. 54-68; EHRM 2 augustus 1984 (*Malone*), Series A, nr. 82; EHRM 24 april 1990 (*Kruslin en Huvig*), Series A, nr. 176-A, *NJ* 1991, nr. 532, m.nt. EJD; EHRM 25 maart 1998 (*Kopp*), NJ 2001, 459. Zij worden uitgebreid behandeld in Asscher 2002, 129-134; Privacy International 2004.

eindgebruiker laat zodoende een digitaal spoor achter dat vrij nauwkeurig aangeeft welke websites en discussiefora hij heeft bezocht en met wie hij heeft gecommuniceerd.

De bescherming van verkeersgegevens is de laatste jaren een steeds terugkerend thema. Sinds enige tijd bestaat bij verschillende Europese lidstaten de wens om te komen tot een algemene bewaarplicht voor deze gegevens. Na de aanslagen op 11 september 2001 hebben deze initiatieven extra prioriteit gekregen. Het voorstel beoogt telecomaanbieders en internetproviders te verplichten tot het bewaren van de verkeers- en locatiegegevens van hun klanten.[10] Aanvaarding hiervan zou een belangrijke uitzondering zijn op de nu nog geldende regel in de richtlijn privacy en elektronische communicatie, de opvolger van de ISDN-richtlijn, dat verkeers- en locatiegegevens moeten worden geanonimiseerd of verwijderd zodra zij niet langer nodig zijn voor de transmissie van elektronische communicatie (zie par. 8.3.3).[11]

7.1.2 De omroep

Uit de telecommunicatietechniek ontstond begin twintigste eeuw ook de omroep.[12] Dit medium onderscheidde zich aanvankelijk van de telefoon en de telegraaf doordat de verspreiding van radio- en televisieprogramma's niet plaatsvond via een fysieke infrastructuur, maar via de ether. Ook het communicatiemodel van de omroep week af. De klassieke omroep heeft een 'point-to-multipoint'-karakter: de informatie stroomt van één zender naar een onbeperkt aantal ontvangers. Bovendien is er alleen éénrichtingsverkeer mogelijk. Dat maakt het technisch onmogelijk om het kijk- of luistergedrag te controleren of te registreren. De anonimiteitsvraagstukken liggen daardoor, evenals bij de drukpers, voornamelijk in het domein van de informatieverspeider, dat wil zeggen de omroeporganisatie, de programmaredactie of de journalist.

Voor zover het anonimiteitsvraagstukken betreft, laat de omroep zich beter vergelijken met de drukpers dan met de eerste telefoniediensten. Drukpers en omroep zijn beide openbare communicatiemiddelen. De komst van de radio bracht, evenals de drukpers, een revolutie te weeg in de verspreiding van nieuws en informatie aan het grote publiek. Ook hier werd al snel censuur toegepast. Het grensoverschrijdende karakter van de radio maakte de politieke uitingsvrijheid tot een belangrijk thema.[13] De identificeerbaarheid van informatieverspreiders en informatiebronnen alsook de verhouding tussen anonimiteit en uitingsvrijheid worden daarmee relevant. Voor de autoriteiten is de anonimiteit van de verspreider bij de omroep echter een minder groot obstakel dan bij de drukpers. Waar in het tijdperk na de uitvinding van de drukpers vaak niet alleen de auteur van het anonieme geschrift maar ook de drukker ervan onvindbaar was, biedt het bouwwerk van

10. Zie Ekker 2002b, 2004a.
11. De constitutionele bescherming van verkeersgegevens is nog niet geheel duidelijk. Asscher 2000, 2002; Asscher en Ekker 2003a; Privacy International 2004.
12. Dommering e.a. 2000, p. 121 e.v.
13. Dommering 2003, p. 191 e.v.

de institutionele omroepinstellingen genoeg mogelijkheden om een verantwoordelijke verspreider te vinden. Doorgaans kan vrij eenvoudig een omroeporganisatie, redactie of journalist worden aangewezen. Bovendien staan omroeporganisaties via het vergunningenstelsel al onder overheidstoezicht. De wetgever heeft dan ook niet de behoefte gevoeld om algemene bepalingen tot stand te brengen die de anonieme verspreiding van informatie via de omroep aan banden leggen of strafbaar stellen.

De identificeerbaarheid van andere personen dan de verspreider van de informatie, speelt bij de omroep in uiteenlopende situaties. Een van de voornaamste problemen is de privacy van personen die ongewild of buiten hun medeweten herkenbaar in beeld worden gebracht of die anderszins het onderwerp zijn van berichtgeving. Deze kwestie speelt bijvoorbeeld wanneer verslag wordt gedaan van strafbare feiten. Onder omstandigheden kan het niet in acht nemen van bepaalde voorzorgsmaatregelen, bijvoorbeeld het plaatsen van een zwarte balk op een foto of het anonimiseren van een achternaam, in strijd komen met de relationele privacy, het portretrecht of de bescherming van eer en goede naam van een verdachte. Aangezien de wens om anoniem te zijn hier niet gerelateerd is aan communicatiehandelingen van de verdachte zelf, laat ik dit onderwerp verder buiten beschouwing. Relevanter voor dit onderzoek is de identificeerbaarheid van personen die via de media zelf informatie in omloop hebben gebracht of uitlatingen hebben gedaan. De wens of de noodzaak om deze personen te identificeren komt doorgaans aan de orde wanneer deze informatie of uitlatingen een strafbaar karakter hebben of wanneer zij schade berokkenen aan een derde partij. Of de verantwoordelijke redactie danwel journalist verplicht kan worden de identiteit te onthullen hangt onder andere af van de vraag in hoeverre informatie onrechtmatig is, in hoeverre de privacy en de eer en goede naam van derden zijn geschonden en of een succesvol beroep kan worden gedaan op het journalistieke verschoningsrecht. Hoewel het journalistieke verschoningsrecht bij de omroep altijd een actueel thema is geweest, wijken de vragen die daaromtrent ontstonden niet fundamenteel af van de vragen welke bij de drukpers reeds waren gerezen (zie het vorige hoofdstuk). Op het internet ontstaan rondom het journalistieke verschoningsrecht wel enige nieuwe vragen. Deze worden besproken in de volgende paragraaf.

Beschouwd vanuit de uitingsvrijheid leken anonieme uitingen via de omroep aanvankelijk weinig nieuwe vragen op te roepen. Langzamerhand voltrok zich echter ook hier een proces van technische verandering waardoor de privacy van kijkers en luisteraars steeds meer in de aandacht kwam te staan. In de eerste plaats ontstonden naast de klassieke omroepdienst stap voor stap gedigitaliseerde en interactieve omroepdiensten die niet langer alleen via de ether, maar ook via kabelnetwerken werden geleverd. Voorbeelden zijn teletekst, abonneetelevisie, en 'video on demand'. Het interactieve karakter van deze diensten bestaat er uit dat op verzoek van de gebruiker informatie wordt opgevraagd en dat deze informatie op individuele basis wordt geleverd en betaald, bijvoorbeeld door middel van 'pay-per-view'. Om dit mogelijk te maken moest het kabelnetwerk geschikt worden gemaakt voor de verzending van informatie van de eindgebruiker

naar de leverancier. Dit 'retourverkeer' maakte het kijk- en luistergedrag voor het eerst registreerbaar.[14]

Met het mogelijk worden van twee-wegverkeer ontstonden privacyvraagstukken die vergelijkbaar zijn met die uit de wereld van de telefonie. Daarnaast was ook hier sprake van een toenemende elektronische gegevensverwerking. Een recente ontwikkeling die de doorzichtbaarheid van het kijk- en luistergedrag nog eens vergroot, is het gebruik van 'conditional access'-systemen. De levensvatbaarheid van commerciële omroepdiensten is veelal afhankelijk van toepassingen die de toegang tot het netwerk en de dienst reguleren en die ervoor zorgen dat de afnemer alleen toegang krijgt wanneer hij betaald heeft. Conditional access systemen creëren een nieuwe mogelijkheid om de gebruiker te identificeren en zijn communicatiegedrag te registreren.[15]

7.1.3 De digitale omgeving

In de voorgaande paragrafen werden telecommunicatie en omroep afzonderlijk behandeld. Deze techniekafhankelijke benadering wordt hierna losgelaten. Door technische ontwikkelingen wordt het steeds lastiger om verschillende communicatiemiddelen los van elkaar te zien. Het huwelijk van informatietechnologie en communicatietechnologie en de daarmee gepaard gaande digitalisering hebben geleid tot een samenvloeiing van communicatietechnieken. Dit proces van 'technische convergentie' is ook wel omschreven als "het verschijnsel dat verschillende typen infrastructuur in wezen gelijksoortige typen diensten kunnen overdragen', of als 'het verschijnsel dat de functies van gebruikersapparaten als telefoon, televisietoestel en computer elkaar gaan overlappen".[16] Convergentie vindt bij alle netwerken en eindapparaten plaats. Het telefoonnet wordt allang niet meer alleen gebruikt voor het voeren van telefoongesprekken maar ook voor andere vormen van telecommunicatie, zoals datacommunicatie, beeldtelefonie, teleconferencing en als toegangsmiddel voor e-mail en het internet. Mobiele telefonie wordt in toenemende mate gebruikt voor de verzending van elektronische berichten en bestanden. Bij de kabel is een vermenging van omroep- en telecommunicatiediensten te constateren. Ook op het niveau van de eindapparatuur is de technische convergentie onstuitbaar. De personal computer en de mobiele telefoon zijn getransformeerd tot multimediamachines die audio, video, telefonie en internetapplicaties in zich verenigen.[17]

14. De eerste experimenten met twee-weg verkeer via het kabelnetwerk stammen uit het begin van de jaren zeventig. Onder de term twee-weg verkeer schaarde men o.a. verschillende diensten op initiatief van de aangeslotene, zoals het vragen van informatie uit naslagwerken (computer time-sharing), elektronisch winkelen, het maken van reserveringen en het afroepen van video-programma's. Zie Stichting Moderne Media 1973, p. 47-48.
15. Zie Helberger 2005; Bygrave & Koelman 2000.
16. Groenboek convergentie 1997, p. 1. Zie ook Asscher 2002, p. 26-30.
17. *Kamerstukken II* 1997/98, 25 880, nrs. 1-2, p. 26-27.

Als gevolg van technische convergentie verdwijnt de vaste relatie tussen de dienst en het netwerk. Uit de koppeling van de oude netwerken ontstaat een nieuw netwerk dat dienstenneutraal is. Hierdoor vervagen de grenzen tussen traditionele communicatiemiddelen als pers, omroep en telecommunicatie en vallen diensten steeds moeilijker in één van deze categorieën in te delen. Vanuit technisch oogpunt hebben de nieuwe elektronische communicatiemiddelen nog maar één ding gemeenschappelijk, namelijk dat zij via elektromagnetische signalen de overdracht van informatie mogelijk maken. De technische convergentie heeft ook 'juridische convergentie' tot gevolg. Het is niet langer mogelijk om de regulering van een bepaalde communicatiedienst te koppelen aan het netwerk waarover deze dienst getransporteerd wordt.[18] Dit roept de vraag op in hoeverre techniekafhankelijke normen nog effectief en houdbaar zijn. Van groot belang is bijvoorbeeld in hoeverre bij de formulering van grondrechten nog langer onderscheid gemaakt kan worden tussen verschillende media. Anders gezegd: in hoeverre moet technische convergentie ook leiden tot constitutionele convergentie?[19]

Technische en juridische convergentie doet zich ook voor waar het gaat om de regulering van anonimiteit. Een aantal decennia geleden kon men aan de hand van technische kenmerken nog een duidelijk onderscheid maken tussen verschillende communicatiemiddelen en de daarbij behorende anonimiteitsvraagstukken. Bij openbare communicatiemiddelen zoals de drukpers en de omroep waren deze vraagstukken voornamelijk gerelateerd aan de bescherming van de uitingsvrijheid, terwijl bij telefonie, een besloten communicatiemedium, de bescherming van de privacy een grotere rol speelde. Nu de technische scheidslijnen vervagen, convergeren als het ware ook de grondrechtelijke beschermingsregimes. Men zou dus kunnen spreken van constitutionele convergentie: privacy en uitingsvrijheid vloeien samen als grondslag voor de bescherming van anonimiteit. Enerzijds wint de informationele privacy als gevolg van toegenomen gegevensverwerking aan belang als juridische basis voor de indamming van de daaruit voortvloeiende maatschappelijke risico's, anderzijds blijft de uitingsvrijheid cruciaal omdat ook de uitoefening van de daaruit voortvloeiende rechten in toenemende mate aan registratie en identificatie onderworpen is. Het belang van anonimiteit in de informatiesamenleving is daarmee komen te liggen op het kruispunt van privacy en uitingsvrijheid.

De constitutionele accentverschuivingen komen zeer duidelijk naar voren bij telefonie. Van oudsher werd deze technologie gebracht onder de bescherming van het recht op privacy, in het bijzonder het communicatiegeheim. Door de opkomst van moderne elektronische communicatiemiddelen krijgt het telefonienetwerk echter steeds meer een functie als infrastructuur voor de verspreiding van openbare digitale informatie, zodat de uitingsvrijheid aan belang wint. Dit werd ook door de Hoge Raad erkend in de zaak *Antelecom*.[20]

18. Asscher 2002, p. 26-30.
19. Asscher 1999, p. 5-6.
20. HR 26 februari 1999, *Mediaforum* 1999-5, nr. 26 (*Antelecom*).

Het ging om Amerikaanse 'call back services' waarmee hoge tarieven voor internationale gesprekken konden worden omzeild. Monopolist Antelecom NV trachtte het functioneren van deze diensten op de Nederlandse Antillen te bemoeilijken door onvoldoende lijnen beschikbaar te stellen. De Hoge Raad oordeelde dat het storen van de lijnen zowel in strijd was met artikel 10 als met artikel 8 EVRM.[21] De bewoordingen van de artikelen 8 en 10 EVRM noch de jurisprudentie van het Europese Hof gaven grond om aan te nemen dat artikel 8 ten aanzien van telefoonverkeer een lex specialis vormt ten opzichte van artikel 10. De Hoge Raad overwoog:

> "In het licht van de technische ontwikkelingen van de laatste decennia, die ertoe hebben geleid dat het telefoonverkeer thans geregeld is als onderdeel van het ruimere verschijnsel van de telecommunicatie, is er voorts thans minder aanleiding dan voorheen om, anders dan in bepaalde opzichten, het gebruik van het telefoonnet met correspondentie gelijk te stellen. Deze ontwikkelingen hebben meegebracht dat het gebruik van het telefoonnet in mindere mate dan voorheen een besloten karakter heeft en een steeds grotere betekenis heeft gekregen voor de uitwisseling van inlichtingen en denkbeelden. Het zou niet met deze ontwikkelingen stroken om aan het gebruik van het telefoonnet de bescherming van art. 10 te onthouden."

De technische ontwikkelingen hebben onder andere gevolgen voor de wijze waarop grondrechtelijke implicaties van gegevensverwerking moeten worden geanalyseerd. Dit komt nog uitgebreider aan de orde in het volgende hoofdstuk.

Door de technische ontwikkelingen is de betekenis van anonimiteit veranderd en zijn juridische vragen complexer geworden. Waar bij de verspreiding met behulp van de drukpers slechts de anonimiteit van auteurs, tussenpersonen en verspreiders van geschriften van belang was, gaat het bij moderne elektronische communicatie om de anonimiteit van zenders en ontvangers van digitale informatie in veel ruimere zin. De toenemende identificatie en registratie van eindgebruikers staat in meerdere opzichten op gespannen voet met een onbelemmerd genot van de verworvenheden van de informatiesamenleving. Om deze problematiek helder voor ogen te krijgen, is het nuttig haar te ontleden in deelproblemen. Daarom onderscheid ik hier drie 'toegangsvraagstukken'. Het eerste vraagstuk betreft de toegang tot het *netwerk*. Reeds op het moment dat de gebruiker hiermee verbinding maakt vindt immers veelal identificatie plaats. Bij telefonie maakt men bijvoorbeeld gebruik van een aansluiting met een uniek identificerend kenmerk (het telefoonnummer) dat in principe niet alleen voor de dienstenleverancier, maar ook voor anderen kenbaar is (nummerherkenning). Aan de gebruiker is de mogelijkheid gegeven

21. Antelecom en de Nederlandse Antillen hadden betoogd dat de bescherming van telefoongesprekken vanwege het besloten karakter exclusief onder artikel 8 EVRM zou vallen. Aanvaarding van dit argument zou voor hen gunstig zijn geweest omdat artikel 8 lid 2 EVRM in tegenstelling tot artikel 10 lid 2 beperkingen toestaat in het belang van het economisch welzijn van het land. Dit was in casu zeer relevant nu het storen van de call back services bedoeld was om de inkomsten van het staatsbedrijf in stand te houden.

om de hieruit voortvloeiende privacyrisico's in te dammen, onder andere door middel van geheime nummers en blokkering van nummerherkenning. Ook op het internet wordt vanaf het moment dat toegang tot het netwerk is verkregen het surfgedrag geregistreerd aan de hand van het IP-adres. Dit roept onder andere de vraag op in hoeverre gebruikers ook recht hebben op anonieme toegang tot elektronische communicatienetwerken en -diensten. Beide aspecten bespreken wij uitgebreider in het volgende hoofdstuk.

Nadat verbinding is gemaakt met het netwerk, betreedt de gebruiker een virtueel publiek domein van ongekende omvang. Dit virtuele domein kenmerkt zich, in hogere mate dan het tastbare publieke domein van boeken, tijdschriften en andere fysieke dragers, door identificatie, registratie en controle. Het tweede toegangsvraagstuk is daarom de vrije toegang van zenders en verspreiders van informatie tot de *openbaarheid*. Het belang hiervan strekt zich niet alleen uit tot daadwerkelijke meningsuitingen, maar ook in meer algemene zin tot de verspreiding van allerlei soorten digitale informatie die niet noodzakelijkerwijs gedachten of gevoelens van de verzender in zich dragen.

Een belangrijk aspect van dit tweede toegangsvraagstuk is de mogelijkheid van de journalistieke bron om op anonieme wijze toegang te krijgen tot de openbaarheid. In dit verband speelt met name de vraag in hoeverre online verspreiders van informatie zich ook op het bronnengeheim zouden kunnen beroepen. De beantwoording van deze vraag is niet eenvoudig. Op het internet is het informatievoorzieningproces en de rolverdeling tussen informatieverspreiders en tussenpersonen een stuk minder overzichtelijk dan bij de traditionele media. De positie van online tussenpersonen laat zich daarnaast maar ten dele vergelijken met die van de traditionele journalist. Vaak zijn bij de verspreiding van informatie bovendien meerdere tussenpersonen betrokken, zodat niet alleen onduidelijk is in hoeverre zij met een journalist gelijkgesteld kunnen worden, maar ook welke van deze tussenpersonen op de bescherming van het verschoningsrecht aanspraak zou kunnen maken. Wanneer een eindgebruiker op een nieuwsforum een anoniem bericht plaatst, zijn bijvoorbeeld zowel de websitehouder als de internetprovider betrokken bij het toegankelijk maken van dit bericht. In theorie zouden zij zich dus beide op het privilege kunnen beroepen. Anderzijds hebben beiden in mindere mate dan de journalist een actieve en inhoudelijke bemoeienis bij de totstandkoming en de verspreiding van de anonieme boodschap. De vergelijking met journalist gaat in dat opzicht mank.[22]

22. Dit afbakeningsprobleem speelt overigens ook in de fysieke wereld. Korthals Altes behandelt in zijn dissertatie bijvoorbeeld de vraag of het verschoningsrecht ook geldt voor personen die in het dagelijks spraakgebruik niet als journalisten worden aangemerkt, maar die wel op de een of andere manier aan de instandhouding van de informatiestroom bijdragen, zoals auteurs van boeken, drukkers, uitgevers en wetenschappelijke onderzoekers. Korthals Altes 1989, p. 160.

Wordt in een zogenaamd 'weblog' verwezen naar een anonieme bron, dan lijkt de vergelijking met de journalist beter mogelijk.[23] Vanuit de traditionele journalistiek wordt hiertegen echter bezwaar gemaakt. Sommigen zijn van mening dat het weblog als journalistieke vorm überhaupt niet deugt, dat het webloggen per definitie niet geschiedt in overeenstemming met de journalistieke mores en dat journalistiek dient te zijn voorbehouden aan betaalde professionals.[24] Hoewel het aantal weblogs met een degelijke journalistieke inhoud inderdaad klein is, moet het standpunt dat een weblogger per definitie niet in aanmerking komt voor bescherming mijns inziens van de hand worden gewezen. Het medium zegt in principe niets over de kwaliteit van de inhoud of de wijze waarop men te werk is gegaan. Ook voor de komst van het internet was voor de vraag of men bescherming kon ontlenen aan het journalistieke verschoningsrecht onverschillig via welk medium, of in welke vorm de informatie wereldkundig werd gemaakt. Uit het feit dat ook sommige professionele journalisten een weblog bijhouden blijkt bovendien dat deze publicatievorm in principe aan de door de beroepsgroep van journalisten gestelde kwalitatieve eisen kan voldoen.

Voor de bescherming van webloggers en andere internetgebruikers is van groot belang hoe men het begrip journalist definieert. Men kan een materiële definitie hanteren, waarbij slechts de journalistieke activiteit als criterium geldt. De aanbeveling van de Raad van Europa over dit onderwerp hanteert een dergelijke omschrijving. Deze aanbeveling verstaat onder een journalist immers "any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication" (zie par. 6.4).[25] In veel rechtsstelsels worden echter formele vereisten gesteld. Zo verstaat artikel 2 van de Belgische wet tot bescherming van de journalistieke bronnen onder een journalist, "eenieder die als zelfstandige loontrekkende werkzaam is, alsook iedere rechtspersoon, en die regelmatig een rechtstreekse bijdrage levert tot het verzamelen, redigeren, produceren of verspreiden van informatie voor het publiek via een medium". De redactiemedewerker kan het verschoningsrecht inroepen wanneer hij "door de uitoefening van zijn functie ertoe gebracht wordt kennis te nemen van informatie die tot de onthulling van een bron kan leiden, ongeacht of dat verloopt via het verzamelen, de redactionele verwerking, de productie of de verspreiding van die informatie".[26] In beide gevallen is dus een dienstverband vereist. Ook in de Verenigde Staten is een wetsontwerp aanhangig, de zogenaamde 'Shield Law', dat de groep van te

23. Een weblog, ook wel aangeduid als 'blog', is persoonlijk van een via het internet voor iedereen toegankelijk logboek. Vaak wordt onderscheid gemaakt tussen persoonlijke blogs, waarop de 'blogger' in dagboek-stijl verhaalt over zijn dagelijks leven, en thematische weblogs.
24. De kritiek die vanuit de journalistiek op weblogs is geuit wordt onder andere besproken door Van Heeswijk. Van Heeswijk 2005.
25. Recommendation R (2000) 7.
26. Wetsontwerp tot bescherming van de journalistieke bronnen, Tekst aangenomen in plenaire vergadering en aan de Koning ter bekrachtiging voorgelegd, Belgische Kamer van Volksvertegenwoordigers, 17 maart 2005, DOC 51 0024/021.

beschermen personen en instellingen beperkt tot de institutionele media.[27] Het is de vraag of men door dergelijke eisen te stellen niet ten onrechte een waardevolle categorie van journalistieke publicaties uitsluit. Aanwezigheid van een dienstverband zegt in principe immers niets over de maatschappelijke waarde van informatie en de bijdrage daarvan aan het publieke debat, noch over de zorgvuldigheid waarmee deze informatie is verworven.[28] Men zou daarnaast kunnen betogen dat het stellen van formele eisen, gezien de formulering van het begrip journalist in de aanbeveling van de Raad van Europa, in strijd komt met artikel 10 EVRM.

Het derde toegangsvraagstuk manifesteert zich aan de ontvangstkant van het communicatieproces. Kon men in de ouderwetse bibliotheek, verscholen tussen de boekenplanken, nog onbekommerd rondneuzen – in het virtuele publieke domein blijft men nooit geheel onopgemerkt. Dit gegeven noopt tot aandacht voor de toegang tot het publieke domein van de gebruiker als consument van elektronische omroep- en communicatiediensten en als verzamelaar van nieuws, kennis en informatie. De afwezigheid van identificatie en registratie is een cruciale voorwaarde voor het onbelemmerd *garen* en *ontvangen* van informatie in online bibliotheken, databanken en op bijvoorbeeld nieuwswebsites.

Hoewel de bewoordingen van artikel 7 Gw geen aandacht schenken aan de ontvangsten de garingsvrijheid, staat reeds geruime tijd vast dat deze rechten binnen de reikwijdte van haar bescherming vallen.[29] Verdragsteksten noemen beide vrijheden wel. Zowel artikel 19 van het Internationale Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) als artikel 19 van de Universele verklaring van de rechten van de mens beschermt de vrijheid om inlichtingen en denkbeelden te garen, te ontvangen en door te

27. Section 7(1) van de Free Flow of Information Act of 2005 luidt: "In this Act:
(1) The term 'covered person' means –
(A) an entity that disseminates information by print, broadcast, cable, satellite, mechanical, photographic, electronic, or other means and that
(i) publishes a newspaper, book, magazine, or other periodical;
(ii) operates a radio or television broadcast station (or network of such stations), cable system, or satellite carrier, or a channel or programming service for any such station, network, system, or carrier;
or
(iii) operates a news agency or wire service;
(B) a parent, subsidiary, or affiliate of such an entity; or
(C) an employee, contractor, or other person who gathers, edits, photographs, records, prepares, or disseminates news or information for such an entity."

28. Korthals Altes schrijft dat in de Verenigde Staten en Duitsland in het verleden veelal eisen werden gesteld met betrekking tot dienstverband, oplage en periodiciteit. Hij is echter van mening dat noch de vorm waarin de communicatie plaatsvindt noch periodiciteit of professionaliteit principieel als eis kunnen worden gesteld aan personen die op een journalistiek privilege aanspraak willen maken. Korthals Altes 1989, p. 271.

29. De Nederlandse regering heeft verklaard dat zowel de ontvangstvrijheid als de garingsvrijheid door artikel 7 Gw worden beschermd. Zie over de ontvangstvrijheid en artikel 7 Grondwet de Meij e.a. 2000, p. 130 e.v. en p. 196. Zie ook *Kamerstukken II* 1981/82, 16 905-16 938, nr. 5, p. 13-15.

geven.[30] In navolging van de Universele verklaring bevat ook artikel 10 EVRM een expliciete vermelding van de ontvangstvrijheid.[31] Garen en ontvangen vormen tezamen een logische aanvulling op het recht van de zender om zijn boodschap te verspreiden. Beide rechten zijn vanzelfsprekende en onmisbare elementen van de uitingsvrijheid. Beperkingen van de uitingsvrijheid hebben immers vaak als doel te verhinderen dat een bepaalde uiting zijn bestemming bereikt. Voordat men als zender op kan treden is het daarnaast vaak noodzakelijk dat men kennis kan nemen van andermans uitingen. Ook voor het functioneren van de democratie is het essentieel dat het publiek geïnformeerd is over de actualiteit.[32]

Het onderscheid tussen garen en ontvangen behoeft enige toelichting. De garingsvrijheid was oorspronkelijk bedoeld voor journalisten.[33] Dit recht is geleidelijk aan losgekoppeld van het publiceren en wordt tegenwoordig ook opgevat als een recht dat toekomt aan eenieder die zich, om wat voor reden dan ook, actief op de hoogte wil stellen.[34] Het belangrijkste onderscheid tussen garen en ontvangen lijkt eruit te bestaan dat de ontvangsthandeling passieve aspecten benadrukt terwijl de garingshandeling meer actief is. In de digitale omgeving vervaagt dit onderscheid: passief ontvangen en actief garen vloeien in elkaar over.[35] In vergelijking met telefonie en klassieke omroep lijkt de actieve component aan belang te hebben gewonnen. Bij radio en televisie stroomt na het inschakelen van het toestel een voorgeprogrammeerd informatieaanbod de huiskamer binnen. De ontvanger kan slechts kiezen tussen een beperkt aantal kanalen. Op het internet is de toegang tot het netwerk slechts de eerste stap. Wanneer verbinding is gemaakt met het netwerk moet de 'ontvanger' zelf actief op zoek naar de gewenste informatie.

30. Artikel 19 van de Universele verklaring van de rechten van de mens luidt: "Een ieder heeft recht op vrijheid van mening en meningsuiting. Dit recht omvat de vrijheid om zonder inmenging een mening te koesteren en om door alle middelen en ongeacht grenzen inlichtingen en denkbeelden op te sporen, te ontvangen en door te geven." Artikel 19 lid 2 IVBPR luidt: "Een ieder heeft het recht op vrijheid van meningsuiting; dit recht omvat mede de vrijheid inlichtingen en denkbeelden van welke aard ook te garen, te ontvangen en door te geven, ongeacht grenzen, hetzij in geschreven of gedrukte vorm, in de vorm van kunst, of met behulp van andere media naar zijn keuze."
31. Artikel 10 EVRM lid 1 luidt: "Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of door te geven, zonder inmenging van overheidswege en ongeacht grenzen. (…)".
32. De Meij e.a. 2000, p. 129-130.
33. Over de precieze inhoud van de garingsvrijheid bestaat al sinds lange tijd onduidelijkheid. Schuijt pleit ervoor om een onderscheid te maken tussen de garingsvrijheid in het algemeen en de vrijheid van *nieuws*garing in het bijzonder. Dat laatste begrip zou hij willen reserveren voor de specifiek aan de media en journalisten toekomende actieve garingsvrijheid ten dienste van de informatievoorziening door de media. De vrijheid van nieuwsgaring is zijns inziens een species van de aan iedere burger toekomende ontvangst- en garingsvrijheid. Schuijt 2003, p. 345-346.
34. De Meij e.a. 2000, p. 134-138 en p. 21.
35. Schuijt 2003, p. 343.

Naarmate de techniek bij de overdracht van informatie een grotere rol gaat spelen, lijken de ontvangstvrijheid en het recht om actief informatie te verzamelen een steeds gewichtiger positie in te nemen. Zoals de Meij terecht opmerkt, was de ontvangstvrijheid bij de omroep reeds van groter belang dan bij de drukpers omdat voor de ontvangst van omroepsignalen aparte apparatuur nodig is en de overheid de ontvangst betrekkelijk makkelijk kan verhinderen, bijvoorbeeld door het storen van uitzendingen, vergunningsvereisten voor ontvangstapparatuur en doorgifteverboden gericht tot kabelbeheerders.[36] Ook in de digitale omgeving doen overheden verwoede pogingen om de toegang tot openbare informatie met behulp van technische ingrepen te blokkeren. De meest rigoureuze maatregelen ziet men in totalitaire regimes. Wanneer blijkt dat het onmogelijk is om ongewenste politieke uitingen bij de bron tegen te houden, wordt nog al eens getracht de toegang en het gebruik van het netwerk volledig onder staatstoezicht te plaatsen. Een iets mildere maatregel is het opleggen van verplichtingen tot 'zonering' of de gedwongen implementatie van filteringsoftware, bijvoorbeeld ter bestrijding van pornografie.[37] De identificatie van gebruikers speelt bij dit soort maatregelen doorgaans een cruciale rol, hetzij om bestraffing mogelijk te maken, hetzij om meerderjarigheid te kunnen vaststellen.

Wie controle heeft over de communicatie-infrastructuur beheerst ook de toegang tot informatie en kan zodoende de uitoefening van de ontvangstvrijheid bemoeilijken of verhinderen. In de zaak *Autronic* oordeelde het Europese Hof dan ook dat de bescherming van de communicatievrijheid in artikel 10 EVRM zich niet alleen richt op de inhoud van informatie, maar ook op de middelen om die informatie door te geven en te ontvangen (r.o. 47).[38] Uit de uitspraak volgt onder andere dat vergunningen voor de aanleg van telecommunicatie-infrastructuur ook moeten voldoen aan de eisen van artikel 10 lid 2 EVRM. Ook de Afdeling Rechtspraak Raad van State oordeelde dat een in een gemeentelijke verordening opgenomen verbod om daar waar een centrale antenne-inrichting aanwezig is op een woning een antenne te plaatsen, een beperking vormt van het recht om zonder inmenging van overheidswege inlichtingen en denkbeelden te ontvangen en door te geven.[39] Op het verbod werd een uitzondering gemaakt voor degenen die een betere ontvangstmogelijkheid wensten dan via de centrale installatie mogelijk

36. De Meij e.a. 2002, p. 196.
37. Een goed voorbeeld is de Amerikaanse Children's Internet Protection Act (CIPA). In *United States* v. *American Library Ass'n, Inc.* oordeelde het Supreme Court dat het Amerikaanse congres de ontvangst van federale subsidies voor internettoegang in openbare bibliotheken aan de voorwaarde mag verbinden dat op de computers met internetaansluiting pornografiefilters zijn geïnstalleerd. *United States* v. *American Library Ass'n, Inc.*, 539 U.S. 194 (2003).
38. EHRM 22 mei 1990, *NJ* 1991, 740 (*Autronic*), m.nt. E.A. Alkema. Het ging om een verbod, behoudens toestemming van de uitzendende Staat, op de ontvangst middels schotelantennes van ongecodeerde uitzendingen van telecommunicatiesatellieten die voor het grote publiek bestemd waren.
39. Dommering 1990, p. 66.

was.[40] Of maatregelen en verboden die de anonieme ontvangst via een bepaald netwerk verhinderen of bemoeilijken ook in strijd zouden kunnen komen met artikel 10 EVRM is echter nog niet aan de orde geweest.

De toegang tot informatie wordt om commerciële redenen ook door private partijen in toenemende mate aan banden gelegd. Informatie wordt immers steeds meer een verhandelbaar goed. Deze ontwikkeling, ook wel aangeduid als de 'commodification of information', gaat gepaard met een expansie van intellectuele eigendomsrechten en leidt tot een inkrimping van het publieke domein.[41] Commodification heeft ook gevolgen voor de anonimiteit van gebruikers. De technische beschermingsmaatregelen die de toegang tot en het gebruik van beschermd materiaal reguleren vereisen vaak identificatie en registratie. Zo worden op grote schaal 'Digital Rights Management'-systemen ontwikkeld die toegang tot digitale informatie alleen mogelijk maken tegen betaling en waarbij de rechthebbende een gedetailleerd inzicht krijgt in het gedrag van de gebruiker.[42]

De bovengenoemde ontwikkelingen roepen de vraag op of men het recht heeft informatie te garen en te ontvangen zonder daarbij geregistreerd te worden. In de Amerikaanse rechtspraak is deze vraag reeds aan de orde geweest. Zoals wij zagen is daar reeds 'a right to read anonymously' aanvaard (zie par. 3.4). Het is echter nog niet duidelijk of dit recht ook onverkort geldt in de digitale omgeving. Ook in het Nederlandse recht is de anonieme uitoefening van de ontvangstvrijheid een onderwerp dat aandacht verdient. Dit belang is onder andere een sterk argument voor het mogelijk maken van anonieme toegang tot elektronische communicatienetwerken en -diensten (zie par. 8.4). Daarnaast heeft het een rol gespeeld in de discussie over de verruiming van strafvorderlijke bevoegdheden tot het vorderen van gegevens. De Nederlandse bibliotheken wezen erop dat een te vergaande toepassing van deze bevoegdheden een onaanvaardbare belemmering van de uitingsvrijheid met zich mee kan brengen (zie par. 9.7.1).

7.2 Bescherming van anonimiteit op het internet

Met de sterke opkomst van het internet kwam de bescherming van anonieme communicatie vanaf het begin van de jaren negentig steeds duidelijker op de politieke agenda te staan. Verschillende nationale en Europese instellingen hebben zich sindsdien over dit onderwerp uitgelaten. Op de Europese ministerconferentie over wereldwijde informatienetwerken in 1997 is het belang van anonimiteit op Europees niveau voor het eerst erkend. In een gezamenlijke verklaring erkenden de ministers het beginsel dat wanneer de gebruiker offline voor anonimiteit kan opteren, deze keuze ook online mogelijk moet zijn. Zij drongen er bij de industrie op aan technische middelen te ontwikkelen waarmee de privacy kan worden gevrijwaard en waarmee persoonsgegevens op de wereldwijde

40. AR 10 oktober 1978, *Ars Aequi* 1979, p. 77 e.v.
41. Elkin-Koren & Weinstock Netanel 2002.
42. Koelman 2003b; Cohen 2003.

informatienetwerken kunnen worden beschermd, zoals voorzieningen om anoniem te browsen, te e-mailen en betalingen te verrichten (zie de overwegingen 51 en 52 van deze verklaring).[43]

Enige tijd later bracht ook de artikel 29-werkgroep van de Europese Commissie een aanbeveling tot stand waarin specifiek werd ingegaan op de bescherming van anonimiteit in privacyregelgeving.[44] De groep was van oordeel dat de bescherming van anonimiteit bij online communicatie essentieel is als middel om privacyproblemen het hoofd te bieden:

> "Transactionele gegevens vormen alleen een bedreiging voor de persoonlijke levenssfeer als de gegevens op een identificeerbare persoon betrekking hebben. Dit betekent dat privacyproblemen onder meer kunnen worden verholpen door er zoveel mogelijk voor te zorgen dat de gegevenssporen die door het gebruik van Internet ontstaan de identificatie van de gebruiker niet mogelijk maken. Wanneer de anonimiteit wordt gegarandeerd, kunnen personen aan de Internetrevolutie deelnemen zonder dat ze bang hoeven te zijn dat elke beweging wordt geregistreerd en informatie over hen wordt verzameld die later kan worden gebruikt voor doeleinden waartegen zij bezwaar hebben."

De artikel 29-werkgroep wijst erop dat de noodzaak van anonimiteit bij online-communicatie in bepaalde situaties reeds als volkomen legitiem wordt erkend. Zo zullen slachtoffers van zedendelicten en personen met een alcohol- of drugsverslaving die op het internet ervaringen willen uitwisselen hiervan weerhouden worden wanneer dit niet anoniem kan geschieden. Daarnaast kan anonimiteit nuttig zijn wanneer iemand een misdaad wil aangeven zonder te hoeven vrezen voor vergeldingsmaatregelen. Ook de vrijheid van meningsuiting moet als belang worden meegewogen. Zo kunnen politieke dissidenten in een totalitair regime zich meestal alleen op anonieme wijze verzetten tegen mensenrechtenschendingen en tegen het politieke bestel waarin zij leven. De noodzaak van anonimiteit is echter niet beperkt tot deze gevallen. Gegevens over communicatiegedrag zijn immers een middel "om meer toezicht en controle op het individuele gedrag uit te oefenen dan ooit tevoren mogelijk is geweest".[45] Nadrukkelijk wordt ook een verband gelegd met het belang van de communicatievrijheid in ruimere zin: indien het recht op de bescherming van de persoonlijke levenssfeer onvoldoende wordt beschermd, durven personen hun gedachten wellicht niet vrijelijk te uiten. Ook het identificeren en beschrijven van lezers en gebruikers van informatiediensten vermindert waarschijnlijk de

43. Verklaring wereldwijde informatienetwerken 1997.
44. De groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens is een adviesorgaan van de Europese Commissie dat in het leven werd geroepen in artikel 29 van de algemene privacyrichtlijn. Haar taak is het bewaken van de homogene toepassing van de bepalingen van deze richtlijn in alle lidstaten en het geven van advies aan de Europese Commissie over voorstellen tot wijziging.
45. Groep gegevensbescherming artikel 29 1997b, p. 5.

bereidheid van personen om inlichtingen of denkbeelden te ontvangen of te verstrekken.[46]

De omstandigheid dat de technologie van het internet de registratie van communicatie-handelingen makkelijker mogelijk maakt, noopt tot extra aandacht voor waarborgen die anonimiteit beschermen. Traditionele punt-tot-punt-communicatietechnologieën bieden immers in hogere mate de mogelijkheid om anoniem te blijven dan bijvoorbeeld e-mail.[47] Een gewone brief kan via de klassieke post in volstrekte anonimiteit worden verstuurd. Betaling geschiedt immers met een volledig anoniem betaalmiddel (postzegels) en de posterijen verzamelen geen gegevens over de verzender van de brief. De laatste hoeft zijn naam niet op de brief de vermelden en kan dus ook ten opzichte van de ontvanger anoniem blijven. Ook de klassieke telefonie biedt gebruikers de mogelijkheid om via openbare telefooncellen anoniem toegang te verkrijgen tot het netwerk (zie par. 8.4).

De artikel 29-werkgroep neemt als uitgangspunt dat het individu moet kunnen kiezen voor anonimiteit bij de verzending van e-mail, bij het surfen op het internet en bij de aankoop van goederen en diensten. Anonieme toegangsmogelijkheden tot het internet en anonieme betalingsmogelijkheden zijn daarbij essentieel. Als de overheid wettelijke beperkingen oplegt aan het recht op anonimiteit of aan de beschikbaarheid van technische middelen die anonimiteit mogelijk maken (bijvoorbeeld encryptieproducten), moet zij er steeds voor waken dat haar maatregelen evenredig zijn en niet restrictiever dan nodig voor de bescherming van een specifiek algemeen belang in een democratische maatschappij.[48]

Zoals ook de werkgroep constateert, botst de bescherming van anonimiteit met initiatieven op het gebied van de bestrijding van strafbare feiten. Dergelijke strijdigheden dienen naar haar oordeel op te worden geheven met behulp van het evenredigheidsbeginsel, zoals ontwikkeld door het Europese Hof voor de Rechten van de Mens. Het evenwicht tussen deze tegenstrijdige doelstellingen is bij traditionele communicatiemiddelen in de jurisprudentie reeds tot stand gekomen. Naar het oordeel van de groep diende in 1997 een soortgelijk evenwicht in de cyberspace-context nog te worden gevonden.[49]

De Nederlandse overheid

In de Nota Wetgeving voor de Elektronische Snelweg (WES) wijdt ook de Nederlandse overheid enige overwegingen aan anonimiteit op het internet. Enerzijds benadrukt zij het belang van rechtshandhaving en kenbaarheid. Ook op de elektronische snelweg dient als uitgangspunt te gelden dat voor onrechtmatige handelingen altijd een verantwoordelijke kan worden aangewezen. Burgers en private instanties met een redelijk belang moeten daarom in staat worden gesteld om via de civiele weg het spoor te volgen van degene

46. Groep gegevensbescherming artikel 29 1997a, p. 5.
47. Groep gegevensbescherming artikel 29 1997b, p. 9.
48. Idem, p. 11-12.
49. Idem, p. 6.

die inbreuk heeft gemaakt op hun rechten.[50] Anderzijds erkent de overheid de behoefte aan anonieme deelname:

> "De elektronische snelweg vergroot zowel de behoefte aan een meer persoonsgebonden identiteitsvaststelling, als aan anoniem deelnemen aan het elektronisch verkeer. Daarbij blijft het huidige uitgangspunt in het maatschappelijke verkeer in feite ongewijzigd: voor zover de wet – bijvoorbeeld bij het afsluiten van wettelijk verplichte verzekeringen – of het maatschappelijk functioneren – bijvoorbeeld het afsluiten van bepaalde overeenkomsten – niet noodzaakt tot opheffing van de identiteit, moet anonimiteit op de elektronische snelweg het uitgangspunt zijn."[51]

Voorzover het de verspreiding van informatie betreft, is dit laatste standpunt in overeenstemming met het eveneens in de nota WES geformuleerde 'online-offline adagium'. Offline is door de wetgever immers aanvaard dat anonimiteit niet strafbaar is, zoals wij zagen in het zesde hoofdstuk. Als restrictie geldt dat indien hogere belangen (o.a. staatsveiligheid en voorkoming, opsporing en vervolging van strafbare feiten) dat vergen, de gegevens te herleiden moeten zijn tot concrete personen.[52]

De commissie Franken

In 2000 bracht de commissie 'Grondrechten in het digitale tijdperk', ook aangeduid als 'de commissie Franken', een rapport tot stand. In dit rapport kwam de suggestie aan de orde om het recht op eerbiediging van de persoonlijke levenssfeer te vervangen door een recht op anonimiteit. Deze suggestie werd door de commissie afgewezen. Voor zover onder het recht op anonimiteit zou moeten worden verstaan dat een ieder het recht heeft zelf te beslissen welke persoonsgegevens hij onder welke omstandigheden wil prijsgeven, zou dit onhaalbaar zijn, aldus de commissie. Zonder het prijsgeven van deze persoonsgegevens kan men maatschappelijk immers niet functioneren. Dat geldt zowel in de verhouding tussen burger en overheid als in de verhouding tussen burgers onderling. Bovendien zou een ruim omschreven recht op anonimiteit ook ruim omschreven beperkingsclausules noodzakelijk maken, hetgeen volgens de commissie diende te worden vermeden.[53] Het kabinet sloot zich bij het standpunt van de commissie aan. Het verwierp de aanvaarding van een het recht op anonimiteit met een verwijzing naar de maatschappelijke behoefte aan kenbaarheid:

> "Reden voor het afwijzen van opname van een recht op anonimiteit in de Grondwet is de opvatting van het kabinet dat er in de samenleving een uitgangspunt van kenbaarheid is. Voor het nakomen van verbintenissen en voor rechtshandhaving is identificeerbaarheid noodzakelijk. Dit is in de online wereld niet anders dan in de offline wereld. Wanneer anonimiteit als recht zou worden opgenomen is

50. *Kamerstukken II* 1997/98, 25 880, nrs. 1-2, p. 117-118.
51. Idem, p. 129-133.
52. Idem, p. 133.
53. Rapport Franken 2000, p. 125.

> hierdoor de omvang van de benodigde regulerende wetgeving niet te overzien. Dat er onder omstandigheden behoefte kan bestaan aan anonimiteit wordt door het kabinet erkend. Echter, deze behoefte is niet zodanig fundamenteel van aard dat daaraan de waarborg van een grondrecht gekoppeld moet worden."[54]

De Raad van Europa

In een verklaring over de regulering van online communicatie heeft ook het Comité van Ministers van de Raad van Europa het principe aanvaard dat internetgebruikers de mogelijkheid moeten hebben om hun identiteit te verbergen:

> "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."[55]

In de toelichting bij de verklaring wordt benadrukt dat een verplichting om de identiteit te onthullen in bepaalde gevallen een te vergaande beperking van de uitingsvrijheid met zich mee kan brengen. Het risico bestaat dat waardevolle informatie en ideeën hierdoor niet in de openbaarheid komen. Daarnaast moeten internetgebruikers worden beschermd tegen ongerechtvaardigd toezicht door publieke of private entiteiten. Gebruikers moeten daarom in staat worden gesteld om zichzelf te beschermen. Dit betekent onder andere dat lidstaten het gebruik van anonimiserende software moeten toestaan. Het principe dat anonimiteit beschermd moet worden is echter niet onbeperkt. Lidstaten moeten de mogelijkheid hebben om informatie te verkrijgen over personen die verantwoordelijk zijn voor onrechtmatige handelingen. De verzameling van dergelijke informatie moet echter wel in overeenstemming zijn met de grenzen die worden gesteld door het nationale recht en door het Europees Verdrag voor de Rechten van de Mens – in het bijzonder artikel 8 daarvan – en andere internationale verdragen.

De bindende kracht van bovengenoemde documenten is beperkt. Zo is een verklaring van het Comité van Ministers van de Raad van Europa niet afdwingbaar in het nationale recht van de lidstaten. Het principe dat anonimiteit beschermd moet worden is echter wel als uitgangspunt genomen bij de totstandkoming van de Europese privacyrichtlijnen. Deze worden in het volgende hoofdstuk behandeld.

54. *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 44.
55. Declaration freedom of communication on the internet 2003.

7.3 Gegevensbescherming als waarborg voor anonieme openbare communicatie

Het toegenomen belang van elektronische gegevensverwerking in de samenleving vraagt om een nadere analyse van de verhouding tussen het recht op privacy en de bescherming van anonimiteit. Daarbij dient in het bijzonder aan de orde te komen hoe het gegevensbeschermingsrecht de mogelijkheid om anoniem te zijn ondersteunt en wat in de sfeer van anonieme openbare communicatie de relatie is met andere grondrechtelijke belangen.

In het voorgaande bleek dat gegevensverwerking vergaande implicaties kan hebben voor de vrijheid en individuele autonomie van burgers. Men kan verschillende bedreigingen onderscheiden. Zo neemt met de groeiende verwerkingscapaciteit van gegevens ook de zucht naar informatie toe, onafhankelijk van de werkelijke behoefte daaraan. Dit leidt tot een alsmaar stijgende 'registratiedichtheid', waardoor steeds meer aspecten van menselijk gedrag worden vastgelegd. Wanneer gegevens eenmaal zijn gegenereerd, kunnen zij een persoon voor een lange tijd blijven achtervolgen. Door het koppelen van bestanden uit verschillende systemen kunnen bovendien nieuwe gegevens en zelfs hele profielen van personen worden gecreëerd. De potentiële gevaren zitten daarnaast voor een deel in de techniek zelf. Het is vrijwel onmogelijk computersystemen zodanig te beveiligen dat inbreuken op de privacy door derden geheel kunnen worden voorkomen. Tenslotte blijven bij gegevensverwerking ook altijd menselijke fouten mogelijk.[56]

De geregistreerde burger kan zich slechts in beperkte mate tegen gegevensverwerking verzetten. Hij is in hoge mate afhankelijk. Op vele gebieden van het maatschappelijke leven worden persoonsgegevens gegenereerd, verwerkt en opgeslagen zonder dat hij zich hieraan kan onttrekken. Wanneer buiten de betrokkene om gegevens worden verzameld is de mogelijkheid om te kiezen zelfs geheel afwezig. Ook wanneer de betrokkene wel op de hoogte is, is zijn vrijheid om grenzen te stellen beperkt. Het verstrekken van persoonsgegevens is vaak een voorwaarde voor allerlei vormen van maatschappelijke activiteit. Zo zijn gegevens omtrent inkomen, huisvesting en levenssituatie als het ware de prijs die men betaalt om te kunnen voldoen aan wettelijke verplichtingen, zoals het doen van belastingaangifte of het aanmelden van een kind voor het basisonderwijs. Hetzelfde geldt wanneer men in aanmerking wenst te komen voor wettelijke voorzieningen zoals een WW-uitkering of huursubsidie.[57]

Tegenover de afhankelijke positie van de geregistreerde staat de machtspositie van de houder van de gegevens. Hij neemt op basis van gegevens beslissingen die de geregistreerde in hoge mate in zijn belangen kunnen raken. Deze machtspositie wordt groter naarmate de intensiviteit van gegevensverwerking toeneemt en verschillende informatiesystemen aan elkaar gekoppeld worden. Blok verwoordt kernachtig hoe de stelling van

56. Ontleend aan Sentrop 1985, p. 13-15 en Kuitenbrouwer 1991, p 28-47.
57. Zie in deze zin ook Sentrop 1985, p. 13.

Francis Bacon dat empirische wetenschap de mens de macht geeft om het object van zijn kennis naar zijn hand te zetten, ook toepasbaar is in de informatiesamenleving:

> "Bacons adagium, dat is verworden tot het cliché 'kennis is macht', biedt tevens de sleutel tot de normatieve problemen van de huidige informatiesamenleving. Als kennis een vorm van macht is, zoals Bacon verkondigt, dan staat kennis met betrekking tot personen gelijk aan macht over personen. Dat maakt kennis verdacht in de Westerse liberale samenleving. Telkens wanneer de overheid of een andere machthebber zich gaat toeleggen op het vergaren van informatie met betrekking tot personen of wanneer een techniek wordt geïntroduceerd die de informatieverwerking vereenvoudigt, staan dan ook critici op die, onder verwijzing naar de woorden van Bacon, waarschuwen dat deze praktijken de macht van de machthebber vergroten en dientengevolge de vrijheid van de burger bedreigen."[58]

In de context van gegevensverwerking wordt de macht die de verwerker over het 'datasubject' heeft ook wel aangeduid als 'informatiemacht'. In feite gaat achter deze term de fundamentele relatie tussen identificatie, controle en machtsuitoefening schuil die reeds in hoofdstuk 1 werd besproken (zie par. 1.3).

De risico's die uit het ontstaan van informatiemacht voortvloeien worden beteugeld door een geheel van beginselen en voorschriften ten aanzien van de opslag en verwerking van persoonsgegevens. Dit 'gegevensbeschermingsrecht', waarop in het volgende hoofdstuk nog dieper wordt ingegaan, vat het recht van datasubjecten om beschermd te worden tegen de risico's van gegevensverwerking op als onderdeel of als uitvloeisel van het recht op 'informationele privacy'. Westin definieerde dit laatste recht als "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[59] Vrijwel alle Nederlandse juristen hebben zich bij deze omschrijving aangesloten door de kern van de informationele privacy te omschrijven als een recht op zeggenschap of 'regie' over persoonsgegevens.[60] Ook de Europese privacyrichtlijnen en de Wet bescherming persoonsgegevens gaan van dit principe uit.[61] Zeggenschap houdt in dat verband in dat het individu het recht heeft om de opslag van informatie te beperken of de opgeslagen informatie te veranderen.

Blok bekritiseert de wijze waarop het gegevensbeschermingsrecht juridisch-dogmatisch is gefundeerd. Hij wijst er op dat het probleem van persoonsregistraties door juristen van begin af aan werd gezien als een machtsprobleem en dat het om die reden voor de hand had gelegen de juridische oplossing te zoeken onder de gevestigde leerstukken inzake macht en machtsbeheersing, zoals bijvoorbeeld rechtsstatelijke eisen en publiekrechtelijke beginselen van behoorlijk bestuur. Vanuit rechtsstatelijk perspectief zou dan direct duidelijk zijn geweest dat de overheid bij de verwerking van gegevens niet alleen

58. Blok 2002, p. 116.
59. Westin 1970, p. 7.
60. Blok 2002, p. 123.
61. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 9.

rekening moet houden met de eerbiediging van het recht op privacy, maar ook met andere grondrechten, zoals het gelijkheidsbeginsel, de vrijheid van meningsuiting, de vrijheid van vereniging en de vrijheid van godsdienst en levensovertuiging.[62] In plaats daarvan heeft men het gegevensbeschermingsrecht echter opgehangen aan één grondrecht, dat, aldus Blok, "voor de gelegenheid werd opgeblazen tot een alomvattende waarde".[63] De problematiek rond informatiemacht is vervolgens kritiekloos vertaald naar inbreuken op de privacy. Om deze vertaling mogelijk te maken moest de betekenis van het recht op privacy worden aangepast. Zo is het gegevensbeschermingsrecht ook van toepassing op de niet-intieme onderdelen van het leven van een persoon. Ook in de openbaarheid heeft het individu immers een recht op vrijheid en op de mogelijkheid tot het nemen van autonome beslissingen en kan hij aanspraak kan maken op bescherming tegen ongecontroleerde macht. Hierdoor komt het gegevensbeschermingsrecht ver af te staan van de persoonlijke levenssfeer in klassieke zin.[64] Bloks analyse stelt het voor dit onderzoek cruciale punt aan de orde dat de uit gegevensverwerking voortvloeiende informatiemacht niet alleen raakt aan het recht op privacy maar ook aan andere grondrechten. Zoals bleek in de hoofdstukken 3 en 4 is dit inzicht in het Amerikaanse recht minder dan in het Nederlandse en het Europese vertroebeld door het privacy-denken. Dit komt bijvoorbeeld naar voren in *NAACP* v. *Alabama,* de eerste uitspraak van het Supreme Court over anonimiteit, waarin de aan een politieke organisatie opgelegde verplichting tot afgifte van haar ledenlijsten aan de orde kwam (zie par. 3.4). Het Supreme Court somt in haar overwegingen verschillende grondrechten op die een rol spelen, waaronder het recht op privacy. Het vraagstuk wordt echter allereerst behandeld in het kader van de vrijheid van vereniging en als een algemeen constitutioneel probleem dat betrekking heeft op de (machts)verhouding tussen overheid en burger. In latere uitspraken komt telkens terug hoe registratieverplichtingen impact kunnen hebben op de uitoefening van publieke vrijheden. Het juridische steekspel tussen eiser en provider in John Doe procedures illustreert daarnaast hoe de opslag en verstrekking van identificerende informatie in de context van openbare communicatie raakt aan de uitingsvrijheid (zie hoofdstuk 4).

De 'monomane obsessie' met het recht op privacy is dus niet alleen een juridisch-dogmatisch probleem. Zij gaat ten koste van de aandacht voor overige fundamentele rechten en staat in de weg aan een zuivere en volledige analyse van de werkelijke implicaties die gegevensverwerking heeft. Dit blijkt bijvoorbeeld uit de wijze waarop aan de uitingsvrijheid gerelateerde belangen op Europees niveau worden benaderd. De artikel 29-werkgroep benadrukt weliswaar dat de vrijheid van meninguiting moet worden meegewogen en ook de Raad van Europa noemt de bescherming tegen 'online surveillance' en de 'free

62. Blok 2002, p. 118-119.
63. Idem, p. 120.
64. Idem, p. 120.

expression of information and ideas' als belangen, maar bij lezing van de rapporten en verklaringen van deze instanties ontstaat toch de indruk dat het recht op privacy centraal staat en dat overige grondrechtelijke belangen slechts zijdelings een rol spelen (zie par. 7.2). Ook in het Nederlandse gegevensbeschermingsrecht is het uitgangspunt dat intensieve registratie de publieke vrijheden kan beknotten nooit goed uit de verf gekomen. Het verbod op de verwerking van 'bijzondere persoonsgegevens' in de Wet bescherming persoonsgegevens beschermt wel publieke vrijheden als de vrijheid van politieke participatie, de vrijheid van vakvereniging en de vrijheid van godsdienst en levensovertuiging, maar de vrijheid van meningsuiting, de vrijheid van informatievergaring, de vrijheid van betoging en de vrijheid van vereniging vallen hier buiten (zie par. 1.3).[65]

Door de opkomst van elektronische openbare communicatiemiddelen zoals het internet dringt gegevensverwerking in toenemende mate door in de publieke sfeer. De kenbaarheid en de registratie van persoonsgegevens is een bepalende factor geworden bij elk van de drie toegangsvraagstukken die in het voorgaande werden beschreven. Gegevensbescherming heeft zodoende een belangrijke waarborgfunctie gekregen voor anonieme openbare communicatie. Door zijn eenzijdige fundering is het bouwwerk van de gegevensbescherming echter slecht bestand tegen de verschuiving van grondrechtelijke belangen en geeft het geen adequaat antwoord op de behoefte van de communicerende burger aan bescherming tegen misbruik van informatiemacht ter waarborging van zijn publieke vrijheden. Het gebrek aan aandacht voor deze vrijheden wordt door de technische ontwikkelingen een steeds nijpender probleem.

7.4 Conclusie

Overziet men de ontwikkelingen in de communicatietechnologie, dan kunnen verschillende factoren worden aangewezen die de gevolgen van gegevensverwerking en de bescherming van anonimiteit tot een actueel juridisch thema hebben gemaakt. Belangrijke technische omslagpunten zijn de introductie van de computer in het telecommunicatienetwerk, de hiermee gepaard gaande digitalisering van telefoniediensten middels de ISDN-standaard en de daaruit voortvloeiende opkomst van elektronische gegevensverwerking. Bij de omroep werd met het beschikbaar worden van interactieve diensten retourverkeer van gebruiker naar zender mogelijk, hetgeen kijk- en luistergedrag registreerbaar maakte.

In de digitale samenleving wordt het steeds moeilijker om een onderscheid te maken tussen verschillende communicatiemiddelen en de daarbij behorende anonimiteitsvraagstukken. De samenvloeiing van openbare en niet-openbare communicatietechnologieën doet traditionele scheidslijnen vervagen en leidt tot een convergentie van grondrechtelijke beschermingsregimes. Men kan nu drie algemene toegangsvraagstukken onderscheiden: de toegang van eindgebruikers tot elektronische communicatienetwerken, de toe-

65. Idem, p. 131-132.

gang van zenders en verspreiders van informatie tot de openbaarheid en de toegang van ontvangers tot het virtuele publieke domein. Met name op het internet lijkt het laatste vraagstuk verhoudingsgewijs aan belang te hebben gewonnen. Het garen en ontvangen van informatie is hier immers makkelijker dan ooit. Tegelijkertijd is het individuele communicatiegedrag, meer dan vroeger, onderhevig aan controle en registratie.

Geautomatiseerde gegevensverwerking creëert in het communicatieproces nieuwe machtsstructuren rondom houders en verwerkers van gegevens. Door te kiezen voor anonimiteit kunnen eindgebruikers echter een punt aanwijzen waar deze macht eindigt. Een aanspraak op anonimiteit kan zodoende fungeren als reparatie van een verstoord informationeel machtsevenwicht en als middel om de privacy te beschermen. Met de opkomst van elektronische openbare communicatie manifesteren de maatschappelijke gevolgen van gegevensverwerking zich echter in toenemende mate ook buiten de private sfeer van het individu en raakt de problematiek van informatiemacht vaker aan publieke vrijheden, met name de uitingsvrijheid. Voorschriften over gegevensverwerking krijgen daardoor een waarborgfunctie voor de uitoefening van deze vrijheden. Deze ontwikkeling stelt de dogmatische fundering van het gegevensbeschermingsrecht op de proef. In het Amerikaanse recht, waar de bescherming van anonimiteit niet aan het recht op privacy maar aan de uitingsvrijheid is opgehangen, speelt dit probleem niet.

In hoofdstuk 4 bleek dat Amerikaanse burgers ook in de digitale omgeving aanspraak kunnen maken op een uit het First Amendment afgeleid recht op anonimiteit. In Europa en Nederland is een dergelijk expliciet geformuleerd en afdwingbaar recht nog niet aanvaard. Het belang van mogelijkheden om anoniem te communiceren is onderschreven door verschillende nationale en Europese instellingen maar wetgever en rechter lijken huiverig om een stap verder te gaan. Dit betekent echter niet dat gebruikers van elektronische communicatiemiddelen geheel aan hun lot zijn overgelaten. Zoals zal blijken in het volgende hoofdstuk, bieden regels omtrent de verwerking van gegevens in de telecommunicatiesector hen reeds een bepaalde mate van bescherming.

8 Gegevensverwerking in de telecommunicatiesector

8.1 Inleiding

Hierboven constateerden wij onder andere dat elektronische gegevensverwerking met de opkomst van openbare elektronische communicatiemiddelen doordringt in het publieke domein en dat dit verschijnsel daardoor in toenemende mate raakt aan de uitoefening van de uitingsvrijheid en andere publieke vrijheden. Daaruit volgt dat de inperking van informatiemacht in de digitale omgeving niet alleen dient als waarborg voor het recht op informationele privacy. Tegelijkertijd werd vastgesteld dat de geldende regels omtrent gegevensverwerking het recht op informationele privacy nog steeds centraal stellen.

Dit hoofdstuk werkt de genoemde bevindingen nader uit waar het de regulering van gegevensverwerking in de telecommunicatiesector betreft. Het behandelt een aantal klassieke privacyproblemen rondom de transparantie, registratie en verwerking van gegevens die zich bij telefonie voor het eerst voordeden, maar die in technisch opzicht niet uniek zijn voor dit communicatiemiddel. Telkens wordt aangegeven hoe in de digitale omgeving een verschuiving optreedt van niet-openbare naar openbare communicatie, waardoor deze problemen evolueren tot vraagstukken met een bredere dimensie. Ten eerste wordt geschetst hoe de traditionele telefoongids langzamerhand plaatsmaakt voor digitale databanken waarin naast telefoonnummers elektronische contactgegevens zoals e-mailadressen en domeinnamen zijn opgenomen. Vervolgens bekijken wij hoe de dienst nummeridentificatie voor telefonie is gereguleerd en hoe deze toepassing zich in technisch en juridisch opzicht verhoudt met gelijksoortige toepassingen bij e-mail en internet. In de derde plaats bespreken wij de grootschalige verwerking en opslag van zogenaamde 'verkeers-' en 'locatiegegevens'. Aan het einde van dit hoofdstuk wordt tenslotte afzonderlijk aandacht besteed aan een onderwerp dat buiten het regelgevend kader van de privacyrichtlijnen valt, te weten: het belang van mogelijkheden tot anonieme toegang. Bij de behandeling van de genoemde onderwerpen zal steeds in kaart worden gebracht hoe een verband ontstaat tussen gegevensverwerking en openbare anonieme communicatie.

Ter inleiding worden hier allereerst de voorschriften van de Europese privacyrichtlijnen en de implementatie daarvan in de Telecommunicatiewet (Tw) behandeld.

8.2 De algemene privacyrichtlijn

In de jaren zeventig en tachtig van de vorige eeuw ontstond voor het eerst de maatschappelijke behoefte om de grootschalige verwerking van persoonsgebonden informatie te reguleren. Na een lange periode van moeizame voorbereidingen werd daartoe in 1988 de Wet persoonsregistraties (WPR) tot stand gebracht.[1] Enige tijd later volgden ook op Europees niveau regelgevende initiatieven. De algemene privacyrichtlijn uit 1995 formuleerde algemene voorschriften omtrent de verwerking van persoonsgegevens.[2] Deze voorschriften werden geïmplementeerd in de nieuwe Wet bescherming persoonsgegevens (Wbp).[3]

De voorschriften van de algemene privacyrichtlijn zijn voornamelijk gericht tot de 'verantwoordelijke voor de gegevensverwerking'. Dit is degene die formeel-juridisch de zeggenschap over de verwerking heeft en bevoegd is om het doel en de middelen van de verwerking vast te stellen.[4] Deze voorschriften creëren voor de verantwoordelijke een aantal verplichtingen. De artikelen 6 en 7 van de algemene privacyrichtlijn stellen algemene voorwaarden voor de rechtmatige verwerking van persoonsgegevens. Artikel 6 formuleert een aantal beginselen betreffende de *kwaliteit*: persoonsgegevens moeten eerlijk en rechtmatig worden verwerkt (art. 6 lid 1 sub a), zij moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden (art. 6 lid 1 sub b). Ook moeten zij, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn (art. 6 lid 1 sub c). Persoonsgegevens dienen daarnaast nauwkeurig te zijn en zij dienen, zo nodig, te worden bijgewerkt. Alle redelijke maatregelen dienen te worden getroffen om de gegevens die, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te corrigeren (art. 6 lid 1 sub d). Van bijzonder belang voor de bescherming van anonimiteit is ten slotte het beginsel dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is (art. 6 lid 1 sub e).

Artikel 7 algemene privacyrichtlijn betreft de toelaatbaarheid van de gegevensverwerking zelf. Deze verwerking mag alleen geschieden indien de betrokkene daarvoor zijn *ondubbelzinnige toestemming* heeft verleend (art. 7 sub a algemene privacyrichtlijn). Ver-

1. Wet persoonsregistraties, *Stb.* 1988, 665. Zie over de totstandkoming van deze wet Prins & Berkvens 2002, p. 33 e.v.; De Graaf 1987.
2. Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PbEG* 1995 L 281/31.
3. Wet van 6 juli 2000, *Stb.* 302, houdende regels inzake de bescherming van persoonsgegevens, laatstelijk gewijzigd bij wet van 22 april 2004, *Stb.* 2004, 198.
4. Hooghiemstra 2001, p. 42.

werking is daarnaast mogelijk wanneer deze noodzakelijk is voor welbepaalde doeleinden. Deze doeleinden komen, voor zover relevant, nog aan de orde in het volgende hoofdstuk (zie par. 9.3). De voorschriften van artikel 6 en 7 van de algemene privacyrichtlijn zijn geïmplementeerd in de artikelen 6 t/m 11 van de Wet bescherming persoonsgegevens.[5]

8.2.1 Het transparantiebeginsel en het recht op inzage, correctie en verzet

De bedreiging van de persoonlijke levenssfeer bestaat in de informatiemaatschappij onder andere uit de vele mogelijkheden om buiten medeweten van de betrokkene om persoonsgegevens te verwerken. Een van de uitgangspunten van de Wet bescherming persoonsgegevens is daarom dat de betrokkene in de gelegenheid moet zijn om na te gaan waar gegevens over hem worden vastgelegd en verwerkt. Dit 'transparantiebeginsel' is uitgewerkt in de hoofdstukken 5 en 6 van de Wet bescherming persoonsgegevens. Aan de betrokkene, dat wil zeggen de persoon wiens gegevens het betreft, wordt in deze hoofdstukken een aantal rechten toegekend die hem in staat stellen de verwerking van hem betreffende persoonsgegevens te controleren.

Hoofdstuk 5 bestaat uit twee artikelen. Beide leggen aan de verantwoordelijke een verplichting op om de betrokkene op eigen initiatief op de hoogte te stellen van de gegevensverwerking. Artikel 33 Wbp heeft betrekking op gevallen waarin persoonsgegevens bij de betrokkene zelf zijn verkregen, bijvoorbeeld door het invullen van een formulier. Het artikel bepaalt dat de verantwoordelijke de betrokkene in dat geval vóór het moment van de verkrijging van gegevens op de hoogte moet stellen van zijn identiteit en van de doeleinden van de verwerking (art. 33 lid 1 en 2 Wbp). Daarnaast moet nadere informatie worden verstrekt die, gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen. Artikel 34 Wbp regelt de situaties waarin persoonsgegevens op andere wijze (dat wil zeggen: niet direct bij de betrokkene) zijn verkregen. In dat geval moet dezelfde informatie worden verstrekt met dien verstande dat dit pas hoeft te gebeuren op het moment van vastlegging van de gegevens of, wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking (art. 34 lid 1 sub a en b Wbp). De informatieplicht blijft krachtens artikel 34 lid 4 Wbp buiten toepassing wanneer mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost.

Hoofdstuk 6 regelt een aantal rechten van de betrokkene. De belangrijkste rechten zijn het inzagerecht (art. 35 Wbp), het recht op correctie (art. 36 Wbp) en het recht op verzet (art. 40 en 41 Wbp). Het inzagerecht houdt in dat de betrokkene het recht heeft

5. De formulering in de Wet bescherming persoonsgegevens wijkt slechts af op punten die hier van ondergeschikt belang zijn, zodat nadere bespreking van deze artikelen achterwege wordt gelaten.

zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke is verplicht om de betrokkene binnen vier werken mee te delen of dit het geval is (art. 35 lid 1 Wbp). Indien gegevens zijn verwerkt dient de mededeling een begrijpelijk en volledig overzicht daarvan te bevatten alsmede een omschrijving van de doeleinden van de verwerking, de categorieën van verwerkte gegevens, de ontvangers, en de herkomst (art. 35 lid 2 Wbp). Het recht op correctie geeft de betrokkene de mogelijkheid om de verantwoordelijke te verzoeken om persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen wanneer deze feitelijk onjuist zijn, wanneer zij voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn of wanneer zij anderszins in strijd met een wettelijk voorschrift worden verwerkt (art. 36 lid 1 Wbp).

De meest vergaande bevoegdheid van de betrokkene is het recht om zich te verzetten tegen de verwerking van persoonsgegevens als zodanig, wanneer dit gerechtvaardigd is op basis van zijn bijzondere persoonlijke omstandigheden. Dit recht kan blijkens artikel 40 lid 1 Wbp in twee situaties worden ingeroepen. In de eerste plaats kan men opkomen tegen de verwerking van gegevens door de overheid, dat wil zeggen wanneer gegevensverwerking op basis van artikel 8 sub e Wbp heeft plaatsgevonden ten behoeve van de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt. Afwijzing van het verzoek tot honorering van het verzet door een bestuursorgaan geldt krachtens artikel 45 Wbp als een besluit in de zin van de Algemene wet bestuursrecht waartegen bezwaar en beroep kan worden ingediend. Verzet kan daarnaast worden aangetekend wanneer gegevens zijn verwerkt op basis van de restbepaling van artikel 8 sub f Wbp. Dit artikellid maakt verwerking mogelijk wanneer dit noodzakelijk is voor de behartiging van een belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. Wanneer een betrokkene gebruik maakt van het recht op verzet, volgt hieruit een plicht voor de verantwoordelijke om de belangen van de betrokkene opnieuw af te wegen tegen de belangen die met de verwerking zijn gemoeid.[6]

Voor de verwerking van persoonsgegevens ten behoeve van direct marketing voorziet artikel 41 Wbp in een specifieke regeling. Hier is het recht van verzet absoluut. Dit betekent dat het verzet in alle gevallen moet worden gehonoreerd zonder dat van de betrokkene kan worden geëist dat hij zijn bezwaar tegen de verwerking motiveert. De verantwoordelijke dient de verwerking terstond te beëindigen (art. 41 lid 2 Wbp). Er vindt dus geen hernieuwde afweging van belangen plaats. Aan de behandeling van het verzet mogen bovendien, anders dan in de regeling in artikel 40 Wbp, geen kosten zijn verbonden.

6. Hooghiemstra 2001, p. 107.

8.3 De richtlijn privacy en elektronische communicatie

De introductie van de ISDN-standaard leidde, met name in de sfeer van telefonie, tot specifieke problemen rondom de verwerking van gegevens en de identificeerbaarheid van gebruikers (zie ook par. 7.1.1).[7] Voor de telecommunicatiesector werd daarom een bijzonder regime gecreëerd, eerst in de ISDN-richtlijn en later in de richtlijn privacy en elektronische communicatie.[8] De verwerking van gegevens over elektronische communicatie is zodoende onderworpen aan twee elkaar overlappende regelgevingskaders: het algemene kader van de algemene privacyrichtlijn en de Wet bescherming persoonsgegevens en het telecomspecifieke kader van de richtlijn privacy en elektronische communicatie, zoals uitgewerkt in de Telecommunicatiewet. Telecomaanbieders zijn op basis van het algemene privacykader in de hoedanigheid van 'verantwoordelijke voor de gegevensverwerking' gebonden aan algemene voorwaarden voor de verwerking van persoonsgegevens. Dit algemene kader is van belang voor verwerkingshandelingen waarvoor geen specifieke regels gelden. Daarbij moet men met name denken aan verwerkingshandelingen met betrekking tot abonneegegevens. Het telecomspecifieke kader sluit aan bij het businessmodel van telefoniemaatschappijen en internetproviders en legt meer specifieke verplichtingen op aan 'aanbieders van elektronische communicatienetwerken- en diensten'. Dit is bijvoorbeeld het geval bij de verwerking van verkeers- en locatiegegevens. De begrippen uit het algemene en het telecomspecieke reguleringskader overlappen elkaar hier overigens. Locatiegegevens kunnen in de meeste gevallen als verkeersgegevens worden aangemerkt en verkeersgegevens zijn op hun beurt vaak persoonsgegevens (zie par. 8.3.3).

Ook ten aanzien van communicerende gebruikers en consumenten zijn verschillende wettelijke begrippen toepasselijk. Zij kunnen in de meeste gevallen worden aangemerkt als 'betrokkene' in de zin van de Wet bescherming persoonsgegevens. Het telecomspecifieke kader voorziet in een specifieke privacybescherming en maakt daarbij onderscheid tussen 'gebruikers' en 'abonnees'. Sommige verplichtingen van aanbieders gelden alleen ten aanzien van de abonnees waarmee zij een contractuele relatie hebben. Het onderscheid tussen 'betrokkenen' enerzijds en 'gebruikers' en 'abonnees' anderzijds reflecteert dus een verschil in beschermingsniveau voor verschillende groepen van consumenten.

De richtlijn privacy en elektronische communicatie bevat een reeks verplichtingen voor de aanbieder van elektronische communicatienetwerken en -diensten en een aantal rechten voor de gebruiker daarvan. In de overwegingen bij de richtlijn wordt expliciet

7. Een aantal belangrijke vraagstukken rondom anonimiteit en telecommunicatie speelt al vanaf begin jaren negentig. Zie over nummeridentificatie en gespecificeerde rekeningen bijvoorbeeld Nugter & Smits 1991 en Sciarone-Gorgels 1994.
8. Richtlijn 97/66/EG van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *PbEG* 1998 L 24/1; Richtlijn 2002/58/EG van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEG* 2002 L 201/37.

ingegaan op de mogelijkheid om anoniem gebruik te maken van elektronische communicatienetwerken en -diensten. Zo stelt overweging 9 dat de lidstaten, de betrokken aanbieders en gebruikers alsmede de bevoegde communautaire instanties zouden moeten samenwerken bij de introductie en ontwikkeling van de benodigde technieken waar zulks noodzakelijk is met het oog op de waarborgen die door de richtlijn worden geboden, daarbij met name rekening houdend met de doelstelling de verwerking van persoonsgegevens zoveel mogelijk te beperken en waar mogelijk gebruik te maken van anonieme of onder pseudoniem opgeslagen gegevens. Systemen voor elektronische-communicatienetwerken en -diensten moeten op dusdanige wijze worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt. Overweging 30 benadrukt dat voor verkeersgegevens als hoofdregel geldt dat verwerking die verder gaat dan strikt noodzakelijk is voor transmissie en facturering moet worden gebaseerd op geaggregeerde verkeersgegevens die niet met abonnees of gebruikers in verband kunnen worden gebracht.

Reeds in de oude ISDN-richtlijn was de registratie en verwerking van gegevens in de telecommunicatiesector aan banden gelegd. In de richtlijn privacy en elektronische communicatie zijn de geldende voorschriften vervolgens verder uitgebreid en uitgewerkt.

Men kan drie stadia van het communicatieproces onderscheiden waarin de anonimiteit van gebruikers relevant is. Voorafgaand aan de eigenlijke communicatie speelt allereerst de kenbaarheid van adresseringsinformatie, zoals telefoonnummers, e-mailadressen en domeinnamen, die nodig is om communicatie mogelijk te maken. Gebruikers kunnen aanspraak maken op zeggenschap hierover. Het tweede stadium betreft informatie die direct voorafgaand aan of tijdens de communicatie via het netwerk tussen gebruikers wordt uitgewisseld, bijvoorbeeld via nummerherkenning bij telefonie. Het derde stadium is de registratie van gegevens door de elektronische tussenpersoon bij het afhandelen van de communicatie.

In de komende paragrafen worden de drie genoemde onderwerpen besproken. Hierbij wordt, uitgaande van het model van de klassieke telefonie, geïnventariseerd hoe zich steeds duidelijker een verband aftekent tussen gegevensverwerking, openbare communicatie en de anonieme uitoefening van de uitingsvrijheid.

8.3.1 Opname van persoonsgegevens in abonneelijsten

Om via elektronische communicatiediensten te kunnen communiceren met anderen, dienen gebruikers te beschikken over elektronische contactgegevens van andere gebruikers. Bij telefonie was men daarvoor van oudsher aangewezen op de traditionele telefoongids. Tegenwoordig bestaan er echter ook elektronische gidsen. De richtlijn privacy en elektronische communicatie en de gewijzigde Telecommunicatiewet spreken daarom niet langer meer van een telefoongids, maar van een abonneelijst.[9]

9. *Kamerstukken II* 2002-2003, 28 851, nr. 3, p. 158.

In elektronische telefoongidsen en andere databanken zijn steeds vaker ook elektronische contactgegevens opgenomen, zoals bijvoorbeeld domeinnamen en e-mailadressen. Bovendien is het vaak mogelijk om deze contactgegevens door 'omgekeerd' te zoeken te koppelen aan naam-, adres en woonplaatsgegevens – iets wat bij de ouderwetse telefoongids nog niet mogelijk was. Dit leidt er toe dat ook verspreiders van openbare informatie vrij eenvoudig kunnen worden achterhaald. Daarmee raakt de transparantie van deze gegevens ook aan de mogelijkheid om de uitingsvrijheid anoniem uit te oefenen. De identiteit van een informatiebron, bijvoorbeeld de houder van een website, is dankzij de genoemde databanken voor andere gebruikers immers kenbaar.

Hieronder wordt eerst de wettelijke regeling ten aanzien van abonneelijsten in de Telecommunicatiewet besproken. Vervolgens wordt ingegaan op de problemen rond gegevensverwerking die zich voordoen bij zogenaamde 'whois databanken'. Bij de behandeling van dat laatste onderwerp komt voren de relatie met openbare communicatie en de verhouding met de uitingsvrijheid duidelijk naar voren.

Regeling in de Telecommunicatiewet

Openbare abonneelijsten vormen een essentieel hulpmiddel voor toegang tot openbare telefoondiensten. Artikel 5 van de Universeledienstrichtlijn verplicht de lidstaten daarom om ervoor zorg te dragen dat ten minste één volledige telefoongids beschikbaar is.[10] Om de beschikbaarheid van universele telefoongidsen te waarborgen en om daadwerkelijke concurrentie op de markt voor universele telefoongidsen mogelijk te maken, is het noodzakelijk dat uitgevers van universele telefoongidsen toegang hebben tot de abonneegegevens van operators. Operators zijn daarom verplicht om de telefoonnummers van hun abonnees met bijbehorende gegevens aan hen ter beschikking te stellen.[11] Abonnees hebben echter het recht om te bepalen of, en zo ja met welke gegevens, zij in een openbare abonneelijst wensen te worden vermeld. Dit vloeit voort uit het recht op zeggenschap over de vermelding van persoonsgegevens.[12]

Het recht op zeggenschap is, waar het abonneelijsten betreft, uitgewerkt in artikel 12 van de richtlijn privacy en elektronische communicatie. Dit artikel is vervolgens geïmplementeerd in artikel 11.6 Tw. De richtlijn elektronische communicatie introduceert voor de opname van persoonsgegevens in abonneelijsten een zogenaamd 'opt-in regime'.[13] Waar abonnees vroeger automatisch in een abonneelijst werden opgenomen, tenzij zij daartegen bezwaar maakten, is in de nieuwe situatie krachtens artikel 11.6 lid 2 Tw vooraf-

10. Richtlijn 2002/22/EG van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, *PbEG* 2002 L 108/51.
11. Wie in Nederland een universele gids wil uitgeven kan voor de verzameling van abonneegegevens een beroep doen op artikel 43 van het Besluit ONP huurlijnen en telefonie (Boht). Zie besluit van 10 november 1998, *Stb.* 1998, 639.
12. Overweging 38 bij de richtlijn betreffende privacy en elektronische communicatie.
13. Lichtenberg 2003.

gaande toestemming van de abonnee vereist.[14] Voor degene die een algemeen beschikbare abonneelijst uitgeeft of een algemeen beschikbare abonnee-informatiedienst verzorgt geldt een informatieplicht. Artikel 11.6 lid 1 Tw bepaalt dat de abonnee voorafgaand aan opneming van hem betreffende persoonsgegevens in een abonneelijst of -bestand kosteloos op de hoogte moet worden gesteld van de doeleinden van deze lijst, de gebruiksmogelijkheden op basis van daarin opgenomen zoekfuncties en de soorten persoonsgegevens die worden opgenomen. Persoonsgegevens worden uitsluitend opgenomen indien en voor zover de abonnee daarvoor toestemming heeft gegeven. Aan het niet opgenomen zijn mogen geen kosten zijn verbonden (art. 11.6 lid 2 Tw). Ook hier gelden de rechten van de betrokkene op inzage en correctie. De abonnee heeft het recht om hem betreffende persoonsgegevens te verifiëren, te laten verbeteren of te laten verwijderen zonder dat daaraan kosten zijn verbonden (art. 11.6 lid 4 Tw). De huidige bepalingen in de telecommunicatiewet brengen met zich mee dat gebruikers voorafgaand aan opname in een tweede universele gids apart toestemming moeten geven (tweede opt-in). Naar alle waarschijnlijkheid zal aangaande dit onderwerp bij AMVB regelgeving tot stand worden gebracht.[15]

Als gevolg van technische ontwikkelingen speelt het recht om zelf te bepalen of persoonsgegevens worden opgenomen niet langer slechts bij opname in fysieke telefoongidsen.[16] Er

14. Het College bescherming persoonsgegevens (Cbp) constateerde in 2003 dat KPN reeds geruime tijd adresgegevens van abonnees met een geheim nummer voor direct marketing doeleinden ter beschikking stelde aan derden zonder dat haar abonnees daarover expliciet waren geïnformeerd. Deze handelwijze werd door het Cbp in strijd bevonden met met de bij abonnees door KPN zelf opgeroepen verwachting dat een dergelijke verstrekking niet plaats zou vinden en met het principe dat verwerking van persoonsgegevens verenigbaar dient te zijn met de doeleinden waarvoor deze zijn verkregen. Daarnaast werd het voorschrift van artikel 43 lid 3 Wbp genegeerd. Hierin is bepaald dat de betrokkenen in gevallen van verstrekking ten behoeve van direct marketing op de hoogte dienen te worden gesteld van het recht om hiertegen verzet aan te tekenen. Ten slotte was evenmin voorzien in een eenvoudige en kosteloze bezwaarmogelijkheid. College bescherming persoonsgegevens 2003.
15. Het College bescherming persoonsgegevens adviseerde de Minister elke telecomprovider te verplichten om abonnees expliciet om toestemming te vragen bij het afsluiten van een abonnement voor publicatie in één, meerdere of alle standaard telefoongidsen. College bescherming persoonsgegevens 2004, p. 2-3.
16. Het omgekeerd zoeken kwam aan de orde in de zaak *Denda/KPN*. Denda was voornemens een elektronische telefoongids uit te geven. Bij het leveren van de benodigde abonneegegevens stelde KPN ter bescherming van de privacybelangen van haar abonnees onder andere de eis dat omgekeerd zoeken in de door Denda te vervaardigen gids onmogelijk moest zijn. KPN vreesde dat het toelaten van de zoekfunctie een toename van het aantal afgeschermde nummers tot gevolg zou kunnen hebben, waardoor het primaire doel van het bestand – nummerinformatie – zou worden geschaad. Denda spande hierop een zaak aan wegens misbruik van economische machtspositie. Het college van de OPTA oordeelde echter dat KPN zich terecht beriep op geldende en toekomstige privacyregelgeving en op de privacy van haar abonees, die deze zoekfunctie als een inbreuk op hun privacy zouden kunnen ervaren. KPN legde zichzelf bovendien bij het openbaar maken van de gegevens dezelfde beperkingen op. Zie Besluit van het college van de Onafhankelijke Post en Telecommunicatie Autoriteit van 29 september 1999 inzake Denda Multimedia B.V. en Topware CD-service A.G. versus KPN Telecom B.V.

komen steeds meer elektronische telefoongidsen op de markt die de namen, adressen en telefoonnummers van miljoenen mensen bevatten.[17] In veel gevallen bieden deze producten naast de traditionele zoekmethoden om het telefoonnummer van een abonnee te vinden op basis van zijn of haar naam de mogelijkheid om omgekeerd of met meervoudige criteria te zoeken.[18] De nieuwe zoekmethoden maken het bijvoorbeeld mogelijk om aan de hand van een telefoonnummer de naam en het adres van een abonnee te vinden of om op basis van het adres de naam en het telefoonnummer te achterhalen. Daarnaast is het soms mogelijk om de namen en telefoonnummers van alle personen in een bepaalde gebied (bijvoorbeeld een straat) te vinden. De Nederlandse wetgever heeft er voor gekozen om voor omgekeerd zoeken afzonderlijke toestemming van de abonnee te eisen (art. 11.6 lid 3 Tw). De bescherming van de privacy van de abonnee gaat daarmee verder dan het niveau dat door de richtlijn privacy en elektronische communicatie wordt voorschreven.[19]

De mogelijkheid tot omgekeerd zoeken heeft gevolgen voor de privacyverwachtingen van burgers. Wie de beschikking heeft over een telefoonnummer kan nu immers de volledige naam en het adres en in sommige gevallen het beroep en de werkkring van de betrokken gebruiker achterhalen. Bovendien kan aan de hand van een gespecificeerde telefoonrekening, waarop alleen de gebelde telefoonnummers zijn vermeld, een lijst worden opgesteld met de namen en adressen van alle personen die in een bepaalde periode zijn gebeld. Tenslotte kunnen de gegevens uit een elektronische telefoongids worden gekoppeld aan andere informatie uit openbare bestanden zoals bijvoorbeeld geografische informatie. Zodoende kan op basis van een telefoonnummer veel meer informatie worden achterhaald dan de gemiddelde burger redelijkerwijze zal verwachten.

Whois-databanken

Een met het omgekeerd zoeken vergelijkbaar probleem speelt bij de zogenaamde 'whois-databanken' op het internet. Whois-gegevens hebben betrekking op degene die een bepaalde domeinnaam heeft geregistreerd. Zij bevatten in het bijzonder contactgegevens van degene op wiens naam een domeinnaam is geregistreerd, zoals telefoonnummers, e-mailadressen en andere persoonlijke informatie. Deze gegevens werden oorspronkelijk openbaar gemaakt ten behoeve van netwerkbeheerders. In de loop der tijd zijn daar andere doelen bijgekomen, zoals de aanvraag van (nog vrije) domeinnamen, de bescherming van intellectuele eigendomsrechten en de voorkoming en bestrijding van illegale en schadelijke inhoud op het internet.[20] Nu steeds meer particulieren een domeinnaam

17. Groep gegevensbescherming artikel 29 2000.
18. *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 159.
19. Op basis van artikel 12 lid 3 van de richtlijn privacy en elektronische communicatie is het vereisen van afzonderlijke toestemming optioneel. In sommige andere lidstaten, zoals bijvoorbeeld België, is afzonderlijke toestemming niet vereist.
20. Artikel 2.1 sub e Wbp-regeling SIDN.

laten registeren (in Nederland is dit mogelijk sinds 2003) ontstaan echter klachten over het onbehoorlijk gebruik van deze informatie. De registratie en het publiek toegankelijk maken van whois-gegevens van individuele personen moet dan ook anders worden beoordeeld. Rechtspersonen zijn in het kader van commerciële activiteiten in het algemeen al wettelijk verplicht tot het publiceren van informatie over hun bedrijf of organisatie, terwijl er bij registratie door individuen doorgaans geen wettelijke grond is voor een verplichte publicatie van persoonsgegevens.

De artikel 29-werkgroep meent dat particuliere gebruikers het recht hebben om domeinnamen te registreren zonder dat hun persoonsgegevens in openbare registers worden opgenomen. Dit recht vloeit voort uit de gegevensbeschermingsbeginselen en is daarnaast expliciet erkend in de richtlijn privacy en elektronische communicatie. Verder is het van groot belang dat in duidelijke bewoordingen wordt vastgesteld wat het doel is van de gegevensverwerking in whois-databanken.[21] Dit doel kan niet zomaar worden uitgebreid enkel omdat sommige potentiële gebruikers van de bestanden dit wenselijk vinden. De groep is bezorgd over voorstellen voor meer doorzoekbare whois-faciliteiten en noemt met name het gebruik door private partijen die inbreuk op hun intellectuele eigendomsrechten willen tegengaan (zie par. 9.6). Zij steunt voorstellen voor de bevordering van nauwkeurigheid van de gegevens en voor beperking van massale toegang voor direct marketing. In dat verband wordt een beroep gedaan op ICANN om privacybevorderende methoden te hanteren bij het beheer van de databanken.[22]

De opname van persoonlijke gegevens in whois-databanken kwam in Nederland aan de orde in een beroepsprocedure tegen de Stichting Internet Domeinregistratie Nederland (SIDN). Krachtens het privacyreglement van SIDN kunnen domeinnaamaanvragers en domeinnaamhouders die in verband met bijzondere omstandigheden bezwaar hebben tegen opname in het openbare deel van de databank SIDN verzoeken deze gegevens te vervangen door de gegevens van de provider die de bewuste site toegankelijk maakt.[23] De appellant, journalist Sander Simons, had een dergelijk verzoek ingediend omdat hij, na publicatie van een boek met controversiële uitspraken over criminaliteit, immigratie en andere gevoelige politieke onderwerpen, vreesde voor de veiligheid van zijn gezin. Het verzoek betrof uitsluitend zijn adresgegevens. Appellants naam was voor bezoekers van de website reeds kenbaar nu deze site via de domeinnaam 'www.sandersimons.nl' toegankelijk was. Verwijdering van de adresgegevens zou bescherming bieden tegen mogelijke represaillemaatregelen van partijen die de openbaar gemaakte informatie, om wat voor reden dan ook, niet welgevallig was. Zolang de NAW-gegevens van de domeinnaamhouder bij de provider bekend waren, vergde zijns inziens geen van de doelen ten behoeve waarvan openbaarmaking in de whois-databank geschiedt, dat de NAW-

21. Groep gegevensbescherming artikel 29 2003.
22. Center for Democracy & Technology 2003.
23. Artikel 23.4 Reglement voor registratie van .nl-domeinnamen.

gegevens van een natuurlijke persoon openbaar gemaakt werden. Het verzoek werd echter ongegrond verklaard. Helaas ging het College voor Klachten en Beroep (CvKB) nauwelijks in op het door appellant aangevoerde belang van de uitingsvrijheid. Opmerkelijk is daarnaast de volgende overweging van het college:

> "Appellant geeft ook geen uitleg waarom gekozen is voor een openbaar medium als internet om aandacht te vragen voor een boek met controversiële inhoud via een domeinnaam die met de adresgegevens naar het woonadres van de schrijver verwijst. Ook geeft Appellant niet aan waarom andere alternatieven geen mogelijkheid bieden. Wat daarnaast voor het CvKB zwaar weegt is dat dezelfde adresgegevens van de eenmanszaak ook in het openbare handelsregister van de Kamer van Koophandel en Fabrieken zijn opgenomen en tevens opvraagbaar zijn via KvK on-line, het on-line handelsregister."[24]

Het College lijkt uit te gaan van de redenering dat bij gebruikmaking van een openbaar medium minder snel of in het geheel geen aanspraak kan worden gemaakt op bescherming van persoonlijke gegevens. Dit is onjuist. Uit het feit dat het internet een openbaar medium is, volgt nog niet dat natuurlijke personen bij het toegankelijk maken van informatie via een website te allen tijde hun persoonlijke gegevens zouden moeten prijsgeven. Zoals wij zagen blijkt dit uit verschillende officiële documenten en uit de privacyrichtlijnen (zie par. 7.2, 8.2 en 8.3). Vreemd genoeg gaat het College in zijn overwegingen geheel niet in op het rapport van de artikel 29 werkgroep of op het in de privacyrichtlijnen erkende recht op zeggenschap.

De geciteerde overweging is eveneens strijdig met de door artikel 29-werkgroep geformuleerde uitgangspunten. De groep overweegt immers uitdrukkelijk dat de gegevensbeschermingsbeginselen ook van toepassing zijn op whois-databanken.[25] Een verplichte publicatie van persoonsgegevens van een natuurlijke persoon is naar zijn oordeel in strijd met het recht om zelf te bepalen of men persoonsgegevens in een openbaar bestand wil laten opnemen. Hiervan uitgaande is het onwenselijk dat SIDN zelfstandig gaat toetsen of verzoekers in een concreet geval een zwaarwegend belang hebben. Houders van domeinnamen hebben immers net als gebruikers van telefoniediensten een uit het recht op zeggenschap over persoonsgegevens voortvloeiend recht om *zelf* te bepalen of zij hun gegevens in een openbare lijst vermeld willen hebben. Als een abonnee toestemming weigert voor omgekeerd zoeken in een *telefoongids* dan is het niet de taak van de telefonie-

24. Beslissing van het College voor Klachten en Beroep SIDN inzake het beroep tegen het besluit van de SIDN d.d. 8 september 2003 (*domeinnaam sandersimons.nl*), zaaknr. 2004/10, Arnhem 9 februari 2004.
25. Of whois-databanken kunnen worden aangemerkt als openbare abonneelijsten in de zin van de Telecommunicatiewet, is onduidelijk. De Memorie van Toelichting bij de Telecommunicatiewet geeft hierover geen uitsluitsel. Zie *Kamerstukken II* 2002/03, 28851, nr. 3, p. 49 e.v. De artikel-29 werkgroep laat zich over deze vraag evenmin uit, maar verwijst in haar rapport over whois-databanken wel naar haar eerdere rapport over omgekeerd zoeken in openbare abonneelijsten. Groep gegevensbescherming artikel 29 2003, p. 3-4.

aanbieder om te toetsen of de abonnee daarvoor een zwaarwegend belang aannemelijk kan maken. Evenmin is van belang of de bewuste adresgegevens al ergens anders in een openbaar bestand beschikbaar zijn. Niet valt in te zien waarom dit bij de vermelding van adresgegevens in whois-databanken anders zou zijn. Voor de bescherming van de anonimiteit van de gebruiker zou het immers niet uit moeten maken van welke technologie hij gebruikt maakt. Dat het adres van appellant al beschikbaar was bij de Kamer van Koophandel doet hier dan ook niet ter zake.

In feite speelden in de besproken casus zowel private als publieke belangen een rol. Zo moet men de wens van appellant om zijn familie te beschermen zien als een wens om de private sfeer af te schermen. Voorzover het verzoek ook was ingegeven om appellants werkzaamheden als journalist mogelijk te maken door de vrees voor represailles weg te nemen, bestond er echter ook een direct verband met de uitingsvrijheid en de bescherming van het publieke debat. Het College had op dat laatste belang dieper in moeten gaan. Daarbij had onder andere aan de orde moeten komen dat er in de context van boeken en geschriften een door de wetgever erkend belang bestaat om anoniem te kunnen publiceren.

8.3.2 Blokkering van nummeridentificatie

Vóór de invoering van de ISDN-standaard bleef de identiteit van een beller onbekend totdat de opgeroepen gebruiker de oproep beantwoordde en de beller zijn naam noemde. De digitalisering van het netwerk heeft het echter technisch mogelijk gemaakt om nummergegevens te zenden aan de opgeroepen gebruiker, die dit nummer reeds voordat hij de oproep beantwoord op zijn toestel ziet verschijnen. In de Universeledienstrichtlijn is vervolgens aan aanbieders van openbare telefoonnetwerken de verplichting opgelegd om nummeridentificatie aan alle gebruikers aan te bieden.[26]

De algemene beschikbaarheid van nummeridentificatie heeft kenbaarheid van identiteit voor gebruikers van vaste en mobiele telecommunicatiediensten tot hoofdregel gemaakt. Indien het nummer van de oproepende gebruiker reeds is opgenomen in de adressenlijst van het (mobiele) telefoontoestel van de opgeroepen gebruiker, wordt dit nummer gekoppeld aan de in die lijst opgenomen naam, die vervolgens voor de gebruiker zichtbaar wordt. Zodoende is niet alleen het nummer maar ook de naam van de oproepende gebruiker kenbaar. Ook in andere gevallen geeft het oproepende nummer aanknopingspunten om de identiteit te achterhalen. Het netnummer kan een aanwijzing zijn en bovendien kan men de oproepende gebruiker terugbellen. Nummerherkenning

26. Deze eisen zijn uitgewerkt in par. 4 van de Regeling universele dienstverlening en eindgebruikersbelangen. Zie regeling van de Minister van Economische Zaken van 10 mei 2004, *Stcrt.* 14 mei 2004, 92, p. 11 (Regeling universele dienstverlening en eindgebruikersbelangen).

doorbreekt zodoende de anonimiteit van de oproepende gebruiker ten opzichte van andere gebruikers.[27]

Om voor de hand liggende redenen is het belang van de gebruiker om nummerherkenning te kunnen uitschakelen van het begin af aan opgevat als een privacybelang. Het klassieke telefoongesprek is immers een niet-openbare vorm van communicatie, die als zodanig valt binnen de privé-sfeer van de beller. De beller geeft voorafgaand aan het totstandbrengen van de oproep zijn nummer prijs en kan legitieme belangen hebben om nummeridentificatie uit te schakelen. In de meeste gevallen zullen ook deze belangen liggen binnen zijn private sfeer, zelfs wanneer het uitschakelen van de nummerherkenning geschiedt om onbevreesd toegang te hebben tot instanties zoals hulp- en kliklijnen en meldpunten waar men terecht kan met klachten, anonieme tips of psychische en sociale problemen. De beller uit zich dan weliswaar, maar zijn uitingen blijven doorgaans binnen de vertrouwelijke relatie met de hulpverlener en ontberen een openbaar karakter. Pas wanneer nummerherkenning wordt uitgeschakeld om belangen te beschermen die liggen buiten de private sfeer, ligt het meer voor de hand om het vraagstuk primair te analyseren vanuit de uitingsvrijheid. Dit is bijvoorbeeld het geval wanneer de beller anoniem informatie wenst door te spelen aan een journalist.

In feite gaat het bij nummerherkenning om een technologische toepassing die niet uniek is voor telefonie. Iedere elektronische communicatietechniek heeft een systeem van technische adressering, waarbij gebruik wordt gemaakt van gegevens die in zekere zin vergelijkbaar zijn met het telefoonnummer. Bij het versturen van een e-mailbericht wordt het e-mailadres van de afzender meegezonden en tijdens het raadplegen van een website worden tussen de aanbieder van de site en de gebruiker IP-adressen uitgewisseld. De raadplegende gebruiker ziet het IP-adres van de website, gepresenteerd als een URL, verschijnen in de adresbalk van zijn browser. De websitehost op zijn beurt kan doorgaans het IP-adres van bezoekers zien. Anders dan bij telefonie is de doorgifte van adresseringsinformatie bij internet en e-mail echter niet wettelijk gereguleerd. De verplichting tot het aanbieden van nummeridentificatie is alleen opgelegd aan aanbieders van telefoniediensten en de regeling aangaande nummerherkenning in de Telecommunicatiewet is alleen voor telefonie nader uitgewerkt. Bij nieuwe elektronische communicatiemiddelen bestond de noodzaak om de verzending van het identificerende kenmerk verplicht te stellen overigens niet omdat deze toepassing vanaf het begin technisch was ingebakken.

27. Zoals Holvast opmerkt is bij nummeridentificatie onder andere de vraag relevant welk belang hoger geprioriteerd moet worden: dat van de beller of dat van de gebelde. Voor het antwoord op deze vraag zijn onder meer culturele factoren bepalend. In de Verenigde Staten is het gebruikelijk dat de gebelde opneemt met 'hallo'. Pas nadat de beller zich bekend heeft gemaakt, is hij bereid zijn identiteit te onthullen. Aan deze gewoonte ligt de gedachte ten grondslag dat de beller door te bellen een inbreuk maakt op de privacy van de gebelde, aldus Holvast. Holvast is zelf van oordeel dat de belangen van beller en gebelde in verhoudingen tussen consumenten onderling even groot geacht moeten worden. Holvast 1994, p. 227.

Hoewel een wettelijke regeling ontbreekt, bestaat er bij e-mail en internet in gelijke mate behoefte aan normering van de transparantie en doorgifte van de genoemde gegevens. Het gaat daar in essentie immers om het zelfde probleem: de verstrekking van identificerende gegevens door elektronische tussenpersonen aan andere gebruikers of derde partijen. Toch wijkt de problematiek hier enigszins af. Waar de gebruiker van de telefoondienst in principe slechts de door de aanbieder gewaarborgde mogelijkheid heeft om zijn nummerherkenning uit te schakelen, kunnen internetgebruikers de verzending van identificerende informatie softwarematig op uiteenlopende manieren bewerkstelligen. Bovendien komt wederom aan het licht dat digitale gegevensverwerking sterk verweven is met openbare informatie. Verwees het telefoonnummer oorspronkelijk naar een aansluiting op het netwerk waar men een bepaalde persoon of instantie kon bereiken voor besloten conversatie – de technische adresseringsgegevens die bij e-mail en internet worden uitgewisseld verwijzen dikwijls naar bronnen en vindplaatsen van digitale openbare informatie, zoals websites, digitale nieuwsbrieven en e-mails in online discussiefora. Daarmee komt ook deze materie steeds meer los te staan van het recht op privacy, terwijl de uitingsvrijheid aan belang toeneemt.

Ook gaan er andere belangen een rol spelen bij de doorbreking van anonimiteit. Men denke met name aan belediging en de verspreiding van informatie die onrechtmatig is jegens derde partijen of inbreuk maakt op het auteursrecht.

De centrale vraag is bij iedere communicatietechniek telkens opnieuw wanneer adresseringsgegevens ter identificatie kunnen en mogen worden doorgegeven aan andere gebruikers of derde partijen. Nu e-mail en internet buiten de regeling in de Telecommunicatiewet vallen, moet deze vraag daar worden beantwoord aan de hand van de bepalingen in de Wet bescherming persoonsgegevens en de jurisprudentie. Wij spreken dientengevolge niet langer van nummeridentificatie maar, in de terminologie van de Wet bescherming persoonsgegevens, van 'verstrekking van persoonsgegevens'. De juridische vragen die zich bij verstrekking via deze weg voordoen en het verband met anonieme openbare communicatie worden behandeld in het volgende hoofdstuk.

Tot slot dient hier te worden opgemerkt dat technische convergentie en de daarmee gepaard gaande samenvloeiing van niet-openbare en openbare communicatie bestaande regelgeving in de toekomst naar alle waarschijnlijkheid op de proef zullen stellen. De scheiding van telefonie en andere communicatiemiddelen en de technologiespecifieke regulering van nummeridentificatie zal op termijn onhoudbaar blijken. Er is al een aantal technische ontwikkelingen gaande die dit vermoeden ondersteunen. Zo is het de vraag in hoeverre de voorschriften over het aanbieden van nummerherkenning en de blokkering daarvan toepasbaar zijn op digitale telefonie. Daarnaast is het onduidelijk hoe de afzonderlijke normering stand kan houden wanneer domeinnamen en telefoonnummers technisch worden samengevoegd, bijvoorbeeld via de zogenaamde 'ENUM-standaard'.

Hoewel telefonie en andere technologieën feitelijk niet los van elkaar kunnen worden gezien, wordt de geldende regelgeving voor telefonie hier toch afzonderlijk behandeld

omdat deze onderdeel is van het kader van de privacyrichtlijnen en de Telecommunicatiewet.

Regeling in de Telecommunicatiewet

Aanbieders van openbare telefoonnetwerken moeten krachtens artikel 8 van de richtlijn privacy en elektronische communicatie voorzien in de mogelijkheid om op eenvoudige en kosteloze wijze en voor iedere oproep afzonderlijk de nummeridentificatie te blokkeren.[28] Ter uitvoering van de Universeledienstrichtlijn en de richtlijn privacy en elektronische communicatie zijn in par. 11.2 van de Telecommunicatiewet voorschriften opgenomen met betrekking tot de blokkering van nummeridentificatie.[29]

Artikel 11.9 Tw legt aan aanbieders van openbare elektronische telecommunicatienetwerken en -diensten de verplichting op om blokkering van nummeridentificatie voor de verstrekking van het zowel het oproepende als het opgeroepen nummer mogelijk te maken. Daarnaast moet het mogelijk zijn om op eenvoudige wijze inkomende oproepen te weigeren wanneer de verstrekking van het nummer is geblokkeerd (art. 11.9 lid 1 sub a onder ten tweede Tw). Artikel 11.9 Tw luidt:

> "1. De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst die door middel van dat netwerk of als onderdeel van die dienst nummeridentificatie aanbiedt, biedt:
>
> a. aan iedere oproepende gebruiker onderscheidenlijk abonnee mogelijkheden aan om kosteloos de verstrekking van het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd te blokkeren onderscheidenlijk de verstrekking van nummers van oproepende netwerkaansluitpunten dan wel nummers waarmee individuele gebruikers kunnen worden geïdentificeerd voor elke afzonderlijke abonneelijn te blokkeren;
>
> b. aan iedere opgeroepen abonnee mogelijkheden aan om:
>
> 1°. de verstrekking van het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd te verhinderen;
>
> 2°. oproepen waarbij de verstrekking van het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd is geblokkeerd, te weigeren;

28. Artikel 1.1, onderdeel cc. Tw definieert nummeridentificatie als een (1) faciliteit om het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd aan het opgeroepen netwerkaansluitpunt te verstrekken, voordat de verbinding tot stand wordt gebracht of (2) een faciliteit om het nummer van het opgeroepen netwerkaansluitpunt dan wel het nummer waarmee een individuele gebruiker kan worden geïdentificeerd aan het oproepende netwerkaansluitpunt te verstrekken, voordat de verbinding tot stand wordt gebracht.
29. Richtlijn 2002/22/EG van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, *PbEG* 2002 L 108/51, Bijlage I, deel B sub b. Identificatie van de oproepende lijn houdt blijkens deze richtlijn in dat aan de opgeroepene het abonneenummer van de oproeper wordt meegedeeld voordat de oproep tot stand is gebracht.

> 3°. indien nummeridentificatie als bedoeld in artikel 1.1, onderdeel cc, onder 2°, wordt aangeboden, kosteloos de verstrekking van het nummer van het opgeroepen netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd aan het oproepende netwerkaansluitpunt te blokkeren."

Wanneer zwaarwegende belangen daartoe aanleiding geven kan de blokkering van nummeridentificatie ongedaan worden gemaakt. Zo zijn telecomaanbieders bij de afwikkeling van communicatie met een alarmnummer voor publieke diensten verplicht om aan de beheerders daarvan gelijktijdig het oproepende nummer te verstrekken, ook wanneer de nummeridentificatie is geblokkeerd. Hetzelfde geldt voor de naam en de beschikbare adres-, postcode- en woonplaatsgegevens van de abonnee, dan wel de locatie van de openbare betaaltelefoon, die onder het desbetreffende nummer is aangesloten en voor locatiegegevens omtrent abonnees en gebruikers, indien deze beschikbaar zijn (art. 11.10 lid 1 en 2 Tw). De verstrekte gegevens worden vastgelegd met het oog op de hulpverlening in noodsituaties of de bestrijding van het misbruik van het alarmnummer en kunnen slechts voor een beperkte periode worden bewaard.[30] Artikel 11.9 Tw kan eveneens buiten toepassing worden gelaten wanneer dit noodzakelijk is in het belang van de nationale veiligheid en de voorkoming, opsporing en vervolging van strafbare feiten (art. 11.13 lid 1 Tw).

Een abonnee die last heeft van hinderlijke of kwaadwillige oproepen, waarbij de verstrekking van het nummer van het oproepende netwerkaansluitpunt is geblokkeerd, kan aan de telecommunicatieaanbieder verzoeken om het nummer van de oproepende abonnee en de beschikbare daarop betrekking hebbende naam-, adres-, postcode en woonplaatsgegevens te verstrekken (art. 11.11 lid 1 Tw).[31] Het verzoek dient schriftelijk te worden ingediend en dient de naam-, adres-, postcode- en woonplaatsgegevens van de verzoeker te vermelden alsmede het nummer waarop de oproepen betrekking hebben. Daarnaast dient het een indicatie te bevatten van de data en tijdstippen waarop de desbetreffende oproepen hebben plaatsgevonden (artikel 11.11 lid 2 Tw). Deze eisen dienen te voorkomen dat verzoeken te lichtvaardig worden gedaan. Oorspronkelijk bevatte het wetsvoorstel in artikel 11.11 lid 2 sub b Tw de eis dat het verzoek een omschrijving van de aard en ernst van de ondervonden last als gevolg van de oproepen zou behelzen. Deze artikellid werd echter geschrapt omdat een dergelijke verplichting voor burgers een onnodige drempel op zou werpen. Bovendien zou een dienstverlener in de praktijk met een dergelijke toelichting niets kunnen.[32]

30. De termijn bedraagt één maand voor gegevens die worden bewaard ten behoeve van de hulpverlening, zes maanden in gevallen waarin sprake is van misbruik en 24 uur in alle overige gevallen. Zie artikel 11.10 lid 7 Tw.
31. Deze regeling is een implementatie van artikel 10, onderdeel a van de richtlijn privacy en elektronische communicatie.
32. *Kamerstukken II* 2003/04, 28 851, nr. 43.

Na ontvangst van het verzoek stelt de aanbieder een onderzoek in, teneinde te bepalen of tot verstrekking van de gegevens dient te worden overgegaan (art. 11.11 lid 4 Tw). Dit moet van geval tot geval worden vastgesteld. Er dient blijkens de Memorie van Toelichting in ieder geval sprake te zijn van een bepaald belpatroon dat in het maatschappelijk verkeer als hinderlijk moet worden gekarakteriseerd.[33]

De procedure is blijkens de Memorie van Toelichting bij de Telecommunicatiewet met nadruk bedoeld om slachtoffers van hinderlijke of kwaadwillige oproepen in staat te stellen de verantwoordelijke op te sporen:

> "Het verzoek is erop gericht om de oproepende abonnee te identificeren, zodat de opgeroepen abonnee of gebruiker aan de hand van de door de aanbieder te verstrekken gegevens nadere actie tegen betrokkene kan ondernemen; daarbij kan worden gedacht aan een civielrechtelijke actie of het indienen van een klacht als bedoeld in artikel 285b, tweede lid, van het Wetboek van Strafrecht."[34]

De abonnee wiens gegevens het betreft dient van de gegevensverstrekking aan een verzoeker op de hoogte te worden gesteld (art. 11.11 lid 6 Tw).[35] Zijn uit het recht op de bescherming van de persoonlijke levenssfeer voortvloeiende recht op blokkering van nummeridentificatie wordt immers opzij gezet. De abonnee is zodoende tevens voorbereid op eventuele acties van de verzoeker en wellicht kan worden bewerkstelligd dat hij het gewraakte gedrag in de toekomst achterwege laat.[36]

Artikel 11.11 lid 7 Tw schept de mogelijkheid om bij algemene maatregel van bestuur nadere regels te stellen met betrekking tot het onderzoek dat door de aanbieder dient te worden ingesteld, de gegevensverstrekking, de medewerkingsverplichting van andere aanbieders en de kennisgeving van de verstrekking. De wetgever heeft er in eerste instantie echter voor gekozen om aan de aanbieders zelf over te laten onder welke voorwaarden zij een verzoek tot verstrekking van NAW-gegevens inwilligen. Het is de vraag of dit een wenselijke oplossing is. Dit zou in de praktijk immers kunnen leiden tot een warboel van verschillende criteria. Bovendien is onduidelijk in hoeverre de aanbieder een verzoek inhoudelijk kan en moet toetsen en hoe hij dient vast te stellen dat sprake is van kwaad-

33. *Kamerstukken II* 2002/03, 28 962, nr. 3, p. 13.
34. Idem, p. 12. In artikel 285b Sr is stalking strafbaar gesteld: "(1) Hij, die wederrechtelijk stelselmatig opzettelijk inbreuk maakt op eens anders persoonlijke levenssfeer met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen wordt, als schuldig aan belaging, gestraft met een gevangenisstraf van ten hoogste drie jaren of een geldboete van de vierde categorie. (2) Vervolging vindt niet plaats dan op klacht van hem tegen wie het misdrijf is begaan."
35. De procedure van artikel 11.11. Tw staat er overigens niet aan in de weg dat de aanbieder eerst met degene aan wie het oproepende nummer toebehoort contact opneemt en daarbij de betrokkene confronteert met het verzoek en diens bevindingen, voordat hij tot verstrekking overgaat. *Kamerstukken II* 2002/03, 28 962, nr. 3, p. 14.
36. *Kamerstukken II* 2002/03, 28 962, nr. 3, p. 13-14.

willige of hinderlijke oproepen. In de praktijk lijken aanbieders voornamelijk te kijken naar het aantal oproepen dat binnen een bepaalde tijdsspanne is ontvangen. Om de genoemde onduidelijkheden weg te nemen lijken richtlijnen, bijvoorbeeld van het College bescherming persoonsgegevens, wenselijk.

Het is nog niet geheel duidelijk in hoeverre het bijzondere regime van artikel 11.9 Tw toepasselijk is op nieuwere elektronische communicatiediensten zoals e-mail, SMS en internettelefonie. Volgens het College Bescherming persoonsgegevens is bij SMS-diensten geen sprake van het aanbieden van nummeridentificatie in de zin van de Telecommunicatiewet omdat bij dergelijke berichten geen nummers worden verstrekt voordat de verbinding tot stand wordt gebracht. Dit betekent dat de verstrekking van nummers bij de verzending van SMS-berichten moet worden beoordeeld aan de hand van artikel 8 sub f Wbp (zie par. 9.3). Over internettelefonie kunnen geen categorische uitspraken worden gedaan omdat er te veel verschillende technieken bestaan.[37]

8.3.3 Anonimisering en verwijdering van verkeers- en locatiegegevens

Zonder dat de gebruiker zich daarvan bewust is, verwerken elektronische tussenpersonen gedurende de afhandeling van communicatie grote hoeveelheden gegevens over zijn communicatiegedrag. Deze gegevens zijn primair bedoeld om de transmissie van informatie mogelijk te maken. Daarnaast worden zij gebruikt voor het opstellen van rekeningen en voor direct marketing.

Artikel 2 van de richtlijn privacy en elektronische communicatie onderscheidt twee soorten van aan communicatie gerelateerde gegevens. De eerste categorie betreft de zogenaamde 'verkeersgegevens'. Deze worden gedefinieerd als 'gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan'. Zij hebben onder andere betrekking op duur, tijdstip, volume en routering.[38] Een aparte categorie vormen de locatiegegevens, in de richtlijn omschreven als "gegevens die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven". Beide categorieën kunnen aanwijzingen bevatten omtrent gevoelige aspecten van het communicatiegedrag. Opslag en verwerking is daarom aan voorwaarden verbonden.

Ook bij de verwerking van verkeersgegevens is het zeer relevant te constateren dat er een overgang heeft plaatsgevonden van de klassieke telefoniedienst als medium voor niet-openbare conversatie naar elektronische communicatiediensten als medium voor de beschikbaarstelling en consultatie van *openbare* digitale informatie. Hoe deze verschui-

37. Zie de CBP-consultatie over nummeridentificatie en de bescherming van persoonsgegevens van oktober 2004.
38. Overweging 15 bij de richtlijn vult het begrip verkeersgegeven verder in. Zie over de afbakening van de begrippen verkeersgegeven en locatiegegeven en over de privacygevoeligheid hiervan Ekker 2002b; Asscher & Ekker 2003, p. 41-58.

ving zich voordoet, kan het beste worden geïllustreerd aan de hand van een aantal voorbeelden. Wij beginnen met een voorbeeld uit de telefonie:

1. Gebruiker X belt gebruiker Y. Telecomaanbieder Z registreert het oproepende en het opgeroepen nummer alsmede het tijdstip en de duur van het gesprek.

Vervolgen wij met drie voorbeelden uit de digitale omgeving:

2. Gebruiker X maakt verbinding met het internet via provider Y. Provider Y registreert het IP-adres van X.
3. Gebruiker X laat een e-mailbericht achter in een publiek discussieforum. De websitebeheerder registreert het tijdstip van verzending, zijn IP-adres en zijn e-mailadres.
4. Gebruiker X heeft via een zoekmachine een website gevonden. Vervolgens heeft hij op de website informatie geraadpleegd en gechat met andere gebruikers. Provider Y registreert het IP-adres van X, de URL van de website waar de zoekmachine zich bevindt, de URL's die X bij zijn zoekbewerking heeft bezocht, inclusief de daarbij gebruikte zoekwoorden en gegevens over de chatsessie.

Uit de laatste drie voorbeelden blijkt direct dat gegevensverwerking in de digitale omgeving technisch en juridisch complexer is dan voorheen het geval was. In de eerste plaats is zij in deze context aanzienlijk intensiever en heeft zij betrekking op meer aspecten van communicatiegedrag. In de tweede plaats geschiedt de aggregatie van deze gegevens bij een waslijst van verschillende communicatietechnologieën en ongeacht de inhoud of het vertrouwelijke karakter van de communicatie. Gegevensverwerking stoort zich niet aan het maatschappelijke onderscheid tussen het publieke en het private. In de derde plaats voltrekt zich een samenvloeiing van niet-openbare (telefonie, SMS, e-mail, chatten) en openbare communicatie (websites). Tenslotte bevatten verkeersgegevens steeds vaker ook informatie die moet worden gerekend tot de inhoud van een boodschap. Onder de opgeslagen informatie bevinden zich immers ook gegevens als domeinnamen en zoekwoorden.[39]

Verkeers- en locatiegegevens worden door het hele communicatieproces gegenereerd. Bij het verkrijgen van toegang tot het netwerk en bij het zenden en vergaren van informatie laat de gebruiker dus een digitaal gegevensspoor achter. De verwerking van verkeersgegevens speelt zodoende bij alle van de in het vorige hoofdstuk genoemde 'toegangsvraagstukken' een rol (zie par. 7.1.3). Daarmee raakt dit fenomeen ook aan verschillende aspecten van de uitingsvrijheid, met name de bescherming van het publieke debat en het recht om informatie te ontvangen. Weer blijkt dus dat een uitsluitend op de informationele privacy gebaseerde benadering te kort schiet bij het vinden van een adequaat antwoord op de uit gegevensverwerking voortvloeiende risico's.

39. Zie hierover Asscher & Ekker 2003a, met name de bijdrage van Koops.

Regeling in de Telecommunicatiewet

Het belang van een zorgvuldige verwerking van verkeersgegevens wordt benadrukt in overweging 26 bij de richtlijn privacy en elektronische communicatie:

> "Dergelijke gegevens mogen slechts worden opgeslagen voorzover dat nodig is voor het leveren van de dienst, voor facturering en voor interconnectiebetalingen, en slechts gedurende een beperkte tijd. Elke verdere verwerking van dergelijke gegevens die de aanbieder van de openbare elektronische-communicatiedienst zou willen verrichten ten behoeve van de marketing van zijn elektronische-communicatiediensten of voor de levering van diensten met toegevoegde waarde, is slechts toegestaan indien de abonnee daarmee heeft ingestemd op basis van precieze en volledige informatie van de aanbieder van de openbare elektronische-communicatiedienst over de door hem geplande verder verwerking van de gegevens en over het recht van de abonnee een dergelijke verwerking niet toe te staan of de toestemming daartoe in te trekken."

De voorschriften omtrent opslag en verwerking van verkeersgegevens in artikel 6 van de richtlijn zijn omgezet in artikel 11.5 lid 1 Tw. Dit laatste artikel bepaalt dat aanbieders van openbare elektronische communicatienetwerken en -diensten de door hen verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees of gebruikers, verwijderen dan wel anonimiseren zodra deze niet langer nodig zijn ten behoeve van de overbrenging van communicatie. Verwerking is daarnaast toegestaan voor een aantal nader omschreven doelen. Artikel 11.5 lid 2 Tw noemt het opstellen van facturen. De aanbieder mag voorts verkeersgegevens verwerken voor zover en voor zolang dat noodzakelijk is voor: (a) marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten, of (b) de levering van diensten met toegevoegde waarde,[40] mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor zijn toestemming heeft gegeven. Deze toestemming kan te allen tijde worden ingetrokken.

Artikel 15 lid 4 Tw creëert een informatieverplichting voor de aanbieder. De abonnee of gebruiker dient in kennis gesteld te worden van de soorten verkeersgegevens die worden verwerkt en van de duur van de verwerking. Voor zover het verwerking betreft ten behoeve van de doeleinden, genoemd in het derde lid, wordt de desbetreffende informatie verstrekt voorafgaand aan het verkrijgen van de in dat lid bedoelde toestemming.

In mobiele telecommunicatiesystemen worden in toenemende mate ook zogenaamde locatiegegevens verzameld. Voorzover locatiegegevens kunnen worden aangemerkt als verkeersgegevens, verdienen zij dezelfde bescherming. Dit is echter niet altijd het geval aangezien locatiegegevens niet alleen betrekking kunnen hebben op het aan communica-

40. Onder een dienst met toegevoegde waarde verstaat de richtlijn een "dienst die de verwerking vereist van verkeersgegevens of locatiegegevens anders dan verkeersgegevens, en die verder gaat dan hetgeen nodig is voor het overbrengen van een communicatie of de facturering ervan" (art. 2 sub g richtlijn privacy en elektronische communicatie). Blijkens overweging 18 bij de richtlijn kunnen diensten met toegevoegde waarde bijvoorbeeld bestaan uit adviezen over de voordeligste tariefpakketten, routegeleiding, verkeersinformatie, weerberichten en toeristische informatie.

tie gerelateerde gedrag van de gebruiker maar ook op zijn feitelijk gedrag op momenten dat er niet wordt gecommuniceerd. Locatiegegevens worden dus niet in alle gevallen verwerkt 'voor het overbrengen van communicatie of voor facturering'.[41] Artikel 11.5a Tw ziet daarom op de verwerking van locatiegegevens, niet zijnde verkeersgegevens. De verwerking hiervan is slechts geoorloofd indien deze gegevens zijn geanonimiseerd of indien de desbetreffende abonnee of gebruiker voor de verwerking toestemming heeft gegeven ten behoeve van de levering van een dienst met toegevoegde waarde. Abonnees en gebruikers kunnen de verleende toestemming krachtens artikel 11.5 lid 4 Tw op elk moment intrekken.

Ook op de aanbieder van een toegevoegde waardedienst rust een informatieverplichting. Voorafgaand aan de in het eerste lid bedoelde toestemming dient hij de abonnee of de gebruiker op de hoogte te stellen van (a) de soort locatiegegevens die zullen worden verwerkt, (b) de doeleinden waarvoor de locatiegegevens worden verwerkt, (c) de duur van de verwerking en (d) of de gegevens aan een derde zullen worden verstrekt ten behoeve van de levering van de dienst met toegevoegde waarde. Naast het vereiste van toestemming geldt krachtens het derde lid evenals bij verkeersgegevens dat verwerking slechts is toegestaan voor bepaalde doeleinden. Bij locatiegegevens zijn dit er slechts twee. Verwerking mag plaatsvinden voor zover en voor zolang dat noodzakelijk is voor de levering van de dienst met toegevoegde waarde of voorzover die gegevens noodzakelijk zijn voor het opstellen van een factuur. Ten slotte is van belang dat de aanbieder van de toegevoegde waarde-dienst de abonnee of gebruiker de mogelijkheid dient te bieden om kosteloos en op eenvoudige wijze de verwerking van diens locatiegegevens tijdelijk te beletten voor elke overbrenging van communicatie of elke verbinding met het netwerk dat gebruikt wordt voor de levering van die dienst (art 11.5 lid 5 Tw).

8.4 Anonieme toegang tot elektronische communicatienetwerken en -diensten

Een van de meest effectieve manieren om de anonimiteit van handelingen en transacties van eindgebruikers te garanderen, is het veiligstellen van mogelijkheden tot anonieme toegang. Hoewel omtrent dit onderwerp in de privacyrichtlijnen geen dwingende voorschriften zijn opgenomen, hangt het nauw samen met hetgeen in dit hoofdstuk reeds is behandeld. Daarom worden hier enkele relevante aspecten besproken.

Wie spreekt over anonieme toegang doet er goed aan een onderscheid te maken tussen anonieme toegang tot het netwerk en anonieme toegang tot communicatiediensten. Van anonieme toegang tot het netwerk is mijns inziens sprake wanneer de gebruiker een verbinding tot stand kan brengen zonder dat hij zich daaraan voorafgaand hoeft te identificeren en zonder dat op andere wijze gegevens worden verzameld aan de hand waarvan zijn communicatiehandelingen tot hem kunnen worden herleid. Zijn identiteit blijft dan

41. Asscher & Ekker 2003a, p. 46.

voor de aanbieder van het netwerk onbekend zodat verwerkte verkeers- en locatiegegevens niet aan hem kunnen worden gerelateerd. Het achteraf wissen van identificerende gegevens die tijdens het totstandbrengen van de verbinding werden geregistreerd kan er naar mijn mening dan ook niet toe leiden dat sprake is van anonieme toegang, mede gezien het feit dat de verplichting tot het wissen en anonimiseren van verkeers- en locatiegegevens een uit de privacyrichtlijnen voortvloeiende algemene verplichting is.

Anonieme toegangsmogelijkheden tot telecommunicatienetwerken zijn in de publieke ruimte al sinds lange tijd ruimschoots voorhanden, met name via openbare telecommunicatie-voorzieningen, zoals openbare munttelefoons, e-mail- en internetvoorzieningen in openbare bibliotheken en openbare internetzuilen.[42] De anonimiteit van de verbinding met het netwerk is in deze gevallen gewaarborgd doordat betaling kan geschieden met muntgeld of met elektronische betalingstechnieken die de anonimiteit van de betaling garanderen, zoals de Chipknip.[43]

Bij private aansluitingen op een telecommunicatienetwerk liggen de zaken anders. Daar bestaat doorgaans een contractuele relatie tussen de aanbieder van het netwerk en de gebruiker. In deze klantrelatie worden abonneegegevens zoals naam, adres en woonplaats verzameld, onder andere om communicatie tussen de aanbieder en de abonnee en betaling voor de afgenomen diensten mogelijk te maken. Het verstrekken van anonieme toegang vereist dan technische maatregelen van de aanbieder van het netwerk. Dat anonieme toegang tot het netwerk is verkregen betekent overigens niet dat de gebruiker bij al zijn communicatiehandelingen ook daadwerkelijk anoniem is. Zowel de inhoud van communicatie als de verkeers- en locatiegegevens kunnen immers aanknopingspunten bieden voor identificatie. Dit neemt niet weg dat een goed geïnformeerde gebruiker voor zichzelf een aanmerkelijk hogere mate van privacy zal kunnen bewerkstelligen, wanneer mogelijkheden tot anonieme toegang in ruime mate en laagdrempelig voorhanden zijn.

Of anonieme toegang tot telecommunicatie*diensten* kan worden verkregen hangt samen met de vraag of sprake is van anonieme toegang tot het netwerk. Wanneer anonieme toegang tot het netwerk is verkregen zijn voor de dienstenaanbieder, afgezien van de reeds genoemde communicatie-inhoud, verkeers- en locatiegegevens en eventueel door de gebruiker zelf verstrekte gegevens, immers geen identificerende gegevens voorhanden. Is geen anonieme toegang verkregen, dan is traceerbaarheid hoofdregel en die-

42. Uit artikel 6 van de Universeledienstrichtlijn vloeit voor lidstaten een verplichting voort om te waarborgen dat wordt voorzien in de redelijke behoeften van eindgebruikers aan openbare betaaltelefoons onder andere ten aanzien van de geografische spreiding en het aantal. Onder een openbare betaaltelefoon wordt in dat verband verstaan "een voor het publiek beschikbaar telefoontoestel voor het gebruik waarvan met munten en/of krediet-/debetkaarten en/of vooruitbetaalde telefoonkaarten, waaronder kaarten met een toegangscode, kan worden betaald" (artikel 2 sub a Universeledienstrichtlijn).
43. Asscher 2000.

nen technische maatregelen te worden getroffen om te verzekeren dat gegevenssporen die bij het gebruik van de betreffende dienst zijn achtergebleven achteraf te worden gewist.

Het belang van anonieme toegangsmogelijkheden voor de privacy van gebruikers is erkend door het Comité van Ministers van de Raad van Europa. Het Comité constateert dat het toenemende gebruik van geautomatiseerde gegevensverwerking en nieuwe toepassingen zoals nummerherkenning en gespecificeerde rekeningen, nieuwe privacyrisico's met zich meebrengen. Informatietechnologie moet daarom zodanig worden aangewend dat de privacy van gebruikers wordt beschermd. Dit kan onder andere door anonieme toegang mogelijk te maken:

> "Network operators, service providers and equipment and software suppliers should exploit information technology for constructing and operating networks, equipment and software, in a way which ensures the privacy of users. Anonymous means of accessing the telecommunication network and services should be made available."[44]

Ook de artikel 29-werkgroep houdt een pleidooi voor mogelijkheden tot anonieme toegang. Privacyproblemen kunnen immers onder meer kunnen worden verholpen door zoveel mogelijk te garanderen dat gegevenssporen de identificatie van de gebruiker niet mogelijk maken, aldus de groep. Gebruikers moeten om die reden kunnen kiezen voor het anonieme gebruik van internettoepassingen en voor anonieme toegang (zie par. 7.2).[45] Conform het standpunt van de groep luidt overweging 33 van de richtlijn betreffende privacy en elektronische communicatie:

> "De invoering van gespecificeerde facturen biedt de abonnees betere mogelijkheden om de juistheid van de door de dienstenaanbieder aangerekende bedragen te toetsen, maar kan tegelijkertijd ook een bedreiging vormen voor de persoonlijke levenssfeer van de gebruikers van openbare elektronische-communicatiediensten. De lidstaten moeten derhalve met het oog op de vrijwaring van de persoonlijke levenssfeer van de gebruikers de ontwikkeling aanmoedigen van elektronische-communicatiediensten waaraan opties zijn gekoppeld zoals alternatieve betalingsfaciliteiten die anonieme of strikt persoonlijke toegang tot openbare elektronische-communicatiediensten waarborgen, bijvoorbeeld telefoonkaarten en mogelijkheden tot betaling met kredietkaarten."[46]

De vraag of een recht op anonieme toegang bestaat kwam in Nederland reeds in 1997 aan de orde. Aanleiding was het voornemen van het kabinet om een identificatieplicht in het leven te roepen voor gebruikers van vooruitbetaalde telefoonkaarten (de zogenaamde

44. Paragraaf 2.2 van de appendix bij Recommendation R (95) 4.
45. Groep gegevensbescherming artikel 29 1997b.
46. De formulering van deze overweging wekt overigens ten onrechte de indruk dat anonieme toegang uitsluitend noodzakelijk zou zijn om het privacyrisico dat voortvloeit uit de invoering van gespecificeerde facturen af te wenden. Dit is echter niet geheel juist. Ook voordat gespecificeerde facturen werden ingevoerd was anonieme toegang immers al een effectief middel om de privacy van gebruikers te beschermen.

'prepaid cards'). In artikel 13.4 Tw zou daartoe voor aanbieders van deze kaarten een verplichting worden gecreëerd om afnemers te identificeren en te registreren.[47] Vanuit opsporingsinstanties werd aangedrongen op het onmogelijk maken van anoniem telecommunicatieverkeer om te voorkomen dat criminelen hun telefonische activiteiten aan de waarneming van politie en justitie zouden kunnen onttrekken. De maatregel was in overeenstemming met het streven van de regering om te komen tot een algehele identificatieplicht voor gebruikers van telecommunicatie.

Mede als gevolg van zwaarwegende principiële en praktische bezwaren van de kant van de Registratiekamer (tegenwoordig het College bescherming persoonsgegevens) zag het kabinet uiteindelijk van het voornemen af. Volgens de Registratiekamer bestond in de praktijk een reële maatschappelijk behoefte aan anonieme toegangsmogelijkheden. Een identificatieplicht zou gebruikers van prepaid cards naar het oordeel van de Registratiekamer ten onrechte op één lijn zetten met een kleine minderheid van wetsovertreders en een eerste stap zijn op weg naar een algemeen verbod op anoniem gebruik van telecommunicatiediensten en van de elektronische snelweg.[48] Een dergelijk algemeen verbod zou een breuk met de bestaande praktijk betekenen en in strijd zijn met het geldende recht en toekomstige Europese regelgeving. De beoogde wettelijke verplichting tot identificatie en registratie vormde naar het oordeel van de Registratiekamer een onrechtmatige inbreuk op het uit artikel 8 EVRM voortvloeiende recht op eerbiediging van de persoonlijke levenssfeer, dat ook het recht op vertrouwelijkheid van telecommunicatie omvat. Het aan de maatregel ten grondslag liggende verbod op anonieme toegang tot telecommunicatiediensten zou de vrije toegang tot het internet wezenlijk belemmeren en was daarom in het licht van de communicatievrijheid onaanvaardbaar.

Als praktisch bezwaar bracht de Registratiekamer naar voren dat een wettelijke identificatieverplichting waarschijnlijk weinig effectief zou zijn bij de opsporing van criminele gedragingen. Registratie kon immers makkelijk worden ontdoken door de prepaid cards te betrekken van onverdachte burgers of bedrijven, of uit een land waar registratie niet plaatsvindt. De voorgenomen maatregel moest naar het oordeel van de Registratiekamer alleen al om deze reden als disproportioneel en derhalve in strijd met artikel 8 EVRM worden gekwalificeerd. Als tweede praktisch bezwaar werd aangevoerd dat een consequente uitvoering van het voornemen om tot een algemene elektronische identificatieplicht te komen er toe zou leiden dat ook andere bestaande openbare telecommunicatiediensten die anonieme toegang mogelijk maken (de reeds genoemde munttelefoons en openbare internetzuilen), alsmede de daarvoor gebruikte betalingsmiddelen (zoals 'E-cash', Chipper en de Chipknip) zodanig zouden moeten worden aangepast dat tele-

47. Dommering e.a. 1999, p. 661-662.
48. Brief van de Registratiekamer aan de Tweede Kamer d.d. 12 december 1997, kenmerk 97.A.961.01. Zie ook het jaarverslag van het College bescherming persoonsgegevens uit 1998.

communicatieaanbieders de identiteit van gebruikers te allen tijde zouden kunnen achterhalen.

Ten slotte wees de Registratiekamer erop dat Nederland met de bewuste maatregel in Europees verband uit de pas zou lopen.[49] In vergelijking met Duitsland zou zelfs een schril contrast ontstaan. par. 4 Absatz 1 van het Duitse Teledienstedatenschutzgesetz (TDDSG) verplichtte aanbieders van telecommunicatiediensten om het gebruik van 'Telediensten' en de betaling daarvoor anoniem of onder een pseudoniem mogelijk te maken voor zover dat technische mogelijk en redelijk was.[50] Hoewel deze regel zich richtte tot de aanbieder, kon daaruit een recht van de gebruiker op het anonieme gebruik van diensten worden afgeleid. De Duitse bepaling was een uitwerking van het in de privacyrichtlijnen vastgelegde principe dat bij het aanbieden van telecommunicatiediensten zo weinig mogelijk persoonsgegevens worden gegenereerd, verwerkt en gebruikt. Dit principe was als een 'Gebot der Datenvermeidung' ook opgenomen in par. 3 Absatz 4 TDDSG, en gold voor het hele gebruiksproces, aldus de toelichting bij par. 4 Absatz 1.[51] De Registratiekamer adviseerde om het recht op anonieme toegang tot telecommunicatienetwerken en -diensten ook in de Nederlandse Telecommunicatiewet te garanderen.[52] Aan dit advies is door het kabinet echter geen gehoor gegeven.

8.5 Conclusie

De gegevensverwerking in de telecommunicatiesector raakt meer dan voorheen aan de anonieme uitoefening van de uitingsvrijheid doordat elektronische communicatiemiddelen zich hebben ontwikkeld tot media voor de verspreiding van openbare informatie. Dit bleek te gelden in uiteenlopende contexten, dat wil zeggen: voor verschillende stadia van het communicatieproces en voor verschillende technische toepassingen. De problematiek die zich in al deze contexten manifesteert weerspiegelt de drie toegangsvraagstukken die in het vorige hoofdstuk werden benoemd: de toegang van de gebruiker tot het netwerk, de toegang van zenders en ontvangers van informatie tot de openbaarheid en de toegang van ontvangers tot het publieke domein.

49. Brief van de Registratiekamer aan de Tweede Kamer d.d. 13 november 1997, kenmerk 97.A.894.01.
50. Par. 4 Absatz 1 van het Teledienstdatenschutzgesetz betreffende Datenschutzrechtliche Pflichten des Diensteanbieters luidt: "(1) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren."
51. Begründung zum Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz IuKDG), Bundesrat 20 december 1996, *Drucksache* 966/96, p. 25.
52. Brief van de Registratiekamer aan de Tweede Kamer d.d. 13 november 1997, kenmerk 97.A.894.01.

Zoals in het vorige hoofdstuk al werd geconstateerd, komt het ontegenzeggelijke belang van de uitingsvrijheid in het geldende gegevensbeschermingsrecht niet tot uitdrukking. Deze conclusie lijkt ook te gelden in de telecommunicatiesector. Op de materiële vraag in hoeverre uit de uitingsvrijheid en de daaraan gerelateerde publieke vrijheden voor uiters, bronnen en ontvangers een recht volgt om bij gebruikmaking van elektronische communicatiemiddelen anoniem te zijn formuleert het privacykader geen duidelijk antwoord. In de fysieke wereld is het verband met de uitingsvrijheid nog duidelijk, bij gegevensverwerking wordt een heldere analyse echter bemoeilijkt door het paradigma van de privacybescherming.

Men zou kunnen betogen dat aan het bezwaar tegen de eenzijdige dogmatische fundering van gegevensbescherming in praktische zin niet zo zwaar getild moet worden. De geldende voorschriften bieden de gebruiker via de informationele privacy immers middelen die hij ook kan aanwenden om andere grondrechtelijke belangen te beschermen. Hoewel een dergelijke doel-middel verhouding tussen het recht op privacy en de uitingsvrijheid feitelijk wel aanwezig is, lijkt het bezwaarlijk de vraagstukken rondom gegevensverwerking op deze wijze te analyseren. In dit opzicht sluit ik mij aan bij de kritiek van Blok. Men moet de impact van gegevensverwerking mijns inziens niet uitsluitend zien als een privacyprobleem, maar als een machtsprobleem dat raakt aan verschillende grondrechten, waaronder het recht op (informationele) privacy en de uitingsvrijheid. De informatiemacht die uit gegevensverwerking voorvloeit, manifesteert zich immers ook buiten de persoonlijke levenssfeer. Problematisch is in dit verband overigens wel dat geldende regelgeving en rechtspraak het privacyparadigma tot uitgangspunt blijven nemen. In toekomstige privacyrichtlijnen en de implementatie daarvan zou het verband met andere grondrechten dan het recht op privacy daarom duidelijker gelegd moeten worden. Ook het Europese Hof zou in de toekomst aan een heldere analyse bij kunnen dragen door dit verband meer expliciet te erkennen.

Vergelijkt men de problematiek van gegevensverwerking in de digitale omgeving met de vraagstukken die speelden in de fysieke wereld, dan blijkt de positie van de gebruiker aan belang te hebben toegenomen. De intensieve gegevensverwerking die met het gebruik van elektronische communicatiemiddelen gepaard gaat en de daaruit voortvloeiende risico's voor het communicerende individu hebben tot gevolg dat zich in toenemende mate de vraag opdringt of eindgebruikers een zelfstandig recht op anonimiteit hebben met een daaruit voortvloeiende aanspraak op bescherming door de tussenpersoon. In het vorige hoofdstuk bleek dat deze vraag bij traditionele communicatiemiddelen nog nauwelijks aan de orde kwam omdat de regulering van anonimiteit zich daar primair richt op de tussenpersoon. Bij de regulering van elektronische communicatiemiddelen is de positie van het communicerende individu echter van de periferie naar het centrum van de aandacht verschoven.

Geconstateerd moet worden dat het in dit hoofdstuk behandelde regelgevingskader ook aan de eindgebruiker zelf afdwingbare rechten toekent waarmee hij zijn anonimiteit kan beschermen. Men zou daarom kunnen spreken van een subjectiveringstendens. Deze

ontwikkeling biedt aanknopingspunten voor de constructie van een aan het subject, dat wil zeggen de eindgebruiker, toekomend recht om anoniem te communiceren. De Europese privacyrichtlijnen, de Wet bescherming persoonsgegevens en de Telecommunicatiewet creëren gezamenlijk een bescherming waarin de contouren van een dergelijk aan het subject toekomend recht zich aftekenen. De kern van deze bescherming wordt gevormd door een reeks op het recht op informationele privacy gebaseerde controlemogelijkheden van de gebruiker met betrekking tot hem betreffende gegevens, omgeven door een schil van verplichtingen, gericht tot de aanbieders van elektronische communicatienetwerken en -diensten.

De bescherming van anonimiteit heeft in de telecommunicatiesector op drie niveaus vorm gekregen. Zoals in het vorige hoofdstuk bleek, rusten blijkens verklaringen van verschillende nationale en Europese instellingen allereerst diverse inspanningsverplichtingen op de overheid, voorvloeiend uit het recht op bescherming van de persoonlijke levenssfeer en de communicatievrijheid (zie par. 7.2). De verklaring van het Comité van Ministers van de Raad van Europa roept de aangesloten lidstaten op de wens van internetgebruikers om anoniem te blijven te respecteren. Dit betekent bijvoorbeeld dat zij het gebruik van anonimiserende software moeten toestaan. Daarnaast moet de verzameling van identificerende informatie om het recht te handhaven in overeenstemming zijn met artikel 8 EVRM. Uit de overwegingen bij de privacyrichtlijnen volgt voor EU-lidstaten eveneens een inspanningsplicht. Zo dienen zij samen te werken met de betrokken aanbieders en gebruikers alsmede de bevoegde communautaire instanties bij de introductie en ontwikkeling van technieken die de verwerking van persoonsgegevens zoveel mogelijk beperken en die, waar mogelijk, gebruik maken van anonieme of onder pseudoniem opgeslagen gegevens. Tevens dienen zij middels nationale bepalingen het recht op bescherming van de persoonlijke levenssfeer te waarborgen van gebruikers en abonnees die op gespecificeerde facturen worden vermeld. Ten slotte dienen lidstaten zich in te spannen om mogelijkheden tot anonieme toegang te verzekeren. Wel moet worden opgemerkt dat de genoemde inspanningsverplichtingen niet uitdrukkelijk in regelgeving zijn vastgelegd, waardoor zij slechts in beperkte mate afdwingbaar zijn.

Het tweede niveau van bescherming knoopt aan bij de positie van telecommunicatieaanbieders en internetproviders als tussenpersonen in het communicatieproces. De rol van elektronische tussenpersonen is essentieel omdat het relatief anonieme karakter van de meeste communicatiehandelingen ten aanzien van derden slechts met hun hulp kan worden doorbroken. Bij de verwerking van gegevens rusten op telecomaanbieders diverse uit de Wet bescherming persoonsgegevens en de Telecommunicatiewet voortvloeiende verplichtingen. In de eerste plaats is de verwerking van gegevens gebonden aan de algemene voorwaarden voor de verwerking van persoonsgegevens uit de algemene privacyrichtlijn. Deze voorschriften zijn voor de verwerking van abonneegegevens en verkeers- en locatiegegevens in de telecommunicatiesector specifiek uitgewerkt in de richtlijn privacy en elektronische communicatie. Belangrijk is daarnaast de verplichting tot het verwijderen van verkeers- en locatiegegevens, zodra deze niet langer nodig zijn ten

behoeve van de overbrenging van communicatie of voor de in de wet omschreven doelen. De verwerking van locatiegegevens, niet zijnde verkeersgegevens is slechts toegestaan indien deze gegevens zijn geanonimiseerd of indien de desbetreffende abonnee of gebruiker voor de verwerking toestemming heeft gegeven ten behoeve van de levering van een dienst met toegevoegde waarde. Verplichtingen tot het wissen dan wel anonimiseren van gegevens bewerkstelligen met terugwerkende kracht dat communicatiehandelingen ten opzichte van de tussenpersoon en dus ook ten opzichte van derden een absoluut anoniem karakter krijgen. De voornaamste aanknopingspunten voor identificatie worden immers verwijderd.

In de derde plaats rusten op de tussenpersoon uit het transparantiebeginsel voortvloeiende informatieverplichtingen ten aanzien van bepaalde verwerkingshandelingen met betrekking tot verschillende categorieën van gegevens. Zo dienen abonnees en gebruikers in kennis gesteld te worden van de soorten verkeersgegevens die worden verwerkt en van de duur van de verwerking. Soortgelijke verplichtingen gelden voor de aanbieder van een toegevoegde waardedienst bij de verwerking van locatiegegevens. Een informatieplicht geldt eveneens voorafgaand aan opneming van persoonsgegevens in een abonneelijst of -bestand. Abonnees moeten kosteloos op de hoogte worden gesteld van de doeleinden van deze lijst, de gebruiksmogelijkheden op basis van daarin opgenomen zoekfuncties en de soorten persoonsgegevens die worden opgenomen. In de vierde plaats zijn tussenpersonen verplicht om verzoeken tot inzage, correctie en verzet in behandeling te nemen. Wanneer verwerking plaatsvindt ten behoeve van direct marketing is het recht op verzet zelfs absoluut. Ten slotte is door het Comité van Ministers van de Raad van Europa, de artikel 29-werkgroep en door het College bescherming persoonsgegevens een recht op anonieme toegang erkend. Uit de Europese richtlijnen volgt echter geen plicht voor aanbieders om anonieme toegang te verzekeren. Een verplichting voor aanbieders van telecommunicatienetwerken- en diensten om anonieme toegang te verzekeren, ondanks aandringen van de Registratiekamer, is ook in de Telecommunicatiewet niet opgenomen.

Het derde niveau van bescherming omvat de rechten van de communicerende eindgebruiker zelf. In de hoedanigheid van betrokkene in de zin van de Wet bescherming persoonsgegevens en in de hoedanigheid van gebruiker of abonnee in de zin van de Telecommunicatiewet heeft hij recht op zeggenschap over hem betreffende informatie. Dit recht komt onder andere naar voren in het op verschillende plaatsen opgenomen vereiste dat voor bepaalde verwerkingshandelingen zijn toestemming wordt verkregen. Het transparantiebeginsel, en het recht op inzage als uitwerking daarvan, zijn bedoeld om de betrokkene inzicht in en controle op de gegevensverwerking te verschaffen. De in hoofdstuk 6 Wbp opgenomen bepalingen betreffende het recht op inzage, correctie en verzet zijn in de Telecommunicatiewet voor de verwerking van abonneegegevens en verkeers- en locatiegegevens uitgewerkt.

De bescherming van de anonimiteit van eindgebruikers werkt in verschillende verhoudingen. In de eerste plaats ten opzichte van de tussenpersoon: aanbieders zijn als

gevolg van hun verplichting om gegevens te wissen of te anonimiseren na verloop van tijd niet meer in staat om gegevens over communicatie te koppelen aan abonneegegevens van gebruikers. In de tweede plaats werkt de bescherming ten opzichte van andere eindgebruikers doordat de kenbaarheid van identificerende informatie beheersbaar is gemaakt. Aanbieders zijn verplicht om de blokkering van nummerherkenning mogelijk te maken en persoonsgegevens mogen slechts in abonneelijsten worden opgenomen wanneer de gebruiker daarvoor uitdrukkelijk toestemming heeft gegeven. De doorgifte van gegevens aan derde partijen is in dit hoofdstuk nog niet uitgebreid aan de orde gekomen. Doorgifte van gegevens op eigen initiatief van de aanbieder voor commerciële doeleinden, zoals direct marketing, is gebonden aan het principe van doelbinding en kan alleen geschieden met toestemming van de betrokken gebruikers. Van groot belang is echter ook de gedwongen afgifte van identificerende gegevens. Hier kan in grote lijnen een onderscheid worden gemaakt tussen afgifte op basis van een vordering van een private partij die deze gegevens wenst te verkrijgen om zijn eigen belangen te handhaven, zoals bijvoorbeeld het auteursrecht, en afgifte op basis van een bevel van politie en justitie. De regelgeving en jurisprudentie op dit punt komt aan de orde in het volgende hoofdstuk.

9 Verstrekking van identificerende gegevens

9.1 Inleiding

In de fysieke wereld laat het menselijk handelen doorgaans tastbare of zintuiglijk waarneembare sporen na, bijvoorbeeld in de vorm van vinger- of voetafdrukken, DNA-materiaal en geursporen. De digitale omgeving kent dit soort sporen niet. Toch zijn communicerende burgers ook in de virtuele wereld traceerbaar. Alle elektronische communicatietechnologieën kennen immers de mogelijkheid om communicatiehandelingen en communicatie-inhoud door middel van technische adresseringsgegevens te koppelen aan individuele gebruikers. Soms verwijzen deze adresseringsgegevens direct naar een identificeerbare persoon. Dit is bijvoorbeeld het geval wanneer gebruik wordt gemaakt van een e-mailadres waarin de naam van de verzender is opgenomen. Meestal bestaan adresseringsgegevens echter louter uit cijfers en verwijzen zij naar een aansluitpunt op het netwerk of naar bepaalde randapparatuur. Een dergelijk nummer, zoals een telefoonnummer of een IP-adres, volstaat lang niet altijd om de verantwoordelijke voor bepaalde informatie te achterhalen.

Om daadwerkelijke identificatie tot stand te brengen is het in de regel noodzakelijk om de technische adresseringsinformatie te koppelen aan andere identificerende gegevens, zoals naam-, adres- en woonplaatsgegevens (NAW-gegevens). Deze gegevens kunnen normaalgesproken alleen met medewerking van de tussenpersoon, dat wil zeggen: de telecom- of internetprovider, worden verkregen. Providers hebben in veel gevallen een contractuele relatie met de bewuste gebruiker in het kader waarvan NAW-gegevens zijn verzameld. Bovendien hebben zij vaak als enige toegang tot de benodigde gegevensbestanden.

Providers zijn niet altijd bereid de voor identificatie benodigde gegevens op vrijwillige basis te verstrekken. In de praktijk rijst daarom al snel de vraag wat de juridische mogelijkheden zijn om hen hiertoe te verplichten. Zoals wij zagen in het vorige hoofdstuk reguleert de huidige Telecommunicatiewet de verstrekking van identificerende gegevens alleen waar het telefonie betreft (zie par. 8.3.2). De regeling aangaande nummeridentificatie voorziet in criteria waarmee het privacybelang van de anonymus moet worden afgewogen tegen andere belangen en regelt hoe de telecommunicatieaanbieder precies te werk moet gaan. Vorderingen tot verstrekking van gegevens over verzenders van e-mailberichten, uitwisselaars van digitale bestanden en andere internetgebruikers vallen echter buiten deze regeling. Dit hoofdstuk stelt de vraag aan de orde onder welke voorwaarden

elektronische tussenpersonen in dergelijke gevallen bevoegd zijn en verplicht kunnen worden tot verstrekking van identificerende gegevens.

Bij de bespreking van relevante wettelijke bepalingen en rechtspraak zullen de procedurele aspecten van de verstrekking centraal staan. Er wordt met name aandacht besteed aan de vraag wie de verstrekking beoordeelt en in hoeverre daarbij een afweging wordt gemaakt tussen de belangen van de partij die identificatie nastreeft, de belangen van de tussenpersoon en de belangen van de anonymus. Waar het de civielrechtelijke verstrekking van identificerende gegevens betreft, zal op verschillende punten aan de orde komen hoe het Nederlandse recht dienaangaande zich verhoudt tot het Amerikaanse, zoals behandeld in hoofdstuk 4. Dit hoofdstuk gaat daarnaast ook in op mogelijkheden tot verstrekking in Europese richtlijnen en op strafvorderlijke bevoegdheden tot het vorderen van gegevens. In dat opzicht is het enigszins ruimer van opzet dan hoofdstuk 4.

In voorgaande hoofdstukken werden verschillende grondrechtelijke en historische aspecten van anonieme communicatie geanalyseerd. Deze analyse bracht een aantal verbindingslijnen aan de oppervlakte die ook in dit hoofdstuk terugkomen. Het is van belang hierbij kort stil te staan nu sommige van deze lijnen zich in de digitale omgeving vertakken of diffuser worden. Dit geldt in de eerste plaats voor het verband tussen de bestrijding van anonimiteit en machtsuitoefening, dat zich aanvankelijk met name manifesteerde in de verhouding tussen overheid en burger. De erkenning van het recht om anoniem te publiceren had een klassieke grondrechtelijke dimensie doordat het de burger beschermde tegen censuur en andere vormen van overheidsbemoeienis. Hoewel dit belang ook in de digitale omgeving van betekenis blijft, ontstaat daarnaast een nieuw spanningsveld in de horizontale verhouding tussen de communicerende burger, de tussenpersoon en private derde partijen. De anonieme verspreiding van openbare digitale informatie raakt immers meer dan vroeger aan private commerciële belangen die in het tijdperk van de drukpers nog niet bestonden of een minder belangrijke rol speelden. Bij de beschrijving van het Amerikaanse recht bleek dat pogingen om anonieme internetgebruikers te identificeren vaak bedoeld zijn om uitlatingen tegen te gaan die het imago van een onderneming kunnen beschadigen. Ook de bestrijding van auteursrechtschending is een privaat belang. De beschikbaarheid van identificerende informatie en de juridische mogelijkheden om verstrekking daarvan af te dwingen blijven ook in deze context bepalend voor de machtsverhoudingen tussen de verschillende actoren in het communicatieproces. Men zou kunnen zeggen dat anonimiteit de eindgebruiker onder omstandigheden ook in private verhoudingen beschermt tegen ongecontroleerde informatiemacht.

De hoofdstukken 7 en 8 toonden aan dat gegevensverwerking met de opkomst van openbare elektronische communicatiemiddelen doordringt in het publieke domein en dat dit verschijnsel daardoor steeds meer raakt aan de uitoefening van de uitingsvrijheid en andere publieke vrijheden. Het verband tussen anonimiteit en uitingsvrijheid, de belangrijkste verbindingslijn in dit onderzoek, is daardoor in de digitale omgeving inmiddels even sterk aanwezig als bij de drukpers. Nu dit hoofdstuk zich met name richt

op de procedurele aspecten van de verstrekking worden deze bevindingen hierna als vaststaand aangenomen.

Wel wordt bekeken in hoeverre het verband tussen de bescherming van anonimiteit en de uitoefening van de uitingsvrijheid en andere publieke vrijheden in wetgeving en rechtspraak daadwerkelijk wordt gelegd.

Algemene bepalingen over de verstrekking van identificerende gegevens zijn versnipperd over een aantal wettelijke regelingen. Zij hebben allen hun eigen strekking en reikwijdte. Hieronder zal eerst kort in worden gegaan op de betekenis van het begrip identificerend gegeven. Vervolgens wordt het geldende recht besproken. Allereerst komen de meest algemene bepalingen in de Wet bescherming persoonsgegevens en de richtlijn elektronische handel aan bod. Vervolgens bespreken wij enkele juridische aspecten van de civielrechtelijke verstrekking. Daarna wordt verstrekking ten behoeve van de handhaving van intellectuele eigendomsrechten behandeld. Over dit onderwerp bestaat, naast rechtspraak, een bepaling in de richtlijn handhaving intellectuele eigendomsrechten. Het laatste deel van dit hoofdstuk is gewijd aan strafvorderlijke bevoegdheden tot het vorderen van gegevens.

9.2 Identificerende gegevens

Wil men achterhalen wat de juridische betekenis is van het begrip identificerend gegeven, dan ligt het voor de hand te rade te gaan bij de Wet bescherming persoonsgegevens (Wbp). Art. 1 sub a Wbp omschrijft een persoonsgegeven immers als "elk gegeven betreffende een *geïdentificeerde* of *identificeerbare* natuurlijke persoon" [curs. AE]. De definitie bevat zodoende twee elementen: (1) het moet gaan om gegevens betreffende een natuurlijke persoon en (2) de persoon moet identificeerbaar zijn. Met name dat laatste punt is hier van belang. Het uitgangspunt is dat een persoon identificeerbaar is, indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Of daarvan sprake is, hangt vervolgens af van twee factoren, te weten: (1) de aard van de gegevens en (2) de mogelijkheden van de verantwoordelijke om de identificatie tot stand te brengen.[1] Ook de Memorie van Toelichting bij artikel 1 sub a bevat enige beschouwingen over de betekenis van de begrippen identificatie en identificeerbaarheid:

> "Een persoon is identificeerbaar indien sprake is van gegevens die alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor een bepaalde persoon dat deze aan de hand daarvan kan worden geïdentificeerd. Artikel 2, onder a, van de richtlijn bepaalt dat als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit."[2]

1. Hooghiemstra 2001, p. 38-40.
2. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47-48.

Een gegeven is dus een persoonsgegeven wanneer het betrekking heeft op een identificeerbare persoon. Dit betekent echter niet dat ieder persoonsgegeven een identificerend gegeven is in de zin van de Wet bescherming persoonsgegevens. Identificerende gegevens worden beschouwd als een bijzondere categorie van persoonsgegevens. De wetgever maakt een onderscheid tussen *direct* en *indirect* identificerende gegevens:

> "Van direct identificerende gegevens is sprake wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is. Direct identificerende gegevens zijn gegevens als naam, adres, geboortedatum, die in combinatie met elkaar dermate uniek en dus kenmerkend zijn voor een bepaalde persoon dat deze in brede kring met zekerheid of met een grote mate van waarschijnlijkheid, kan worden geïdentificeerd. Dergelijke gegevens worden in het maatschappelijk verkeer ook gebruikt om personen van elkaar te onderscheiden. Anders ligt dit wanneer de gegevens niet direct tot identificatie van een bepaald persoon leiden maar via nadere stappen de gegevens in verband kunnen worden gebracht met een bepaalde persoon. Dit soort gegevens heten indirect identificerende gegevens. Zij kunnen zijn ontdaan van de naam, doch onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon."[3]

Het voornaamste onderscheid tussen de twee categorieën is dat direct identificerende gegevens 'zonder veel omwegen' en 'met zekerheid of een grote mate van waarschijnlijkheid' tot identificatie leiden, terwijl bij indirect identificerende gegevens 'nadere stappen' moeten worden genomen. Met 'nadere stappen' wordt dan voornamelijk gedoeld op het combineren van deze gegevens met andere gegevens. Dit onderscheid lijkt te impliceren dat direct identificerende gegevens tot identificatie kunnen leiden zonder dat een combinatie met andere gegevens nodig zou zijn. Als direct identificerende gegevens noemt de wetgever echter "gegevens als naam, adres, geboortedatum die *in combinatie* [curs. AE] met elkaar dermate uniek en dus kenmerkend zijn voor een bepaalde persoon dat deze (…) kan worden geïdentificeerd". Tot op zekere hoogte is de indeling in direct en indirect identificerende gegevens dus innerlijk tegenstrijdig.

De wetgever gaat er bij de indeling in direct en indirect identificerende gegevens impliciet van uit dat van bepaalde soorten gegevens op voorhand kan worden vastgesteld of zij identificatie mogelijk maken. Tegelijkertijd erkent hij dat het onderscheidend vermogen van een persoonsgegeven sterk afhankelijk is van de omstandigheden:

> "Het onderscheidend vermogen van (…) (combinaties van) gegevens is mede afhankelijk van de context, bij voorbeeld afhankelijk van de omvang van de bevolkingsgroep waarop de gegevensverwerking betrekking heeft."[4]

3. Idem, p. 48.
4. Idem, p. 48.

Ieder gegeven over een persoon kan onder omstandigheden dus een identificerend gegeven zijn. Het onderscheidend en identificerend vermogen van een gegeven wordt bepaald door factoren die van geval tot geval verschillen en die vaak afhankelijk zijn van het toeval. Of een gegeven kan leiden tot identificatie hangt onder andere samen met de uniekheid van het gegeven in een bepaalde context en met het aantal andere personen dat moet worden uitgesloten. Het gegeven dat iemand blond haar heeft is in Nederland meestal niet voldoende om hem te identificeren maar kan dat in een Afrikaans land wel zijn. Andersom zijn er situaties waarin gegevens die doorgaans in de categorie identificerende gegevens worden geplaatst, iedere onderscheidende waarde missen. Zo wordt de naam door de wetgever genoemd als een direct identificerend gegeven. De naam 'Jan Jansen' heeft doorgaans echter onvoldoende onderscheidend vermogen om tot identificatie te leiden.

De constatering dat het onderscheidend vermogen van gegevens contextafhankelijk is, verdraagt zich dus slecht met de indeling in direct en indirect identificerende gegevens. Aannames omtrent het onderscheidend vermogen gelden immers slechts in een bepaalde context. In de communicatiesfeer dient bijvoorbeeld rekening te worden gehouden met de specifieke kenmerken van de gebruikte communicatietechniek en de aard van de daarbij gegenereerde gegevens. Indien men de afzender van een brief wil traceren, zal men eerst bezien of de afzender zijn naam heeft vermeld en waar de brief is afgestempeld. Bij telefonie zal men in eerste instantie kijken naar het oproepende telefoonnummer en vervolgens naar eventueel beschikbare verkeers- en locatiegegevens. Bij internetverkeer heeft het IP-adres een hoge onderscheidende waarde.

De bedoeling van het onderscheid tussen direct en indirect identificerende gegevens is niet geheel duidelijk. De Wet bescherming persoonsgegevens kent geen aparte regeling voor de verwerking van identificerende gegevens of een gedifferentieerd beschermingsniveau voor direct en indirect identificerende gegevens. Het kan zijn dat de wetgever toch op een of andere manier tot uitdrukking heeft willen brengen dat gegevens met een hoge onderscheidende waarde in principe meer bescherming verdienen. Redenerend vanuit de strekking van de Wet bescherming persoonsgegevens lijkt het logisch om te stellen dat gegevens die makkelijk tot identificatie kunnen leiden in hogere mate raken aan het recht op de eerbiediging van de persoonlijke levenssfeer. Als men een verschil in beschermingsniveau aan zou willen brengen tussen categorieën van persoonsgegevens naar gelang hun onderscheidend vermogen, dan zou het voor de hand liggen om aan 'direct' identificerende gegevens een hogere bescherming toe te kennen.

9.3 Verstrekking op basis van de Wet bescherming persoonsgegevens

Aanbieders van elektronische communicatienetwerken en -diensten registreren en verwerken op grote schaal NAW-gegevens over gebruikers van deze netwerken en diensten. In veel gevallen betreft het abonneegegevens. Voor zover deze gegevens betrekking hebben op identificeerbare natuurlijke personen, moeten zij worden aangemerkt als persoonsgegevens in de zin van de Wet bescherming persoonsgegevens (Wbp). De verstrek-

king van identificerende gegevens aan een derde partij is dan ook onderworpen aan de in de Wbp opgenomen voorschriften.[5]

Artikel 8 Wbp bevat een limitatieve opsomming van gronden voor toelaatbare gegevensverwerking. Het artikel staat verstrekking onder andere toe wanneer daarvoor toestemming van de betrokkene is verkregen (art. 8 sub a Wbp). Hetzelfde geldt indien verstrekking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (art. 8 sub b Wbp) en wanneer de gegevens werden verkregen met verstrekking aan derden als doeleinde.[6] In deze paragraaf komt echter slechts de situatie aan de orde waarin verstrekking van identificerende gegevens die niet voor dat doel zijn verzameld, plaatsvindt buiten de betrokkene om, zonder dat hij hiervoor toestemming heeft gegeven en mogelijkerwijs zonder dat hij hiervan op de hoogte is of wordt gesteld. Er zijn dan twee mogelijkheden. Artikel 8 sub c Wbp staat verwerking toe indien deze noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is. Verstrekking van persoonsgegevens aan overheidsinstanties zal doorgaans op deze bepaling gebaseerd zijn.[7] Bij verstrekking aan private partijen dient de weg van artikel 8 sub f Wbp te worden gevolgd. Dit artikellid maakt verwerking mogelijk indien "de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert".

De verwerkingsgronden in artikel 8 Wbp scheppen voor de verantwoordelijke slechts een *bevoegdheid* om op vrijwillige basis persoonsgegevens te verstrekken. De aanhef van artikel 8 bepaalt immers dat de verwerking van gegevens, en dus ook de verstrekking daarvan, *mag* plaatsvinden indien dit noodzakelijk is met het oog op de in dat artikel genoemde belangen. De Wbp schept dus nooit een zelfstandige verplichting om gegevens te verstrekken aan derden. Wanneer moet worden voldaan aan een wettelijke verplichting tot verstrekking, bijvoorbeeld op basis van de Telecommunicatiewet, vloeit die verplichting voort uit de wettelijke bepaling waarin die verplichting is opgenomen.

5. Verstrekking van persoonsgegevens is een verwerkingshandeling in de zin van de Wbp. Artikel 1 sub b Wbp verstaat onder de verwerking van persoonsgegevens onder andere het "verstrekken door middel van doorzending, verspreiden of op enigerlei andere vorm van terbeschikkingstelling' van persoonsgegevens. Artikel 1 sub 1 definieert het verstrekken van persoonsgegevens vervolgens nader als "het bekend maken of ter beschikking stellen van persoonsgegevens". Verstrekking kan mondeling, schriftelijk of langs elektronische weg geschieden. Van verstrekken is bijvoorbeeld ook sprake indien een derde over de schouder van een ander meekijkt naar een bestand met persoonsgegevens. Zie Hooghiemstra 2003, p. 48.
6. Wanneer de persoonsgegevens oorspronkelijk werden verkregen met verstrekking aan derden als doeleinde, is immers sprake van verenigbaar gebruik in de zin van artikel 9 Wbp.
7. Na de invoering van de nieuwe strafvorderlijke bevoegdheden tot het opvragen van gegevens is dit zeker het geval. Deze nieuwe bevoegdheden waren immers onder andere bedoeld om een einde te maken aan de praktijk van vrijwillige verstrekking.

Artikel 8 sub c Wbp maakt het in dergelijke gevallen mogelijk dat aan de wettelijke verplichtingen tot verstrekking wordt voldaan zonder dat men in strijd handelt met de Wbp.

Onderdeel f is bij de totstandkoming van de Wbp opgenomen als restbepaling. Omdat een sluitende regeling van verwerkingsgronden in de praktijk niet mogelijk bleek te zijn, werd hier in het algemeen verwezen naar het gerechtvaardigde belang van de verantwoordelijke of van een derde.[8] Een gerechtvaardigd belang van de verantwoordelijke kan aanwezig worden geacht in het geval dat de betreffende verwerking voor hem noodzakelijk is om zijn reguliere bedrijfsactiviteiten te kunnen verrichten, tenzij het belang van degene van wie de gegevens worden verwerkt prevaleert. De bepaling impliceert een motiveringsplicht voor de verantwoordelijke. Blijkens de Memorie van Toelichting bij de Wbp dient hij zich, voordat hij tot verstrekking overgaat, onder andere de volgende vragen te stellen:

– Is er werkelijk een belang dat verwerking van persoonsgegevens rechtvaardigt?
– Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan – afhankelijk van de ernst van de inbreuk – gegevensverwerking niet achterwege te blijven?
– Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg – zonder verwerking – worden bereikt?
– Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel?

De verantwoordelijke dient de belangen af te wegen zoals deze aan hem bekend zijn. Indien de omstandigheden daartoe aanleiding geven zal van hem kunnen worden verwacht nader onderzoek te doen naar het gewicht van deze belangen.[9] Bij de in onderdeel f voorgeschreven afweging spelen de gevoeligheid van de gegevens die de verantwoordelijke wil verwerken en de maatregelen die hij heeft genomen ten einde rekening te houden met de belangen van de betrokkene een rol.[10] De verantwoordelijke dient op de hoogte te zijn van het belang dat de derde heeft bij de gegevensverwerking en welke hem ter beschikking staande gegevens in het licht van even bedoelde belang van betekenis zijn. Ongeacht de verantwoordelijkheid van de derde dient de verantwoordelijke daarbij af te wegen of de verwerking noodzakelijk is met het oog op dat belang en of het belang van de betrokkene niet dient te prevaleren. De noodzakelijkheidseis die in artikel 8 besloten ligt, veronderstelt dat de verantwoordelijke op dergelijke vragen een bevredi-

8. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 86.
9. Idem, p. 87.
10. Idem, p. 88.

gend antwoord heeft. Desgevraagd dienen deze antwoorden ook zichtbaar te worden gemaakt, zodat zij eventueel door de rechter kunnen worden getoetst.[11]

De Wbp voorziet niet in een verplichting om de betrokkene voorafgaand aan de verstrekking op de hoogte te stellen van het voornemen daartoe. In de praktijk zal de betrokkene dus pas achteraf vernemen dat verstrekking heeft plaatsgevonden. Wanneer de betrokkene echter reeds voorafgaand op de hoogte is van de poging van de derde om zijn gegevens te achterhalen, dan kan hij zich tegen de verstrekking verzetten op basis van artikel 40 lid 1 Wbp (zie hierover ook par. 8.3.2.).

9.4 De richtlijn elektronische handel

De opkomst van internet- en e-mailverkeer leidde eind jaren negentig tot een enorme toename van het aantal elektronische transacties. In 2000 werd daarom de richtlijn elektronische handel tot stand gebracht. Deze richtlijn stelt regels met betrekking tot de verlening van 'diensten van de informatiemaatschappij' en heeft als doel bij te dragen aan de goede werking van de interne markt door het vrije verkeer van deze diensten te waarborgen.[12] Op verschillende terreinen wordt een homogeen juridisch kader voor elektronische dienstverlening tot stand gebracht, onder andere ten aanzien van vrije vestiging en informatieplichten, commerciële communicatie en het sluiten van overeenkomsten langs elektronische weg.[13] Afdeling vier van de richtlijn regelt daarnaast de aansprakelijkheid van online tussenpersonen voor het doorgeven en toegankelijk maken van informatie. Deze afdeling bevat ook een bepaling over de verstrekking van identificerende gegevens. Hieronder zullen beiden onderwerpen achtereenvolgens worden behandeld.

9.4.1 Aansprakelijkheid voor informatie

Bij de bestrijding van onrechtmatige en strafbare informatie op het internet doet zich, evenals bij drukkers en uitgevers, de vraag voor onder welke omstandigheden de tussenpersoon strafrechtelijk en civielrechtelijk aansprakelijk kan worden gesteld voor het verspreiden en toegankelijk maken van die informatie. Enerzijds is het belang van een effectieve rechtshandhaving ermee gediend dat men de tussenpersoon aan kan spreken en kan verplichten tot medewerking bij het ontoegankelijk maken danwel verwijderen van schadelijke informatie, anderzijds is het maatschappelijk onwenselijk dat tussenpersonen bij

11. HR 10 december 1993, *NJ* 1994, 667. Zie ook *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 89.
12. Richtlijn 2000/31/EG van 8 juni 2000 betreffende bepaalde juridische aspecten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn elektronische handel'), *PbEG* 2000 L 178/1.
13. Een dienstverlener is iedere natuurlijke of rechtspersoon die een dienst van de informatiemaatschappij levert, terwijl onder een dienst van de informatiemaatschappij verstaan moet worden "elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn". Zie artikel 2 sub b van de richtlijn elektronische handel en artikel 3:15d lid 3 BW.

de uitoefening van hun werkzaamheden onophoudelijk worden gehinderd door juridische claims. In de richtlijn elektronische handel is getracht tussen beide belangen een evenwicht te vinden. Afdeling vier van die richtlijn omschrijft de voorwaarden waaronder een tussenpersoon gevrijwaard blijft van aansprakelijkheid.

De richtlijn onderscheid drie verschillende activiteiten van de tussenpersoon. Van 'mere conduit' is sprake als hij zich enkel bezig houdt met het *doorgeven* van door een afnemer van de dienst verstrekte informatie of met het *verschaffen van toegang* tot een communicatienetwerk (art. 12 richtlijn elektronische handel). Voorbeelden zijn het doorsturen van een e-mail of het mogelijk maken van toegang tot een website. Aansprakelijkheid van de dienstverlener is in deze situatie uitgesloten wanneer: a) het initiatief tot de doorgifte niet bij de dienstverlener ligt, b) de ontvanger van de doorgegeven informatie niet door de dienstverlener wordt geselecteerd, en c) de doorgegeven informatie niet door de dienstverlener wordt gewijzigd. De tussenpersoon vervult hier een passieve rol. Zijn taak is beperkt tot het technische proces van verwerking. Hij heeft noch kennis noch controle over de informatie die wordt opgeslagen en wordt daarom niet verantwoordelijk gehouden voor de inhoud daarvan.[14]

De tweede categorie van activiteiten wordt aangeduid met de term 'caching': de dienstverlener is niet aansprakelijk voor de *automatische*, *tussentijdse* en *tijdelijke opslag* van informatie, wanneer deze opslag enkel geschiedt om latere doorgifte van die informatie aan andere afnemers van de dienst doeltreffender te maken. Caching wordt onder andere toegepast om ervoor te zorgen dat populaire websites niet overbelast raken. Ook hier geldt als voornaamste bijkomende voorwaarde dat de informatie niet door de dienstverlener wordt gewijzigd (art. 13 lid 1 sub a richtlijn elektronische handel). Daarnaast moet de dienstverlener prompt handelen om de door hem opgeslagen informatie te verwijderen of de toegang ertoe onmogelijk te maken zodra hij er daadwerkelijk kennis van heeft dat de informatie verwijderd werd van de plaats waar zij zich oorspronkelijk in het net bevond, of dat de toegang ertoe onmogelijk werd gemaakt. Hetzelfde geldt wanneer een rechtbank of administratieve autoriteit heeft bevolen om de informatie te verwijderen of ontoegankelijk te maken (art. 13 lid 1 sub e richtlijn elektronische handel).

Artikel 14 van de richtlijn regelt ten slotte de aansprakelijkheid voor 'hosting'. Wanneer de activiteit van de dienstverlener bestaat uit de *opslag* van de door een afnemer van de dienst verstrekte informatie, bijvoorbeeld een homepage van een private gebruiker of een bedrijf, is hij niet aansprakelijk voor deze informatie wanneer hij niet daadwerkelijk kennis heeft van de onwettige activiteit of informatie en wanneer hij zodra hij hiervan daadwerkelijk kennis heeft, prompt handelt om de informatie te verwijderen of ontoegankelijk te maken. De artikelen 12 t/m 14 staan overigens niet in de weg aan een aan de dienstverlener gericht rechterlijk bevel of een bevel van een administratieve autoriteit om

14. Zie hierover ook overweging 42 bij de richtlijn elektronische handel.

een inbreuk te beëindigen of te voorkomen (art. 12 lid 3, art. 13 lid 3 en art. 14 lid 3 richtlijn elektronische handel).

9.4.2 Verstrekking van identificerende gegevens

De Europese wetgever was bevreesd dat de bepalingen in afdeling vier van de richtlijn het onderzoek naar delicten op het gebied van de elektronische handel zouden belemmeren.[15] Daarom werd in artikel 15 lid 2 voor de lidstaten uitdrukkelijk de mogelijkheid geschapen om aan dienstverleners in dat kader bepaalde medewerkingsverplichtingen op te leggen:

> "De lidstaten kunnen voorschrijven dat dienstverleners de bevoegde autoriteiten onverwijld in kennis dienen te stellen van vermeende onwettige activiteiten of informatie door afnemers van hun dienst, alsook dat zij de bevoegde autoriteiten op hun verzoek informatie dienen te verstrekken waarmee de afnemers van hun dienst met wie zij opslagovereenkomsten hebben gesloten, kunnen worden geïdentificeerd."

Lidstaten kunnen dienstverleners dus verplichten om identificerende informatie te verstrekken, maar deze mogelijkheid bestaat blijkens de tekst van artikel 15 lid 2 alleen in gevallen van hosting. De bepaling werd zonder nadere toelichting bij amendement ingevoegd zodat de reden van deze beperking onduidelijk is.[16] De formulering van het artikel is, voor zover het de verstrekking van identificerende gegevens betreft, verwarrend en overbodig omdat het geldende recht verstrekking van identificerende gegevens, ook in gevallen waarin geen sprake is van hosting, reeds mogelijk maakt. De privacyrichtlijnen en de Wet bescherming persoonsgegevens verzetten zich niet tegen wettelijke verplichtingen tot verstrekking van identificerende gegevens.[17]. Dit blijkt onder meer uit artikel 8 sub c Wbp dat verwerking van persoonsgegevens toestaat indien dit noodzakelijk is voor het nakomen van een wettelijke verplichting (zie de voorgaande paragraaf). In Nederland kan bovendien ook via civiele rechter een bevel tot verstrekking worden

15. Gemeenschappelijk standpunt van de Raad. *PbEG* 2000 C 128/32, overweging B.1.b.
16. Het zou kunnen zijn dat men heeft aangesloten bij de regeling in de Digital Millenium Copyricht Act. Opmerkelijk is dat de DMCA, juist door het feit dat deze regeling verstrekking alleen toestaat wanneer sprake is van hosting, door de technische werkelijkheid bleek te zijn ingehaald toen men met behulp van deze regeling trachtte de identiteit van anonieme filesharers te achterhalen (zie par. 4.6).
17. In de overwegingen bij de richtlijn elektronische handel wordt enige aandacht geschonken aan de verhouding tot de privacyrichtlijnen. Zo bepaalt overweging 14 dat de richtlijn elektronische handel moet worden uitgevoerd en toegepast met volledige inachtneming van de beginselen inzake de bescherming van persoonsgegevens, onder andere waar het de aansprakelijkheid van tussenpersonen betreft. De richtlijn kan het anoniem gebruik van open netwerken zoals het internet niet voorkomen. In overweging 9 wordt daarnaast bepaald dat de in de richtlijn opgenomen voorschriften niet zijn bedoeld om afbreuk te doen aan fundamentele nationale regels en beginselen in verband met de vrijheid van meningsuiting

verkregen. Dat lidstaten bevoegd zijn om verplichtingen tot verstrekking van identificerende gegevens te creëren staat dus reeds vast.

De Nederlandse wetgever heeft, mede gezien het belang van de opsporing en vervolging van ernstige delicten, gekozen voor een 'technologie-neutrale' interpretatie. Hij stelt zich op het standpunt dat ook de dienstverlener die 'doorgifte-overeenkomsten' heeft gesloten onder omstandigheden binnen de reikwijdte van de bepaling kan vallen, bijvoorbeeld in gevallen waarin door technische ontwikkelingen hosting niet langer nodig is en de benodigde gegevens alleen kunnen worden verkregen bij de dienstverlener die de informatie doorgeeft. Artikel 15 zou aan een dergelijke interpretatie naar het oordeel van de wetgever niet in de weg staan.

Ook de wetgever wijst er op dat de rechter de dienstverlener naar geldend Nederlands recht reeds kan verplichten tot het verstrekken van informatie waarmee de voor de inhoud verantwoordelijke kan worden geïdentificeerd, indien de dienstverlener daartoe redelijkerwijs in staat is. Dat is volgens de wetgever het geval wanneer de dienstverlener in een contractuele relatie staat met de verantwoordelijke, ongeacht de precieze inhoud daarvan. In die contractuele relatie zullen immers identificerende gegevens zijn verzameld, bijvoorbeeld om betaling mogelijk te maken. Ook het Cybercrimeverdrag maakt geen onderscheid tussen de verschillende activiteiten van dienstverleners, aldus de wetgever.[18] In feite komt het er op neer dat artikel 15 lid 2, voor zover het verstrekking van identificerende gegevens betreft, welbewust is genegeerd.[19]

Uit de tekst van artikel 15 lid 2, noch uit de toelichting daarop, wordt duidelijk wat precies verstaan moet worden onder 'de bevoegde autoriteiten'. Er is betoogd dat alleen strafvorderlijke instanties en inlichtingendiensten als zodanig kunnen worden aangemerkt en dat verstrekking aan civielrechtelijke partijen a contrario dus niet mogelijk is. Dit zou volgen uit het feit dat de voorziening in artikel 15 lid 2 werd gecreëerd om de opsporing van strafbare feiten veilig te stellen.[20] Bovendien werd een algemene verplichting om informatieaanbieders te kunnen identificeren in de richtlijn uiteindelijk niet

18. *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 28, 51 en 66. Bevoegdheden tot het vorderen van gebruiksgegevens zijn inmiddels opgenomen in de Wet vorderen gegevens telecommunicatie. Ook daar wordt geen onderscheid gemaakt tussen de verschillende activiteiten van de tussenpersoon.
19. Dit standpunt werd bijvoorbeeld ingenomen door de gedaagde in de zaak *Pessers/Lycos*. Zie par. 9.5.2.
20. Uit de toelichting bij het Gemeenschappelijk Standpunt van de Raad, waarbij de bepaling is ingevoegd, lijkt te volgen dat artikel 15 lid 2 van de richtlijn uitsluitend ziet op informatieverschaffing ten behoeve van de opsporing van strafbare feiten: "Het was er de Raad om te doen dat de ontwerprichtlijn het onderzoek naar delicten op het gebied van elektronische handel niet zou bemoeilijken, en hij heeft daartoe een aantal wijzigingen in het Commissievoorstel aangebracht. (…) Artikel 15, lid 2, stelt nu duidelijk dat de lidstaten mogen eisen dat dienstverleners de bevoegde overheidsinstanties op de hoogte brengen van vermeende illegale activiteiten of, in bepaalde gevallen, gegevens over hun klanten verstrekken. (…)" *PbEG 2000*, C128/32, r.o. B.1.b.

opgenomen omdat dit zich slecht zou verhouden met het recht op privacy en de bescherming van persoonlijke gegevens.[21] In de zaak *Brein/UPC* heeft de voorzieningenrechter echter geoordeeld dat de in artikel 15 lid 2 geboden mogelijkheid niet in de weg staat aan een bevel van de civiele rechter tot afgifte van NAW-gegevens.[22]

In de zaak *Pessers/Lycos* betoogde provider Lycos dat de richtlijn zich verzet tegen een aan een hosting provider gerichte veroordeling tot het verstrekken van NAW-gegevens en dat de richtlijn zich in ieder geval tegen een zodanige veroordeling verzet wanneer de gewraakte informatie niet onmiskenbaar ontrechtmatig is jegens degene die de vordering instelt.[23] Aan dit standpunt lag de opvatting ten grondslag dat de richtlijn een als uitputtend bedoelde regeling bevat die ertoe strekt dat een hosting provider uitstuitend civielrechtelijk of strafrechtelijk aansprakelijk is wanneer aan de in artikel 14 gestelde voorwaarden niet is voldaan (r.o. 5.1.2.). Nu het Hof had vastgesteld dat de gewraakte informatie in casu niet onmiskenbaar onrechtmatig was, meende Lycos aan de voorwaarden van van artikel 14 te hebben voldaan, zodat zij gevrijwaard was van iedere aansprakelijkheid. Deze limitiatieve interpretatie van de richtlijn werd door de Hoge Raad niet gevolgd. In navolging van Advocaat Generaal Huydecoper oordeelde hij dat de tekst van de richtlijn niet inhoudt dat, buiten de in artikel 15 lid 2 bedoelde gevallen, het verstrekken van de NAW-gegevens door een hosting provider niet is toegelaten.[24] De Hoge Raad voegde hier nog de volgende overweging aan toe (r.o. 5.1.6):

21. In eerste lezing diende het Europese Parlement een amendement in voor een nieuwe overweging 9bis. Deze overweging zou stellen dat de verleners van diensten van de informatiemaatschappij in staat moeten zijn om alle nuttige informatie te verstrekken voor het opsporen en identificeren van leveranciers van onwettige inhouden. Zie *PbEG* 1999, C279/389. Het amendement werd in het gewijzigde voorstel uiteindelijk niet opgenomen omdat een dergelijke overweging zou kunnen worden geïnterpreteerd op een wijze die in strijd is met de regels inzake de bescherming van persoonlijke gegevens, aldus de Raad. Zie paragraaf 2.3.2 van de toelichting bij het gewijzigd voorstel d.d. 17 augustus 1998, COM(1999) 427 def., *PbEG* 2000, C248/96. Het Parlement kwam in tweede lezing tot dezelfde conclusie. A5-0106/2000, p. 10.
22. Vzngr. Rb. Utrecht 12 juli 2005, KG-nr: 194741/KGZA 05-462, LJN: AT9073. Deze uitspraak wordt uitgebreider besproken in par. 9.6.
23. HR 25 november 2005 (*Pesser/Lycos*), LJN: AU4019, Hoge Raad, Co4/234HR.
24. De Hoge Raad motiveert de keuze voor deze niet-limitatieve opvatting door te wijzen op het derde lid van artikel 14 van de richtlijn elektronische handel, welk artikel voor het overige bepaalt onder welke voorwaarden een hosting provider niet aansprakelijk is voor de opgeslagen informatie en art. 18 lid 1, waarin is bepaald dat de lidstaten ervoor zorgen dat hun nationale wetgeving op het gebied van diensten van de informatiemaatschappij voorziet in rechtsgedingen waarbij snel – ook voorlopige – maatregelen kunnen worden getroffen, niet alleen om de vermeende inbreuk te doen eindigen, maar ook om te verhinderen dat de betrokken belangen verder worden geschaad (r.o. 5.1.3). Daarnaast verwijst hij naar de preambule van de richtlijn en overwegingen van de Europese en de Nederlandse wetgever (r.o 5.1.4 en 5.1.5).

> "In het licht van het vorenstaande kan de door het middel verdedigde opvatting aangaande (doel en strekking van) de Richtlijn niet als juist worden aanvaard. Een andere opvatting zou bovendien tot het, uit een oogpunt van een effectieve rechtsbescherming tegen (beweerdelijk) onrechtmatige activiteiten, onwenselijke resultaat leiden dat slechts een zeer beperkte groep van benadeelden van door een websitehouder anoniem verspreide informatie – namelijk alleen zij ten aanzien van wie (het voor de hosting provider duidelijk moet zijn geweest dat) onmiskenbaar onrechtmatig is gehandeld of jegens wie een strafbaar feit is gepleegd terzake waarvan de strafrechtelijke autoriteiten bereid zijn op te treden – zich tegen dergelijke activiteiten bij de burgerlijke rechter teweer kunnen stellen en dat andere benadeelden, in weerwil van het bepaalde in art. 3:296 lid 1 BW, in ieder geval praktisch gesproken op voorhand van zodanig rechtsmiddel verstoken blijven."

Zoals ook Guibault constateert draagt de onduidelijkheid over de werkingssfeer van artikel 15 lid 2 niet bij aan een effectieve en evenwichtige implementatie in alle lidstaten. Dit blijkt ook in de praktijk. Vier lidstaten, te weten Spanje, Ierland, Luxemburg en het Verenigd Koninkrijk, hebben ervoor gekozen de verplichting tot verstrekking niet in het nationale recht om te zetten. Alle andere lidstaten, behalve Duitsland, hebben een algemene verplichting ingevoerd, dat wil zeggen een verplichting die ook in civiele procedures toepasselijk is. Alleen in Duitsland is de bepaling uitsluitend toepasselijk in strafprocedures. In Oostenrijk, België, Italië en Portugal geldt de verplichting alleen wanneer sprake is van hosting. In Frankrijk is de verplichting, evenals in Nederland, ook van toepassing op andere gevallen dan hosting maar kan de verstrekking alleen worden bevolen door een rechterlijke autoriteit.[25]

9.4.3 Implementatie

De voorschriften aangaande de civielrechtelijke aansprakelijkheid van de dienstverlener zijn geïmplementeerd in het nieuwe artikel 6:196c BW.[26] In het Wetboek van Strafrecht is daarnaast een nieuw artikel 54a ingevoegd dat de strafrechtelijke aansprakelijkheid voor informatie regelt.[27] Dit artikel vertoont een grote verwantschap met het drukkers- en uitgeversprivilege, hetgeen onder andere tot uitdrukking komt in het feit dat het meteen daarna is opgenomen. De ratio van artikel 54a Sr is de vrijheid van meningsuiting in een digitale omgeving zo veel mogelijk te ondersteunen door de neiging tot preventieve censuur weg te nemen. Tussenpersonen moeten zonder angst voor strafrechtelijke vervol-

25. Guibault 2004.
26. Dit artikel is een bijna letterlijke vertaling van de artikelen 12 t/m 14 van de richtlijn elektronische handel.
27. Artikel 54a Sr luidt: "Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken."

ging van een ander afkomstige gegevens kunnen doorgeven en opslaan.[28] De wetgever ligt dit alsvolgt toe:

> "Artikel 7 van de Grondwet geeft aan de overheid de opdracht de vrijheid van meningsuiting te waarborgen en te stimuleren. Censuur van staatswege dient te worden voorkomen. Artikel 54a beoogt het gevaar in te dammen dat de tussenpersoon, mede gelet op zijn in belang toenemende rol in het proces van gegevensuitwisseling door middel van communicatienetwerken, zich genoodzaakt voelt tot preventieve censuur over te gaan teneinde strafrechtelijke aansprakelijkheid te voorkomen. De regeling dient een onbelemmerde informatie-uitwisseling en daarmee een grondbeginsel van de democratische rechtsstaat."[29]

De vervolgingsuitsluitingsgrond van artikel 54a Sr omvat alle delicten die gelieerd zijn aan de doorgegeven of opgeslagen gegevens. De reikwijdte van het artikel is in dat opzicht dus ruimer dan bij de artikelen 53 en 54 Sr, die uitsluitend betrekking hebben op uitingsdelicten door middel van de drukpers gepleegd. De wetgever motiveert dit onderscheid door te verwijzen naar de algemene intermediaire functie die de tussenpersoon in het huidige en toekomstige, internationale maatschappelijke verkeer vervult.[30]

Noch artikel 6:196c BW, noch artikel 54a Sr zegt iets over de verstrekking van identificerende gegevens. Met name in de strafrechtelijke context ontstaat hierdoor een belangrijk verschil met de aansprakelijkheidsregeling ten aanzien van het drukkers- en uitgevers in de artikelen 53 en 54 Sr. Van de tussenpersoon online wordt niet geëist dat hij de verantwoordelijke voor de informatie bekend maakt. Volgens de Nederlandse wetgever staat de richtlijn elektronische handel er aan in de weg dat aan de niet-vervolgbaarheid van de provider de voorwaarde wordt verbonden dat de dader bekend wordt gemaakt omdat de aansprakelijkheidsregeling in artikelen 12 tot en met 14 niet in deze mogelijkheid voorziet.[31]

9.5 Ontmaskering van anonieme internetgebruikers in civiele procedures

De laatste jaren dringt zich in toenemende mate de vraag op of ook civiele partijen een tussenpersoon kunnen verplichten tot het verstrekken van identificerende informatie. Voor de praktijk is deze vraag zeer relevant omdat de eiser doorgaans alleen met behulp van de tussenpersoon in staat is de verantwoordelijke voor een beweerdelijk onrechtmatige handeling of beweerdelijk onrechtmatige informatie te achterhalen en aansprakelijk te stellen.

28. De formulering 'doorgifte of opslag van gegevens die van een ander afkomstig zijn' omvat zowel mere conduit als caching als hosting. *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 62.
29. Idem, p. 62-63.
30. Idem, p. 63.
31. Idem, p. 66.

Hieronder behandel ik drie juridische vraagstukken rondom de civielrechtelijke verstrekking. Het eerste vraagstuk heeft betrekking op een procedureel aspect. Zoals in het voorgaande werd beschreven wordt de Amerikaanse John Doe procedure aangespannen tegen de gebruiker zelf terwijl een Nederlandse civielrechtelijke procedure over de verstrekking van identificerende gegevens wordt begonnen tegen de provider. Dit verschil in aanpak heeft consequenties voor de verdere verloop van het geding. Hieronder wordt bekeken in hoeverre ook het Nederlandse recht de mogelijkheid biedt om de anonieme internetgebruiker zelf aan te spreken met behulp van een zogenaamde anonieme dagvaarding.

Een tweede belangrijke kwestie is de juridische grondslag voor een op de tussenpersoon rustende civielrechtelijke verplichting tot verstrekking. De hierboven besproken bepalingen in de Wet bescherming persoonsgegevens en de richtlijn elektronische handel geven hierover geen duidelijkheid. Artikel 8 sub f Wbp creëert voor gegevensverwerkers slechts een *bevoegdheid* om persoonsgegevens op vrijwillige basis te verstrekken aan derde partijen en de ruimte die in artikel 15 lid 2 van de richtlijn elektronische handel voor lidstaten van de Europese Unie is geschapen om voor tussenpersonen een *verplichting* tot verstrekking in het leven te roepen is door de Nederlandse wetgever, voor zover het civielrechtelijke verstrekking betreft, onbenut gelaten. In de rechtspraak zijn voor het aannemen van een verplichting verschillende wettelijke bepalingen en juridische leerstukken gehanteerd. Een met dit onderwerp samenhangend probleem is in hoeverre de betrokkenheid van de tussenpersoon bij de beweerdelijk onrechtmatige uitingen of handelingen bij het aannemen van een verstrekkingsverplichting relevant is. Kan als voorwaarde voor het toewijzen van een vordering tot verstrekking de eis worden gesteld dat de tussenpersoon zelf onrechtmatig gehandeld heeft?

De derde vraag die juristen verdeeld houdt betreft de overige criteria waaraan de vordering tot verstrekking getoetst dient te worden. Van belang is allereerst wat de eiser precies aannemelijk moet maken om de vordering te doen slagen. Daarnaast moeten proportionaliteit en subsidiariteit van de verstrekking worden beoordeeld. In dat kader dient duidelijkheid te bestaan over de wijze waarop de belangen van de eiser worden afgewogen tegen de mogelijke grondrechtelijke aanspraken van de anonymus.

9.5.1 De provider als gedaagde

Bij de bespreking van het Amerikaanse recht inzake de ontmaskering van anonieme internetgebruikers in hoofdstuk 4 bleek dat John Doe-procedures niet worden aangespannen tegen de provider, maar tegen de anonymus zelf. De provider wordt vervolgens als derde partij in het geding betrokken (zie hierover par. 4.2). Het Nederlandse burgerlijk procesrecht voorziet niet in deze mogelijkheid. Hieronder zal worden uiteengezet waarom het uitbrengen van een anonieme dagvaarding aan een onbekende internetgebruiker in Nederland niet mogelijk is en welke consequenties dit heeft voor het verloop van het geding.

Om een natuurlijke of rechtspersoon in rechte te betrekken dient men aan hem een dagvaarding uit te brengen.[32] Dit vereiste levert problemen op indien men een anonieme natuurlijke persoon wenst aan te spreken. Het exploot van dagvaarding dient krachtens artikel 45 lid 2 sub d van het Wetboek van Burgerlijke Rechtsvordering (Rv) namelijk naam en woonplaats van de gedaagde te vermelden. Op deze regel bestaat een aantal uitzonderingen. Zo kan aan krakers een anonieme dagvaarding worden uitgebracht: indien het exploot een vordering tot ontruiming betreft van een gebouwde onroerende zaak door anderen dan gebruikers of gewezen gebruikers van wie naam en woonplaats in redelijkheid niet kunnen worden achterhaald, behoeft het deze naam en woonplaats niet te vermelden (art. 45 lid 3 Rv). Deze mogelijkheid werd in 1987 ingevoerd om te verhinderen dat krakers een rechtsgeldige dagvaarding tot ontruiming onmogelijk maken door anoniem te blijven en diende eveneens te voorkomen dat eigenaren van gekraakte panden het recht in eigen hand zouden nemen.[33] Vermelding van naam en woonplaats mag in bepaalde gevallen ook achterwege worden gelaten bij de betekening van exploten aan de gezamenlijke erfgenamen van een overledene (art. 53 Rv) en aan houders van aandelen of andere effecten aan toonder (art. 54 lid 2 Rv). De naam van de gedaagden is in het laatste geval uit de aard der zaak onbekend. Ten slotte kunnen consumentenorganisaties bij het gerechtshof te Den Haag een rechtsvordering instellen die er toe strekt om een verklaring te verkrijgen dat bedingen in algemene voorwaarden onredelijk bezwarend zijn (art. 6:240 en 6:241 BW). In dat geval hoeven de naam en de woonplaats van hen die deze algemene voorwaarden gebruiken, niet afzonderlijk in het exploot te worden vermeld (art. 62 Rv).

Uit het bovenstaande blijkt dat de wetgever slechts in zeer specifieke gevallen een uitzondering heeft willen maken op het vereiste dat naam en woonplaats van de gedaagde worden vermeld. Het uitbrengen van een dagvaarding aan een anonieme internetgebruiker valt niet onder een van de genoemde uitzonderingen.

Ook het uitbrengen van de dagvaarding is een obstakel. Dit kan immers enkel geschieden aan de gedaagde in persoon (art. 46 lid 1 Rv), aan de woonplaats van de gedaagde (art. 46 en 47 Rv) of door middel van terpostbezorging (art. 47 Rv). Zodoende wordt voorkomen dat de gedaagde door onvindbaar te zijn de aanvang van het geding kan beletten.[34] Wanneer de deurwaarder een exploot conform de wettelijke voorschriften heeft uitgereikt, wordt deze dan ook geacht de wederpartij te hebben bereikt zonder dat tegenbewijs mogelijk is. Indien de woonplaats van de gedaagde onbekend is, geschiedt betekening ter plaatse van het werkelijk verblijf. Is ook het werkelijk verblijf onbekend, dan kan een 'openbare dagvaarding' worden betekend aan het parket van de ambtenaar

32. Deze regel lijdt krachtens artikel 255 lid 2 Rv uitzondering wanneer partijen in kort geding vrijwillig, zonder dagvaarding, voor de rechter verschijnen om hem over de door de eiser gewenste voorziening te laten beslissen.
33. Stein & Rueb 2002, p. 3; Heemskerk 2004.
34. Stein & Rueb 2002, p. 82.

van het openbaar ministerie bij het gerecht waar de zaak moet dienen of dient (art. 54 Rv).[35] In al deze gevallen moet de naam van de gedaagde worden vermeld.

Al met al moet worden geconcludeerd dat de Amerikaanse wijze van procederen onder het Nederlandse recht niet tot de mogelijkheden behoort. Deze omstandigheid leidt ertoe dat een procedure ter verkrijging van identificerende gegevens wordt aangespannen tegen de tussenpersoon en heeft als gevolg dat de verdere loop van het geding en de positie van de anonymus daarin afwijken van de Amerikaanse situatie. In de eerste plaats kan de anonymus slechts indien hij in de hoedanigheid van procespartij bij de beslissing over de onthulling van zijn identiteit is betrokken, aanspraak maken op het uit het beginsel van hoor en wederhoor voortvloeiende recht om van het geding op de hoogte te worden gesteld.[36] In de huidige praktijk wordt de anonymus soms in het geheel niet verwittigt terwijl hij wel in hoge mate in zijn belangen wordt geraakt. Een belangrijke vraag is dan ook of op de eiser in het geding, danwel op de tussenpersoon, onder omstandigheden een notificatieplicht zou kunnen rusten. In de tweede plaats wordt de anonymus doorgaans niet in de gelegenheid gesteld om zelf, hetzij schriftelijk, hetzij bij monde van zijn raadsman, zijn verdediging te voeren. De tussenpersoon die de communicatie van de anonymus heeft afgehandeld wordt als het ware in zijn plaats gesteld. In de praktijk komt op de tussenpersoon nogal eens de taak te rusten om de belangen van de anonymus te behartigen. Het kan zelfs gebeuren dat hij wordt belast met het bewijs, bijvoorbeeld omtrent de waarheid van een uiting, om te voorkomen dat hij tot onthulling van identificerende informatie wordt verplicht (zie par. 9.5.2).

Het is overigens onjuist te veronderstellen dat een anonieme persoon om praktische redenen niet in het geding zou kunnen worden betrokken. Hoewel fysieke betekening van een dagvaarding aan een onbekende 'virtuele' persoon niet mogelijk is en de anonymus doorgaans niet in persoon voor de rechter zal willen verschijnen, kan met hem worden gecommuniceerd via de provider of via zijn raadsman. Ook notificatie kan via deze weg geschieden. In het Amerikaanse recht zijn voorbeelden te vinden van procedures waarin een dergelijke methode werd gevolgd. In het Californische recht bestaan daarnaast voorstellen om het uitbrengen van een dagvaarding via elektronische weg mogelijk

35. In dit geval moet een uittreksel van het exploot zo spoedig mogelijk bekend worden gemaakt in een landelijk dagblad of in een dagblad verschijnend in de streek waar voormeld gerecht zitting houdt onder vermelding van naam en kantooradres van de deurwaarder of van de advocaat van wie afschrift van het exploot kan worden verkregen (art. 54 lid 2 Rv).
36. Het recht op hoor en wederhoor is één van de meest fundamentele beginselen van burgerlijk procesrecht en wordt ook wel aangeduid als het verdedigings- of gelijkheidsbeginsel. Dit beginsel komt terug in het vereiste dat de gedaagde door middel van een exploot van dagvaarding wordt opgeroepen. Artikel 19 Rv bepaalt daarnaast dat de rechter partijen over en weer in de gelegenheid dient te stellen hun standpunten naar voren te brengen en toe te lichten en zich uit te laten over elkaars standpunten en over alle bescheiden en andere gegevens die in de procedure ter kennis van de rechter zijn gebracht.

te maken (zie par. 4.3). Het is opvallend dat ook Advocaat-generaal Huydecoper, die overigens niet geneigd is om aan de anonimiteit van gebruikers een hoog niveau van bescherming toe te kennen, in zijn conclusie bij de zaak *Pessers/Lycos* (zie hieronder par. 9.5.2) de mogelijkheid oppert dat een provider bij de anonymus informatie opvraagt over de basis van de anonieme boodschappen om diens toelichting vervolgens met respectering van de anonimiteit te betrekken bij zijn eigen beoordeling en bij het debat met de wederpartij.

Het voorgaande in ogenschouw nemend zou men kunnen betogen dat het ook in het Nederlandse recht mogelijk zou moeten zijn om een civiele procedure aan te spannen tegen de anonymus. Vanuit procedureel oogpunt lijkt dit zuiverder omdat de anonymus zodoende zelf zijn eventuele bezwaren tegen de verstrekking naar voren kan brengen. Een dergelijke benadering doet daarnaast meer recht aan de functie van de provider als doorgeefluik. Hij hoeft de belangen van de anonymus niet langer te verdedigen maar wordt slechts belast met de plicht om de anonieme persoon te notificeren en met het mogelijk maken van communicatie met de eiser.[37]

9.5.2 De grondslag voor de verstrekking

Een aan een provider gerichte civiele vordering tot verstrekking van identificerende gegevens wordt eind jaren negentig voor het eerst aan de civiele rechter voorgelegd in de zaak *Scientology/XS4all*.[38] Deze procedure is het begin van een zoektocht naar de juiste juridische grondslag voor een civielrechtelijke verplichting tot verstrekking.

In de Scientology-zaak gaat het om de onrechtmatige publicatie van auteursrechtelijk beschermde werken van de Scientology-kerk door abonnees van provider XS4all. Scientology wil dat deze informatie ontoegankelijk wordt gemaakt en vordert daarnaast afgifte van namen en adressen van de verantwoordelijke abonnees. De Rechtbank 's-Gravenhage overweegt dat de activiteiten van een provider zich beperken tot doorgifte en opslag van informatie en dat daarom geen sprake is van auteursrechtelijk relevante verveelvoudiging en/of openbaarmaking door de provider zelf. Hij is niettemin van oordeel dat een provider op grond van de zorgvuldigheid die in het maatschappelijk verkeer betaamt, gehouden kan zijn om medewerking te verlenen en adequate maatregelen te nemen als hij ervan in kennis wordt gesteld dat een gebruiker van zijn computersysteem door middel van die homepage auteursrechtinbreuk pleegt of anderszins onrechtmatig handelt:

> "Van de Service Provider mag een zekere mate van zorg worden verwacht ten aanzien van het voorkomen van verdere inbreuk. Mede gelet op de omstandigheid dat de Service Providers bedrijfsmatig handelen, de mogelijkheid die hun ten dienste staat de toegang tot de home page af te sluiten en de

37. Zie hierover ook mijn ook mijn annotatie bij Vzngr. Rb. Haarlem, 11 september 2003 (*Pessers/Lycos*), verschenen in *Computerrecht* 2003-6, p. 363-367.
38. Rb. 's-Gravenhage 9 juni 1999, *Mediaforum* 1999-7/8, nr. 37 m.nt. D.J.G. Visser (*Scientology/XS4ALL*).

> schade die van verdere inbreuken het gevolg zou kunnen zijn, moet worden geoordeeld dat de Service Provider die ervan in kennis wordt gesteld dat een gebruiker van zijn diensten op diens home page auteursrechtinbreuk pleegt of anderszins onrechtmatig handelt, terwijl aan de juistheid van die kennisgeving in redelijkheid niet valt te twijfelen, zelf onrechtmatig handelt indien hij alsdan niet ingrijpt. Van de Service Provider mag dan onder andere worden verwacht dat hij de inbreukmakende documenten uit zijn computersysteem verwijdert en tevens dat hij aan de rechthebbende op diens verzoek de naam en het adres van de desbetreffende gebruiker bekend maakt."

Het door de rechter gehanteerde criterium is afkomstig uit afdeling vier van het voorstel voor de richtlijn elektronische handel, dat enige tijd later zal worden aangenomen (zie par. 9.4). De rechter past dit criterium, dat slechts bedoeld is om de aansprakelijkheid voor informatie te regelen, echter fout toe door het ook van toepassing te laten zijn op de verstrekking van NAW-gegevens.[39]

De verstrekking van identificerende gegevens wordt wel afzonderlijk beoordeeld in *Deutsche Bahn/XS4all*. Deutsche Bahn vordert in kort geding dat provider XS4all een website ontoegankelijk maakt waar artikelen te vinden zijn van het in Duitsland verboden linkse blad *Radikal*.[40] In deze artikelen wordt uiteengezet hoe men het Duitse spoorwegnet onklaar kan maken. De eis van Deutsche Bahn wordt door de voorzieningenrechter ingewilligd met toepassing van het Scientology-criterium. Daarnaast vordert Deutsche Bahn afgifte van de namen en adressen van de gebruikers van de website. Zij stelt dat toegang tot de bron voor haar noodzakelijk was teneinde te voorkomen dat de informatie met betrekking tot de sabotagehandleiding opnieuw gepubliceerd wordt, bijvoorbeeld via andere service providers. De rechter is van oordeel dat Deutsche Bahn daarmee voldoende aannemelijk heeft gemaakt een 'rechtens te respecteren belang' te hebben bij afgifte van de namen en adressen, voorzover het gaat om de houder(s) van de website. Een bevel tot afgifte van de namen en adressen van de bezoekers van de websites, strekt naar zijn oordeel echter te ver, aangezien het raadplegen van een website op zichzelf niet onrechtmatig is. Het Hof Amsterdam laat dit oordeel in stand. Het is van oordeel dat XS4ALL in de gegeven omstandigheden onrechtmatig handelt door afgifte te weigeren (r.o. 4.14):

> "Juist is dat XS4all niet lichtvaardig de privacy van haar abonnees mag prijsgeven. Hier gaat het echter om een abonnee die onmiskenbaar onrechtmatig jegens Deutsche Bahn handelt door het publiceren van de gewraakte informatie op het internet, terwijl aannemelijk is dat de abonnee zal trachten de informatie via andere websites te publiceren wanneer de onderhavige websites geblokkeerd worden. Ter voorkoming dan wel beperking van verdere kansen op aanzienlijke schade heeft Deutsche Bahn er dan ook groot belang bij de abonnee zelf in rechte aan te kunnen spreken. Met het oog op dat zwaarwegende belang is XS4all gehouden de namen en adressen van de gebruiker(s) van de web-

39. Zie hierover Ekker 2002c, p. 349.
40. Vzngr. Rb. Amsterdam, 25 april 2002, *KG* 02/790 OdC, *Mediaforum* 2002-6, nr. 24 (*Deutsche Bahn/XS4all*).

> sites aan Deutsche Bahn te geven; in de gegeven omstandigheden handelt zij onrechtmatig door dat na te laten."

De voorzieningenrechter in *Teleatlas* kiest een geheel andere benadering. Teleatlas, een producent van computerprogrammatuur, vordert dat Planet wordt veroordeeld om naam, adres en woonplaats vrij te geven van een abonnee die op grote schaal illegale kopieën maakt van software waarop Teleatlas het auteursrecht had.[41] De vordering is gebaseerd op artikel 8 sub f Wbp (zie par. 9.3). Hoewel de voorzieningenrechter de verstrekking van identificerende gegevens terecht als een op zichzelf staand probleem beoordeelt, past hij artikel 8 sub f Wbp verkeerd toe door aan te nemen dat voor de verantwoordelijke, dat wil zeggen: de provider, een rechtsplicht tot verstrekking ontstaat wanneer voldaan is aan de criteria van die artikel. Zoals hierboven reeds aan de orde kwam, schept artikel 8 sub f Wbp weliswaar een basis voor rechtmatige vrijwillige verstrekking wanneer naar het oordeel van de verantwoordelijke sprake is van een gerechtvaardigd belang van een derde, maar roept het in geen geval een plicht tot verstrekking in het leven. Wanneer een verantwoordelijke gevraagd wordt gegevens te verstrekken en hij dat verzoek afwijst, heeft de rechter dan ook geen taak op grond van de Wbp. Een *plicht* tot verstrekking dient op een andere grondslag te worden gebaseerd.[42]

Weer anders is de argumentatie van het Hof 's-Hertogenbosch in *Tibetaanse Hondenfokster*.[43] Het Hof oordeelt dat er geen algemene rechtsregel bestaat op grond waarvan provider Concepts ICT zo spoedig mogelijk nadat hij kennis heeft gekregen van onrechtmatige handelingen, verplicht is mee te werken aan het ter beschikking stellen van gegevens die nodig zijn om vast te stellen wie voor die handelingen verantwoordelijk is (r.o. 4.7.2.). De vordering van eiseres Rutloh, die de verzender van een aantal misleidende e-mailberichten wenste te achterhalen, wordt daarom afgewezen. Dit onder andere omdat de account van de bewuste gebruiker inmiddels is afgesloten en omdat niet is gebleken dat sindsdien nog soortgelijke berichten via Concepts ICT zijn verzonden.

In *Onsfrieschepaard.nl* wordt ten slotte getracht de verstrekking af te dwingen met de regels van het burgerlijk procesrecht.[44] Op het forum van de website www.onsfrieschepaard.nl zijn boze berichten geplaatst over het bestuur van vereniging 'het Friesche paardenstamboek'. Het bestuur meent dat sprake was van lasterlijke en smadelijke uitlatingen en wenst de namen en adressen van een zevental internetgebruikers te achterhalen

41. Vzngr. Rb. Utrecht, 9 juli 2002, *KG* ZA 02-563, *(Teleatlas N.V./Planet Media Group N.V.)*.
42. Zie ook de noot van Steenbruggen bij Rb. Utrecht, 9 juli 2002, KG ZA 02-563, *Computerrecht* 2002/5, p. 297-298.
43. Hof 's-Hertogenbosch, 25 juli 2002, *KG* 2002, 259. Zie ook mijn annotatie bij Hof Amsterdam 7 november 2002 (*XS4all/Deutsche Bahn*), *Mediaforum* 2003-1, p. 40-41.
44. Beschikking van de rechtbank Leeuwarden d.d. 26 maart 2004, rekestnummer 61984 HA RK 04-3.

door een webmaster op te roepen als getuige in het voorlopig getuigenverhoor.[45] De rechtbank Leeuwarden oordeelt echter dat het getuigenverhoor niet bedoeld is om namen en adressen van personen te achterhalen omdat de namen en adressen van die gebruikers niet kunnen worden aangemerkt als 'feiten of rechten die men wil bewijzen' als bedoeld in artikel 187 Rv. Deze benadering lijkt strijdig met een uitspraak van de Hoge Raad, waarin kwam vast te staan dat het voorlopig getuigenverhoor juist wel mede bedoeld is om duidelijkheid te verkrijgen omtrent de identiteit van een aan te spreken partij. Het voorlopig getuigenverhoor beoogt blijkens deze uitspraak niet alleen mogelijk te maken dat spoedig na het plaatsvinden van omstreden feiten daaromtrent getuigenverklaringen kunnen worden afgelegd alsmede te voorkomen dat bewijs verloren gaat, het strekt ook en vooral ertoe belanghebbenden bij een eventueel naderhand bij de burgerlijke rechter aanhangig te maken geding de gelegenheid te bieden vooraf opheldering te verkrijgen omtrent de (hun wellicht nog niet precies bekende) feiten, zulks teneinde hen in staat te stellen hun positie beter te beoordelen, met name ook ten aanzien van de vraag tegen wie het geding precies moet worden aangespannen.[46] Ook het Hof Amsterdam oordeelde reeds in deze zin.[47]

Na deze eerste procedures bleef al met al onduidelijk binnen welk kader de verstrekking van NAW-gegevens moest worden beoordeeld. Toepassing van het Scientology-criterium leek onjuist omdat daarmee de aansprakelijkheid voor de inhoud en de verplichting tot verstrekking op één hoop woeden gegooid. Het criterium van onmiskenbare onrechtmatigheid lijkt bovendien een erg strenge standaard. Het kan immers voorkomen dat de identiteit van een gedaagde benodigd is om de onrechtmatigheid van zijn handelen of zijn uitingen aan te kunnen tonen. Ook artikel 8 sub f Wbp bracht geen uitkomst. Deze bepaling roept geen plicht tot verstrekking in het leven en werd door de rechter dus foutief toegepast. Over het voorlopig getuigenverhoor waren de meningen verdeeld.

Met de zaak *Pessers/Lycos* dient zich een gelegenheid aan om meer helderheid te verkrijgen. Provider Lycos wordt geconfronteerd met een vordering tot verstrekking van gegevens afkomstig van Pessers, die via de virtuele veilingsite E-bay postzegels verhandelt. Op een door Lycos gehoste website, 'stop the fraud' genaamd, had een anonieme persoon uitlatingen over hem gedaan. Het bericht luidde:

45. Krachtens artikel 186 Rv kan voorafgaand aan of tijdens het geding een voorlopig getuigenverhoor worden bevolen. Het verzoekschrift dat daartoe moet worden ingediend houdt in: a. de aard en het beloop van de vordering; b. de feiten of rechten die men wil bewijzen; c. de namen en woonplaatsen van de personen die men als getuigen wil doen horen; en d. de naam en de woonplaats van de wederpartij of de redenen waarom de wederpartij onbekend is (art. 187 lid 3 Rv).
46. HR 24 maart 1995 *NJ* 1998, 414. Zie tevens A-G Bakels in zijn conclusie (nr. 2.7) bij HR 6 februari 1998, *NJ* 1999, 478 m.nt. HJS.
47. Hof Amsterdam 7 juli 1984, *NJ* 1985, 432. A-G Huydecoper verwijst in zijn conclusie bij de zaak Pessers/Lycos naar deze uitspraak (zie noot 31). Volgens hem wordt het voorlopig getuigenverhoor in de praktijk regelmatig toegepast om de identiteit van een wederpartij te achterhalen.

> "Have you ever been ripped off by Pessers@home.nl on E-bay, join our quest for justice!! How does he work? You buy a small lot. Which he ships directly. So he gains your trust. You feel confident to buy a more expensive lot. That's when he strikes. He will keep your money and no stamps for you. That's not all. According to some of his victims he also sends fakes. Have you been ripped off and you want also to publish your story? Mail your story to stopthefraud@hotmail.com (…)."[48]

Pessers stelt dat hij door dit bericht aanzienlijke financiële schade leidt. Hij is van oordeel dat Lycos onrechtmatig handelde door hem de NAW-gegevens te onthouden.

Omdat de tekst van artikel 8 sub f Wbp geen verplichting tot verstrekking in het leven roept, had Steenbruggen in zijn annotatie bij de zaak *Teleatlas* gesuggereerd de stappentoets uit de Memorie van Toelichting bij de Wbp (zie par. 9.3) in onrechtmatige daadsprocedures analoog toe te passen.[49] De voorzieningenrechter van de rechtbank Haarlem neemt deze suggestie over. Tegelijkertijd verwijst hij echter naar het Scientology-criterium (zie r.o. 5.13).[50] Hierdoor blijft onduidelijkheid bestaan. In hoger beroep wordt dit manco verholpen.[51] Het Hof Amsterdam stelt hier duidelijk vast dat de vordering tot verstrekking van NAW-gegevens op haar eigen merites beoordeeld moet worden:

> "Ook indien de op een website gepubliceerde informatie niet onmiskenbaar onrechtmatig is, kan een serviceprovider onder omstandigheden onrechtmatig handelen door de bij haar bekende NAW-gegevens van de desbetreffende websitehouder niet op verzoek aan een belanghebbende derde bekend te maken. Indien voldoende aannemelijk is dat de gepubliceerde informatie jegens de derde wel onrechtmatig zou kunnen zijn en dat deze daardoor schade kan lijden, zou het maatschappelijk bezien ongewenst zijn indien die derde geen enkele reële mogelijkheid heeft de websitehouder daarop – zonodig in rechte – aan te spreken. Onder omstandigheden kan dan ook een weigering van

48. De tekst van dit bericht wordt ook geciteerd in de conclusie bij de uitspraak van de Hoge Raad in deze zaak.
49. Alvorens een bevel tot verstrekking te geven zouden volgens Steenbruggen de volgende vragen moeten worden beantwoord:
    – Is er werkelijk een belang dat verstrekking van NAW-gegevens rechtvaardigt?
    – Wordt met de verstrekking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan – afhankelijk van de ernst van de inbreuk – opheffing van anonimiteit niet achterwege te blijven?
    – Kan het doel dat met de verstrekking wordt nagestreefd ook langs andere minder ingrijpende weg – zonder opheffing van anonimiteit – worden bereikt?
    – Is de verstrekking in de mate die is beoogd evenredig aan het nagestreefde doel?
50. De rechter noemt hier als mogelijke grondslag voor verstrekking eveneens de exhibitieplicht van artikel 843 van het Wetboek van Burgerlijke Rechtsvordering. Artikel 843 lid 1 Rv luidt: "Hij die daarbij rechtmatig belang heeft, kan op zijn kosten inzage, afschrift of uittreksel vorderen van bepaalde bescheiden aangaande een rechtsbetrekking waarin hij of zijn rechtsvoorgangers partij zijn, van degene die deze bescheiden te zijner beschikking of onder zijn berusting heeft. Onder bescheiden worden mede verstaan: op een gegevensdrager aangebrachte gegevens." Mijns inziens zijn de NAW-gegevens die door de provider zijn verzameld niet aan te merken als 'bescheiden' in de zin van dit artikel aangezien zij geen verband houden met een rechtsbetrekking tussen de provider en de eiser, mocht die al bestaan.
51. Hof Amsterdam 24 juni 2004, *JAVI* 2004-5, p. 137-140 (*Pessers/Lycos*).

de serviceprovider om de NAW-gegevens van de websitehouder aan de derde bekend te maken in strijd komen met de zorgvuldigheid die de serviceprovider jegens een zodanige derde in acht dient te nemen."

Het Hof gaat dus uit van een zorgvuldigheidsverplichting van de tussenpersoon jegens de derde. Om te kunnen beoordelen of deze verplichting aanwezig is, introduceert hij een stappentoets. Deze wordt uitgebreider besproken in paragraaf 9.5.4. Eerst gaan wij hier nog verder in op de discussie over de grondslag van een verplichting tot verstrekking.

Voor de volledigheid dient hier te worden ingegaan op de binnen het intellectuele eigendomsrecht bestaande jurisprudentie aangaande de 'verplichting tot het noemen van de voorman'. Dit leerstuk, met name ontwikkeld in procedures over merkpiraterij, strekt er toe de belangen van een rechthebbende te beschermen door een pleger van merkinbreuk te verplichten tot het noemen van zijn leveranciers. Het standaardarrest over de verplichting tot het noemen van de voorman is *Chloé/Peeters*. In deze zaak oordeelde de Hoge Raad dat op degene die ervan kennis draagt dat een derde onrechtmatig gehandeld heeft, handelt of zal handelen, slechts in uitzonderlijke gevallen een rechtsplicht rust om daarvan mededeling te doen aan de benadeelde.[52] Of een dergelijke plicht kan worden aangenomen, hangt in de eerste plaats af van de aard van de aan de derde(n) verweten handelingen. Daarnaast is vereist dat bij het uitblijven van de benodigde inlichtingen het gevaar bestaat dat de betreffende derden zullen voortgaan met het verrichten van deze handelingen of dat geen vergoeding zal kunnen worden verkregen voor de schade die door de in die handelingen besloten liggende merkinbreuken aan de rechthebbende is of zal worden toegebracht (r.o. 3.4).

Een inbreukmaker kan ook worden veroordeeld tot het verschaffen van een lijst van afnemers. In *Hameco/SKF* aanvaarde de Hoge Raad dat een dergelijke veroordeling in een onrechtmatige daadsprocedure een aanvaardbaar zijdelings middel kan zijn om nakoming te verzekeren van een veroordeling tot het terugnemen van de zaken door middel waarvan de onrechtmatige daad is gepleegd.[53] Door de inbreukmaker was in cassatie naar voren gebracht dat de veroordeling tot afgifte van de lijst door het Hof ten onrechte was bekrachtigd omdat het Hof niet had vastgesteld dat de inbreukmaker jegens de eiser onrechtmatig zou handelen door deze lijst niet aan haar te doen toekomen. Een dergelijke veroordeling zou naar Nederlands recht niet zonder meer kunnen worden gegrond op de omstandigheid dat dit een deugdelijk middel oplevert voor de eiser om na te gaan of de gedaagde aan haar verplichtingen jegens de eiser voldoet. De Hoge Raad verwierp dit betoog. Hij was van oordeel dat voor de veroordeling tot afgifte onrechtmatig handelen jegens de eiser niet vereist was (r.o. 3).

52. HR 27 november 1987, *NJ* 1988, 722 m.nt. LWH.
53. HR 23 februari 1990, *NJ* 1990, 664 m.nt. DWFV.

De vraag wat de rechtsgrond is van de veroordeling tot het overleggen van een lijst van afnemers wordt zowel door Advocaat-generaal Asser als annotator Verkade besproken. Volgens Asser is in literatuur en rechtspraak op deze vraag geen eenduidig antwoord te vinden.[54] Uit de toelichting van Verkade komt eveneens een onduidelijk beeld naar voren. Verkade onderscheidt voor het terugroepbevel en het bevel tot verstrekking van een lijst van afnemers als potentiële grondslagen: (a) schadevergoeding in natura, (b) een ongeschreven rechtsplicht van de inbreukmaker om de in het leven geroepen onrechtmatige toestand (zo veel mogelijk) op te heffen en (c) een afzonderlijke of toegevoegde (mogelijke) zorgvuldigheidsplicht.[55] Volgens Verkade verwerpt de Hoge Raad expliciet het, in het arrest *Chloé/Peeters* en ook door de Advocaat-generaal tot uitgangspunt genomen, alternatief c (zie par. 10 van zijn conclusie). De Hoge Raad oordeelt immers (r.o. 3, derde alinea):

> "Onderdeel 2 (…) betoogt dat de veroordeling om de lijst met namen en adressen te verstreken 'rechtens onjuist dan wel onvoldoende gemotiveerd is', nu het hof niet heeft vastgesteld dat Hameco onrechtmatig jegens SKF zou handelen door deze lijst niet aan SKF of haar advocaat te doen toekomen. Het onderdeel faalt, omdat voor zulk een veroordeling zulk een onrechtmatig handelen jegens SKF niet vereist was. De rechter kan op vordering van degene jegens wie een onrechtmatige daad is gepleegd, naast een veroordeling om zaken door middel waarvan de onrechtmatige daad is gepleegd van afnemers terug te nemen, de aansprakelijke persoon veroordelen op een door de rechter te bepalen wijze een lijst van afnemers van die zaken te verstrekken. Zulks vormt, zoals het hof uitdrukt, een deugdelijk middel om na te gaan of gedaagde aan de veroordeling de zaken terug te nemen voldoet en daarmede een aanvaardbaar zijdelings middel om nakoming van deze veroordeling te verzekeren."[56]

De alternatieven a) en b) worden blijkens deze overweging evenmin als theoretische grondslag omhelsd, aldus Verkade. De Hoge Raad aanvaardt het 'zijdelings middel' als basis zonder daarbij te verwijzen naar een wettelijke grondslag of naar ongeschreven recht. Deze constructie ligt volgens Verkade dogmatisch het dichtst bij een door Van Nispen geopperd alternatief: een naar ongeschreven recht aan te nemen bevoegdheid van de rechter om voorzieningen te treffen die moeten voorkomen dat na zijn uitspraak nieuwe geschillen ontstaan over de naleving van het vonnis. De rechterlijke bevoegdheid tot toewijzing is zijns inziens niet discretionair, maar wordt gebonden aan een afweging van criteria van "wederzijdse belangen en de verdere omstandigheden van het geval, zoals

54. Zie overweging 2.8 van zijn conclusie. De standpunten van Van Nispen, Verkade en De Ranitz worden besproken in de overwegingen 2.9-2.12.
55. Par. 6 en 7 van zijn annotatie. Over de dogmatische grondslagen van het bevel tot noemen van de voorman is ook geschreven door van Nispen. Van Nispen 1988, p. 71.
56. Bij het onder c. genoemde alternatief beoordeelt de rechter, met inachtneming van alle omstandigheden van het geval, aan de hand van een al dan niet door hem (als vervuld) aangenomen ongeschreven zorgvuldigheidsplicht of de inbreukmaker (ook) tot terugroep gehouden is, omdat deze door zulks niet te doen (bijkomend) onrechtmatig jegens de eiser zou handelen, aldus Verkade.

de aard en de ernst van de onrechtmatige daad en het belang (…) commerciële gegevens niet aan de concurrentie ter beschikking te stellen".[57] Het aldus aanvaarde systeem vergt volgens Verkade van de feitenrechter niet dat schuld c.q. desbewustheid wordt aangenomen, noch de overweging dat een plicht tot verstrekking ook zonder dat onrechtmatig wordt gehandeld bestaat. Afwijzing van de vordering vergt zijns inziens evenmin dat overwogen moet worden dat de gedaagde niet onrechtmatig handelt door niet te voldoen aan de bevelsvordering (anders dan in het *Chloé/Peeters*-arrest). Wel moet de rechter ook de zwaarwegende belangen van de gedaagde meewegen.[58]

In het licht van het bovenstaande moet men een duidelijk onderscheid maken tussen het onrechtmatig handelen van de elektronische tussenpersoon als *voorwaarde* voor het aannemen van een verplichting tot verstrekking en het ontstaan van onrechtmatigheid als *gevolg* van een weigering van de tussenpersoon om te voldoen aan een door de rechter gegeven bevel tot verstrekking. Tot het arrest van de Hoge Raad in de zaak *Pessers/Lycos* bestond onder juristen met name over het eerste punt verschil van mening als gevolg van de nog onbesliste discussie over de dogmatische grondslag van de verplichting tot verstrekking. Verschillende auteurs waren, in tegenstelling tot Verkade, van mening dat deze verplichting sterk samenhing met het onrechtmatig handelen van degene die tot het noemen van zijn voorman wordt verplicht.[59] Ook buiten het intellectuele-eigendomsrecht werd dit argument naar voren gebracht. In het Duitse recht werd het vraagstuk besproken door Spindler en Dorschel. Zij wezen erop dat bij alle in het Duitse recht aangenomen verplichtingen tot het verstrekken van informatie als voorwaarde werd gesteld dat sprake is van een objectief vaststelbare onrechtmatige gedraging en dus van een aansprakelijkheid van degene die tot verstrekking verplicht is.[60] Ook in de reeds aangehaalde

57. Zie de conclusie van Verkade par. 7 en 10.
58. Zie de conclusie van Verkade par. 11.
59. Spindler en Dorschel zijn van mening: "(…) dass der Auskunftsanspruch dogmatisch von der Haftung des Verletzers abhängig und eng mit den diesbezüglichen Ansprüchen verknüpft ist. Er steht und fällt mit der Passivlegitimation des Providers, hier als Störer. Es wäre nicht recht einzusehen, warum einerseits eine Störerhaftung eingreifen sollte, andererseits aber die damit verbundenen Ansprüche nur zum Teil durchgesetzt werden könnten. Ziel des par. 8 Abs. 2 S. 2 TDG, der auf Art. 15 der E-Commerce-Richtlinie zurückgeht, ist das Verbot proaktiver Überwachungspflichten – diese werden gerade nicht durch Auskünftsansprüche tangiert, da diese den Provider nicht zu einer Überwachung zwingen, sondern nur zur Herausgabe ihm bereits bekannter Daten." Spindler & Dorschel 2005, p. 41. Krachtens par. 101a Urhebergesetz (UrhG), dat voorziet in de verplichting tot het noemen van de voorman, kan de informatieverplichting alleen worden opgelegd aan degene die "das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht verletzt (…)". Sieber & Höfinger 2004, p. 576.
60. "Entscheidend für Internet-Sachverhalte ist vor allem, dass alle bislang dargestellten Auskunftsansprüche ein zumindest objektiv rechtswidriges Verhalten, mithin eine Haftung des Auskunftspflichtigen für die Rechtsverletzung voraussetzen. Die Frage liegt daher auf der Hand, inwieweit ein solcher Anspruch überhaupt gegen Provider gerichtet werden kann, da diese in den Genuss der weitreichenden Haftungsprivilegierungen in par. 8-11 TDG [Teledienstgesetz, AE] kommen." Spindler & Dorschel 2005, p. 41.

zaak *Pessers/Lycos* werd door de gedaagde, provider Lycos, betoogd dat een vordering tot verstrekking van NAW-gegevens door een hosting provider hoogstens kon worden toegewezen wanneer de provider vooafgaand onrechtmatig had gehandeld terzake het hosten van de gewraakte informatie en/of niet (tijdig) verwijderen of ontoegankelijk maken van dat materiaal.[61] Dit standpunt werd onder andere onderbouwd door te verwijzen naar *Chloé/Peeters* en *Hameco/SKF*. De Hoge Raad verwierp dit standpunt. Naar zijn oordeel dient van de concrete omstandigheden van het geval af te hangen of Lycos onrechtmatig handelt door te weigeren de NAW-gegevens aan de beschuldigde te verstrekken (r.o. 5.2.2).[62]

Volgens de Hoge Raad kan men dus ook ook zonder dat sprake is van voorafgaand onrechtmatig handelen van de tussenpersoon een verplichting tot verstrekking aannemen. Dit standpunt lijkt mij om een aantal redenen juist. In de eerste plaats is van belang dat andere rechtsinstituten die de verstrekking van identificerende gegevens reguleren voor het aannemen van een verstrekkingsplicht niet de eis stellen dat de verstrekker zelf onrechtmatig handelt. Bij drukkers en uitgevers is het enkele feit dat zij als tussenpersonen bij de verspreiding van de gewraakte informatie betrokken waren voldoende, ook als zij van het onrechtmatige of strafbare karakter niet wisten. De journalist kan zich tegen een tot hem gerichte vordering om zijn bronnen bekend te maken evenmin verweren met de stelling dat hij zelf niet onrechtmatig gehandeld heeft. Deze omstandigheid doet in het licht van de afweging die in dergelijke gevallen door de rechter wordt gemaakt niet ter zake. Men zou op basis hiervan kunnen stellen dat de verplichting tot verstrekking dogmatisch niet gebaseerd zou moeten zijn op de betrokkenheid van de tussenpersoon bij de inhoud van informatie – providers zijn in verreweg de meeste gevallen van de inhoud immers niet op de hoogte – maar op het feit dat hij in het maatschappelijke verkeer nu eenmaal de meest aangewezen en vaak de enige partij is om identificatie tot stand te brengen.[63]

Ter onderbouwing van het bovengenoemde standpunt kan men er ten slotte op wijzen dat de verplichting om informatie te verstrekken over herkomst en distributiekanalen van inbreukmakende goederen of diensten krachtens artikel 8 lid 1 van de recent aangenomen richtlijn handhaving intellectuele-eigendomsrechten niet alleen kan worden opgelegd aan een inbreukmaker, maar ook aan een andere persoon die de inbreukmakende goederen in zijn bezit heeft, met de inbreukmakende handelingen verbonden commerciële diensten verleent of is aangewezen als zijnde betrokken bij het verlenen van

61. Zie de schriftelijke toelichting namens Lycos, Hoge Raad der Nederlanden, Rolzitting d.d. 22 oktober 2004, Rolnummer C04/234, p. 23.
62. HR 25 november 2005 (*Pessers/Lycos*), LJN: AU4019, Hoge Raad, Co4/234HR.
63. Dit standpunt werd in de reeds genoemde zaak *Pessers/Lycos* naar voren gebracht door de eiser. Hij meende dat de vordering tot verstrekking van de NAW-gegevens is gebaseerd op het gegeven dat Lycos de intermediair is met wie de websitehouder een contractuele relatie had en dat door de dienstverlening van Lycos deze website via het internet toegankelijk was.

deze diensten. Gaat men er van uit dat de in de handhavingsrichtlijn opgenomen regel in de plaats treedt van de in het *Chloé*-arrest aanvaarde regel, dan is de discussie over de grondslag van de verstrekking, voor zover het het intellectuele-eigendomsrecht betreft, daarmee geëindigd. Hieronder wordt deze richtlijn besproken.

In zijn conclusie bij het cassatieberoep in de zaak *Pessers/Lycos* gaat ook Advocaat-generaal Huydecoper in op de dogmatische fundering (overweging 32 t/m 51). Hij komt tot de bevinding dat in het geldende Nederlandse recht geen civielrechtelijke verplichting bestaat om, enkel omdat men kennis heeft omtrent gegevens die voor de beoordeling van een (mogelijk) onrechtmatig handelen van belang zijn, die gegevens aan de benadeelde (of aan iemand anders die aanleiding ziet om over de kwestie te gaan procederen) mee te delen. Volgens Huydecoper moet er meer aan de hand zijn, wil een dergelijke verplichting aangenomen kunnen worden (overweging 41). Ook hij verwerpt overigens het standpunt dat voor het aannemen van een verplichting tot verstrekking onrechtmatig handelen van de tussenpersoon vereist is.

Huydecoper is van oordeel dat het ontbreken van een civielrechtelijke verplichting tot verstrekking van NAW-gegevens maatschappelijk onaanvaardbare consequenties heeft.[64] Om een dergelijke verplichting toch aan te kunnen nemen, zoekt hij aansluiting bij de leer omtrent uit zorgvuldigheidsnormen voortvloeiende verplichtingen om, in geëigende omstandigheden, handelend op te treden. Uit deze leer volgt dat het nalaten van handelend optreden onder omstandigheden onrechtmatig kan zijn (overweging 44 t/m 46). Het arrest *Zutphense waterleiding*, de aanleiding voor de totstandkoming van deze leer, geeft volgens Huydecoper één belangrijk aanknopingspunt voor de beoordeling van een dergelijke verplichting: degene die werd aangesproken had als enige toegang tot de middelen waarmee verder onheil voor de benadeelde relatief eenvoudig kon worden voorkomen.[65] In de woning van de gedaagde bevond zich een kraan waarmee de watertoevoer tot een gesprongen waterleiding kon worden afgesloten. Huydecoper wijst ook op andere bronnen (overweging 46 en 47) waaruit blijkt dat het weliswaar uitzondering is dat men verplicht is een ander voor schade te behoeden of bij te staan bij het beperken of ongedaan maken van schade, maar dat uitzonderingen zich bijvoorbeeld voordoen wanneer men:

– in een unieke dan wel (qua informatie) geprivilegieerde positie verkeert, en andere mogelijkheden om de schade af te wenden niet, of niet op aannemelijke voorwaarden beschikbaar zijn;
– men zich voor het bieden van de verlangde hulp geen ernstige risico's of onevenredige belasting hoeft te getroosten;

64. Huydecoper somt een aantal van deze ongewenste consequenties op (zie overweging 21). Hij legt de nadruk op het belang van kenbaarheid in het elektronische handelsverkeer.
65. HR 10 juni 1910, *W.* 9038.

– men zelf (al is het dan zonder dáárvoor aansprakelijk te zijn) aan de schade heeft bijgedragen of aan het verder oplopen van de schade bijdraagt, doordat men instrumenteel is aan de handelwijze (of andersoortige gebeurtenis) die de schade mede (heeft) veroorzaakt.

Al met al luidt Huydecopers conclusie dat ook in het voorliggende geval plaats is voor aanvaarding van een uitzondering (overweging 48):

> "De ISP bevindt zich als het om anonieme en onrechtmatige (maar niet evident onrechtmatige of strafbare) uitingen gaat die door zijn tussenkomst worden 'aangeboden', in een unieke positie, omdat (vaak) alleen met zijn hulp, in de vorm van verstrekking van NAW-gegevens, bestrijding van het onrechtmatige handelen mogelijk is. De ISP werkt bovendien, al handelt hij daardoor niet onrechtmatig, de aanbieding van de onrechtmatige informatie in de hand: zijn diensten zijn daarvoor noodzakelijk (geweest). Zowel het een als het ander plaatst de ISP in een positie die rechtvaardigt, dat de betrekkelijk geringe inspanning van verstrekking van NAW-gegevens van hem gevergd mag worden – althans, wanneer niet andere belangen, hierna nog te onderzoeken, weer tot andere uitkomst nopen. Ik bedoel dan de belangen, berustend op het recht op vrije meningsuiting en de belangen, betrokken bij de bescherming van de privacy (en dan speciaal: geregistreerde persoonsgegevens)."

Op zich lijkt deze benadering verdedigbaar. Het is echter wel van belang te onderkennen dat in de casus *Pessers/Lycos* ook (grondrechtelijke) belangen van de derde partij en de provider meespelen. Daarnaast kan men, gezien de mogelijke aansprakelijkheid van de provider voor een onterechte verstrekking of een weigering daartoe, van mening verschillen over het standpunt dat verstrekking voor de provider nauwelijks belastend is. De Hoge Raad is in haar oordeel op dit onderwerp overigens niet verder ingegaan.

9.5.3 Toetsingscriteria

Bij de beoordeling van een vordering tot verstrekking dient de rechter een afweging te maken tussen het belang van de eiser en de belang van de anonieme internetgebruiker. Ook dient hij rekening te houden met de positie van de tussenpersoon. In wezen doet zich ook hier de reeds beschreven spanning voor tussen enerzijds het maatschappelijke belang van een effectieve rechtshandhaving, corresponderend met het maatschappelijke principe van 'kenbaarheid', en anderzijds de grondrechtelijke waarden van het recht op privacy en de uitingsvrijheid met daaraan gekoppeld de aanspraak van het communicerend individu op vertrouwelijkheid van zijn (identificerende) gegevens. Kort samengevat spelen bij de afweging de volgende vragen:

1. Wat is het belang van de eiser bij de verstrekking en wat dient hij hieromtrent aannemelijk te maken?
2. Wat dient de eiser aannemelijk te maken omtrent het handelen van de anonymus danwel omtrent de door hem verspreide informatie?
3. Wat is het belang van de tussenpersoon?

4. Wat is het belang van de anonymus?
5. Hoe moeten, de genoemde belangen in aanmerking genomen, de proportionaliteit en de subsidiariteit van de vordering worden beoordeeld?

Bij de bespreking van zowel het Amerikaanse als het Nederlandse recht kwamen wij reeds verschillende 'stappentoetsen' tegen. De meeste hiervan bevatten ten aanzien van ten minste een aantal van de genoemde elementen een standaard. Dit geldt ook voor de toets die het Hof Amsterdam in de zaak *Pessers/Lycos* introduceerde. Het Hof oordeelde immers (r.o. 4.9 en 4.10):

> "Ook indien de op een website gepubliceerde informatie niet onmiskenbaar onrechtmatig is, kan een serviceprovider onder omstandigheden onrechtmatig handelen door de bij haar bekende NAW-gegevens van de desbetreffende websitehouder niet op verzoek aan een belanghebbende derde bekend te maken. Indien voldoende aannemelijk is dat de gepubliceerde informatie jegens de derde wel onrechtmatig zou kunnen zijn en dat deze daardoor schade kan lijden, zou het maatschappelijk bezien ongewenst zijn indien die derde geen enkele reële mogelijkheid heeft de websitehouder daarop – zonodig in rechte – aan te spreken. Onder omstandigheden kan dan ook een weigering van de serviceprovider om de NAW-gegevens van de websitehouder aan de derde bekend te maken in strijd komen met de zorgvuldigheid die de serviceprovider jegens een zodanige derde in acht dient te nemen.
>
> 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."

De door het hof gehanteerde stappentoets is een specifieke invulling van de hierboven reeds besproken stappentoets uit de Memorie van Toelichting bij de Wet bescherming persoonsgegevens (zie par. 9.3). Hieronder nemen wij de verschillende elementen van de stappentoets nader in beschouwing.

Over het belang van de eiser kunnen wij vrij kort zijn. Volgens het hof geldt aan zijn kant als belang "dat hij de mogelijkheid moet hebben om zijn rechten en vrijheden te beschermen, door de websitehouder zo nodig in rechte aan te spreken op diens mogelijk onrechtmatige gedragingen en daarvoor schadevergoeding en een verbod te vorderen" (r.o. 4.14.). Uit de hierboven geciteerde overweging valt daarnaast af te leiden dat de eiser een 'reëel' belang moet hebben en dat dit belang in de meeste gevallen bestaat uit het kunnen beëindigen danwel voorkomen van (verder) onrechtmatig handelen en het beperken van de schade die daaruit voortvloeit. In de zaak *Deutsche Bahn/XS4all* had het Hof Amsterdam een dergelijk criterium al eerder als uitgangspunt genomen. In die uitspraak was daarnaast doorslaggevend dat het aannemelijk was dat de abonnee zou trach-

ten de bestreden informatie via andere websites te publiceren wanneer de onderhavige websites geblokkeerd worden (kort gezegd: er was verspreidingsgevaar). Zowel wat betreft het verspreidingsgevaar als wat betreft het risico van de te lopen schade kan men bij de motivering in deze uitspraak overigens vraagtekens zetten.[66]

De tweede vraag is: Wat dient de eiser aannemelijk te maken omtrent het handelen van de anonymus danwel omtrent de door hem verspreide informatie? In verschillende eerdere procedures werden strengere eisen gesteld dan door het Hof Amsterdam. In *Scientology* oordeelde de Rechtbank 's-Gravenhage dat sprake moest zijn van een "kennisgeving van onrechtmatig handelen, aan de juistheid waarvan in redelijkheid niet getwijfeld kan worden". In *Deutsche Bahn* moest 'onmiskenbaar onrechtmatig handelen' zijn aangetoond. Beide benaderingen vallen om hierboven reeds genoemde redenen af (zie par. 9.5.2) en worden overigens opzij gezet door het oordeel van het Hof Amsterdam. Het hof overweegt immers uitdrukkelijk dat onmiskenbare onrechtmatigheid niet vereist is. In plaats daarvan hanteert het het criterium dat de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, *voldoende aannemelijk* is. De precieze betekenis van dit criterium staat nog niet vast.

Ook het derde belang, dat van de tussenpersoon, leent zich voor een beknopte behandeling. In verschillende uitspraken is reeds erkend dat de provider niet alleen op mag komen voor zijn eigen belang om zo min mogelijk belast te worden met verzoeken tot verstrekking van persoonsgegevens, maar ook voor het belang van zijn klanten bij vertrouwelijkheid van deze gegevens.[67] Dit mede gezien de contractuele verplichting die providers jegens hun klanten doorgaans hebben om vertrouwelijke informatie zo veel mogelijk te beveiligen. Veel service providers hebben zich krachtens toepasselijke algemene voorwaarden verbonden om NAW-gegevens uitsluitend te gebruiken in het kader van de uitvoering van hun overeenkomsten met abonnees, en deze gegevens niet aan derden te zullen verstrekken, tenzij zij daartoe verplicht zijn krachtens wet of rechterlijke uitspraak. Providers wensen verstrekking dus ook zo veel mogelijk te vermijden om te voorkomen dat zij wegens een onterechte verstrekking aansprakelijk zijn jegens een abonnee.

Nu komen wij toe aan het element dat het meest raakt aan de kernvragen van dit onderzoek: het grondrechtelijke belang van de anonymus. In *Pessers/Lycos* brengt het Hof Amsterdam de mogelijkheid om op het internet anoniem te communiceren veel duidelijker dan in eerdere uitspraken in verband met de uitingsvrijheid en het recht op de bescherming van de persoonlijke levenssfeer. Het Hof overweegt:

66. Zie mijn annotatie bij Hof Amsterdam 7 november 2002 *(XS4all/Deutsche Bahn)*, *Mediaforum* 2003-1, p. 40-41.
67. Hof 's-Hertogenbosch, 25 juli 2002, *KG* 2002, 259 (Zie *Tibetaanse Hondenfokster*); Hof Amsterdam 7 november 2002 (*XS4all/Deutsche Bahn*), *Mediaforum* 2003-1, p. 40-41.

> "Aan de zijde van de websitehouder geldt als belang dat hij vrijelijk zijn mening kan uiten en dat zijn privacy en zijn zelfverkozen anonimiteit niet door Lycos, aan wie hij NAW-gegevens heeft verschaft, worden geschonden. Deze belangen hebben echter geen absolute waarde en mogen in het bijzonder niet misbruikt worden om (potentieel) schadelijke uitlatingen over een derde te doen en zich daarbij volledig te onttrekken aan iedere mogelijkheid om door die derde ter verantwoording te worden geroepen."

Het Hof relativeert de grondrechtelijke belangen dus onmiddellijk. In casu was de door de anonieme websitehouder aan de orde gestelde beweerdelijke misstand, te weten: fraude bij de online verkoop van postzegels, naar haar oordeel niet zodanig van aard of impact, dat waarborging van zijn anonimiteit noodzakelijk zou zijn om die beweerdelijke misstand vrijelijk aan de orde te kunnen stellen. Verstrekking van de gegevens zou bovendien slechts een beperkte inbreuk zijn op het privacybelang van de anonymus, nu deze gegevens slechts aan de eiser bekend gemaakt zouden worden (r.o. 4.14).

Ook advocaat-generaal Huydecoper legt bij de bespreking van de door Lycos tegen het oordeel van het Hof naar voren gebrachte cassatiemiddelen de nadruk op het belang van transparantie en toerekenbaarheid in het rechtsverkeer. Hij erkent het publieke belang bij ongehinderde informatie-uitwisseling en de rol die in dat verband toekomt aan anonieme uitingen maar lijkt het belang van degene die schade ondervindt van anonieme uitingen in principe hoger te waarderen (overweging 14 e.v.). Huydecoper gaat dan ook niet mee in het volgens hem door Lycos naar voren gebrachte standpunt dat een provider alleen tot verstrekking kan worden gedwongen als het om evidentelijk onrechtmatig uitingen gaat en de provider in verband daarmee zelf onrechtmatig handelt, óf als dat door bevoegde autoriteiten in verband met ernstige strafbare feiten wordt gevorderd. Volgens Huydecoper zet gewaarborgde anonimiteit voor deelnemers aan het elektronische handelsverkeer de deur open voor een scala aan onwenselijke praktijken. Hij noemt onder ander het zich onttrekken aan klachten van gedupeerde wederpartijen over nakoming van elektronische gesloten overeenkomsten, het straffeloos bedrijven van misleidende reclame en het ontgaan van aansprakelijkheid voor onrechtmatige uitingen. In geen van de zojuist genoemde categorieën is gewoonlijk sprake van evident onrechtmatige handelingen of van strafbare feiten (overweging 21).

Huydecoper komt tot de conclusie dat noch het recht op privacy noch de uitingsvrijheid als doorslaggevend kunnen worden beoordeeld en dat deze belangen dus niet in de weg kunnen staan aan het aannemen van een verplichting tot verstrekking. Het risico dat procedurele middelen worden misbruikt om legitieme uitingen de kop in te drukken bestempelt hij als welhaast denkbeeldig. Hij lijkt een beroep op uitingsvrijheid en privacy dan ook categorisch af te wijzen.

Tegen Huydecopers benadering kan mijns inziens een aantal bezwaren worden ingebracht. In de eerste plaats is het belang van grondrechtelijke belangen niet zo denkbeeldig als hij stelt. Zou in casu sprake zijn geweest van legitieme beschuldigingen van fraude, begaan door een hooggeplaatste politicus of overheidsfunctionaris, dan had het

maatschappelijk belang bij de bescherming van de anonieme bron wel degelijk een rol gespeeld. Huydecoper lijkt het belang van rechtshandhaving bovendien in abstracto af te wegen tegen grondrechtelijke aanspraken van de anonymus terwijl een dergelijke afweging alleen in concrete gevallen kan worden gemaakt. De benadering van Huydecoper bevat tenslotte in het geheel geen toetsing aan grondrechten en zou daarom al snel in strijd kunnen komen met de artikelen 8 en 10 EVRM.

Als men Huydecopers standpunt afzet tegen de geldende regels in de offline wereld, zou door aanvaarding daarvan bovendien een vreemd contrast ontstaan. Drukkers, uitgevers en journalisten zouden als hoofdregel niet tot openbaarmaking van een anonieme bron kunnen worden verplicht, maar providers wel. Dit was ook een van de argumenten die in het cassatieberoep door Lycos naar voren werd gebracht. Volgens Lycos speelt een hosting provider in een democratische samenleving een met de vrije pers vergelijkbare rol, waarbij een vergelijkbaar verschoningsrecht hoort. Dit zou volgens Lycos moeten leiden tot de hoofdregel dat, in een situatie waarin de informatie niet onmiskenbaar onrechtmatig is, in beginsel geen NAW-gegevens hoeven te worden verstrekt, tenzij zich uitzonderlijke omstandigheden voordoen. De Hoge Raad meent echter dat Lycos aan het belang van de websitehouder om zich anoniem te uiten zodoende een te absoluut gewicht toekent (r.o. 5.3.7):

> "Het standpunt van Lycos komt erop neer dat, behoudens evidente onrechtmatigheid van de inhoud van de anoniem gepubliceerde informatie, voor een op de hosting provider rustende zorgvuldigheidsverplichting tot het verstrekken van de NAW-gegevens geen plaats meer is. Dat standpunt is hiervoor in 5.2.2 reeds in zijn algemeenheid onjuist bevonden. 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. Dat neemt niet weg 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. De hier vereiste terughoudendheid heeft het hof evenwel niet uit het oog verloren."

Het vijfde en laatste element dat wij hier bespreken heeft van doen met de wijze waarop de proportionaliteit en de subsidiariteit van de verstrekking worden getoetst. De proportionaliteit van een vordering tot verstrekking hangt sterk samen met de belangen van eiser en gedaagde in een concreet geval. Hierover kan in zijn algemeenheid dus niet veel worden gezegd. Een aspect van de verstrekking is in dit verband echter van bijzonder belang: de verstrekking van identificerende gegevens en de opheffing van anonimiteit die daarvan het gevolg is, is onomkeerbaar. Verwijderde informatie kan weer terug worden geplaatst op het internet maar de anonimiteit van een internetgebruiker kan niet meer worden hersteld. De voorzieningenrechter in *Teleatlas* was van oordeel dat deze omstandigheid er toe

leidt dat de noodzaak van een onthulling in kort geding daarom extra streng moet worden beoordeeld. De gevraagde voorziening kon volgens hem alleen dan worden toegewezen als met aan zekerheid grenzende waarschijnlijkheid vaststaat dat de bodemrechter eveneens zal beslissen dat Planet de gevraagde NAW-gegevens dient te verschaffen (r.o. 4.2). In de zaak *Brein* oordeelde de voorzieningenrechter daarentegen dat noch het feit dat de gevorderde maatregel onherstelbaar nadeel kon toebrengen aan de betrokken abonnees, noch het onomkeerbaar zijn van de gevolgen van een beslissing in kort geding een aanleiding kon zijn voor toewijzing van een beroep op niet-ontvankelijkheid (r.o. 4.2).[68] Enige tijd later oordeelde de Hoge Raad in de zaak *Pessers/Lycos* in gelijke zin (r.o. 5.3.9).[69]

Het vereiste van subsidiariteit brengt met zich mee dat bij de beoordeling van de toelaatbaarheid van de verstrekking ook de vraag beantwoord dient te worden of het doel dat met de verwerking wordt nagestreefd ook langs andere weg kan worden bereikt. Verschillende malen is betoogd dat een private partij die identificerende gegevens wenst te bekomen, het 'met meer waarborgen beklede' alternatief van de strafrechtelijke weg zouden kunnen benutten. Om verschillende redenen moet dit betoog echter van de hand worden gewezen. In de eerste plaats is het een algemeen aanvaard uitgangspunt dat een burger of private instantie met een redelijk belang ook in staat moet worden gesteld om via de civiele weg het spoor te volgen van degene die inbreuk heeft gemaakt op zijn rechten.[70] De strafrechtelijke weg is bovendien geen daadwerkelijk alternatief omdat het Openbaar Ministerie niet verplicht is om tot vervolging over te gaan. Afhandeling via het strafrecht biedt de burger onvoldoende controle op een adequate behartiging van zijn belangen en heeft een te kleine kans van slagen.[71] Zowel de voorzieningenrechter in de *Brein*-zaak (r.o. 4.4.-4.7) als de Hoge Raad in *Pesser/Lycos* (r.o. 5.3.10) oordeelde dat de civielrechtelijke aanpak de voorkeur verdient.[72]

9.6 De richtlijn handhaving intellectuele-eigendomsrechten

Om de handhaving van het auteursrecht in de digitale omgeving te ondersteunen werd in 2004 de richtlijn ter handhaving van intellectuele-eigendomsrechten tot stand gebracht (hierna: de handhavingsrichtlijn).[73] Evenals de Amerikaanse Digital Millenium

68. Vzngr. Rb. Utrecht 12 juli 2005, KG-nr: 194741/KGZA 05-462, LJN: AT9073.
69. HR 25 november 2005 (Pessers/Lycos), LJN:AU 4019, Hoge Raad, C04/234HR.
70. In de nota 'Wetgeving voor de elektronische snelweg' nam de overheid het standpunt in dat voor onrechtmatige handelingen in de digitale omgeving altijd een verantwoordelijke moet zijn aan te wijzen. Het handhaven van rechten is voor de burger alleen mogelijk wanneer hij, net als de opsporingsautoriteiten, in staat wordt gesteld om het elektronische spoor van de inbreukmaker te volgen. *Kamerstukken II* 1997/98, 25 880, nrs. 1-2, p. 5-6.
71. Ook Chavannes is van mening dat de strafrechtelijke weg doodloopt. Zie zijn annotatie bij Hof Amsterdam 24 juni 2004, *Mediaforum* 2003-11/12, p. 378-381 (*Pessers/Lycos*).
72. Vzngr. Rb. Utrecht 12 juli 2005, KG-nr: 194741/KGZA 05-462, LJN: AT9073.
73. Richtlijn 2004/48/EG van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten, *PbEG* 2004 L 195/16.

Copyright Act (DMCA) (zie par. 4.6) stelt deze richtlijn auteursrechthebbenden in staat om met behulp van de provider de identiteit van anonieme internetgebruikers te achterhalen. Krachtens artikel 8 van de richtlijn kunnen rechterlijke autoriteiten op verzoek van een auteursrechthebbende bepaalde personen gelasten informatie te verstrekken over de herkomst en de distributiekanalen van goederen of diensten die worden verondersteld inbreuk te maken op een intellectuele eigendomsrecht. De bepaling is een uitwerking van het recht op informatie van de auteursrechthebbende en de daarmee corresponderende verplichting van de inbreukmaker tot het noemen van zijn voorman, zoals vastgelegd in artikel 47 van het TRIPS-verdrag. De leden 1 en 2 van artikel 8 luiden:

> "1. De lidstaten dragen er zorg voor dat de bevoegde rechterlijke instanties tijdens een gerechtelijke procedure wegens inbreuk op een intellectuele-eigendomsrecht, op gerechtvaardigd en redelijk verzoek van de eiser kunnen gelasten dat informatie over de herkomst en de distributiekanalen van de goederen of diensten die inbreuk maken op een intellectuele-eigendomsrecht, wordt verstrekt door de inbreukmaker en/of door een andere persoon die:
> a) de inbreukmakende goederen op commerciële schaal in zijn bezit blijkt te hebben;
> b) de inbreukmakende diensten op commerciële schaal blijkt te gebruiken;
> c) op commerciële schaal diensten die bij inbreukmakende handelingen worden gebruikt, blijkt te verlenen; of
> d) door een onder a), b) of c) bedoelde persoon is aangewezen als zijnde betrokken bij de productie, de fabricage of de distributie van deze goederen of bij het verlenen van deze diensten.
>
> 2. De in lid 1 bedoelde informatie omvat naar gelang passend is:
> a) de naam en het adres van de producenten, fabrikanten, distributeurs, leveranciers en andere eerdere bezitters van de goederen of diensten, alsmede van de beoogde groot- en kleinhandelaren;
> b) inlichtingen over de geproduceerde, gefabriceerde, geleverde, ontvangen of bestelde hoeveelheden, alsmede over de voor de desbetreffende goederen of diensten verkregen prijs."

Bij de toepassing van artikel 8 dient de rechter rekening te houden met andere regelgeving waarin het gebruik van de bedoelde informatie in burgerlijke of strafzaken wordt geregeld, alsmede met geldende privacyregelgeving (art. 8 lid 3 sub b en e handhavingsrichtlijn).

De verplichting om informatie te verstrekken is ook toepasselijk in de digitale omgeving. Een provider die inbreukmakende informatie doorgeeft of toegankelijk maakt kan immers worden aangemerkt als 'een andere persoon die op commerciële schaal diensten die bij inbreukmakende handelingen worden gebruikt, blijkt te verlenen' in de zin van artikel 8 lid 1 sub b. Identificerende gegevens van een internetgebruiker die inbreukmakend materiaal verspreidt zijn dan te beschouwen als informatie over de herkomst en de distributiekanalen van de desbetreffende dienst. Het is ook nadrukkelijk de bedoeling van de Europese wetgever geweest om het recht op informatie van toepassing te doen zijn op providers. Met name de bestrijding van peer-to-peer filesharing van muziekbestanden heeft op politiek niveau een belangrijke rol gespeeld. Op aandringen van orga-

nisaties van auteursrechthebbenden werd zelfs een wijziging in het oorspronkelijke voorstel voor de richtlijn aangebracht. De werkingssfeer van de richtlijn was aanvankelijk beperkt tot inbreuken met een commercieel karakter. Deze beperking zou in de weg hebben gestaan aan de bestrijding van uitwisseling van auteursrechtelijk beschermde informatie via peer-to-peernetwerken. Uiteindelijk werd deze beperking uit het voorstel gehaald.[74]

De waarborgen waarin artikel 8 van de handhavingsrichtlijn voorziet, zijn op een aantal punten sterker dan die in de Amerikaanse regeling. In de eerste plaats kan het bevel tot verstrekking alleen worden gegeven door 'de bevoegde rechterlijke instanties tijdens een gerechtelijke procedure wegens inbreuk op een intellectuele-eigendomsrecht'. Beoordeling van het verzoek van de eiser geschiedt dus zowel in het strafrechtelijke als in het civielrechtelijke kader door de rechter en het bevel tot verstrekking wordt ook door de rechter gegeven. De eis dat het verzoek wordt gedaan tijdens een inbreukprocedure lijkt bovendien te impliceren dat door de eiser tenminste aannemelijk is gemaakt dat sprake is van een inbreuk. Dit is een belangrijk verschil met de regeling in de DMCA, die de rechthebbende in staat stelt om identificerende gegevens op eigen houtje te achterhalen zonder dat hij daarvoor iets aannemelijk behoeft te maken (zie par. 4.6). Daarnaast is van belang dat de regeling blijkens artikel 8 lid 3 sub c nadrukkelijk ruimte laat voor lidstaten om sancties te stellen op misbruik van het recht op informatie.[75]

Artikel 8 bevat verschillende criteria voor een afweging van belangen. Het verzoek van de eiser moet 'gerechtvaardigd' en 'redelijk' zijn en het criterium van het commerciële karakter is in deze bepaling gehandhaafd (zie artikel 8 lid 1 sub a, b en c). Het verzoek van de eiser kan immers alleen worden ingewilligd wanneer een provider 'op commerciële schaal' diensten verleent die bij de inbreukmakende handeling worden gebruikt.[76] Belangrijker lijkt echter dat de in lid 1 bedoelde informatie krachtens het tweede lid slechts 'naar gelang passend is' de daar genoemde gegevens omvat. Deze zinsnede beoogt naar mag worden aangenomen onder andere een afweging mogelijk te maken tussen het belang van de rechthebbende en eventuele aanspraken van verzenders van digitale informatie op bescherming door de uitingsvrijheid of het recht op privacy. Met name het laatstgenoemde belang speelt in de praktijk een belangrijke rol. De informatieverplichting van artikel 8 handhavingsrichtlijn kan onder omstandigheden immers op gespannen voet komen te staan met het gegevensbeschermingsrecht. Dat dit een actueel probleem

74. Europees parlement, Commissie juridische zaken en interne markt, Ontwerpverslag over het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de maatregelen en procedures om de handhaving van intellectuele-eigendomsrechten te waarborgen, 11 november 2003, 2003/2004(COD), PE 332.534/10-19, p. 4-5.
75. Artikel 8 lid 3 aanhef en onder sub c bepaalt namelijk: "De leden 1 en 2 van dit artikel gelden onverminderd regelgeving waarbij (…) de aansprakelijkheid wegens misbruik van het recht op informatie wordt geregeld."
76. Zie hierover ook Groep gegevensbescherming artikel 29 2005, p. 8.

is, blijkt onder andere uit een aanbeveling van de artikel 29 werkgroep van de Europese Commissie.[77] Hierin schenkt de werkgroep bijzondere aandacht aan pogingen van auteursrechthebbenden om inbreukmakers op te sporen met medewerking van service providers.[78] Zij herbevestigt, onder verwijzing naar haar eerdere aanbeveling over anonimiteit op het internet[79] (zie par. 7.2), de noodzaak om pseudonieme en anonieme transacties toe te staan.[80] Aangezien de handhavingsrichtlijn, krachtens artikel 2 lid 3 sub a daarvan, niets afdoet aan de gelding van gegevensbeschermingsbeginselen, dienen ook auteursrechthebbenden en andere actoren, zoals service providers, zich daaraan te houden.[81] Over de verstrekking van persoonsgegevens zegt de werkgroep:

> "On the basis of the compatibility principle as well as in compliance with the confidentiality principle included in Directives 2002/58 and 95/46, data detained by ISPs processed for specific purposes including mainly the performance of a telecommunication service cannot be transferred to third parties such as right holders, except, in defined circumstances provided by law, to public law enforcement authorities."[82]

Deze passage lijkt uit te sluiten dat providers nog langer op vrijwillige basis identificerende gegevens zouden kunnen verstrekken aan rechthebbenden. Hiervoor is naar het oordeel van de werkgroep blijkbaar altijd tussenkomst van de rechter vereist.

Dat auteursrechthebbenden bij hun pogingen om filesharers te ontmaskeren rekening moeten houden met privacyregelgeving bleek ook in de procedure die Brein, de Stichting Bescherming Rechten Entertainment Industrie Nederland, aanspande tegen een vijftal providers.[83] Brein vorderde in kort geding de NAW-gegevens van 41 abonnees die zich schuldig zouden hebben gemaakt aan het aanbieden van ongeautoriseerde muziekbestan-

77. Groep gegevensbescherming artikel 29 2005. De werkgroep constateert meer in zijn algemeenheid dat de handhaving van het auteursrecht in toenemende mate verbonden is met de verwerking van persoongebonden informatie. Zij wijst in dit verband op de opkomst van zogenaamde 'Digital Rights Management Systemen' ('DRMs') en op de reeds eerder genoemde problematiek rondom het gebruik van openbare registers, zoals 'whois databases', bij pogingen om inbreukmakers te achterhalen (zie par. 8.3.1). De groep benadrukt dat DRM-technologieën zodanig moeten worden ingericht dat de anonimiteit van de gebruiker behouden blijft.
78. Interessant is de opmerking van de werkgroep dat het opsporen van inbreukmakers de laatste jaren makkelijker is geworden doordat met de komst van internet via kabel en ADSL aan gebruikers in plaats van dynamische nu voornamelijk permanente IP-adressen worden toegewezen. Zie Groep gegevensbescherming artikel 29 2005, p. 3.
79. Groep gegevensbescherming artikel 29 1997b.
80. Groep gegevensbescherming artikel 29 2005, p. 5-6.
81. Idem, p. 4.
82. Idem, p. 7.
83. Vzngr. Rb. Utrecht 12 juli 2005, KG-nr: 194741/KGZA 05-462, LJN: AT9073. Een uiteenzetting van de technische en juridische aspecten van peer-to-peer software en filesharing kan men vinden bij Alberdingk Thijm 2003; Van Daalen & Ekker 2003. De OECD heeft daarnaast een internationaal overzicht opgesteld van juridische procedures tegen aanbieders en gebruikers van file-sharingsoftware. OECD 2005, p. 98-104.

den. Om de daarbij benodigde IP-adressen te verkrijgen was een Amerikaans onderzoeksbureau ingeschakeld. De voorzieningenrechter stelde vast dat op het verzamelen van deze adressen de Wet bescherming persoonsgegevens (Wbp) van toepassing was (r.o. 4.23). De service providers konden naar zijn oordeel niet gedwongen worden tot het bekend maken van NAW-gegevens omdat aan de voorschriften van de Wbp in twee opzichten niet was voldaan. In de eerste plaats waren de in opdracht van Brein verzamelde IP-adressen geëxporteerd naar de Verenigde Staten, dat niet kan worden aangemerkt als een land met een passend beschermingsniveau voor persoonsgegevens in de zin van de Wbp. Bovendien had het onderzoeksbureau evenmin een zogenaamde 'Safe Harbour'-overeenkomst getekend, waarin zij zich conformeerde aan de Europese privacywaarborgen. Dit was te meer bezwaarlijk nu door de service providers voldoende aannemelijk was gemaakt dat het bureau ook de inhoud van 'shared folders' van de betrokken internetgebruikers had onderzocht. In deze folders bevonden zich ook niet-inbreukmakende bestanden met een persoonlijk karakter. De verwerking van de persoonsgegevens had zodoende plaatsgevonden op een wijze die niet te rijmen viel met een advies dat door het College bescherming persoonsgegevens over dit onderwerp was uitgebracht. In de tweede plaats was de nauwkeurigheid van de door Brein verzamelde gegevens door de providers in twijfel getrokken, welke twijfel door Brein niet in voldoende mate was weggenomen. De voorzieningenrechter merkte in dit verband op dat voor toewijzing van een vordering slechts plaats is indien buiten redelijke twijfel is dat de IP-adressen betrekking hebben op de gebruikers die daadwerkelijk illegaal muziek- of andere bestanden aanbieden op hun computer. Om vast te stellen vanaf welke computer de ongeautoriseerde muziekbestanden worden aangeboden dient nauwkeurig de datum en het tijdstip van de inbreukmakende handeling te worden bepaald. Dit impliceert dat moet worden aangegeven op welk moment derden van de desbetreffende computer bestanden hebben gedownload (r.o. 4.30).

9.7 Strafvorderlijke bevoegdheden

Een effectieve handhaving van het strafrecht vereist dat ook opsporingsinstanties in staat zijn om de identiteit van burgers te achterhalen. Het Wetboek van Strafvordering voorziet daarom in bevoegdheden om bij bepaalde instanties en personen identificerende gegevens te vorderen. Recentelijk zijn de bestaande bepalingen middels de wet bevoegdheden vorderen gegevens[84] en de wet vorderen gegevens telecommunicatie[85] aangevuld en gewijzigd.

84. Wet van 16 juli 2005 tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens), *Stb.* 2005, 390.
85. Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), *Stb.* 2004, 105.

Over de voorstellen tot wetswijziging was aan het kabinet advies uitgebracht door de commissie 'Strafvorderlijke gegevensvergaring in de informatiemaatschappij', ook aangeduid als de 'commissie Mevis'. Deze commissie constateerde dat de bestaande dwangmiddelen het opvragen van allerlei soorten gegevens bij bedrijven, zoals financiële gegevens, locatiegegevens van het gebruik van betaalpassen en gegevens over de aanschaf van producten, onvoldoende mogelijk maakten. Bovendien was vaak onduidelijk op welke basis gegevens verstrekt konden en mochten worden. Opsporingsambtenaren waren vaak aangewezen op vrijwillige verstrekking. De Wet bescherming persoonsgegevens staat vrijwillige verstrekking immers wel toe, maar voorziet niet in een verplichting.[86] De houder van de gegevens diende zodoende zelf af te wegen of verstrekking noodzakelijk was, terwijl hij vaak niet op de hoogte was van de relevante feiten en omstandigheden. Deze situatie leidde zowel voor de houder van de gegevens als voor de betrokken opsporingsinstanties tot rechtsonzekerheid. In de nieuwe regeling is de houder daarom verplicht om aan de vordering te voldoen, terwijl de verantwoordelijkheid voor de verstrekking bij de opsporingsinstantie ligt.[87]

De voorstellen van de commissie werden overwegend kritisch ontvangen.[88] Hoewel de nieuwe bepalingen meer duidelijkheid creëren over de wijze waarop verstrekking van gegevens dient plaats te vinden, wordt de positie van verdachte én onverdachte burgers volgens kritische auteurs aanmerkelijk verzwakt.[89] De nieuwe regeling betekent naar het oordeel van deze auteurs een vergaande informatieplicht voor burgers en bedrijfsleven, waar voorheen geen algemene strafvorderlijke medewerkingsverplichting bestond. De SP-fractie sprak, verwijzend naar een kritische publicatie van Asscher en Koops, van een "muisstille revolutie in het strafrecht".[90]

In deze paragraaf wordt specifiek ingegaan op situaties waarin het vorderen van gegevens raakt aan de uitingsvrijheid. Hiervan is bijvoorbeeld sprake wanneer de algemene bevoegdheden in het Wetboek van Strafvordering door een opsporingsambtenaar worden toegepast om de politieke of andere interesses van een burger in kaart te brengen door informatie op te vragen bij bibliotheken en soortgelijke instanties. Ook bij het vorderen van gegevens over telecommunicatie is er een verband met de uitingsvrijheid. Deze categorie van gegevens heeft immers betrekking op de identiteit van communicerende burgers en op communicatiehandelingen en -inhoud.

9.7.1 De Wet bevoegdheden vorderen gegevens

De nieuwe regeling in het Wetboek van Strafvordering voorziet in een getrapt stelsel van algemene bevoegdheden tot het vorderen van gegevens. Er wordt daarbij onderscheid

86. Mac Gillavry 2001, p. 1412.
87. *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 1.
88. Dommering 2001, Mac Gillavry 2001.
89. Mac Gillavry 2001, p. 1418.
90. *Kamerstukken II* 2003/04, 29 441, nr. 5. p. 3. Zie ook Asscher & Koops 2004.

gemaakt tussen verschillende categorieën van gegevens op basis van privacygevoeligheid.[91] De commissie Mevis beschouwde 'identificerende gegevens' als de minst privacygevoelige categorie. Krachtens artikel 126nc lid 1 Sv mogen deze gegevens daarom worden gevorderd door iedere opsporingsambtenaar. Dit artikellid luidt:

> "In geval van verdenking van een misdrijf kan de opsporingsambtenaar in het belang van het onderzoek van degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, vorderen bepaalde opgeslagen of vastgelegde identificerende gegevens van een persoon te verstrekken."

Identificerende gegevens zijn blijkens artikel 126 lid 2 Sv: naam, adres, woonplaats en postadres, geboortedatum, geslacht en administratieve kenmerken.[92] De bevoegdheid kan worden uitgeoefend jegens "degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt". Hieronder vallen bijvoorbeeld rechtspersonen en natuurlijke personen die, al dan niet op commerciële basis, diensten verlenen op het terrein van cultuur, sport, en vrijetijdsbesteding en die in dat kader gegevens verwerken, zoals overheidsdiensten, verenigingen en professionele dienstverleners. Gegevens die in dat kader verwerkt worden vallen volgens de wetgever buiten de strikt persoonlijke sfeer.

Identificerende gegevens die worden vastgelegd voor persoonlijk gebruik vallen buiten de bevoegdheid van artikel 126 lid 3 Sv. Deze gegevens kunnen uitsluitend worden gevorderd door de officier van justitie. De commissie Mevis was bevreesd dat de bevoegdheid tot het vorderen van identificerende gegevens de opsporingsambtenaar de bevoegdheid zou geven gegevens te vorderen van iemand die uitsluitend persoonlijke contacten onderhoudt met de persoon op wie het onderzoek zich richt. Dit zou als ingrijpend voor de persoonlijke levenssfeer kunnen worden ervaren.[93]

---

91. Onder het begrip gegevens wordt verstaan: informatie die is vastgelegd of opgeslagen op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7.
92. Administratieve kenmerken zijn de kenmerken die de relatie tussen de persoon die onderwerp is van onderzoek en de derde van wie de gegevens worden gevorderd aanduiden, dan wel de kenmerken van de diensten die de derde aan de persoon verleent. Het kan bijvoorbeeld gaan om een klantnummer, een nummer van een polis, een bankrekeningnummer, of een lidmaatschapsnummer. Een administratief kenmerk is met andere woorden het nummer of de code waaronder een persoon bekend is, of geregistreerd staat, of met behulp waarvan hij een dienst ontvangt of toegang heeft tot een dienst, dan wel waarmee een geboden dienst wordt aangeduid. Ook letters en andere tekens, alsmede biometrische gegevens zijn administratieve kenmerken. Het vorderen daarvan vergt naar het oordeel van de wetgever geen bijzondere regeling. Wanneer de opsporingsambtenaar voldoende heeft aan de gegevens omtrent naam, adres, woonplaats, geboortedatum en geslacht, dient hij de gegevens omtrent administratieve kenmerken overigens niet te vorderen. Zie *Kamerstukken II* 2003-2004, 29 441, nr. 3, p. 7 en 21.
93. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7-8.

De tweede categorie betreft 'andere dan identificerende gegevens'. Deze kunnen worden gevorderd op basis van artikel 126nd Sv:

> "In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, vorderen deze gegevens te verstrekken."

Onder deze bepaling vallen bijvoorbeeld gegevens over diensten die verleend zijn, zoals de duur, de data, de plaats en de aard van de dienstverlening en rekening- en betalingsgegevens. Deze gegevens zijn in een verder stadium van het opsporingsonderzoek van belang omdat zij inzicht kunnen geven in het gedragspatroon van een persoon, zijn feitelijke verblijfplaats en zijn bewegingen en financiële transacties. Volgens de commissie Mevis zijn zij meer omvattend en kunnen zij meer blootgeven van iemands persoonlijk leven dan identificerende gegevens. Daarom is voor deze categorie voorzien in sterkere waarborgen. Alleen de officier van justitie kan deze 'andere gegevens' vorderen in gevallen van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan.[94] Bij lichtere strafbare feiten is ingevolge artikel 126nd lid 6 Sv een voorafgaande schriftelijke machtiging van de rechter-commissaris vereist. De bevoegdheid in artikel 126nd omvat de lichtere bevoegdheid tot het vorderen van identificerende gegevens. Als de officier van justitie zowel identificerende als andere gegevens wenst te verkrijgen kan hij dus volstaan met één vordering.

De derde en meest privacygevoelige categorie omvat de 'gevoelige gegevens'. Het gaat hier om gegevens die 'vanwege hun aard een indringende inbreuk kunnen maken op de persoonlijke levenssfeer'.[95] In de bepalingen met betrekking tot het vorderen van identificerende gegevens en andere dan identificerende gegevens wordt nadrukkelijk bepaald dat op basis van de hierin opgenomen bevoegdheden geen gegevens mogen worden gevorderd die betrekking hebben op iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging (art. 126nc lid 3 en 126nd lid 2 Sv). Zodoende wordt aangesloten bij hetgeen bepaald is in artikel 16 van de Wet bescherming persoongegevens (zie par. 1.3). Wanneer vooraf vaststaat dat de te verkrijgen gegevens gevoelige gegevens zullen zijn, kan alleen worden gevorderd op basis van artikel 126nf Sv. Hiervan is bijvoorbeeld sprake wanneer de vordering is gericht tot een kerkgenootschap, een vakvereniging of een vereniging van personen die een bepaalde aandoening hebben. Gevoelige gegevens kunnen alleen worden gevorderd door de officier van justitie, met een machtiging van de rechter-commissaris in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan indien dat misdrijf, gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven, een ernstige inbreuk op de

94. Idem, p. 8.
95. Idem, p. 10.

rechtsorde oplevert (art. 126nf Sv). Wanneer op basis van een vordering tot identificerende of andere dan identificerende gegevens onbedoeld ook gevoelige gegevens worden verkregen, maakt dit de toepassing van die bevoegdheid niet met terugwerkende kracht onrechtmatig. Pas achteraf kan namelijk worden vastgesteld dat tussen de gevraagde gegevens ook gevoelige gegevens zitten. De op deze wijze verkregen gegevens kunnen dan ook voor het opsporingsonderzoek worden gebruikt.[96]

Het is de vraag in hoeverre het speciale regime voor gevoelige gegevens daadwerkelijke bescherming biedt. Zoals de wetgever ook zelf erkent, kan immers vaak pas worden vastgesteld dat een persoonsgegeven een gevoelig gegeven is wanneer kennisname al heeft plaatsgevonden. De PvdA-fractie wees er daarnaast op dat gevoelige gegevens vaak ook heel eenvoudig zijn af te leiden uit andere gegevens, bijvoorbeeld gegevens die betrekking hebben op het verkeer tussen een rekeninghouder en een bank. Het is niet duidelijk hoe wordt voorkomen dat er zonder machtiging van de rechter-commissaris toch gegevens worden verstrekt die vrij eenvoudig zijn te herleiden tot gevoelige gegevens. Indien bij het vorderen van identificerende gegevens of andere niet-gevoelige gegevens niet expliciet de mededeling wordt gedaan dat die gegevens geschoond moeten zijn of worden van alles wat is te herleiden tot gevoelige gegevens, dan is de bescherming door de rechter-commissaris in een groot aantal gevallen feitelijk illusoir.[97]

Een andere waarborg is de notificatieplicht in artikel 126 bb Sv.[98] Krachtens deze bepaling doet de officier van justitie aan de betrokkene schriftelijk mededeling van de uitoefening van bevoegdheden zodra het belang van het onderzoek dat toelaat. Ook hier is de daadwerkelijke effectiviteit weinig aannemelijk. Notificatie blijft namelijk achterwege, indien uitreiking van de mededeling 'redelijkerwijs niet mogelijk is'. Volgens Mac Gillavry betekent dit in de praktijk dat notificatie vrijwel nooit plaats zal vinden.[99] Bovendien is de verplichting krachtens het vierde lid niet toepasselijk bij het vorderen van identificerende gegevens.[100] Deze beperking wordt door de commissie Mevis wederom beargumenteerd met de stelling dat de bevraging van identificerende gegevens nauwelijks ingrijpend is te noemen.[101] Een verplichting tot notificatie zou bovendien een

96. Idem, p. 10-11.
97. *Kamerstukken II* 29 441, 2003/04, nr. 5, p. 4. Ook het College bescherming persoonsgegevens brengt in zijn advies naar voren dat bij het opvragen van identificerende gegevens sprake kan zijn van gevoelige gegevens, bijvoorbeeld indien adresgegevens worden gevraagd aan een kerkgenootschap. *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 18.
98. Zie voor een overzicht van de waarborgen het kabinetsstandpunt over het rapport van de commissie Mevis, *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 9.
99. Zie Mac Gillavry 2001, p. 1418.
100. In de wet vorderen gegevens telecommunicatie is de toepasselijkheid van de notificatieverplichting op het vorderen van identificerende gegevens uitgesloten in artikel 126na lid 3 Sv. De Nederlandse Orde van Advocaten (NOvA) en de leden van de D66-fractie meenden dat de notificatieplicht bij het vorderen van gebruikersgegevens ten onrechte buiten toepassing bleef. *Kamerstukken II* 2001/02, 28 059, nr. 4, p. 11.
101. Zie ook *Kamerstukken I* 2004/2005, 29441, C, p. 12.

onevenredig zware belasting opleveren voor de bevoegde autoriteit. Ook Mac Gillavry plaatst gezien deze overwegingen vraagtekens bij het uitgangspunt dat de bevraging van identificerende gegevens nauwelijks ingrijpend is.[102] Het vijfde lid van artikel 126bb Sv legt aan degene tot wie een vordering is gericht overigens de verplichting op om geheimhouding in acht te nemen omtrent al hetgeen hem terzake van de vordering bekend is.

Hoe de uitoefening van de nieuwe bevoegdheden een bedreiging kan vormen voor de uitingsvrijheid van burgers, met name het daaruit voortvloeiende recht om informatie te garen en te ontvangen, komt zeer duidelijk naar voren in de kritiek die vanuit de Nederlandse bibliotheken op het wetsvoorstel werd geuit.[103] De Federatie van Organisaties in het Bibliotheek, Informatie- en Documentatiewezen (FOBID) stuurde twee brieven aan de Commissie voor Justitie van de Eerste Kamer. Hierin stelde zij aan de orde dat te ruime mogelijkheden om informatie omtrent het leengedrag van burgers op te vragen indruisen tegen de doelstelling van bibliotheken om gebruikers onbelemmerde toegang tot informatiebronnen te verschaffen.[104] Met name de vrije toegang tot bibliotheken in het hoger onderwijs zou belemmerd kunnen worden. Het behoort immers tot de taak van deze bibliotheken om ook afwijkende meningen en afkeurenswaardige opvattingen te documenteren en voor studie beschikbaar te stellen. Deze bibliotheken bevatten zodoende vele publicaties die om technische of ideologische redenen de nieuwsgierigheid van opsporingsambtenaren kunnen wekken. Zo zouden studenten Biologie, Scheikunde, Natuurkunde of Medicijnen met bijvoorbeeld een Arabische achtergrond gemakkelijk het doelwit kunnen worden van misplaatste en ongerechtvaardigde belangstelling. Hetzelfde geldt voor studenten Culturele Studies, Middenoosten Studies, Sociale Wetenschappen en Geschiedenis die een in de ogen van de opsporingsinstanties ongezonde belangstelling aan de dag leggen voor theologische, filosofische, ideologische of dissidente publicaties. De beoogde bestrijding van terrorisme kan hierdoor gemakkelijk ontaarden in een vorm van moreel politietoezicht. De FOBID sprak de vrees uit dat de wetswijziging uiteindelijk zou kunnen leiden tot de ongewenste situatie dat bibliotheken gebruikers vooraf moeten waarschuwen dat lees- en leengedrag aanleiding kan zijn voor verdenking van het voornemen tot een strafbaar feit.[105]

In zijn reactie op de opmerkingen van de FOBID stelde de Minister van Justitie zich op het standpunt dat de regeling in het Wetboek van Strafvordering 'institutionele mechanismen' bevat die een te ruime toepassing van de bevoegdheden voorkomen. Zowel de vordering als het proces verbaal worden op schrift gesteld en dienen bepaalde informatie te bevatten. De grond voor het vorderen van gegevens moet bovendien gelegen zijn in "concrete strafbare feiten en omstandigheden die onderzocht worden", aldus de minister.[106] FOBID liet zich door deze argumenten mijns inziens terecht niet overtuigen. Ook na het

102. Mac Gillavry 2001, p. 1418.
103. De Wit 2005.
104. FOBID 2005a.
105. FOBID 2005b.
106. *Kamerstukken I* 2004/2005, 29441, C, p. 10-11.

antwoord van de minister bleef zij van mening dat sprake is van een onaanvaardbare inbreuk op de bescherming van de persoonlijke levenssfeer en een schending van het recht op vrije toegang tot informatie. Het is immers erg onduidelijk wat de minister bedoelt met 'omstandigheden die onderzocht worden'. FOBID wees er bovendien op dat de minister in zijn antwoord verdoezelde dat de nieuwe bevoegdheden ook kunnen worden aangewend om de gangen na te gaan van mensen die zich nog in het geheel niet aan iets schuldig hebben gemaakt en zelfs van mensen die de opsporingsambtenaar helemaal niet verdenkt van plannen om iets strafbaars te doen, maar die alleen in betrekking staan tot iemand die daar wel van verdacht wordt. Daar komt nog bij dat bestaande waarborgen, zoals de notificatieplicht, in de huidige praktijk al slecht worden nageleefd en bovendien in het belang van het onderzoek zeer makkelijk terzijde kunnen worden geschoven. Al met al rijst volgens FODID de verdenking "dat het wetsvoorstel wel degelijk bedoeld is om de overheid een vrijwel onbeperkte ruimte te bieden om de gangen van burgers na te gaan, ook wanneer zij niet van concrete feiten worden verdacht, maar enkel het wantrouwen van de overheid hebben gewekt of in relatie staan tot iemand die dat wantrouwen te beurt valt".[107]

Bij lezing van de kamerstukken dringt de vergelijking met de Verenigde Staten zich op. De Amerikaanse PATRIOT ACT die na de aanvallen op 11 september 2001 werd ingevoerd om terrorisme tegen te gaan, kent soortgelijke bepalingen.[108] Section 215 van deze wet stelt opsporingsambtenaren van de FBI in staat om bij iedere persoon of bedrijf 'tastbare dingen' op te vragen, waaronder boeken, bestanden, papieren, documenten en dergelijke.[109] De FBI hoeft geen 'probable cause' aannemelijk te maken. Notificatie aan de betrokkene wordt in het geheel achterwege gelaten en wie van de FBI een verzoek tot afgifte van 'tastbare dingen' heeft ontvangen mag dit bovendien niet melden aan anderen.[110] Zowel de Amerikaanse als de Nederlandse regeling zijn een reactie op de toegeno-

107. FOBID 2005c.
108. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001
109. Section 215 van de USA PATRIOT ACT bevat een aanpassing van Titel V van de Foreign Intelligence Surveillance Act van 1978 (50 U.S.C. 1861 et seq.). In deze wet wordt onder andere een nieuwe sectie 501 ingevoegd, getiteld 'Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations'. Subsectie (a)(1) van deze bepaling luidt: "The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."
110. Section 501(c) van de USA PATRIOT ACT luidt: "No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section." Zie voor een overzicht van de constitutionele bezwaren tegen de PATRIOT ACT de website van de American Civil Liberties Union (ACLU).

men dreiging van terrorisme. Nu criminaliteits- en terrorismebestrijding als gevolg van de maatschappelijke ontwikkelingen bovenaan de publieke en politieke agenda staan, worden de bezwaren van bibliotheken vrij gemakkelijk terzijde geschoven.

Het voorgaande neemt niet weg dat de bibliotheken over een krachtig argument beschikken. Onder het Amerikaanse recht kan men verwijzen naar het recht 'to communicate anonymously'. Te vergaande en ongeclausuleerde bevoegdheden om gegevens over leengedrag op te vragen kunnen in strijd komen met het First Amendment. In Europa kunnen de bibliotheken de anonimiteit van het leengedrag verdedigen met een beroep op de ontvangstvrijheid in artikel 10 EVRM (zie par. 7.1.3).

9.7.2 De Wet vorderen gegevens telecommunicatie

De hierboven geschetste problematiek doet zich ook voor buiten de papieren wereld van de traditionele bibliotheek. De wet vorderen gegevens telecommunicatie schept immers verruimde bevoegdheden tot het opvragen van gegevens die veel kunnen zeggen over communicatiehandelingen en -inhoud.[111] De uitoefening van deze bevoegdheden kan zodoende een beperking vormen van de uitingsvrijheid en het recht op privacy van gebruikers van elektronische communicatienetwerken en -diensten.

Het Wetboek van Strafvordering maakt waar het telecommunicatie betreft een onderscheid tussen twee categorieën van gegevens, te weten 'gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker', kortweg: 'gebruikersgegevens', en 'identificerende gegevens'. Gebruikersgegevens kunnen krachtens artikel 126n Sv door de officier van justitie worden gevorderd:

> "In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. De vordering kan slechts betrekking hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan gegevens betreffen die:
> a. ten tijde van de vordering zijn verwerkt, dan wel
> b. na het tijdstip van de vordering worden verwerkt."

Onder een gebruiker van telecommunicatie wordt krachtens het tweede lid van artikel 126n verstaan: "de natuurlijke persoon of rechtspersoon die met de aanbieder een overeenkomst is aangegaan met betrekking tot het gebruik van een openbaar telecommunicatienetwerk of de levering van een openbare telecommunicatiedienst, alsmede de natuurlijke persoon of rechtspersoon die daadwerkelijk gebruik maakt van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst". Krachtens het

111. Hoofdstuk 13 van de Telecommunicatiewet legt aan aanbieders van openbare telecommunicatienetwerken en -diensten de verplichting op om de gevorderde informatie te verstrekken.

derde lid kan de vordering worden gericht tot iedere aanbieder van een telecommunicatienetwerk of -dienst. De bevoegdheid kan alleen worden toegepast in geval van verdenking van een misdrijf waarvoor krachtens artikel 67, eerste lid Sv voorlopige hechtenis is toegestaan.

In het Besluit vorderen gegevens telecommunicatie is nader aangegeven op welke gegevens de vordering betrekking kan hebben.[112] Het besluit noemt de naam, het adres en de woonplaats van de gebruiker, de nummers van de gebruiker, de naam, het adres, de woonplaats en het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft, heeft gehad of heeft getracht tot stand te brengen, of van de natuurlijke persoon of rechtspersoon die heeft getracht met de gebruiker verbinding tot stand te brengen. Daarnaast vallen binnen de reikwijdte gegevens over datum, tijdstip en duur van de verbinding, locatiegegevens, nummers van randapparatuur, de soorten diensten waarvan gebruikt is gemaakt en naam, adres en woonplaats van degene die de rekening betaalt voor de telecommunicatiediensten en -netwerken. Het scala van gegevens dat in het Besluit vorderen gegevens telecommunicatie genoemd wordt, is zodoende ruimer dan de inhoud van het begrip verkeersgegevens in de privacyrichtlijnen en de Telecommunicatiewet. Zo bestrijkt het besluit ook NAW-gegevens om te voorkomen dat de officier van justitie gedwongen zou zijn telkens twee bevoegdheden toe te passen.[113] Doordat in de tekst van de artikelen 126n en 126u niet meer wordt gesproken over 'inlichtingen (…) terzake van alle verkeer', maar van "gegevens (…) over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker" is er geen misverstand over dat de NAW-gegevens onder de bevoegdheid begrepen kunnen worden.[114]

Het vorderen van identificerende gegevens is geregeld in artikel 126na Sv:

> "In geval van verdenking van een misdrijf kan de opsporingsambtenaar in het belang van het onderzoek een vordering doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie. Indien de gegevens niet bij de telecomaanbieder bekend zijn, kan de officier van justitie in het belang van het onderzoek vorderen dat hij deze op bij algemene maatregel van bestuur te bepalen wijze achterhaalt en verstrekt."

Deze bepaling verschilt in twee opzichten van de bepaling inzake gebruikersgegevens: hij kan worden toegepast bij verdenking van *alle* misdrijven en de vordering kan worden

112. Besluit van 3 augustus 2004, houdende aanwijzing van de gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker die van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst kunnen worden gevorderd (Besluit vorderen gegevens telecommunicatie), *Stb.* 2004, 394.
113. *Kamerstukken I* 2001/2002, 28 059, p. 20.
114. *Kamerstukken II* 2001/02, 28 059, nr. 3, p. 7-8. De CDA-fractie meende dat het enigszins vreemd was om NAW-gegevens in het Besluit vorderen gegevens telecommunicatie als verkeersgegevens aan te wijzen. *Kamerstukken II* 2001/02, 28 059, nr. 4, p. 9.

gedaan door iedere opsporingsambtenaar. Ook hier is dus minder bescherming toegekend aan de identificerende gegevens.

9.7.3 Kritiek

Zoals gezegd zijn tegen beide wetsvoorstellen reeds de nodige bezwaren naar voren gebracht. Daarom beperk ik mij hier tot die zaken die met de bescherming van de uitingsvrijheid in het achterhoofd het meest in het oog springen. Vanuit dat perspectief is met name van belang dat de commissie Mevis in haar rapport nauwelijks ingaat op het belang van andere grondrechten dan het recht op eerbiediging van de privacy. Hoewel de voorstellen van de commissie grotendeels een reactie waren op de ontwikkelingen van de informatiemaatschappij, wordt noch in het rapport van de commissie Mevis noch in de Memorie van Toelichting afdoende ingegaan op de impact die gegevensverstrekking juist in de context van elektronische communicatie kan hebben op de uitoefening van politieke grondrechten en de uitingsvrijheid. Ook in de Memorie van Toelichting bij de Wet vorderen gegevens telecommunicatie ligt de nadruk zeer sterk op de bescherming van de persoonlijke levenssfeer.[115] Het rapport getuigt daarnaast van weinig affiniteit met informatietechnologie. De noodzaak van de verruiming van bevoegdheden wordt beargumenteerd door te wijzen op digitalisering en de opkomst van automatische gegevensverwerking, maar vervolgens worden ter illustratie voornamelijk voorbeelden uit de offline wereld gegeven.

Dat aan de uitingsvrijheid weinig aandacht wordt besteed is vreemd nu de artikelen 126nc lid 3 en 126nd lid 2 Sv wel uitdrukkelijk een verhoogde mate van bescherming toekennen aan gegevens die betrekking hebben op iemands godsdienst of levensovertuiging, ras, politieke gezindheid, seksuele leven en lidmaatschap van een vakvereniging. Het had voor de hand gelegen om ook voor situaties waarin van te voren vaststaat dat het toepassing van de bevoegdheden een beperking vormt van de uitingsvrijheid te voorzien in extra waarborgen. Waarschijnlijk is deze lacune te wijten aan het feit dat de commissie Mevis voor de bescherming van gevoelige gegevens heeft aangesloten bij het regime aangaande de bescherming van bijzondere persoonsgegevens in de Wet bescherming persoonsgegevens. Zoals eerder werd geconstateerd wordt ook daar de uitingsvrijheid niet genoemd (zie par. 7.3). Deze weeffout in de Wet bescherming persoonsgegevens is dus overgenomen in het Wetboek van Strafvordering.

In de Wet vorderen gegevens telecommunicatie ontbreekt een bijzonder regime voor gevoelige persoonsgegevens. Het is gissen naar de reden van dit verschil tussen beide regelingen. Waarschijnlijk is de wetgever er van uitgegaan dat gegevens over telecommunicatie in zijn algemeenheid niet als gevoelige gegevens kunnen worden aangemerkt. Een telecomaanbieder lijkt op het eerste gezicht niet een instantie die dergelijke gegevens uit de aard van zijn functie verwerkt, zoals een kerkgenootschap of een vakbond. Zoals in de voor-

115. *Kamerstukken II* 2001/02, 28 059, nr. 3, p. 3-4.

gaande hoofdstukken is gebleken, kan de opslag en verwerking van gegevens over (elektronische) communicatie echter zeer wel raken aan de uitoefening van constitutionele rechten. Voorzover de wetgever, door in de telecomspecifieke regeling geen aparte bescherming voor bijzondere gegevens op te nemen, tot uitdrukking heeft willen brengen dat aan communicatie gerelateerde identificerende gegevens niet, of in mindere mate, raken aan de uitoefening van grondrechten, geeft hij mijns inziens blijk van een onjuiste opvatting.

Een tweede bezwaar tegen de juridische onderbouwing van de bevoegdheden geldt de wijze waarop de privacygevoeligheid van verschillende categorieën gegevens wordt beargumenteerd. In beide wettelijke regelingen is aan identificerende gegevens een minder hoog beschermingsniveau toegekend dan aan andere categorieën van gegevens. Identificerende gegevens kunnen immers worden opgevraagd door iedere opsporingsambtenaar, terwijl tot kennisname van 'andere dan identificerende gegevens' alleen de officier van justitie bevoegd is.[116] De commissie Mevis had bij de voorbereiding van haar advies nog overwogen de bevoegdheid om identificerende gegevens op te vragen, in plaats van bij de opsporingsambtenaar, bij de officier van justitie neer te leggen, dan wel de officier van justitie de vordering te laten toetsen. Zij hechtte er veel belang aan dat de strafvorderlijke autoriteiten bij toepassingen van de bevoegdheden een nadrukkelijke afweging maken van de proportionaliteit en subsidiariteit van de vordering. Uiteindelijk werd van deze mogelijkheid toch afgezien. De commissie motiveerde deze beslissing als volgt:

> "De vergaring van identificerende gegevens, voor zover die niet gevoelige gegevens betreft, wordt in het algemeen als minder van betekenis beschouwd voor de persoonlijke levenssfeer. De gegevens waar het hier om gaat zijn door alle houders van gegevens eenvoudig te verstrekken. (…) Het past niet in het huidige strafvorderlijk systeem, in een dergelijk geval de bevoegdheid toe te delen aan de officier van justitie."[117]

De stelling dat identificerende gegevens minder privacygevoelig zijn vindt men in het kabinetsstandpunt over het rapport van de commissie Mevis en in de Memorie van Toelichting bij de wet vorderen gegevens en de wet vorderen gegevens telecommunicatie een aantal keren terug. Zo wordt in het kabinetsstandpunt over het rapport van de commissie Mevis het volgende overwogen:

> "De mate waarin de persoonlijke levenssfeer van degene op wie de gegevens betrekking hebben in het geding is, verschilt per bevoegdheid. Zo kan de bevoegdheid tot het vorderen van identificerende gegevens in beperkte mate raken aan de persoonlijke levenssfeer, terwijl de bevoegdheid tot het vorderen van gevoelige gegevens in grote mate aan de persoonlijke levenssfeer kan raken."[118]

116. Onder identificerende gegevens verstaat de commissie de naam, het adres en de woonplaats van een persoon, diens geboortedatum en geslacht, alsmede het gegeven of deze persoon een bepaalde dienst afneemt van of anderszins een relatie onderhoudt met de houder van de gegevens en – indien dit het geval is – onder welk nummer of kenmerk dit gebeurt. Zie Rapport Mevis 2001, p. 51.
117. Rapport Mevis 2001, p. 73.

Dit standpunt wordt nergens nader gemotiveerd. Het lijkt erop dat het door de wetgever klakkeloos is overgenomen van de commissie Mevis. De geciteerde passage schept bovendien verwarring omdat ten onrechte de indruk wordt gewekt dat de bescherming van gevoelige gegevens primair bedoeld is om de persoonlijke levenssfeer te beschermen.

Het onderscheid in privacygevoeligheid wordt gepresenteerd als een juridische vanzelfsprekendheid. Mijns inziens gaat achter dit onderscheid in werkelijkheid echter het verlangen schuil om bij de uitoefening van bevoegdheden zo min mogelijk gehinderd te worden door grondrechtelijke aanspraken van burgers. Dit schemert ook door in de argumentatie van de commissie Mevis. De commissie wijst er immers op dat identificerende gegevens met name in de beginfase van het strafvorderlijk onderzoek van cruciaal belang zijn omdat aan de hand hiervan kan worden vastgesteld met welke personen men van doen heeft. Met behulp van identificerende gegevens kunnen verbanden worden gelegd tussen situaties en personen. Identificerende gegevens zijn daarnaast benodigd om bepaalde strafvorderlijke bevoegdheden toe te kunnen passen, bijvoorbeeld de bevoegdheid tot het vorderen van gegevens uit een geautomatiseerd werk of de bevoegdheid tot inbeslagneming. De commissie stelt zich dan ook op het standpunt dat de vergaring van deze gegevens gelet op de behoefte hieraan (sic!) in elk strafvorderlijk onderzoek in beginsel mogelijk moet zijn ter opsporing van elk strafbaar feit, voor het onderzoek naar het in georganiseerd verband beramen of plegen van ernstige misdrijven en voor het verkennend onderzoek.[119] Te veel privacywaarborgen zouden de opsporing in de ogen van de commissie waarschijnlijk te veel belemmeren.

In plaats van te erkennen dat zij het belang van het recht op privacy in de beschreven situaties minder zwaarwegend achten, verschuilen commissie en wetgever zich achter het

118. Zie *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 7, p. 13 en p. 15. In de Memorie van Toelichting bij het wetsvoorstel vorderen gegevens wordt dit uitgangspunt in andere bewoordingen herhaald: 'andere dan identificerende gegevens' zouden meer omvattend zijn en zij zouden meer kunnen blootgeven van iemands persoonlijk leven dan identificerende gegevens. Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.

119. Rapport Mevis 2001, p. 51. Deze zienswijze is door het kabinet overgenomen: "Voor de vraag in welke gevallen de bevoegdheid tot het vorderen van identificerende gegevens moet zijn toegestaan is het van belang dat de categorie identificerende gegevens een beperkte categorie gegevens betreft die op zichzelf slechts in beperkte mate kan raken aan de persoonlijke levenssfeer en waarvan de vordering niet zeer belastend is voor de houder van de gegevens. Om die reden kan zij in meer gevallen zijn toegestaan dan de bevoegdheid tot het vorderen van andere dan identificerende gegevens. Daarnaast is van belang dat de zogenaamde identificerende gegevens de basis vormen van het opsporingsonderzoek, met name bij de start daarvan. Cruciaal is immers vast te kunnen stellen met welke personen men van doen heeft in het opsporingsonderzoek en verbanden te kunnen leggen tussen situaties en personen. Identificerende gegevens zijn ook nodig alvorens andere bevoegdheden kunnen worden toegepast. Het belang dat de tot opsporing bevoegde instanties bij deze categorie gegevens hebben is daarom groot. Om die reden dient de bevoegdheid beschikbaar te zijn voor een ruimere categorie strafbare feiten dan die is omschreven in artikel 67, eerste lid, Sv." Zie het kabinetsstandpunt over het rapport 'Gegevensvergaring in strafvordering' van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij. *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 13.

standpunt dat identificerende gegevens minder privacygevoelig zijn dan 'andere gegevens'. Mijns inziens betreft het hier een gelegenheidsargument en is deze visie onvoldoende gemotiveerd en onjuist.[120] Uit het rapport van de commissie Mevis blijkt duidelijk dat identificerende gegevens onmisbaar zijn bij de opsporing omdat zij toegang geven tot de persoonlijke levenssfeer van verdachte en onverdachte burgers. Hieruit volgt logischerwijs dat kennisname van die gegevens een zware inbreuk op die persoonlijke levenssfeer met zich mee kan brengen. Identificatie is als het ware het moment waarop men de staatsvrije sfeer van het individu binnendringt. Inbreuken op de persoonlijke levenssfeer zijn pas mogelijk vanaf het moment dat gegevens en handelingen aan een persoon kunnen worden gekoppeld. De Wet bescherming persoonsgegevens is precies om die reden toepasselijk zodra gegevens betrekking hebben op een *identificeerbare* natuurlijke persoon.

9.8 Conclusie

In geldende regelgeving en jurisprudentie bestaan verschillende juridische grondslagen voor verstrekking van identificerende gegevens. De belangen die met de verstrekking zijn gediend zijn verschillend van karakter en zij lopen uiteen van algemeen tot zeer specifiek. De meest algemene regeling vindt men in de Wet bescherming persoonsgegevens. Artikel 8 sub f Wbp ziet immers op de verwerking van alle persoonsgegevens. Deze bepaling schept een algemene bevoegdheid voor iedere 'verantwoordelijke voor de gegevensverwerking' in de zin van de Wbp om zelfstandig en op vrijwillige basis persoonsgegevens te verstrekken. De Wbp en Memorie van Toelichting bij deze wet vermelden de criteria waaraan bij de verstrekking getoetst moet worden. De verantwoordelijke dient bij de beoordeling van verzoeken tot verstrekking bovendien een afweging te maken tussen het gerechtvaardigde belang van de verantwoordelijke of een derde enerzijds en de fundamentele rechten en vrijheden van de betrokkene anderzijds. Daartoe moet eerst worden vastgesteld of werkelijk sprake is van een belang dat de verwerking van persoonsgegevens rechtvaardigt. Indien de verwerking een inbreuk maakt op de belangen of fundamentele rechten van de betrokkene, dan moet worden beoordeeld of verstrekking proportioneel is en of voldaan is aan het vereiste van subsidiariteit.

Artikel 15 lid 2 van de richtlijn elektronische handel kwam aan de orde als een mogelijke grondslag voor wettelijke mogelijkheden tot verplichte verstrekking. Deze bepaling schept geen directe bevoegdheden om identificerende gegevens te vorderen danwel te verstrekken maar creëert slechts een mogelijkheid voor lidstaten om verplichtingen daartoe in het leven te roepen. De introductie van een zodanige verplichting dient blijkens de richtlijn specifiek de bestrijding van strafbare feiten in de digitale omgeving, hoewel een behoorlijk aantal lidstaten ook heeft voorzien in civielrechtelijke bepalingen. De richtlijn

120. Ook Mac Gillavry bestrijdt dit uitgangspunt van de commissie Mevis. Mac Gillavry 2001, p. 1418.

bepaalt niet hoe een verplichting tot verstrekking moet worden geformuleerd, noch welke criteria bij de verstrekking moeten worden gehanteerd. Afweging met de belangen van de provider of de anonieme gebruiker is evenmin voorgeschreven. De formulering van artikel 15 lid 2 roept daarnaast een aantal vragen op. Zo is niet aangegeven wat verstaan dient te worden onder 'bevoegde autoriteiten' en is onduidelijk waarom het artikel alleen van toepassing is op hosting. De Nederlandse wetgever hangt wat dat laatste betreft een 'technologieneutrale' interpretatie aan. In de Nederlandse implementatie van de richtlijn zijn overigens geen bepalingen over de verstrekking van identificerende gegevens opgenomen. Wel heeft de wetgever te kennen gegeven dat de verstrekking van identificerende gegevens geen voorwaarde mag zijn voor de uitsluiting van aansprakelijkheid van informatie in de zin van afdeling vier van de richtlijn elektronische handel.

In de civielrechtelijke jurisprudentie dient de verstrekking de bestrijding van onrechtmatige digitale informatie, het voorkomen van de verdere verspreiding van die informatie en het verhalen van schade. De door het Hof Amsterdam in *Pessers/Lycos* aanvaarde stappentoets is afgeleid van de Wet bescherming persoonsgegevens, maar meer toegespitst op de problemen rond anonimiteit op het internet. Deze toets betreft niet de verwerking van persoonsgegevens in zijn algemeenheid maar de verstrekking van NAW-gegevens over internetgebruikers in het bijzonder en ziet zodoende op een afgebakende reeks van gevallen, te weten situaties waarin een civiele derde partij de identiteit van een internetgebruiker wenst te achterhalen. Voorafgaand aan de verstrekking vindt een duidelijke afweging plaats tussen de verschillende bij de verstrekking betrokken belangen, waarbij ook aandacht is voor de grondrechtelijke aanspraken van de anonieme internetgebruiker.

Vergelijkt men de Nederlandse civielrechtelijke jurisprudentie met de Amerikaanse John Doe procedure die hiervoor werd besproken in hoofdstuk 4, dan valt een aantal zaken op. Allereerst ontlenen internetgebruikers in de Verenigde Staten aan het First Amendment een zelfstandig recht om anoniem te communiceren. Dit dwingt de rechter om grondrechtelijke aanspraken serieus te nemen en in zijn afweging te betrekken. Doordat de bescherming van anonieme uitingen zowel in de fysieke als in de digitale wereld is gebracht onder één en hetzelfde leerstuk is bovendien sprake van een meer consistente benadering. De onduidelijkheid over de grondslag van de verstrekking speelt in de Verenigde Staten niet. Daar kan in pre trial discovery immers gebruik worden gemaakt van de zogenaamde 'subpoena duces tecum'. Kijkt men naar de procedurele aspecten dan blijkt dat het Californische systeem afwijkt van het Nederlandse door de daar bestaande mogelijkheid om de procedure aan te spannen tegen de anonymus zelf. Welke gevolgen deze omstandigheid heeft voor het verdere verloop van het geding is in het voorgaande beschreven.

De criteria waaraan John Doe subpoenas worden getoetst zijn in grote lijnen vergelijkbaar met de standaard die het Hof Amsterdam hanteert. De in een John Doe procedure gestelde eis dat sprake is van een 'prima facie case' komt ongeveer op hetzelfde neer als de door het Hof Amsterdam gestelde eis dat onrechtmatigheid voldoende aannemelijk is. De Amerikaanse balancing tests stellen daarnaast evenals het Hof Amsterdam de eis van proportionaliteit en subsidiariteit. Wel bestaat in het Californische recht meer

aandacht voor procedurele waarborgen ten behoeve van de anonymus. Dit komt onder andere tot uitdrukking in de in veel staten bestaande 'anti-SLAPP statutes' en in de door sommige rechters aan de eiser opgelegde verplichting om de anonymus te notificeren.

De totstandkoming van de handhavingsrichtlijn, in het bijzonder artikel 8 daarvan, heeft enkele belangrijke consequenties voor gegevensverstrekking binnen het intellectuele-eigendomsrecht. In de eerste plaats is hiermee naar men mag aannemen de discussie over de grondslag van de verstrekking binnen dat rechtsgebied geëindigd. Belangrijk is daarnaast dat artikel 8, in tegenstelling tot de Nederlandse civielrechtelijke jurisprudentie over het noemen van de voorman, is toegespitst op de digitale omgeving en dat zowel in de bewoordingen van deze bepalingen als in de toelichting daarop aandacht bestaat voor de grondrechtelijke belangen die bij de verspreiding van digitale informatie een rol spelen. Een vraag die nog moet worden beantwoord is in hoeverre het wenselijk is dat providers bij verzoeken tot verstrekking wegens beweerdelijke auteursrechtinbreuk vrijwillig en op basis van een zelfstandige afweging verstrekken. De artikel 29-werkgroep lijkt een dergelijke gang van zaken onwenselijk te vinden.

Waar bij de civielrechtelijke verstrekking van NAW-gegevens door de provider van geval tot geval een afweging moet worden gemaakt, heeft deze afweging in de strafvordering reeds vooraf plaatsgevonden. De strafvorderlijke bevoegdheden tot het vorderen van identificerende gegevens over gebruikers van telecommunicatienetwerken en -diensten zijn in de wet vastgelegd en kunnen worden toegepast wanneer is voldaan aan de daar omschreven criteria. Het belang van de opsporing weegt dan zwaarder dan de fundamentele rechten van de verdachte. Identificerende gegevens kunnen zowel in de algemene als in de telecomspecifieke regeling bij verdenking van een misdrijf door iedere opsporingsambtenaar worden opgevraagd. Zodoende geniet deze categorie van gegevens het laagste niveau van bescherming.

Het strafrechtelijke regime voor tussenpersonen online verschilt op een aantal essentiële punten met het drukkers- en uitgeversprivilege. In die laatste regeling is het bekend maken van de vermoedelijke dader een voorwaarde om aansprakelijkheid voor de drukpersdelicten te ontlopen. Deze verplichting ontstaat echter pas op het moment dat door de rechter-commissaris een gerechtelijk vooronderzoek naar het drukpersdelict is gestart en er een aanmaning van de Officier van Justitie is uitgegaan. De nieuwe strafvorderlijke bevoegdheden tot het opvragen van identificerende gegevens staan daarentegen op zichzelf en kunnen bij verdenking van een misdrijf door iedere opsporingsambtenaar worden uitgeoefend. Verstrekking van identificerende gegevens kan hier volgens de Nederlandse wetgever geen voorwaarde zijn voor uitsluiting van aansprakelijkheid voor de inhoud.

De doorbreking van de blokkering van nummeridentificatie bij hinderlijke en kwaadwillige oproepen werd behandeld in hoofdstuk 7 (zie par. 8.3.2).[121] Deze regeling is

121. Dit onderwerp is in hoofdstuk zeven besproken omdat daar ook andere bepalingen uit de Telecommunicatiewet aan de orde kwamen.

alleen van toepassing op telefonie en geeft abonnees de mogelijkheid om bij hun telecommunicatieaanbieder een verzoek tot verstrekking van NAW-gegevens in te dienen. Het verzoek wordt beoordeeld door de aanbieder. De Memorie van Toelichting bij de Telecommunicatiewet geeft als criteria voor de beoordeling van het verzoeken slechts dat deze van geval tot geval moeten worden beoordeeld en dat in ieder geval sprake moet zijn van "een bepaald belpatroon dat in het maatschappelijk verkeer als hinderlijk moet worden gekarakteriseerd". In de praktijk komt het er op neer dat de telefonieaanbieder aan de hand van de frequentie van de oproepen en de beweringen van de getroffen gebruiker dient te beoordelen of inderdaad sprake is van stalking. Een belangrijk verschil met de verstrekking van NAW-gegevens door internetproviders is in dat verband dat de laatsten het verzoek van de eiser vaak kunnen beoordelen aan de hand van de door de eiser als onrechtmatig bestempelde informatie. Deze informatie is in de meeste gevallen immers openbaar, want toegankelijk gemaakt op een website. Bij stalking in de sfeer van telefonie is hiervan geen sprake. Vaak bestaat het stalken immers alleen uit het herhaaldelijk opbellen van een persoon, zonder dat een gesprek tot stand komt. Ook als er wel een verbinding tot stand komt hebben telefonieaanbieders in principe geen toegang tot de inhoud van de als hinderlijk of kwaadwillig ervaren gesprekken. Het is hen in verband met het communicatiegeheim immers niet toegestaan daarvan kennis te nemen.

Geconcludeerd kan worden dat in de behandelde rechtsgebieden op zeer uiteenlopende wijze wordt omgegaan met vorderingen tot verstrekking van identificerende gegevens. Bij de afweging van belangen worden verschillende criteria gehanteerd. De beoordeling van de verstrekking is in de richtlijn elektronische handel en de handhavingsrichtlijn voorbehouden aan de 'bevoegde autoriteiten' respectievelijk 'de bevoegde rechterlijke instanties', maar wordt in andere gevallen overgelaten aan de tussenpersoon. Wanneer een tussenpersoon vrijwillige verstrekking op basis van de Wet bescherming persoonsgegevens weigert, kan het voorkomen dat een verzoek tot verstrekking aan de rechter wordt voorgelegd. In de strafvorderlijke sfeer ligt de afweging daarentegen reeds in de wet besloten.

Erkenning van grondrechtelijke implicaties

Het effect dat ruime mogelijkheden tot verstrekking van identificerende gegevens kunnen hebben op de uitoefening van communicatiegrondrechten wordt niet in alle behandelde rechtsgebieden even duidelijk erkend. Met name in de strafvordering wordt hieraan te weinig aandacht besteed. Het rapport van de commissie Mevis bevat een magere analyse waarin de verhouding met andere rechten dan het recht op privacy onvoldoende wordt opgemerkt. Daarnaast bestaat in regelgeving en rechtspraak te weinig aandacht voor andere grondrechten dan het recht op bescherming van de persoonlijke levenssfeer. De vernauwde blik van het gegevensbeschermingsrecht leidt te vaak tot een eenzijdige benadering.

In de civielrechtelijke context bestaat, met name in de rechtspraak, wel een groeiende aandacht voor de constitutionele implicaties. Dit blijkt met name uit de uitspraak van

het Hof Amsterdam in *Presser/Lycos*. In de civiele rechtspraak is het besef doorgedrongen dat doorbreking van anonimiteit een op zichzelf staand juridisch probleem is waaraan in de sfeer van communicatie grondrechtelijke belangen zijn verbonden. Dit probleem kan niet kan worden afgedaan als een deelprobleem van de aansprakelijkheid voor informatie. Deze ontwikkeling valt samen met de in het vorige hoofdstuk geconstateerde subjectiveringstendens, die inhoudt dat aan de eindgebruiker in toenemende mate bevoegdheden worden verleend om eigenhandig zijn anonimiteit te beschermen.

De bestaande theorievorming over de betekenis van anonimiteit en identificatie in de informatiesamenleving is op bepaalde punten inconsequent en onvoldoende doordacht. Zo heeft de wetgever weinig oog voor de afbakeningsproblemen die voortvloeien uit de door hem zelf geconstateerde 'contextafhankelijkheid'. Zowel in de Wet bescherming persoonsgegevens als in de strafvorderlijke regeling met betrekking tot het vorderen van identificerende gegevens bestaat de neiging gegevens bij voorbaat in te delen in categorieën met een daaraan gekoppeld oordeel over privacygevoeligheid en het vereiste niveau van bescherming. Ook in de digitale omgeving blijft men uitgaan van de vooronderstelling dat er een duidelijk onderscheid kan worden gemaakt tussen communicatie-inhoud, 'gegevens over communicatie' en identificerende gegevens. Moderne communicatietechnologieën ondergraven dit onderscheid echter en stellen de huidige systematiek van het gegevensbeschermingsrecht daarmee op de proef. De impact die kennisname van gegevens in een concrete situatie heeft op de uitoefening van de uitingsvrijheid en politieke grondrechten kan vaak niet van te voren worden vastgesteld. De wetgever is daarnaast niet consequent in haar oordeel over de privacygevoeligheid van identificerende gegevens. Met name het niet verder gemotiveerde uitgangspunt dat kennisname van identificerende gegevens in de strafvordering een minder zware inbreuk op de persoonlijke levenssfeer zou zijn dan kennisname van andere gegevens is onvoldoende gemotiveerd en onjuist.

De positie van de eindgebruiker

De vraagstelling van dit hoofdstuk leidt ertoe dat de juridische problemen rondom verstrekking voornamelijk wordt beschouwd vanuit het perspectief van de eiser. Dit onderzoek bedoelt echter juist ook aandacht te besteden aan de belangen van de anonymus. In dat verband verdient hier met name het recht op notificatie enige aandacht. Voor de eindgebruiker van wie identificerende gegevens worden verstrekt telt niet alleen of zijn grondrechtelijke aanspraken worden meegewogen maar ook of hij op de hoogte wordt gebracht van een vordering tot verstrekking of van de verstrekking zelf. De vraag rijst in hoeverre er op de tussenpersoon, of op andere instanties, een verplichting zou kunnen rusten om de betrokkene te notificeren van de verstrekking en of het wenselijk is om een dergelijke verplichting wettelijk te regelen. Een sterk argument voor een notificatieplicht is het feit dat een betrokkene alleen tegen een beperking van zijn rechten op kan komen als hij weet dat die beperking heeft plaatsgevonden. Notificatie stelt de betrokkene in staat om de verstrekker ter verantwoording te roepen voor een schending van zijn rech-

ten. Naar aanleiding van de invoering van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten is door verschillende juristen betoogd dat uit artikel 8 EVRM bij beperkingen op artikel 12 Gw (het huisrecht) en artikel 13 Gw (het brief-, telefoon- en telegraafgeheim) een notificatieplicht voortvloeit.[122] Dit standpunt werd door de regering echter niet gedeeld.[123]

Een verplichting om de betrokkene te notificeren van het feit dat zijn identificerende gegevens zijn verstrekt bestaat in het Nederlandse recht alleen bij de doorbreking van de blokkering van nummeridentificatie. Artikel 11.11 lid 6 Tw bepaalt immers dat van de gegevensverstrekking aan een verzoeker door de aanbieder mededeling wordt gedaan aan de abonnee wiens gegevens het betreft (zie par. 8.3.2). Uit de tekst van deze bepaling wordt niet duidelijk op welk moment de notificatie dient te geschieden. Een verplichting om de betreffende abonnee *voorafgaand* aan de verstrekking op de hoogte te stellen volgt hieruit in ieder geval niet. Ook de Wbp voorziet niet in een voorafgaande notificatieverplichting. Artikel 34 Wbp bevat weliswaar een informatieplicht voor de betrokkene, inhoudende dat hij bij verkrijging van persoonsgegevens buiten de betrokkene om verplicht is om hem de verkregen informatie mee te delen, maar dit mag krachtens die bepaling ook geschieden op het moment van de eerste verstrekking. Bovendien mag de mededeling achterwege worden gelaten wanneer mededeling onmogelijk blijkt of een onevenredige inspanning kost (zie par. 8.2.1). De Wet bevoegdheden vorderen gegevens bevat wel een notificatieplicht, maar deze geldt niet bij het vorderen van identificerende gegevens en is, om onduidelijke redenen, niet opgenomen in de telecomspecifieke regeling.

De mogelijkheid om de anonieme internetgebruiker voorafgaand te notificeren van het verzoek danwel het voornemen tot verstrekking van identificerende gegevens verdient met name aandacht waar het de civielrechtelijke verstrekking betreft. In hoofdstuk 4 bleek reeds dat een verplichting tot voorafgaande notificatie in de Amerikaanse rechtspraak al aan de orde is geweest. Ook het daar besproken Californische wetsvoorstel ter bescherming van anonieme gedaagden voorziet in een dergelijke verplichting (zie par. 4.3). Wil het voor een anonieme internetgebruiker mogelijk zijn om zich op basis van artikel 40 lid 1 Wbp tegen de verstrekking van zijn gegevens te verzetten (zie

122. Zie bijvoorbeeld Van der Pot Donner 2001, p. 354; De Graaff & Janse de Jonge 1999, p. 1930; Hofman 1995, p. 489; *NJCM* 1999, p. 314. De genoemde auteurs brengen voor hun standpunt een aantal argumenten naar voren. In de eerste plaats zal het recht op een daadwerkelijk rechtsmiddel van artikel 13 EVRM zonder notificatie in veel gevallen niet geëffectueerd kunnen worden. Bovendien is de effectiviteit van controle en toezichtmechanismen grotendeels afhankelijk van klachten die worden ingediend. Als geen mededeling wordt gedaan van de uitoefening van inbreukmakende bevoegdheden zullen deze klachten achterwege blijven. Tenslotte wordt betoogd dat controle op initiatief van de betrokkene het meest effectief is en niet kan worden vervangen door het, overigens ook zeer belangrijke, toezicht door onafhankelijke instanties. Zie *NJCM* 1999, p. 315. Zie ook Ekker 2002a.

123. *Kamerstukken II* 2000/01, 27 460, nr. 1, p. 29.

par. 8.2.1) dan lijkt het raadzaam ook in het Nederlandse recht de introductie van een voorafgaande notificatieverplichting te overwegen.

Techniekafhankelijke regulering

De verstrekking van identificerende gegevens is tot op zekere hoogte techniekafhankelijk gereguleerd. Vraagstukken rondom de identificatie van gebruikers worden, afhankelijk van de technische kenmerken van het gebruikte communicatiemiddel, afgehandeld via afzonderlijke regimes. Als gevolg van technische ontwikkelingen valt met name een scheiding aan te wijzen tussen het domein van de klassieke telefonie en datgene wat daar buiten valt. Dit wordt bijvoorbeeld duidelijk wanneer men de regels omtrent de doorbreking van de blokkering van nummeridentificatie vergelijkt met die omtrent de verstrekking van identificerende gegevens van een internetgebruiker of de verzender van een anonieme e-mail. Is de anonieme gebruiker een afnemer van een telefoniedienst, dan is de specifieke regeling in de Telecommunicatiewet van toepassing (zie par. 8.3.2). Betreft het daarentegen een klant van een internetprovider, dan is de verstrekking onderworpen aan de algemene regeling van de Wet bescherming persoonsgegevens (zie par. 9.3). Hoewel het hier in essentie gaat om hetzelfde probleem, wordt het verzoek tot verstrekking beoordeeld aan de hand van verschillende criteria.[124] Vanuit het perspectief van de eindgebruiker leidt deze situatie tot een wirwar van juridische normen en tot een ongerechtvaardigd verschil in beschermingsniveau.[125] Het zou voor de bescherming van de eindgebruiker immers niets uit moeten maken van welk communicatiemiddel hij gebruikt maakt. Bovendien zal de bestaande scheiding door convergentie van communicatietechnieken steeds problematischer worden. Het is bijvoorbeeld de vraag welk kader van toepassing is als verzoeken tot verstrekking zich in de toekomst voordoen bij internettelefonie.

Knelpunten bij de civielrechtelijke verstrekking door de internetprovider

In het Nederlandse recht is het niet mogelijk om een civiele dagvaarding uit te brengen aan een anonieme internetgebruiker. Dit betekent in veel gevallen dat civiele procedures

124. Ook de regels omtrent de opname van gegevens in abonneelijsten en het 'omgekeerd zoeken' zijn techniekafhankelijk geformuleerd. Het verschil in beschermingsniveau tussen 'omgekeerd zoeken' bij telefoonnummers en bij domeinnamen hangt samen met de omstandigheid dat de regulering van telefonie is onderworpen aan het publiekrecht en de regulering van domeinnamen aan het privaatrecht. Dit betekent overigens ook dat het afdwingen van bescherming bij domeinnamen hogere kosten met zich meebrengt. Zie de bespreking van whois databanken in par. 8.3.1. Zie ook Van Eijk 2000.

125. De artikel 29-werkgroep heeft deze inconsequenties in de toepassing van privacybeginselen opgemerkt. De groep stelt dat de bepalingen inzake nummeridentificatie waarin de privacy van gebruikers wordt beschermd een precedent creëren dat ook bij online punt-tot-punt-communicatie het overwegen waard is. Groep gegevensbescherming artikel 29 1997b, p. 8.

waarin men een anonieme internetgebruiker aansprakelijk wenst te stellen voor onrechtmatige informatie, voorafgegaan dienen te worden door een procedure waarin men de provider dwingt tot het verstrekken van identificerende informatie. Deze gang van zaken heeft een aantal consequenties. In de eerste plaats is de internetgebruiker daardoor, nu hij niet als partij in het geding betrokken is, voor de handhaving van zijn anonimiteit in hoge mate afhankelijk van zijn provider. De provider wordt als het ware in zijn plaats gesteld. Zo is hij in een aantal procedures als procespartij opgezadeld met het bewijs omtrent de waarheid van bepaalde beweerdelijk onrechtmatige uitlatingen. Het ontbreken van een mogelijkheid om zich in het geding te mengen anders dan bij monde van de provider is tegengesteld aan de in het vorige hoofdstuk geconstateerde subjectiveringstendens, die nu juist inhoudt dat aan eindgebruikers van elektronische communicatienetwerken en -diensten in toenemende mate afdwingbare rechten worden toegekend waarmee zij hun anonimiteit zelf kunnen beschermen.

Een ander knelpunt betreft de aansprakelijkheid van de provider. De formulering van het Hof brengt met zich mee dat een provider, wanneer hij weigert om de gegevens vrijwillig te verstrekken en er (nog) geen rechterlijk bevel is om dat te doen, onder omstandigheden in strijd kan handelen met de zorgvuldigheid die jegens de provider in acht dient te worden genomen. Het kan ook voorkomen dat de provider de gegevens juist wel verstrekt en dat hij hierop later wordt aangesproken door de anonieme derde die meent ten onrechte in zijn belangen te zijn geschaad. De mogelijkheid van vrijwillige verstrekking dwingt de provider dus tot een zelfstandige afweging. Anderzijds is hij aansprakelijk wanneer hij deze afweging verkeerd maakt. Zodoende wordt de provider in een lastig parket gebracht.

De vraag rijst of het vanuit rechtsstatelijk oogpunt eigenlijk wel wenselijk is dat verstrekking van identificerende gegevens in principe altijd kan geschieden zonder tussenkomst van de rechter en buiten medeweten van de anonieme persoon. De anonymus zou op zijn minst in staat moeten worden gesteld om zich tegen de verstrekking te verzetten door het verzoek aan de rechter voor te leggen. Dit geldt temeer nu is erkend dat verstrekking voor hem een beperking van de uitingsvrijheid en het recht op eerbiediging van de persoonlijke levenssfeer met zich mee kan brengen. De afweging van grondrechtelijke belangen dient mijns inziens bij voorkeur door de rechter te geschieden en niet door een private instantie die daarvoor de juridische expertise meestal niet in huis heeft. Uit de reacties van providers in de media blijkt dat zij bij verstrekking van gegevens uiteenlopend beleid hanteren en dat de uitspraak verschillend wordt geïnterpreteerd. Tegelijkertijd zijn sommige providers zelf van mening dat zij het oordeel over de verstrekking vaak niet eigenhandig kunnen vellen.[126]

Het verdient in dit verband opmerking dat in de strafvordering aan de praktijk van vrijwillige verstrekking op basis van de Wet bescherming persoonsgegevens bewust een

126. Van Ringelestijn 2004.

einde is gemaakt. De commissie Mevis, belast met het advies inzake invoering van de strafvorderlijke bevoegdheden tot het opvragen van gegevens, constateerde dat deze gang van zaken tot te veel onduidelijkheden leidde en dat afweging van belangen door de houder van de gegevens zelf, vaak leidde tot rechtsonzekerheid. Ook de verplichting van de inbreukmaker tot het noemen van zijn voorman in zaken betreffende inbreuken op de intellectuele eigendom ontstaat slechts na tussenkomst van de rechter (zie par. 9.5.2). Als verstrekking van NAW-gegevens in die gevallen slechts mogelijk is met tussenkomst van de rechter, dan dient die waarborg mijns inziens ook te gelden bij andersoortige schade. Een rechtsplicht tot verstrekking buiten de rechter om kan overigens wel worden gevonden in artikel 512 (h) van de Amerikaanse Digital Copyright Millenium Act (DMCA). Krachtens dit artikel ontstaat de verplichting tot het noemen van de voorman enkel op basis van de kennisgeving dat auteursrechtinbreuk is gepleegd. Mede om die reden heeft deze bepaling zwaar onder vuur gelegen (zie par. 4.6).[127]

127. Zie hierover uitgebreider Van Daalen & Ekker 2003. Zie over het hoger beroep in *Pesser/Lycos* ook Ekker 2004b.

10 Conclusies en aanbevelingen

10.1 Slotbeschouwing

In het voorgaande bleek dat de anonieme verspreiding van informatie sinds de uitvinding van de drukpers steeds opnieuw heeft geleid tot juridische vraagstukken. In Nederland kan men een aantal tijdvakken aanwijzen waarin als gevolg van technische en maatschappelijke ontwikkelingen telkens een andere problematiek de boventoon voert. De eerste periode begint met de felle bestrijding van anonieme geschriften in de zestiende eeuw. Door opeenvolgende machthebbers worden herhaaldelijk anonimiteitsverboden en identificatieverplichtingen aangewend om de uitoefening van censuur mogelijk te maken. In de achttiende en de negentiende eeuw volgt een tweede fase waarin Nederlandse juristen zich bezinnen op de wenselijkheid van strafbaarstelling. Deze episode eindigt in 1886 met de afschaffing van de strafbepalingen in de Code Pénal en de invoering van het drukkers- en uitgeversprivilege. Vanaf dat moment is de verspreiding van anonieme boeken en geschriften toegestaan. De uitspraak van het Europese Hof in de zaak *Goodwin* sluit bij de keuze van de Nederlandse wetgever aan door ook de journalist een geprivilegieerde positie te verschaffen.

Het derde en laatste stadium wordt ingeluid door de komst van elektronische communicatie. Uit telefonie en omroep ontstaan geleidelijk de communicatiemiddelen van het informatietijdperk. Deze technische verandering leidt tot nieuwe juridische uitdagingen. In de jaren zeventig en tachtig van de twintigste eeuw dient men een antwoord te vinden op de risico's die voor het individu en de maatschappij voortvloeien uit elektronische gegevensverwerking in het communicatieproces. In de telecommunicatiesector worden daartoe regels gecreëerd die de privacy van gebruikers beschermen. Met de opkomst van openbare elektronische communicatiemiddelen dringt gegevensverwerking vervolgens ook door in het publieke domein, waardoor dit verschijnsel in toenemende mate raakt aan de uitoefening van de uitingsvrijheid en andere publieke vrijheden. De rol van de wetgever is intussen veranderd. Trad hij aanvankelijk slechts repressief op, tegenwoordig erkent hij de grondrechtelijke belangen die bij anonimiteit een rol spelen en moet hij dus een evenwicht vinden tussen de bescherming hiervan en het maatschappelijke belang van rechtshandhaving. Steeds meer wordt daarbij tegemoet gekomen aan de handhaving van private, vaak commerciële, belangen en strafvorderlijke doelen die een behoefte aan kenbaarheid creëren.

De analyse van vraagstukken rondom anonieme communicatie legde verschillende juridische verbindingslijnen bloot. De eerste verbindingslijn is de relatie tussen anonimi-

teit en machtsuitoefening. Dit aspect kwam onder andere tot uitdrukking in de definitie van anonimiteit als het gevrijwaard zijn van identificatie, observatie en controle en in het verband tussen anonimiteit en ontoerekenbaarheid. Vanuit grondrechtelijk perspectief is de relatie met machtsuitoefening eveneens zeer duidelijk: de mogelijkheid om zijn identiteit te verbergen functioneert voor het (communicerend) individu als een afweermechanisme waarmee hij zijn staatsvrije sfeer af kan bakenen. In het communicatieproces is de anonimiteit van uiters, zenders en ontvangers van informatie van oudsher een factor geweest in het krachtenspel tussen de overheid als censor en het individu als participerende, zich uitende, burger. Bij elektronische communicatie is anonimiteit ten slotte een middel om paal en perk te stellen aan de elektronische verwerking van persoonsgegevens en gegevens over communicatiegedrag. Van een schild tegen censuur in het tijdperk van de drukpers heeft de mogelijkheid om anoniem te zijn zich zodoende ontwikkeld tot een wapen tegen informatiemacht in bredere zin.

In het verlengde van het machtsprobleem ligt als tweede verbindingslijn de rol en de positie van tussenpersonen in het communicatieproces. Gedurende lange tijd zijn zij door kerkelijke en wereldlijke machthebbers als instrument gebruikt om auteurs te kunnen ontmaskeren en censuur te handhaven. Medewerking aan de verspreiding van anonieme geschriften alsmede een weigering om een auteur te identificeren werd in het verleden zwaar bestraft. De geprivilegieerde positie van drukkers, uitgevers en journalisten was bedoeld om aan deze praktijk een einde te maken en beoogde tegelijkertijd een ongehinderde uitwisseling van informatie en ideeën te bevorderen. Voor de internetprovider ontbreekt een vergelijkbare positie vooralsnog. Het aansprakelijkheidsregime in de richtlijn elektronische handel, zoals geïmplementeerd in artikel 6:196c van het Burgerlijke Wetboek, ziet immers alleen op aansprakelijkheid voor de inhoud van de informatie. Toch komt bij geschillen rondom anonieme communicatie ook op de internetprovider een bepaalde last te rusten. In de huidige situatie wordt hij als gedaagde betrokken in civiele procedures ter ontmaskering van anonieme internetgebruikers. Daarnaast is hij vaak de enige die de (grondrechtelijke) belangen van de anonymus kan behartigen. Hoe aan dit probleem tegemoet kan worden gekomen komt bij de aanbevelingen nog nader aan de orde.

De vierde verbindingslijn is de scheiding tussen het publieke en het private. Deze scheiding is relevant omdat voor de analyse van de grondrechtelijke belangen die spelen bij de anonieme uiting de private of de publieke inhoud daarvan zeer bepalend is. Uitingen behoren tot de publieke sfeer wanneer zij handelen over of raken aan het algemeen belang. De bescherming van anonimiteit is hier direct gerelateerd aan de uitingsvrijheid, het democratische belang van het publieke debat en ondersteunt de waarden van politieke participatie en burgerschap. De private sfeer omvat daarentegen die uitingen die besloten zijn en die handelen over of raken aan private belangen. In de private sfeer van de zender of de ontvanger van een boodschap is het recht op (informationele) privacy de meest voor de hand liggende grondslag voor bescherming van anonimiteit.

Het onderscheid tussen de publieke en de private sfeer is in het elektronische communicatieproces temeer van belang nu openbare en niet-openbare informatie daar, als gevolg van technische en maatschappelijke ontwikkelingen, steeds meer door elkaar lopen. Nu men niet langer aan kan knopen bij het gebruikte communicatiemedium, dient bij het vaststellen van de mate van bescherming waarop een anonieme uiting aanspraak kan maken, gekeken te worden naar de inhoud van de boodschap. Deze vermenging van het private en het publieke in het elektronische communicatieproces dient daarnaast gevolgen te hebben voor de wijze waarop het gegevensbeschermingsrecht is gefundeerd. Met de opkomst van openbare elektronische communicatiemiddelen manifesteert gegevensverwerking zich in toenemende mate ook buiten de private sfeer van het individu.

10.2 Beantwoording van de onderzoeksvragen

I Hoe is anonieme communicatie in het Nederlandse recht gereguleerd?
Waar het de traditionele communicatiemiddelen betreft, is deze vraag beantwoord in hoofdstuk 6. Het drukkers- en uitgeversprivilege en het journalistieke verschoningsrecht houden hier de relatieve anonimiteit van de bron in stand. Deze rechtsinstituten voorkomen dat de tussenpersoon te allen tijde kan worden verplicht om de bron van informatie kenbaar te maken. Drukkers en uitgevers kunnen slechts worden ingeschakeld om anonimiteit te doorbreken wanneer een gerechtelijk vooronderzoek is begonnen wegens een drukpersmisdrijf. Een aan de journalist gerichte vordering tot verstrekking van identificerende gegevens dient te worden getoetst aan artikel 10 lid 2 EVRM.

In de informatiesamenleving is de regulering van anonimiteit veel minder overzichtelijk. De bescherming en doorbreking van anonimiteit wordt hier genormeerd door uiteenlopende wettelijke regelingen en door jurisprudentie. Enerzijds zijn in het geldende recht, dat wil zeggen in de Europese privacyrichtlijnen en de implementatie daarvan, de contouren van een recht om anoniem te communiceren reeds zichtbaar. Dit bleek in hoofdstuk 8. Anderzijds bestaan er verschillende juridische mogelijkheden tot doorbreking van anonimiteit. Deze zijn verdeeld over een geheel van ongelijksoortige regelingen met een variërend toepassingsbereik. Wettelijke bepalingen die de verstrekking van identificerende gegevens mogelijk maken, zijn in hoge mate toegespitst op de doelen waarvoor identificatie van gebruikers nodig is, zoals de handhaving van het auteursrecht en het civiele recht. Geconcludeerd werd dat in verschillende rechtsgebieden op uiteenlopende wijze met vorderingen tot verstrekking wordt omgegaan. Met name in de civiele rechtspraak over de verstrekking van identificerende gegevens dringt geleidelijk het besef door dat de doorbreking van anonimiteit een op zichzelf staand juridisch probleem is met grondrechtelijke implicaties. Bij de bespreking van de strafvorderlijke bevoegdheden tot het vorderen van identificerende gegevens bleek daarentegen dat in die context veel minder zwaar wordt getild aan de privacygevoeligheid van identificerende gegevens en dat ook het verband tussen anonimiteit en communicatiegrondrechten minder duidelijk wordt gelegd.

II Wat zijn de constitutionele grondslagen voor de bescherming van anonieme openbare communicatie?

Bij de analyse van deze vraag is een onderscheid gemaakt tussen private en publieke belangen. Het publieke aspect stond in dit onderzoek centraal. Er is dan ook met name gekeken naar de functie van anonimiteit in de context van openbare uitingen en het democratische publieke debat. De uitingsvrijheid is daar het meest voor de hand liggende en sterkste argument voor de bescherming van anonimiteit en voor de aanvaarding van een recht om anoniem te communiceren.

Zowel in Nederland en Europa als in de Verenigde Staten heeft het verband met de uitingsvrijheid erkenning gekregen. In de loop van de geschiedenis zijn de Nederlandse wetgever en het Amerikaanse Supreme Court tot het inzicht gekomen dat een waarlijke en onbelemmerde uitingsvrijheid niet kan bestaan indien de uitoefening daarvan steeds is onderworpen aan identificatie en registratie. Dit uitgangspunt kan op verschillende wijzen worden onderbouwd. Beschouwd vanuit het individu is de mogelijkheid om anoniem te blijven essentieel voor het ongehinderd uiten van een mening en voor het anderszins publiceren, verspreiden en ontvangen van informatie. Anonimiteit ondersteunt bovendien het recht van het individu op zelfontplooiing. Wanneer men de positie van de tussenpersoon nader beziet, kan daarnaast een verband worden gelegd met de 'free flow of information'. Tussenpersonen in het communicatieproces zouden hun taak niet goed kunnen vervullen wanneer zij te allen tijde en zonder enig voorbehoud zouden kunnen worden ingeschakeld bij de identificatie van een bron.

Voor zover openbare anonieme uitingen betrekking hebben op politieke en maatschappelijke aangelegenheden speelt het belang van het publieke debat een belangrijke rol. In de discussie over de beschermenswaardigheid van anonieme uitingen komt dit belang telkens terug. Reeds in de achttiende eeuw stelden Nederlandse rechtsgeleerden zich de vraag of naamloze geschriften nog langer verboden dienden te worden. In hun beschouwingen komt reeds duidelijk het idee naar voren dat een ruime uitingsvrijheid, al dan niet anoniem uitgeoefend, maatschappelijk wenselijk was en dat deze het vinden van 'de naakte waarheid' dichterbij zou kunnen brengen. In de negentiende eeuw heeft dat idee verder postgevat. Het denken over 'de publieke mening' loopt parallel met de opkomst van een politiek bewuste middenklasse en de ontwikkeling van de periodieke pers. De rol van het publieke debat en de functie van anonimiteit daarin lijkt, evenals de anonieme verspreiding zelf, een universeel probleem te zijn dat in iedere zich ontwikkelende democratie naar voren komt. In de Verenigde Staten werd immers dezelfde discussie gevoerd als in ons land. Het Supreme Court zou de traditie van anonieme publicaties uiteindelijk verheffen tot een door het First Amendment beschermd recht. De stimulering van 'the marketplace of ideas' was daarvoor een belangrijke reden.

De godsdienstvrijheid en politieke grondrechten zijn met name bij de bespreking van het Amerikaanse recht aan de orde gekomen als fundament voor de bescherming van anonimiteit. Het Supreme Court erkent in verschillende uitspraken dat er een sterk 'chilling effect' uit kan gaan van identificatieverplichtingen, bijvoorbeeld bij demonstraties,

het oprichten en instandhouden van politieke en religieuze organisaties en bij de verspreiding van ideeën van deur tot deur. Ook in het Nederlandse recht heeft het verband met de genoemde rechten, zij het minder expliciet, erkenning gevonden. Voorbeelden zijn de bescherming van bijzondere persoonsgegevens in de Wet bescherming persoonsgegevens en het wettelijke gewaarborgde recht om het kiesrecht anoniem uit te oefenen.

Als laatste belangrijke grondslag moet het recht op informationele privacy worden genoemd. Dit recht is met name van belang omdat het bedoeld is als middel om de informatiemacht van de gegevensverwerker jegens het datasubject te beteugelen. De gegevensbeschermingsbeginselen en de daarop gebaseerde rechten van het communicerend individu, zoals het recht op inzage, correctie en verzet, geven het subject de mogelijkheid om zijn private sfeer en de uitoefening van publieke vrijheden in de digitale omgeving te beschermen. Meer in zijn algemeenheid is het recht op privacy naast de uitingsvrijheid een sterk argument om zich te verzetten tegen maatregelen die identificatie en registratie in het communicatieproces uitbreiden.

III Dient in Nederland bij openbare communicatie een recht op anonimiteit te worden erkend?

Het antwoord op deze vraag dient, gezien hetgeen hierboven is besproken, bevestigend te zijn. Rondom anonieme communicatie spelen in de informatiemaatschappij zwaarwegende maatschappelijke en grondrechtelijke belangen die vragen om een rechtsinstituut dat het individu in beginsel de keuze geeft om anoniem te blijven en dat een kader schept om zijn belang bij anonimiteit af te wegen tegen andere publieke en private belangen.

De meest effectieve manier om te verzekeren dat de constitutionele belangen van de anonymus in concrete gevallen wordt meegewogen, is het toekennen van een zelfstandig en afdwingbaar recht. Hoewel de Europese en de Nederlandse wetgever de suggestie van een dergelijk recht zorgvuldig lijken te vermijden, hebben zij het maatschappelijk belang van een bepaalde mate van bescherming onderschreven. Ook in het geldende recht heeft dit belang reeds herhaaldelijk erkenning gevonden. Expliciete aanvaarding van het recht om anoniem te communiceren is dan ook een minder revolutionaire stap dan op het eerste gezicht het geval lijkt. Tot op zekere hoogte is slechts sprake van een herwaardering van geldende normen binnen een nieuw juridisch concept. In de nieuwe benadering komen de reeds erkende en nog te erkennen elementen van het recht om anoniem te communiceren te rusten op een bouwwerk van de in de vorige paragraaf genoemde klassieke grondrechten. Reeds bestaande elementen die nu nog eenzijdig steunen op één grondrecht en die beschouwd vanuit het bredere constitutionele kader dus gedeeltelijk in het luchtledige hangen, worden zodoende onder één noemer gebracht en krijgen daarmee een meer solide basis die beter aansluit bij de complexe werkelijkheid van het moderne communicatieproces. Zo kunnen de bestaande normen voor telefonie, die nu nog overwegend hun grondslag vinden in het recht op informationele privacy, beter worden ingebed in een algemeen recht om anoniem te communiceren dat ook rust op de

uitingsvrijheid. Het voordeel van een dergelijke benadering is dat de samenhang met de bescherming van anonimiteit bij traditionele communicatie meer aan de oppervlakte komt en dat er een duidelijker verband wordt gelegd met andere grondrechten dan het recht op privacy. Nieuw is wel dat er, ook buiten het gegevensbeschermingsrecht, door de erkenning van een aan de anonymus toekomend recht meer nadruk komt te liggen op zijn bevoegdheid om bescherming eigenhandig af te dwingen.

Het recht om anoniem te communiceren zou mijns inziens een aantal elementen dienen te omvatten. Allereerst dient aan de anonieme persoon de bevoegdheid te worden verleend zich te verzetten tegen de registratie en opslag van identificerende gegevens en tegen de verwerking en verstrekking hiervan, wanneer deze handelingen de in de vorige paragraaf genoemde grondrechten onevenredig beperken. Als accessoir element zou hier een recht op notificatie aan toe moeten worden gevoegd, dat wil zeggen het recht van de anonymus om, zo mogelijk, op de hoogte gesteld te worden van pogingen om zijn anonimiteit te doorbreken. De wetgever dient zich in te spannen om de genoemde rechten te waarborgen. Uit de genoemde rechten vloeit voor hem tevens een onthoudingsverplichting voort: de anonieme publicatie, verspreiding en ontvangst van informatie mag niet in zijn algemeenheid strafbaar worden gesteld, zoals in Nederland het geval was tijdens de Spaanse, de Franse en de Duitse overheersing. Tussenpersonen mogen in concrete gevallen slechts worden verplicht tot het ontmaskeren van een anonieme bron wanneer een afweging heeft plaatsgevonden tussen de belangen die bij de ontmaskering zijn gediend en de grondrechtelijke belangen van de anonymus.

10.3 Aanbevelingen

Is de noodzaak tot bescherming van anonimiteit eenmaal vastgesteld, dan stuit men op de vraag hoe die bescherming dient te worden geformuleerd en op welk wettelijk niveau deze gestalte dient te krijgen. De meest vergaande bescherming van het recht om anoniem te communiceren zou bestaan uit opname in de Nederlandse grondwet. Zoals de commissie Franken terecht heeft opgemerkt past een specifiek en afgebakend recht als het recht op anonimiteit echter niet in het systeem van onze grondwet als een abstracte en algemene catalogus waarin slechts de meest essentiële constitutionele belangen zijn opgenomen. Dit geldt logischerwijs des te meer voor een recht dat alleen betrekking heeft op communicatieve handelingen. Een grondwettelijke regeling ligt daarom niet voor de hand. Effectieve bescherming kan, zoals blijkt uit het Amerikaanse recht, echter ook worden gerealiseerd zonder opname in de tekst van de grondwet.

Met de aanvaarding van het recht om anoniem te communiceren dient een aantal zaken gepaard te gaan. In de eerste plaats dient het verband tussen de uitoefening van grondrechten en anonimiteit duidelijker te worden onderkend. In de rechtsgeleerde discussie moet daartoe aan de orde gesteld worden dat de ongehinderde uitoefening van grondrechten gediend is bij bescherming van anonimiteit. Nu communicatiemiddelen samenvloeien en constitutionele beschermingsregimes convergeren, ligt het belang van die bescherming op het grensvlak van uitingsvrijheid en privacy. In de tweede plaats

dient de wetgever een samenhangende visie te ontwikkelen over de betekenis van anonieme communicatie in de informatiesamenleving en de wijze waarop anonimiteit gereguleerd dient te worden. De techniekafhankelijkheid en de versnipperdheid van de geldende normen en het per rechtsgebied verschillende beschermingsniveau nopen tot een meer consequente en doordachte benadering. Deze kan onder ander dichterbij worden gebracht door te kijken naar de jurisprudentie van het Supreme Court. Hierin is immers een diepgaande analyse van het verband tussen anonimiteit en de uitoefening van grondrechten te vinden.

De verstrekking van identificerende gegevens is zonder twijfel één van de meest actuele juridische problemen die in dit onderzoek aan de orde kwamen. Met name waar het de civielrechtelijke ontmaskering van internetgebruikers betreft, bestaat in de praktijk nog een aantal knelpunten. In de eerste dient in Nederland, bij weigering van een provider om identificerende gegevens te verstrekken, tegen hem een afzonderlijke civiele procedure te worden begonnen om verstrekking af te dwingen. Pas wanneer de benodigde gegevens verkregen zijn, kan de eiser ook een procedure aanspannen tegen de verantwoordelijke internetgebruiker. In de tweede plaats bestaat er nog onduidelijkheid over de criteria waaraan een vordering tot verstrekking getoetst moet worden en speelt de vraag welke instantie de verschillende in het geding zijnde belangen af moet wegen. In de derde plaats zal de positie van de anonymus nog duidelijker aan de orde moeten komen. Het is met name de vraag hoe hij in de gelegenheid kan worden gesteld om zijn stem te laten horen.

Bij het wegnemen van de genoemde knelpunten is het nuttig een voorbeeld te nemen aan de Amerikaanse aanpak. De John Doe subpoena maakt het mogelijk een civiele procedure aan te spannen tegen de anonymus zelf. Hierdoor kunnen de onthulling van de identiteit van de gedaagde tijdens 'limited discovery' én de vordering van de eiser in één en dezelfde procedure aan de orde komen. De provider wordt vervolgens als derde partij in het geding betrokken. In procedureel opzicht is deze gang van zaken zuiverder. Wanneer de provider of de anonieme gedaagde zich tegen de subpoena verzet wordt de vordering van de eiser beoordeeld door de rechter aan de hand van een 'balancing test'. Daarbij is van belang dat de anonieme gedaagde zich direct kan beroepen op een constitutioneel beschermd recht om anoniem informatie te verspreiden en te communiceren. Hierdoor ligt in de rechtspraak een grotere nadruk op constitutionele waarden.

Wil men de civielrechtelijke verstrekking van identificerende gegevens laten verlopen op een wijze die de eiser en de provider zo min mogelijk belast en die daarnaast recht doet aan de bij grondrechtelijke belangen van de anonymus, dan zou men mijns inziens de volgende procedure moeten volgen:

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 waamee de bewuste informatie toegankelijk is gemaakt of is door-

gezonden 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.

De voorgestelde procedure kent ten opzichte van de geldende praktijk een aantal belangrijke voordelen. 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. 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. 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. 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. 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.

In het voorgestelde systeem is verstrekking zonder tussenkomst van de rechter niet langer mogelijk. Vrijwillige verstrekking op basis van de Wet bescherming persoonsgegevens is om een aantal redenen mijns inziens niet langer gewenst. In de eerste plaats is de juridische problematiek rondom de verstrekking van identificerende gegevens van internetgebruiker in veel gevallen ingewikkeld. De provider of websitehost is vaak niet in staat eigenhandig een oordeel te vellen over de onrechtmatigheid van informatie, het beledigende karakter van een uitlating of de vraag of daadwerkelijk sprake is van inbreuk op een intellectuele eigendomsrecht. De afweging van de door de verzoeker naar voren gebrachte belangen tegen de belangen van de anonieme internetgebruiker dient bovendien bij voorkeur te geschieden door een onafhankelijke instantie nu aan de kant van de gedaagde zwaarwegende grondrechtelijke belangen in het geding zijn. Ten slotte sluit men door rechterlijke tussenkomst te vereisen aan bij gang van zaken in het intellectuele eigendomsrecht en de strafvordering. Het bevel tot het noemen van de voorman kan zowel krachtens Nederlands recht als krachtens artikel 8 van de handhavingsrichtlijn alleen in een civiele procedure door de rechter gegeven worden. In de strafrechtelijke sfeer is aan de praktijk van vrijwillige verstrekking een eind gemaakt omdat de commissie Mevis constateerde dat deze gang van zaken leidde tot rechtsonzekerheid.

Zou men de geschetste procedure in het Nederlandse recht willen implementeren, dan doemt als eerste vraag op bij welke rechterlijke instantie en op welke wijze het verzoek zou moeten worden ingediend. Mijns inziens ligt het voor de hand te kiezen voor de verzoekschriftprocedure in de derde titel van het eerste boek van het Wetboek van Burgerlijke Rechtsvordering. Als bevoegde rechterlijke instantie zou de kantonrechter van de woonplaats van de verzoeker kunnen worden aangewezen. Bij de beoordeling van het verzoek zou hij de criteria kunnen toepassen die in de jurisprudentie over de verstrekking van NAW-gegevens zijn ontwikkeld (zie par. 9.5.2 en 9.5.3). De verwijzing naar de verzoekschriftprocedure en de aan de provider gerichte voorschriften met betrekking tot het doorzenden van het verzoekschrift aan de anonieme gebruiker kunnen het beste worden opgenomen in afdeling 11 van de Telecommunicatiewet aangaande de bescherming van persoonsgegevens en de persoonlijke levenssfeer, getuige de hier opgenomen regeling over de doorbreking van de blokkering van nummerherkenning bij hinderlijke of kwaadwillige oproepen (zie par. 8.3.2). Het huidige artikel 11.11 Tw, dat hieromtrent voorschriften bevat, zou dan echter in zijn geheel geschrapt moeten worden. Dit is om drie redenen echter niet bezwaarlijk. In de eerste plaats beantwoordt dit artikel niet langer aan de in de praktijk bestaande problematiek omdat het alleen is gericht op telefonie. In de tweede plaats wordt er geen onderscheid gemaakt tussen civielrechtelijke en strafrechtelijke doeleinden voor de doorbreking van de blokkering van nummerherkenning en de daaraan gekoppelde gegevensverstrekking. In de derde plaats is de beoordeling van het verzoek opgedragen aan de telefonieaanbieder, hetgeen om reeds genoemde redenen onwenselijk is.

Het nieuw in te voegen artikel 11.11 Tw zou op een aantal punten verbetering moeten brengen. In de eerste plaats zou het toepasselijk moeten zijn op alle elektronische com-

municatietechnologieën. De werkingssfeer van deze bepaling zou tegelijkertijd echter beperkt moeten zijn tot verzoeken die beogen een civiele procedure mogelijk te maken. In de strafrechtelijke sfeer gelegen problemen rondom anonimiteit, zoals telefonisch stalken en soortgelijke problematiek via e-mail en internet zouden voortaan niet meer via de regeling in de Telecommunicatiewet moeten worden afgehandeld, maar via een aparte regeling die burgers in staat stelt om via een centraal meldpunt – en niet bij verschillende aanbieders, zoals nu het geval is – een verzoek tot verstrekking van identificerende gegevens in te dienen dat na toetsing vervolgens door politie en justitie met toepassing van de verruimde strafvorderlijke bevoegdheden tot het opvragen van gegevens kan worden ingewilligd.

Het nieuwe artikel 11.11 Tw zou alsvolgt kunnen luiden:

1. De abonnee die last heeft van hinderlijke of kwaadwillige oproepen, waarbij de verstrekking van het nummer van het oproepende netwerkaansluitpunt is geblokkeerd en de natuurlijke persoon of rechtspersoon die schade leidt als gevolg van informatie die is toegankelijk gemaakt of verspreid via een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst, kan zich tot de kantonrechter wenden met het verzoek de aanbieder van een openbaar elektronische communicatienetwerk of een openbare elektronische communicatiedienst te bevelen tot het verstrekken van de beschikbare elektronische adresseringsgegevens van de verantwoordelijke gebruiker alsmede de aan die adresgegevens gerelateerde naam-, adres-, postcode en woonplaatsgegevens.
2. Het verzoekschrift wordt gedaan aan de ingevolge de tweede afdeling van de derde titel van het eerste boek van het Wetboek van Burgerlijke Rechtsvordering bevoegde kantonrechter.
3. Het verzoekschrift bevat naast de in artikel 278 van het Wetboek van Burgerlijke Rechtsvordering genoemde elementen:
   a. indien het hinderlijke of kwaadwillige oproepen betreft, een indicatie van de data en tijdstippen waarop deze hebben plaatsgevonden;
   b. indien het digitale informatie betreft, een nauwkeurige beschrijving van de aard en de inhoud daarvan, de plaats waar deze beschikbaar is of was en een nauwkeurige indicatie van het tijdstip of de tijdstippen waarop deze is verzonden of toegankelijk is gemaakt.
4. De kantonrechter kan het verzoek slechts inwilligen indien:
   a. de onrechtmatigheid van de oproepen of de informatie jegens de verzoeker voldoende aannemelijk is;
   b. afweging van de belangen van de verzoeker en de belangen of fundamentele rechten van de in het eerste lid bedoelde gebruiker met zich meebrengt dat het belang van de verzoeker behoort te prevaleren.
5. Gelijktijdig met het indienen van het verzoekschrift stuurt de verzoeker een kopie daarvan aan de aanbieder.

6. De aanbieder zendt de kopie van het verzoek aan de betrokken gebruiker alsmede een verklaring waarin deze op de hoogte wordt gesteld van de poging om zijn identiteit te achterhalen en van zijn recht om zich tegen het verzoek te verzetten. Indien de aanbieder niet beschikt over de in het eerste lid bedoelde gegevens stelt hij de verzoeker hiervan zo spoedig mogelijk op de hoogte.
7. De betrokken gebruiker dient binnen … dagen te reageren. Indien de aanbieder van de betrokken gebruiker een reactie ontvangt, stuurt hij deze zo spoedig mogelijk door aan de verzoeker en aan de rechterlijke instantie bij wie het verzoekschrift is ingediend.
8. De aanbieder kan redelijke kosten in rekening brengen bij de verzoeker.

Summary

Communicating anonymously: from printing press to weblog. A study of the constitutional protection of anonymous public communication

In the information society, citizens have become increasingly subject to registration and observation. Recent decades have seen a surge of technologies that enable us to watch each other and ourselves. From a legal perspective this development poses the question to what extent individuals should be able to keep themselves free from observation by others. This thesis focuses on problems concerning the identifiability and anonymity of actors in the communication process. In this domain different interests are of importance. On the one hand public and private interests, such as the maintenance of criminal law, libel law and intellectual property law, create a need for traceability and accountability. On the other hand, fundamental values, notably the right to freedom of speech and the right to informational privacy, are in some cases impeded when individuals cannot choose to protect their identity. The conflict between the societal principle of accountability and the need for protection of individual freedom thus creates a legal dilemma that manifests itself in all means of communication.

To reach a better understanding of the function of anonymity in the communication process and how it relates to constitutional values, three research questions are put forward:

– How is anonymous communication regulated in Dutch law?
– What are the constitutional foundations for the protection of anonymous public communication?
– Should a right to communicate anonymously be accepted in Dutch law?

In order to get a broader view of these research questions, besides Dutch law, American law is also examined. The United States Supreme Court has on several occasions granted protection to anonymous speech under the First Amendment. Moreover, in so-called 'John Doe'-litigation it has addressed the circumstances in which Internet Service Providers can be forced to disclose information that can lead to the identification of their customers.

One of the main goals of this research is to analyse the relationship between the protection of anonymity and the exercise of fundamental rights, notably freedom of speech.

Chapter 1 therefore contemplates three different meanings of the word anonymity. Firstly, this word is often used in the etymological sense of 'namelessness', when referring to authors of books and other writings. In everyday usage, however, a broader concept of anonymity is often applied. This concept contains aspects of the right to privacy. The wish to be anonymous often originates from the longing to be unseen and to be free from identification and surveillance by others. In this sense of the word, anonymity is linked to the position of the individual in social structures of hierarchy and power and expresses the absence of social control and the diminished applicability of social and legal rules. Finally, on a more abstract level, one can consider anonymity as 'untraceability', meaning that acts and utterances cannot be traced back to the person who is responsible for them. In the communication process the extent to which a sender or receiver of information can be traced depends heavily on the cooperation of intermediaries, such as printers, publishers, journalists, and telephony and Internet providers. If the intermediary possesses identifying information we speak of 'relative' anonymity. If identifying information is not available at all, one speaks of 'absolute anonymity'. All forms of anonymity have in common that they remove accountability: an anonymous person cannot, or can only to a lesser extent, be held responsible for his acts.

A democratic society cannot exist without open and robust public debate. The stimulation of this debate is not only a strong argument for generous protection of freedom of speech, but also for the possibility to print and publish anonymously. Both in the United States and in the Netherlands, legal scholars have long discussed the desirability of anonymous utterances. To get a clear view of the positive and negative effects of anonymous contributions, Chapter 2 starts with a general exposition of political theories which sum up ideal conditions for democratic public debate. These theories include, for example, the condition that debate should be open to everyone who wishes to participate in it; that it should be based on the exchange of rational arguments, and that participants should respect the motivation of other speakers. Departing from these general conditions, a few strong arguments in favour of anonymity can be distinguished. In the first place, the absence of identification can stimulate participation in debate. Moreover, when the personal features of a speaker are unknown, arguments can only be judged on the bases of rational criteria. This can prevent discrimination, but anonymity can also have negative consequences. A lack of accountability may lead to a contamination of a debate and it may threaten the open character of a discussion. All in all, anonymity turns out to have both benefits and harms. Which will prevail will depend on one's conception of the dynamics of the debate. Nevertheless, it is concluded that the societal harm connected to anonymity generally does not outweigh the benefits. To a certain extent these negative effects are the price which society has to pay for a free trade in ideas.

Chapter 3 and 4 address the protection of anonymous communication in American law. In Chapter 3 the First Amendment jurisprudence of the Supreme Court is examined. Since the 1950s, this Court has addressed questions concerning anonymity within a framework of different constitutional rights, notably freedom of speech, freedom of

religion and freedom of assembly. In the first cases, the Court nullified Federal and State legislation that required citizens to identify themselves before they were allowed to exercise their constitutional rights, such as the founding of a political organisation, the dissemination of (political) pamphlets and speaking in public. Recently, the emergence of electronic communication has posed the question whether the right to speak anonymously can also be invoked by Internet users. In *Reno* v. *American Civil Liberties Union* the Supreme Court answered this question affirmatively. It struck down Federal provisions in the 'Communications Decency Act' (CDA) that forced Internet providers to implement identification technology in order to avoid liability for indecent online content.

Chapter 4 analyses the position of anonymous Internet users that are faced with civil procedures in which the plaintiff attempts to identify them. Special attention is paid to Californian law, which gives a strong protection to anonymous online speech. 'John Doe'-procedures have examined how the interests of a plaintiff in identifying an anonymous poster must be weighed against the constitutional right to communicate anonymously. On several occasions, judges have created procedural safeguards to ensure that the anonymous Internet user is informed about the attempt to identify him so that he can defend his legitimate interests. In this chapter attention is also paid to the surge of 'Strategic Lawsuits Against Public Participation' (SLAPPs) in which powerful plaintiffs attempt to silence utterances that harm their commercial or other interests. Many state legislators have created so-called 'Anti-SLAPP statutes' to prevent this abuse of procedural means. Finally, provisions in the Digital Millennium Copyright Act (DMCA) that enable copyright holders to identify alleged infringers are reviewed. It is concluded that in general, the First Amendment rights of the anonymous defendant and the interest of the public debate are taken seriously in case-law. However, when the enforcement of intellectual property rights is at stake, this principled stance yields to the commercial interests of the entertainment industry.

The Chapters 5 to 9 deal with Dutch law. Before current Dutch provisions and case law are handled, a closer look is taken at Dutch history. Chapter 5 describes how, throughout history, prohibitions of anonymous writings were used to enforce censorship. A ban on anonymous writings was first issued in the sixteenth century by the Spanish occupier. After the invention of the printing press the Spanish authorities sought to curb the dissemination of dissenting religious and political ideas. In 1527, Charles V declared a prohibition of all heretical writings, all anonymous publications and all books that were published without the name of the publisher or the printer. Similar bans returned in later centuries. In 1811, during the occupation of Holland by the French, the French Criminal Code (Code Pénal) came into force. The Code Pénal implemented a system of severe punishments that forced publishers and printers to reveal the identity of authors. During the eighteenth and nineteenth centuries the French provisions were increasingly criticized by Dutch legal scholars. At the end of the nineteenth century, under the influence of the ideals of the Enlightenment, this criticism reached its climax. According to some influential jurists, freedom of the press was greatly impaired. With

the introduction of a new Dutch Criminal Code (*Wetboek van Strafrecht*) in 1886, the French system was finally abandoned. Since then Articles 53 and 54 of the Criminal Code create a legal privilege for printers and publishers (*drukkers- en uitgeversprivilege*), which implies that they can only be forced to identify an author when, after the publication of a writing, it is demonstrated that its content is punishable.

Chapter 6 discusses some new questions that came to the fore in the twentieth century. In 1980, the Dutch Supreme Court held that a municipal provision prohibiting the distribution of anonymous wall posters did not conflict with freedom of speech, as protected in Article 7 of the Dutch Constitution. In contrast to its American equivalent, the Dutch Supreme Court did not consider the ban on anonymity as regulating the content of a document. Furthermore, it overlooked the relationship between anonymity and freedom of speech. Another important issue concerned the position of journalists. For a long time the Dutch Supreme Court was reluctant to recognise a journalist's right to protect his sources. Eventually, a contrary approach was adopted by the European Court of Human Rights in the *Goodwin* case, which granted protection on the basis of Article 10 of the European Convention on Human Rights. Together, privileges of printers, publishers and journalists regulate the distribution of anonymous writings and the communication of information provided by anonymous sources to the public. These privileges create a system of 'relative anonymity', meaning that anonymity is protected, unless a weighty interest can be demonstrated that justifies revealing the identity of a source. The protection was inspired by the wish to prevent self-censorship, to stimulate the free flow of information and to avoid the risk of journalistic sources running dry. The reflections of the legislator on these matters, however, show no thorough analysis of the relationship between anonymity and the exercise of fundamental rights. Also, since the above-mentioned privileges focus on the position of the intermediary, not much attention is given to the legal position of the anonymous source itself. In the digital environment the question whether the anonymous user has an independent and enforceable right to anonymity turns out to be of great importance.

Chapter 7 charts the transition from the era of the printing press to the information society of today. In the last decades of the twentieth century, as a result of technological developments, the meaning of anonymity changed. For a long time after the invention of the printing press, legal questions were mainly related to the right to freedom of speech, but with the emergence of electronic communication technologies, the right to informational privacy gradually gained in relevance. Technological developments, such as the digitalisation of telephone networks, the convergence of computer and telecommunication technology and the increasing processing and storage of 'traffic data', made the communication process transparent and susceptible to observation. Access to personal data of end-users creates 'information power' of telecommunication providers and public authorities, whereas users are in many cases unable to prevent their data from being registered. As a result, the relationship between anonymity and informational privacy became a pivotal issue. Legal rules that curb the processing of data were implemented to

protect the autonomy of the data subject. The merging of information and communication technologies has also caused a phenomenon that is often described as 'technical convergence': in the digital environment the uses of both public and non-public means of communication come together. This development leads to 'constitutional convergence', meaning that legal questions around anonymity in the digital environment touch upon both freedom of speech and privacy. Data protection rules are increasingly used as a means to protect these rights. To illustrate this, three key problems are put forward. The first key problem concerns the access of end-users to electronic communication networks. In most cases, when connecting to the network the end-user is being registered by means of some kind of identifying characteristic, e.g. a phone number, e-mail address or IP-address. The second problem involves the access of senders and distributors of information to publicity. Here it is relevant to examine the extent to which online distributors of information can invoke the journalistic privilege. Finally, the access of collectors of information to the virtual public domain is of growing importance. Although the right to receive and impart information has been recognised in treaties and constitutions, under Dutch and European law, it remains unclear whether this right can also be exercised anonymously. Finally, Chapter 7 provides an overview of official documents, issued by the Dutch Government, the Committee of Ministers of the Council of Europe and the Article 29 Data Protection Working Party of the European Union. Each of these bodies have supported the protection of online anonymity. However, neither the European Privacy Directives nor Dutch statutory law explicitly formulate a right of end-users to communicate anonymously.

Chapter 8 further elaborates the above-mentioned developments. It deals with three issues concerning the transparency, processing and distribution of identifying personal data that first emerged in the sphere of traditional telephony, but are now gradually evolving into problems with a broader dimension. With the emergence of public electronic communication, data processing enters the public domain, as a result of which data protection becomes essential to freedom of speech and the free flow of information. First, the replacement of the traditional telephone directory by digital databases is discussed. These databases contain electronic contact information, like e-mail addresses and domain names, which, unlike telephone numbers, also refer to sources of public information. Subsequently, it is investigated how Caller Line Identification is regulated for telephony and how this application is related to similar applications with e-mail and Internet. Thirdly, rules about the processing of traffic and location data are examined. Here, too, we can clearly see the transition from traditional telephony to electronic communication: as data processing intensifies, more aspects of (communication) behaviour are monitored. Finally, attention is paid to an issue that is not addressed in relevant Directives, but which is nevertheless of the utmost importance: the right to anonymous access to telecommunication networks and services. The chapter concludes with the observation that one can perceive the contours of a 'right to communicate anonymously' in the European Privacy Directives and their implementation in Dutch law.

Chapter 9 explores the conditions under which online intermediaries, such as Internet providers and webhosts, are allowed, or can be compelled, to hand over identifying information of end-users to third parties. Also, it explores to what extent the relationship between anonymity and fundamental rights is recognised in statutory and case-law. Relevant provisions are scattered over a range of statutes. First of all, attention is paid to the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) and the Directive on Electronic Commerce of the European Union. The Data Protection Act contains criteria for the handing-over of personal data by the processing party on a voluntary basis, but it does not create a legal obligation to do so. The Directive on Electronic Commerce gives member states the authority to create legal obligations for the handing over of data. Nevertheless, the exact meaning and scope of this authority is unclear. Dutch civil law is then examined. First some procedural aspects are discussed. In civil law, litigation against an anonymous source of information differs fundamentally from the American John Doe-procedure, because under Dutch law, it is not possible to issue a subpoena to an unknown person. Subsequently, we concentrate on the legal debate about the theoretical basis of a civil obligation to hand over identifying information. Finally, case law is dealt with. Of great importance is the Directive on the Enforcement of Intellectual Property Rights that introduces a 'right to information', similar to the provisions in the Digital Millennium Copyright Act that were discussed in Chapter 4. The last part of Chapter 9 is dedicated to two recent laws that broaden the possibilities of criminal enforcement authorities to request personal data. It is concluded that in the areas of the law discussed claims for identifying information are handled very differently. The 'chilling effect' that the handing over of identifying information can have is not equally recognised everywhere.

Chapter 10 contains some final considerations, general conclusions and recommendations.

In the final considerations, it is pointed out that since the invention of the printing press, the anonymous dissemination of information has been a phenomenon of considerable societal importance that has repeatedly brought about legal problems. The analysis reveals a number of recurrent themes. First and foremost, a fundamental link between anonymity and the exercise of (State) power was demonstrated. In the communication process the anonymity of senders and receivers of information has always been an important factor in the struggle between the government in its capacity as censor and the communicating individual. In the realm of electronic communication, anonymity is a powerful tool for limiting the processing of personal data regarding communication. From a shield against censorship, the possibility of remaining anonymous has thus become a weapon against 'information power' in a broader sense. The position of intermediaries through the ages has also proved to be a pivotal issue. Their refusal to cooperate in the identification of a source was for a long time severely sanctioned. The last line of analysis is the distinction between the private and the public domain. This distinction is particu-

larly relevant for the analysis of the constitutional values at stake in a given case, all the more now that public and non-public information increasingly mingle.

Now the research questions are answered. The first questions related to the way anonymous communication is regulated under Dutch law. As far as traditional means of communication are concerned, this question was answered in Chapter 6. There it was demonstrated that privileges of printers, publisher and journalists support the relative anonymity of authors and anonymous sources. In the digital environment, however, the anonymity of the end-user is regulated by a heterogeneous whole of statutory provisions and case-law. On the one hand, in existing law, the outline of a right to anonymous communication becomes visible, as was shown in Chapter 8. On the other hand, various mechanisms were put in place that make it possible to remove the veil of anonymity for specific purposes. The second question touched upon the constitutional foundations for the protection of anonymous public communication. In the Netherlands, as well as in the United States, the relationship between anonymity and freedom of speech has been recognised. Both the American Supreme Court and the Dutch legislator have come to the conclusion that the true and unhindered exercise of this right cannot take place if the exercise thereof is subject to identification and registration. The possibility to remain anonymous is essential to individual self-fulfilment, the expression of individual opinion, and from a broader perspective, to the free flow of information and the stimulation of robust public debate. Other relevant constitutional rights include freedom of speech, freedom of religion, freedom of association and the right to informational privacy. Finally, the question was posed whether a right to communicate anonymously should be adopted in Dutch law. In light of the foregoing considerations, this question should be answered affirmatively. In the information society, the anonymity of actors in the communication process touches upon weighty societal and constitutional values that require a legal mechanism which, as a principal rule, grants the individual the choice of remaining anonymous and that creates a framework for the balancing of his interests against other individual and societal interests. The most effective way of ensuring that the mentioned interests are taken into consideration would be the recognition of an independent and enforceable right. This right should contain a few elements. Firstly, communicating individuals should be entitled to oppose the registration, storing and processing of identifying information when these actions infringe their constitutional rights in a disproportionate manner. As an accessory element, a right to notification should be adopted, that is to say: a right of the anonymous actor to be informed about an attempt to identify him. For the legislator the right to communicate anonymously would entail the duty to develop a coherent vision of the meaning of anonymity in the information age. Furthermore, the legislator should refrain from drafting statutes that make the anonymous publication, dissemination and reception of information punishable. In other words, no general obligations should be implemented that require a person to reveal his name, to register or to identify himself before he can engage in speech-related activities, unless weighty interests for doing so can be demonstrated.

Literatuurlijst

Alberdingk Thijm 2003
Chr.A. Alberdingk Thijm, 'Tussen droom en daad: peer-to-peer en privacy', *Privacy & informatie* (3) 2003, p. 105-112.

Alexander 1963
J. Alexander, *A brief narrative of the case and trial of John Peter Zenger, printer of the New York weekly journal,* Cambridge, Mass.: Belknap Press of Harvard University 1963.

Allience Public Technology 2003
Brief of Alliance for Public Technology e.a. as Amici Curiae in support of appellant Verizon Internet Services and urging reversal, WWW <http://www.eff.org/legal/cases/RIAA_v_Verizon/20030516_eff_amicus.pdf>, 16 mei 2003.

Asscher 1999
L.F. Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie*, Deventer: Kluwer 1999.

Asscher 2000
L.F. Asscher, 'Niemand als consument. Naar een evenwichtig grondrecht op anonimiteit', in: K. Stuurman, R. Westerdijk & C. Sander (red.), *De e-Consument. Consumentenbescherming in de Nieuwe Economie*, Den Haag: Elsevier Juridisch 2000, p. 7-20.

Asscher 2002
L.F. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving* (diss. Amsterdam UvA), Amsterdam: Cramwinckel 2002.

Asscher & Ekker 2003a
L.F. Asscher & A.H. Ekker (red.), *Verkeersgegevens, een juridische en technische inventarisatie*, Amsterdam: Cramwinckel 2003.

Asscher & Ekker 2003b
L.F. Asscher & A.H. Ekker, 'Anonimiteitswet is hard nodig', *De Volkskrant* 26 augustus 2003.

Asscher & Koops 2004
L.F. Asscher & B.J. Koops, 'Gegevens geven: een muisstille revolutie in het strafrecht', *Het Financieele Dagblad* 1 april 2004, p. 10.

Asscher & Simons 1886
B.E. Asscher & D. Simons, *Het nieuwe wetboek van Strafrecht vergeleken met den Code Pénal*, 's-Gravenhage: Gebr. Belinfante 1886.

Bäumler & Von Mutius 2003
H. Bäumler & A. von Mutius, *Anonymität im Internet, Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts*, Braunschweig; Wiesbaden: Vieweg, 2003.

Berlin1969
I. Berlin, *Four essays on liberty*, Londen: Oxford University Press, 1969.

Bill Analysis 2004
Assembly Bill 1143: Civil Procedure: Production of Consumer Information by Internet Servers, Senate Judiciary Committee, 15 juli 2003, WWW <http:/www.sen.ca.gov> (geraadpleegd 18 augustus 2005).

Blavin & Cohen 2002
J.H. Blavin & I. Glenn Cohen, 'Gore, Gibson & Goldsmith: The evolution of internet metaphors in law and commentary', *Harvard Journal of Law & Technology* (16) 2002, p. 265-285.

Blok 2002
P.H. Blok, *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht* (diss. Tilburg), Den Haag: Boom juridische uitgevers 2002.

Bobbio 1989
N. Bobbio, *Democracy and Dictatorship: The Nature and Limits of State Power*, Cambridge: Polity Press 1989.

Bodel Nyenhuis 1892
J.T. Bodel Nyenhuis, *De wetgeving op drukpers en boekhandel in de Nederlanden tot in het begin der XIXde eeuw* (diss. Leiden), Amsterdam: Vereeniging ter Bevordering van de Belangen des Boekhandels 1892 (*Dissertatio historico-juridica de iuribus typographorum et bibliopolarum in regno Belgico* [z.j.], vertaald door J. Soutendam en R. Jesse Jzn).

Bohman 1998
J. Bohman, 'The coming of age of deliberative democracy', *Journal of Political Philosophy* (6) 1998, p. 400-425.

De Bosch Kemper 1865
J. de Bosch Kemper, *Handleiding tot de kennis van het Nederlandsche staatsregt en staatsbestuur*, Amsterdam: Müller 1865.

Bovens 2003
M.A.P. Bovens, *De digitale republiek: democratie en rechtsstaat in de informatiemaatschappij*, Amsterdam: Amsterdam University Press 2003.

Brief America Online 2000
Appeal from order dated November 15, 2000 by the Court of Common Pleas of Allegheny County, Pennsylvania (Wettick, J.) Civil Division No. GD99-10264, WWW < http://www.politrix.org/foia/courts/melvin-v-doe-aa.htm> (geraadpleegd 18 februari 2005).

Brief Verizon 2003
Verizon's opening brief on appeal, WWW <http://www.epic.org/privacy/copyright/ verizon/Appeal_2_verizon_open.pdf>, 12 mei 2003.

Brown & Raysman 2001
P. Brown & R. Raysman, 'Discovering the identity of anonymous internet posters', *New York Law Journal* 11 september 2001.

Buyn 1867
L.A.P.F. Buyn, *Het regt tot eene volkomen onbelemmerde gedachte-uiting: eene strafregtelijke proeve*, Amsterdam: Müller 1867.

Bygrave & Koelman 2000
L.A. Bygrave & K.J.Koelman, 'Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems', in: P.B. Hugenholtz (ed.), *Copyright and electronic commerce: legal aspects of electronic copyright management*, Den Haag: Kluwer Law International, p. 59-124.

Center for Democracy & Technology 2003
Center for Democracy & Technology, *Domain name management policy*, WWW <http://www.cdt.org/dns/030904cdt.shtml>, 4 september 2003.

Cleiren & Nijboer 2002
C.P.M. Cleiren & J.F. Nijboer, *Strafrecht: de tekst van het Wetboek van Strafrecht en enkele aanverwante wetten voorzien van commentaar*, Deventer: Kluwer 2002.

Cohen 1996
J.E. Cohen, 'A right to read anonymously: A closer look at 'copyright management' in Cyberspace', *Connecticut Law Review* (28) 1996, p. 981.

Cohen 2003
J.E. Cohen, 'DRM and privacy', *Berkeley Technology Law Journal* (18) 2003, p. 575-617.

College bescherming persoonsgegevens 2003
College bescherming persoonsgegevens, *Onderzoek naar beleid omtrent 'geheime' nummers* (kenmerk z2001-0746), WWW <http://www.cbpweb.nl/ downloads_rapporten/ rap_2003_onderzoek_KPN.pdf16>, 16 mei 2003.

College bescherming persoonsgegevens 2004
College bescherming persoonsgegevens, *Implementatie artikel 5 Richtlijn 2002/58/EG en Ontwerp regeling universele dienstverlening en Eindgebruikersbelangen* (kenmerk z2003-1526/1666), WWW <http://www.cbpweb.nl/downloads_adv/z2003-1526.pdf>, 5 februari 2004.

Constant 1980
B. Constant, 'De la Liberté des Anciens Comparée à celle des Modernes', in: B. Constant, *De la liberté chez les modernes: écrits politiques*, Parijs: Le livre de poche 1980.

Van Daalen & Ekker 2003
O.L. van Daalen & A.H. Ekker, 'De provider als speurhond van de muziekindustrie. Kan hij gedwongen worden tot afgifte van identificerende informatie?', *JAVI*, 2003-4, p. 129-134.

Van Dale 1995
Groot woordenboek der Nederlandse taal, Utrecht: Van Dale Lexicografie 1995.

Dahlberg 2000
L.J. Dahlberg, *The internet and the public sphere: A critical analysis of the possibility of online discourse enhancing deliberative democracy* (diss.), Massey University 2000.

Dahlberg 2001
L.J. Dahlberg, 'The Internet and democratic discourse', *Information, Communication & Society* (4) 2001, p. 615-633.

Van Deinse 1867
A.J. van Deinse, *Het Wetboek van Strafregt (Code pénal) met de wijzigingen, daarin aangebragt sedert 1810 en laatstelijk bij de wetten van 29 Junij 1854, Staatsbl. 102 en 103: benevens de opgave van eenige speciale straf-verordeningen*, Middelburg: Altorffer 1867.

Diemer 1937
E. Diemer, *Vrijheid van drukpers, eenige opmerkingen over haar staatsrechtelijke regeling, voornamelijk in Nederland* (diss. Amsterdam VU), Rotterdam: Libertas 1937.

Dommering 1990
E.J. Dommering, 'Groppera en Autonic. Maken de Zwitsers gatenkaas van de Nederlandse Mediawet?', in: P.B. Hugenholtz (Jonge Balie Congrescommissie 1990), *Recht in de kijker: het recht en de media: bundel ter gelegenheid van het Jonge Balie Congres 1990*, Zwolle: Tjeenk Willink 1990, p. 55-70.

Dommering 2001
E.J. Dommering, 'Het ongebreideld verzamelen van gegevens: de voorstellen van de commissie Mevis', WWW <http://www.netkwesties.nl/editie24/column1.html>, 1 november 2001.

Dommering 2003
E.J. Dommering, 'Grensoverschrijdende censuur: het EHRM en oude en nieuwe media', in: J. Corbet & A. Berenboom, *Censuur: referaten van het colloquium van 16 mei 2003*, Brussel: Larcier 2003, p. 177-217.

Dommering e.a. 1999
E.J. Dommering e.a., *Handboek Telecommunicatierecht: inleiding tot het recht en de techniek van de telecommunicatie*, Den Haag: Sdu 1999.

Dommering e.a. 2000
E.J. Dommering e.a., *Informatierecht: fundamentele rechten voor de informatiesamenleving*, Amsterdam: Cramwinckel 2000.

Duke & Tamse 1987
A.C. Duke & C.A. Tamse (ed.), *Too mighty to be free: censorship and the press in Britain and the Netherlands*, Zutphen: De Walburg Pers 1987.

Van Eijk 2000
N.A.N.M. van Eijk, 'Domeinnamen zijn nummers!', *Mediaforum* 2000, p. 360-363.

Ekker 2002a
A.H. Ekker, 'Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2002, p. 77-83.

Ekker 2002b
A.H. Ekker, 'Bewaarplicht verkeersgegevens veroorzaakt digitale boterberg', *I&I* 2002, p. 2-3.

Ekker 2002c
A.H. Ekker, 'Anonimiteit en uitingsvrijheid op het Internet; het onthullen van identificerende gegevens door Internetproviders', *Mediaforum* 2002, p. 348-351.

Ekker 2004a
A.H. Ekker, 'Nog even en de politie kijkt voortdurend mee: Verplichte registratie van alle telefonie- en internetgegevens creëert spionagenetwerk van ongeëvenaarde omvang', *Het Parool* 3 juli 2004.

Elkin-Koren & Weinstock Netanel 2002
N. Elkin-Koren & N. Weinstock Netanel (red.), *The commodification of information*, Den Haag: Kluwer Law International 2002.

Evertsen de Jonge 1855
W.C.K. Evertsen de Jonge, *Tweede bijdrage over de zoogenoemde Délits de la presse*, Utrecht: Kemink 1855.

Fennema 2003
M. Fennema, *Over de kwaliteit van politiek elites* (oratie Amsterdam UvA), Amsterdam: Vossiuspers 2003.

Fennema & Maussen 2000
M. Fennema & M. Maussen, 'Dealing with extremists in public discussion. Front National and "Republican Front" in France', *The Journal of Political Philosophy* (8) 2000, p. 379-400.

FOBID 2005a
Federatie van Organisaties in het Bibliotheek-, Informatie, en Documentatiewezen, *Brief aan de Commissie voor Justitie van de Eerste Kamer der Staten-Generaal* (kenmerk: 6102-01-05), WWW <http://www.sitegenerator.bibliotheek.nl>, (geraadpleegd 8 juli 2005).

FOBID 2005b
Federatie van Organisaties in het Bibliotheek-, Informatie, en Documentatiewezen, *Tweede brief aan de Commissie voor Justitie van de Eerste Kamer der Staten-Generaal* (kenmerk: 6102-04-5), WWW <http://www.sitegenerator.bibliotheek.nl>, (geraadpleegd 8 juli 2005).

FOBID 2005c
Federatie van Organisaties in het Bibliotheek-, Informatie, en Documentatiewezen, *Reactie FOBID op Memorie van Antwoord op vragen Vaste Commissie voor Justitie, naar aanleiding van Wetsvoorstel Bevoegdheden Vorderen Gegevens* (kenmerk: 6102-08-05), WWW <http://www.debibliotheken.nl>, (geraadpleegd 6 juli 2005).

Foucault 1989
M. Foucault, *Discipline, toezicht en straf: de geboorte van de gevangenis*, Groningen: Historische Uitgeverij 1989 (*Surveiller et punir: naissance de la prison* 1975, vertaald door Vertalerscollectief).

Froomkin 1996
A.M. Froomkin, 'Flood Control on the Information Ocean. Living With Anonymity, Dgital Cach, and Distributed Databases', *Pittsburgh Journal of Law and Commerce,* (15) 1996, p. 395.

Gaines 1972
P.W. Gaines, *Political works of concealed authorship during the administrations of Washington, Adams, and Jefferson, 1789-1809*, Hamden Conn.: Shoe String Press 1972.

Garnham & Aksoy 1989
N. Garnham & A. Aksoy (red.), *European telecommunications policy research: proceedings of the Communications Policy Research Conference*, Amsterdam: IOS 1989.

De Graaf 1987
F. de Graaf, *Privacy en persoonsgegevens: het ontwerp van Wet persoonsregistraties*, Lelystad: Koninklijke Vermande 1987.

De Graaff & Janse de Jonge 1999
B.G.J. de Graaff & E.J. Janse de Jonge, 'De wet op de inlichtingen- en veiligheidsdiensten', *NJB* 1999, p. 1925-1931.

Van Gelder 1947
H.A. Enno van Gelder, *Vrijheid en onvrijheid in de Republiek: geschiedenis der vrijheid van drukpers en godsdienst van 1572 tot 1789*, Haarlem: Tjeenk Willink 1947.

Genootschap Amore Patriæ 1781
Genootschap Amore Patriæ, *Consideratien, in hoe verre het verbieden van naamlooze geschriften dienstig is, en welke daar onder moeten begreepen worden*, 1781.

Goedhart 1943
H.A. Goedhart, *De pers in Nederland*, Amsterdam: Nederlandsche Uitgeverij 'opbouw' 1943.

Groenboek convergentie 1997
Europese Commissie, *Groenboek over de convergentie van de sectoren telecommunicatie, media en informatietechnologie en de implicaties daarvan voor de regelgeving. Naar een aanpak voor de informatiemaatschappij*, COM(97)623 def., WWW <http://europa.eu.int/ISPO/convergencegp/97623nl.pdf>, 3 december 1997.

Groenveld 1987
S. Groenveld, 'The Mecca of authors? States assemblies and censorship in the seventeenth-century Dutch republic', in: A.C. Duke & C.A. Tamse (ed.), *Too mighty to be free: censorship and the press in Britain and the Netherlands*, Zutphen: De Walburg Pers 1987, p. 63-86.

Groep gegevensbescherming artikel 29 1997a
Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Aanbeveling 1/97. Wetgeving inzake gegevensbescherming en de media* (XV/5012/97-NL WP 1), WWW <http://europa.eu.int/comm/internal_market/ privacy/workingroup_en.htm>, 25 februari 1997.

Groep gegevensbescherming artikel 29 1997b
Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Aanbeveling 3/97. Anonimiteit op Internet* (XV D/5022/97 def. WP 6), WWW <http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm>, 3 december 1997.

Groep gegevensbescherming artikel 29 2000
Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Advies 5/2000 over het gebruik van openbare abonneelijsten voor omgekeerd zoeken of zoeken met meervoudige criteria* (5058/00/NL/DEF. WP 33), WWW <http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm>, 13 juli 2000.

Groep gegevensbescherming artikel 29 2003
Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Advies 2/2003 over de toepassing van de gegevensbeschermingsbeginselen op de Whois directories* (10972/03/NL/def. WP 76), WWW <http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm>, 13 juni 2003.

Groep gegevensbescherming artikel 29 2005
Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Working document on data protection issues related to intellectual property rights* (xxxx/05/EN WP 104), WWW <http://europa.eu.int/comm/ internal_market/privacy/workingroup_en.htm>, 18 januari 2005.

Guibault 2004
L. Guibault, 'Vous qui téléchargez des œuvres de l'Internet, pourrait-on savoir qui vous êtes?', *Revue du Droit des Technologies de l'Information* 2004-18, p. 9-31.

Habermas 1989
J. Habermas, *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*, Cambridge Mass: The MIT Press 1989 (*Strukturwandel der Öffentlichkeit* 1962, vertaald door T. Burger).

Habermas 1990
J. Habermas, 'Discourse ethics: Notes on philosophical justification', in: S. Benhabib & F. Dallmayr (red.), *The communicative ethics controversy*, Cambridge, Mass.: The MIT Press 1990, p. 60-110.

Van Hasselt 1861
W.J.C. van Hasselt, *Beschouwing over het voortdurend bestaan van Art. 283, 284 en 289 van het Wetboek van strafregt: (eene drukpersquestie)*, Amsterdam: Van Kesteren & zn. 1861.

Hazelhoff Roelfzema 1971
E. Hazelhoff Roelfzema, *Soldaat van Oranje: '40-'45*,'s-Gravenhage: Stok 1971.

Helberger 2005
N. Helberger, *Controlling access to content: regulating conditional access in digital broadcasting*, Den Haag: Kluwer Law International 2005.

Heemskerk 2004
W. Heemskerk, 'Hoe zat het ook alweer met … Anonieme gedaagden?', *Advocatenblad* (19) 2004, p. 885-886.

Van Heeswijk 2005
E. van Heeswijk, 'Kritiek op weblogs kaatst terug. "Dat is toch geen journalistiek"', WWW <http://villa.intermax.nl/digiproject/n/artikelen/uitgeefvormen.htm>, (geraadpleegd 19 augustus 2005).

De Hert 2003
P. de Hert, 'The case of anonymity in Western political philosophy. Benjamin Constant's refutation of republican and utilitarian arguments against anonymity', in: C. Nicoll, J.E.J. Prins & M.J.M. van Dellen (ed.), *Digital Anonymity and the Law. Tensions and Dimensions*, Zutphen: Koninklijke Wöhrmann 2003, p. 47-97.

Hins & Nieuwenhuis 2003
A.W. Hins & A.J. Nieuwenhuis (red.), *Van ontvanger naar zender: opstellen aangeboden aan prof. mr. J.M. de Meij*, Amsterdam: Cramwinckel 2003.

Hofman 1995
J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, Zwolle: W.E.J. Tjeenk Willink 1995.

Holmes 1984
S. Holmes, *Benjamin Constant and the Making of Modern Liberalism*, New Haven: Yale University Press 1984.

Den Hollander 2003
A. den Hollander, *Verboden bijbels: bijbelcensuur in de Nederlanden in de eerste helft van de zestiende eeuw* (oratie Amsterdam UvA), Amsterdam: Vossiuspers 2003.

Holvast 1986
J. Holvast, "*Op weg naar een risicoloze maatschappij?": de vrijheid van de mens in het informatie-tijdperk* (diss. Leiden), Den Haag: Academic Service 1986.

Holvast 1994
J. Holvast, 'ISDN, digitale snelweg en de consument', *Computerrecht* (6) 1994, p. 226-230.

Hooghiemstra 2001
T.F.M. Hooghiemstra, *Teksten en toelichting op de Wet bescherming persoonsgegevens*, Lelystad: Koninklijke Vermande 2001.

Van Hoogstraten & Berkvens 1992
P. van Hoogstraten & J.M.A. Berkvens (red.), *ISDN en privacy*, Amsterdam: Cramwinckel 1992.

Kent & Linette 2003
S.T. Kent & L.I. Millett (red.), *Who goes there?: authentication through the lens of privacy*, Committee on Authentication Technologies and Their Privacy Implications, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, Washington, D.C.: National Academies Press 2003.

Knuttel 1987
W.P.C. Knuttel, *Catalogus van de pamfletten-verzameling berustende in de Koninklijke Bibliotheek*, Utrecht: HES Publishers 1978.

Koelman 2003b
K.J. Koelman, *Auteursrecht en technische voorzieningen: juridische en rechtseconomische aspecten van de bescherming van technische voorzieningen*, Den Haag: Sdu Uitgevers, 2003.

Koolschijn 1997
G. Koolschijn, *Plato, Constitutie, Politeia*, Amsterdam: Polak & Van Gennep 1997.

Korthals Altes 1989
W.F. Korthals Altes, *Naar een journalistiek privilege. Voorstellen voor een journalistiek verschoningsrecht naar aanleiding van de Amerikaanse en Duitse rechtspraktijk* (diss. Amsterdam UvA), Amsterdam: Cramwinckel 1989.

Kronenberg 1948
M.E. Kronenberg, *Verboden boeken en opstandige drukkers in de Hervormingstijd*, Amsterdam: Van Kampen & zn. 1948.

Lawson & Schermers 1997
R.A. Lawson & H.G. Schermers, *Leading cases of the European Court of Human Rights*, Nijmegen: Ars Aequi Libri 1997.

Lessig 1999
L. Lessig, *Code and other laws of cyberspace*, New York: Basic Books 1999.

Lichtenberg 2003
J.I.A. Lichtenberg, 'Opt-in regime voor abonneegegevens: weet de ene hand wat de andere doet?', *Mediaforum* 2003, p. 226-231.

Lidsky 2000
L.B. Lidsky, 'Silencing John Doe: defamation & discourse in cyberspace', *Duke Law Journal* (49) 2000, p. 855-946.

Mac Gillavry 2001
E.C. Mac Gillavry, 'De voorstellen van de Commissie-Mevis: dwangmiddelen voor de informatiemaatschappij', *Nederlands Juristenblad* (76) 2001, p. 1411-1418.

Morrison 1996
A.B. Morrison (red.), *Fundamentals of American law*, New York: Oxford University Press 1996.

De Meij 1980
J.M. de Meij, 'Utrechtse Muurkrant-verordening is onverbindend', *Tijdschrift voor openbaar bestuur* 1980, p. 121-125.

De Meij 1998
J.M. de Meij, 'Uitingsvrijheid naar Zweeds model: een overladen menu van grondwettelijke delicatessen?', *Mediaforum* (10) 1998, p. 44-49.

De Meij e.a. 2000
J.M. de Meij, *Uitingsvrijheid, De vrije informatiestroom in grondwettelijk perspectief,* Amsterdam: Cramwinckel 2000.

Naples & Maher, 2002
G.J. Naples & M. Maher, 'Cybersmearing: a legal conflict between individuals and corporations', *The Journal of Information, Law and Technology (JILT)*, 2002-2.

Nicoll, Prins & van Dellen, 2003.
C. Nicoll, J.E.J. Prins & M.J.M. van Dellen (ed.), *Digital Anonymity and the Law. Tensions and Dimensions*, Zutphen: Koninklijke Wöhrmann 2003.

Nieuwenhuis 1997
A.J. Nieuwenhuis, *Over de grens van de uitingsvrijheid: een rechtsvergelijkende analyse van de regelgeving ten aanzien van pornografie en racistische uitlatingen*, Nijmegen: Ars Aequi Libri 1997.

Van Nispen 1988
C.J.J.C. van Nispen, 'Het rechterlijk bevel tot het noemen van de voorman', *BIE* 1988-4, p. 70-74.

NJCM 1999
'NJCM-commentaar op het wetsvoorstel op de inlichtingen- en veiligheidsdiensten', *NJCM-Bulletin* 1999-2, p. 307-318.

Nugter & Smits 1991
A.C.M. Nugter & J.M. Smits, 'Telecommunicatiediensten en privacybescherming: Ontwerp richtlijn SYN 288', *Computerrecht* 1991-5, p. 266-270.

O'Brien 2002
J. O'Brien, 'Putting a face to a (screen) name: The First Amendment implications of compelling ISPs to reveal the identities of anonymous internet speakers in online defamation cases', *Fordham Law Review* (70) 2002-6, p. 2745.

OECD 2005
Organisation for Economic Co-operation and Development, Working Party on the Information Economy, *Digital Broadband Content: Music* (DSTI/ICCP/IE(2004)12/FINAL), WWW <http://www.oecd.org/dataoecd/13/2/34995041.pdf>, 8 juni 2005.

Opzoomer 1854
C.W. Opzoomer, *Staatsregtelijk onderzoek*, Amsterdam: Gebhard 1854.

Orwell 1951
G. Orwell, *1984: a novel*, New York: New American Library 1951.

Peters 2003
J. Peters, 'Over 'Public Speech'en 'Public Figure': Amerikaanse invloed op 'onze' jurisprudentie.', in: A.W. Hins & A.J. Nieuwenhuis (red.), *Van ontvanger naar zender: opstellen aangeboden aan prof. mr. J.M. de Meij*, Amsterdam: Cramwinckel 2003, p. 273-293.

Du Pont 2001
G. du Pont, 'The criminalization of true anonymity in cyberspace', *Michigan Telecommications and Technology Law review* (7) 2001, p. 191.

Van der Pot/Donner/Prakke e.a. 2001
L. Prakke, J.L. de Reede & G.J.M. van Wissen, *Van der Pot-Donner. Handboek van het Nederlandse staatsrecht*, Deventer: W.E.J. Tjeenk Willink 2001.

Pring & Canan 1996
G.W. Pring & P. Canan, *SLAPPs: getting sued for speaking out*, Philadelphia: Temple University Press 1996.

Prins 2000a
J. E. J. Prins, 'What's in a name? De juridische status van een recht op anonimiteit', *Privacy en Informatie* (3) 2000, p. 153-157.

Prins 2000b
J. E. J. Prins. 'Privacy, consument en het recht op anonimiteit: een oud fenomeen in een nieuw jasje' in: K. Stuurman, R. Westerdijk, C. Sander (red.), *De e-Consument. Consumentenbescherming in de Nieuwe Economie*, Den Haag: Elsevier Juridisch 2000 p. 123-140.

Prins & Berkvens 2002
J. E. J. Prins en J. M. A. Berkvens, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2002.

Privacy International 2004
Privacy International, *Invasive, illusory, illegal, and illegitimate: Privacy International and EDRi response to the consultation on a framework decision on data retention*, WWW <http://www.privacyinternational.org/issues/terrorism/rpt/ responsetoretention.html> (geraadpleegd 16 februari 2005).

De Ranitz 1943
S.M.S. De Ranitz, 'De nieuwe wetgeving op het gebied van de pers', in: H.A. Goedhart, *De pers in Nederland*, Amsterdam: Nederlandsche Uitgeverij "opbouw" 1943, p. 238-259.

Rapport Franken 2000
Rapport Commissie Grondrechten in het digitale tijdperk, Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2000.

Rapport Mevis 2001
Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, *Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*, WWW <http://www.justitie.nl/pers/persberichten/archief/2001/gegevens.pdf>, mei 2001.

Recommendation R (95) 4
Recommendation No. R (95) 4 of the Committee of Ministers to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the Ministers' Deputies, WWW <http://cm.coe.int/ta/rec/1995/95r4.htm> (geraadpleegd 17 februari 2005).

Recommendation R (2000) 7
Recommendation No. R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information, adopted by the Committee of Ministers on 8 March 2000 at the 701st meeting of the Ministers' Deputies, WWW <http://cm.coe.int/ta/rec/2000/2000r7.htm> (geraadpleegd 16 februari 2005).

Van Ringelestijn, 2004
T. van Ringelestijn, 'Lycos-zaak schaadt anonimiteit nauwelijks', WWW <http://www.netkwesties.nl/editie103/artikel2.php>, 2 juli 2004.

Roggeveen 1933
L. Roggeveen, *De ongelofelijke avonturen van Bram Vingerling*, 's-Gravenhage: Van Goor 1933.

Rosen 2001
J. Rosen, *The unwanted gaze: the destruction of privacy in America*, New York: Random House 2001.

Rössler 2003
B. Rössler, 'Anonymität und Privatheit', in: H. Bäumler & A. von Mutius, *Anonymität im Internet, Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts*, Braunschweig; Wiesbaden: Vieweg, 2003, p. 27-40.

Schenk 1945
M.G. Schenk, *Geuzenliedboek 1940-1945*, Amsterdam: Buijten en Schipperheijn 1945.

Schimmel 1882
G.W. Schimmel, *Beschouwingen over de periodieke pers in verband met de verantwoordelijkheid der drukpersdelicten* (diss. Amsterdam UvA), Amsterdam: Muller & Co. 1882.

Schuijt 1998
G.A.I. Schuijt, 'Wet computercriminaliteit II: van uitgever en drukker naar tussenpersoon', *Mediaforum* 1998, p. 70-75.

Schuijt 2001
G.A.I. Schuijt, 'Kroniek van het Nederlandse mediarecht 1998-2001', *Auteurs & Media* 2001-3.

Schuijt 2003
G.A.I. Schuijt, 'Vrijheid van nieuwsgaring en toegang tot informatie' in: A.W. Hins & A.J. Nieuwenhuis (red.), *Van ontvanger naar zender: opstellen aangeboden aan prof. mr. J.M. de Meij*, Amsterdam: Cramwinckel 2003, p. 341-356.

Schuilenga e.a. 1981
J.H. Schuilenga (red.), *Honderd jaar telefoon: geschiedenis van de openbare telefonie in Nederland 1881-1981*, 's-Gravenhage: Staatsbedrijf der Posterijen, Telegrafie en Telefonie 1981.

Sciarone-Gorgels 1994
G.N.M. Sciarone-Gorgels, 'Privacy-aspecten van telecommunicatiediensten in rechtsvergelijkend perspectief', *Computerrecht* 1994-6, p. 230-238.

Sennett 1977
R. Sennett, *The fall of public man*, London: Cambridge University Press 1977.

Sentrop 1985
J.W. Sentrop, *Privacy-bescherming in Nederland: schets van een ontwikkeling*, Zwolle: Van Loghum Slaterus; Tjeenk Willink 1985.

Sieber & Höfinger
U. Sieber & F.M. Höfinger, 'Drittauskunftansprüche nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen', *MultiMedia und Recht* 2004, p. 575-585.

Simons 1883
D. Simons, *De vrijheid van drukpers in verband met het Wetboek van Strafrecht* (diss. Leiden), 's-Gravenhage: Gebr. Belinfante 1883.

Sims 2003
A. Sims, 'Court assisted means of revealing identity on the internet', in: C. Nicoll, J.E.J. Prins & M.J.M. van Dellen (ed.), *Digital Anonymity and the Law. Tensions and Dimensions*, Zutphen: Koninklijke Wöhrmann 2003, p. 271-285.

De Sitter 1869
L.U. de Sitter, *De drukpers als middel tot misdrijf* (diss. Groningen), Groningen: Wolters 1869.

Smidt 1881
H.J. Smidt, *Geschiedenis van het Wetboek van Strafrecht volledige verzameling van regeeringsontwerpen, gewisselde stukken, gevoerde beraadslagingen, etc.*, Haarlem: Tjeenk Willink 1881.

Smolla 1992
R.A. Smolla, *Free Speech in an Open Society*, New York: Vintage 1993.

Sobel 2000
D. Sobel, 'The process that "John Doe" is due: Addressing the legal challenge to internet anonymity', *Virginia Journal of Law and Technology* (5) 2000-3.

Sonofthethunder 2001
Sonofthethunder, *Bailin' Bailye & the Boys*, WWW <http://messages.yahoo.com/bbs?.mm=FN&action=m&board=4688055&tid=drte&sid=4688055&mid=2103> (geraadpleegd 18 februari 2005).

Spindler & Dorschel 2005
G. Spindler & J. Dorschel, 'Auskunftansprüche gegen Internet-Service-Provider. Zivilrechtliche Grundlagen und datenschutzrechtliche Grenzen', *Computer und Recht* 2005, p. 38-47.

Stein & Rueb 2002
P.A. Stein & A.S. Rueb, *Compendium van het nieuwe burgerlijk procesrecht*, Deventer: Kluwer 2002.

Stichting Moderne Media 1973
Stichting Moderne Media, *Visie op kabeltelevisie: medium en maatschappij, medium en techniek, medium en wet, medium en uitgever*, Amsterdam: Stichting Moderne Media 1973.

Stolwijk 2003
S.A.M. Stolwijk, *Biografisch Woordenboek van Nederland*, WWW <http://www.inghist.nl/Onderzoek/Projecten/BWN/>, bijgewerkt 5 september 2003.

Stromer-Galley 2002
J. Stromer-Galley, 'New Voices in the Public Sphere: A Comparative Analysis of Interpersonal and Online Political Talk', *Javnost/The Public* (9) 2002-2, p. 23-42.

Veen & Kop 1987
T.J. Veen & P.C. Kop (red.), *Zestig juristen: bijdragen tot een beeld van de geschiedenis der Nederlandse rechtswetenschap*, Zwolle: W.E.J. Tjeenk Willink 1987.

Van Veen & van der Sijs 1989
P.A.F. van Veen & N. van der Sijs, *Etymologisch woordenboek: de herkomst van onze woorden*, Utrecht: Van Dale Lexicografie 1989.

Verklaring wereldwijde informatienetwerken 1997
Ministeriële verklaring van de Ministerconferentie in Bonn over wereldwijde informatienetwerken, juli 1997, WWW <http://europa.eu.int/ISPO/bonn/Min_ declaration/i_finalnl.html > (geraadpleegd 16 februari 2005).

Declaration freedom of communication on the internet 2003
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, WWW <http://www.coe.int> (geraadpleegd 16 januari 2005).

Voorhoof 2000
D. Voorhoof, 'Raad van Europa wil betere bescherming van journalistiek bronnengeheim', *Mediaforum* 2000, p. 158-160.

Vos 1987
R.A.H. Vos, 'The Dutch Press under the German Occupation, 1940-1945', in: A.C. Duke & C.A. Tamse (ed.), *Too mighty to be free: censorship and the press in Britain and the Netherlands*, Zutphen: De Walburg Pers 1987, p. 179-194.

Vryheid der drukpers 1782
De Vryheid der drukpers, onafscheidelyk verknocht aan de vryheid der Republiek, Amsterdam: Petrus Conradi 1782.

Wallace 1999a
J.D. Wallace, 'Nameless in Cyberspace, Anonymity on the Internet', WWW <http://www.cato.org/pubs/briefs/bp54.pdf> (geraadpleegd 11 februari 2005).

Wallace 1999b
K.A. Wallace, 'Anonymity', *Ethics and Information Technology* (1) 1999-1, p. 21-31.

Weekhout 1998
I. Weekhout, *Boekencensuur in de Noordelijke Nederlanden*, Den Haag: Sdu 1998.

Wein 2002
K. Wein, 'Dendrite v. Doe: A new standard for protecting anonymity on internet message boards', *Jurimetrics* (42) 2002, p. 465-477.

Weintraub 1997
J. Weintraub, 'The Theory and Politics of the Public/Private Distinction', in: J. Weintraub & K. Kumar, *Public and Private in Thought and Practice*, Chicago/Londen: University of Chicago Press 1997, p. 1-42.

Wertheim & Wertheim-Gijse Weenink 1981
W.F. Wertheim & A.H. Wertheim-Gijsse Weenink, *Aan het volk van Nederland: het democratisch manifest van Joan Derk van der Capellen tot den Pol 1781*, Weesp: Heureka 1981.

Westin 1970
A.F. Westin, *Privacy and Freedom*, New York: The Bodley Head 1970.

Wilson & Fiske 1999
J.G. Wilson & J. Fiske (red.), *Appleton's Cyclopedia of American Biography*, New York: D. Appleton and Company 1999.

De Wit 2005
A. de Wit, 'Patriot Act in de polder. Bibliotheken verzetten zich tegen informatieplicht', *Bibliotheek* (5) 2005, p. 20-23.

Afkortingenlijst

BW	Burgerlijk Wetboek
C.C.P.	California Code of Civil Procedure
DMCA	Digital Millenium Copyright Act
DRM	Digital Rights Management
EFF	Electronic Frontier Foundation
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag tot Bescherming van de Rechten van de Mens
Gw	Grondwet
ICANN	Internet Corporation for Assigned Names and Numbers.
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IVBPR	Internationale Verdrag inzake Burgerrechten en Politieke Rechten
NAACP	National Association for the Advancement of Colored People
NAW-gegevens	Naam-, adres- en woonplaatsgegevens
Rb.	Rechtbank
RIAA	Recording Industry Association of America
SIDN	Stichting Internet Domeinregistratie Nederland
SLAPP	Strategic Lawsuit Against Public Participation
SMS	Short Message Service
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
Tw	Telecommunicatiewet
URL	Uniform Resource Locator
Vzngr.	Voorzieningenrechter
WPR	Wet Persoonsregistraties
Wbp	Wet bescherming persoonsgegevens

Trefwoordenregister

Over de auteur

Mr A.H. Ekker
Anton Ekker (1976) studeerde aan de Faculteit der rechtsgeleerdheid van de Universiteit van Amsterdam (1994-2001) en aan de Faculteit der rechtsgeleerdheid van de Universitat Autònoma te Barcelona (2000). Na het afronden van zijn studie was hij van 2002 tot 2005 als projectonderzoeker in dienst bij het Instituut voor Informatierecht van de Universiteit van Amsterdam (IViR). In het kader van het dissertatieonderzoek dat hij daar verrichtte, verbleef hij aan Georgetown University te Washington D.C. en aan University of California at Berkeley (Boalt Hall Law School). Sinds 2005 is hij als advocaat werkzaam bij SOLV advocaten te Amsterdam.

In de publicatiereeks van het Nationaal Programma voor Informatietechnologie en Recht zijn verschenen:

- ITeR nr. 1: J.E.J. Prins e.a., *In het licht van de Wet persoonsregistraties: zon, maan of ster? Verslag van een sociaal-wetenschappelijke evaluatie van de WPR,* Alphen aan den Rijn: Samsom BedrijfsInformatie 1995. [ISBN 90-14-05403-3]
- ITeR nr. 2: Jan Holvast, *Persoonsgegevens of niet: dat is de vraag*. Wim van de Donk e.a., *De WPR als zon, maan of ster*. Dirk Visser, *Auteursrechtvergoedingen in Europa en de VS*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1996. [ISBN 90-14-05427-0]
- ITeR nr. 3: Anne-Marie Kemna & Astrid Tuinder, met medewerking van Hans Franken & Dries Neisingh, *Regulering van encryptie*. Theo de Roos, Gerard Schuijt & Louisa Wissink, met medewerking van Peter Mostert & Lynn van der Velden, *Smaad, laster, discriminatie en porno op het Internet*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1996. [ISBN 90-14-05455-6]
- ITeR nr. 4: Wouter Hins, *De eeuwigdurende telecom-licentie*. Steven de Leeuw, met medewerking van Thijs Drupsteen, *Graafrechten voor telecommunicatievoorzieningen*. Maartje Verberne, Nico van Eijk & Egbert Dommering, *Veilen van frequenties voor Personal Communications Services*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1996. [ISBN 90-14-05469-6]
- ITeR nr. 5: Simone van der Hof, *Overheidsinformatie in de etalage. Belangen rondom de toegang tot overheidsinformatie*. Jitske de Jong, Marcel Rietdijk & Yvette Pluijmers, *Vastgoed persoonlijk benaderd. Bescherming van persoonsgegevens binnen vastgoedregistraties*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05559-5]
- ITeR nr. 6: Annemarie Beunen, *Digitale manipulatie van beeldmateriaal: grenzen aan de grenzeloosheid*. Mars van Leent, *Overheidstoezicht op bemiddelingsorganisaties in het auteursrecht*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05567-6]
- ITeR nr. 7: Simone van der Hof, met medewerking van Andreas Mitrakas, *De juridische status van de digitale handtekening*. Sylvia Huydecoper & Rob van Esch, *Geschriften en handtekeningen: een achterhaald concept?* Erik Schut en Elke Wiersema, met medewerking van Dries Neisingh, Anne-Marie Kemna & Peter Enneking, *Betrouwbaarheid van elektronische berichten in het betalingsverkeer.* ITeR workshop-verslag 17 december 1996, *De digitale handtekening. Juridische en organisatorische aspecten*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05568-4]
- ITeR nr. 8: Robert van Kralingen, Corien Prins & Jan Grijpink, met medewerking van Jan van Arkel & Franke van der Klaauw-Koops, *Het lichaam als sleutel. Juridische beschouwingen over biometrie*. Miriam Lips & Paul Frissen, *Wiring government. Integrated public service delivery through ICT.* Heleen de Vlaam, Hans de Bruijn & Ernst ten Heuvelhof, *Interconnection disputes. Sweden, Great Britain and the United States*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05569-2]

- ITeR nr. 9: Ingrid van den Berg, Hielke Hijmans & Aernout Schmidt (red.), *Regulering van het Internet*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997. [ISBN 90-14-05570-6]
- ITeR nr. 10: Dirk Visser, *Naar een multimedia-bestendig auteursrecht*. Kamiel Koelman, *Multimedialicenties. Enkele juridische en praktische knelpunten*. Jacqueline Seignette, *Exploitatie en clearance van intellectuele eigendomsrechten in een digitale omgeving*, Alphen aan den Rijn: Samsom BedrijfsInformatie 1998. [ISBN 90-14-05775-X]
- ITeR nr. 11: Anne-Wil Duthler, *Met recht een TTP! Een onderzoek naar juridische modellen voor een Trusted Third Party*, Deventer: Kluwer 1998. [ISBN 90-14-05776-8]
- ITeR nr. 12: Kees Stuurman & Hugo Wijnands, *Electronic commerce. Een privaatrechtelijk kader voor multilaterale EDI*. Yao-Hua Tan, Andreas Mitrakas & Walter Thoen, *A formal analysis of Incoterms for electronic commerce*. Pascal Kolkman & Robert van Kralingen, *Verschuivend vertrouwen. Methoden voor het waarborgen van betrouwbaarheid in het elektronisch rechtsverkeer*, Deventer: Kluwer 1998. [ISBN 90-14-05777-6]
- ITeR nr. 13: Maurice Schellekens, *Strafbare feiten op de elektronische snelweg*. Rik Kaspersen, André Hofman & Joop Verbeek, *Vertrouwelijkheid van e-mail*. Joop Verbeek, Cyril van der Net & Jaap Tempelman, *Netwerkzoeking in theorie en praktijk*, Deventer: Kluwer 1999. [ISBN 90-14-05778-4]
- ITeR nr. 14: Mireille van Eechoud & Jan Kabel, *Prijsbepaling voor elektronische overheidsinformatie*, Deventer: Kluwer 1998. [ISBN 90-26-83357-1]
- ITeR nr. 15: *Telecommunicatienummers en domeinnamen*. Egbert Dommering, *Het adres in cyberspace heeft geen plaats. Over adressen, telefoonnummers en domeinnamen*. Ted Clarkson e.a., *Mechanismen voor de verdeling van telecommunicatienummers*. Nico van Eijk, *Toekenning van servicenummers met alfanumerieke betekenis*. Ido Hurkmans, *Regulering van informatienummers*. Babiche Westerbrink, *De merken- en handelsnaamrechtelijke aspecten van het Domain Name System*, Deventer: Kluwer 1999. [ISBN 90-268-3426-8]
- ITeR nr. 16: Hielke Hijmans & Annemique de Kroon (red.), *Wetgeving voor de elektronische snelweg: nadere beschouwingen*, Deventer: Kluwer 1999. [ISBN 90-268-3486-1]
- ITeR nr. 17: Evert Neppelenbroek, Kees Stuurman & Hugo Wijnands, *Aansprakelijkheid voor schade aan apparatuur door mobiele telefoons*. Mark van Twist, Hans de Bruijn & Ernst ten Heuvelhof, *Verhandelbaarheid van vergunningen in de telecomsector*. Miriam Lips, Paul Frissen & Corien Prins, *Regulatory review through new media in Sweden, the UK, and the USA: convergence or divergence of regulation?* Willem Grosheide & Claire de Schepper, *De juridische status van telefoonnummers. Opmerkingen over de plaats van het regio-telefoonnummer in het Nederlandse vermogensrecht*, Deventer: Kluwer 1999. [ISBN 90-268-3475-6]
- ITeR nr. 18: Bernd van der Meulen e.a., *Vertrouwelijk gegeven. Juridische beschouwingen over de verstrekking van bedrijfsgegevens aan de overheid en het beheer daarvan door de overheid*, Deventer: Kluwer 1999. [ISBN 90-268-3474-8]
- ITeR nr. 19: Joop Verbeek e.a., *Politie en Intranet. Normering van netwerkkoppeling en grensoverschrijdend gebruik van multimediale databases op een internationaal politieel Intranet*, Deventer: Kluwer 1999. [ISBN 90-268-3476-4]

- ITeR nr. 20: Sylvia Huydecoper, *Aansprakelijkheid, intermediairs en Electronic Data Interchange*. Merijn Seelt, *Aansprakelijkheid van de softwareleverancier voor de Millenniumbug*, Deventer: Kluwer 1999. [ISBN 90-268-3538-8]
- ITeR nr. 21: Rik Kaspersen e.a., *Contracten van Internetproviders: een adequate basis voor zelfregulering?*, Deventer: Kluwer 1999. [ISBN 90-268-3553-1]
- ITeR nr. 22: H. Franken e.a., *ICT en straftoemeting: de conferentie van 23 april 1998*. A.H.J. Schmidt, *ICT en rechtvaardige strafoplegging bij zeden- en opiumzaken*, Deventer: Kluwer 1999. [ISBN 90-268-3564-7]
- ITeR nr. 23: Tomas Oudejans, *Electronic Highway of Electronic Subway? Verborgen merkinformatie op het Internet in Amerikaans perspectief*, Deventer: Kluwer 1999. [ISBN 90-268-3551-5]
- ITeR nr. 24: *Toepassing van privacyregels op elektronische berichten*. Sjaak Nouwt, *Privacyregels voor Internetberichten*. Jan Holvast, *Privacyregels voor EDI-berichten*, Deventer: Kluwer 1999. [ISBN 90-268-3598-1]
- ITeR nr. 25: Laurens Mommers, *Knowing the law. Legal information systems as a source of knowledge*, Deventer: Kluwer 1999. [ISBN 90-268-3596-5]
- ITeR nr. 26: Lodewijk Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie*, Deventer: Kluwer 1999. [ISBN 90-268-3601-5]
- ITeR nr. 27: Maartje Louise Verberne, *Verdeling van het spectrum*, Deventer: Kluwer 2000. [ISBN 90-268-3600-7]
- ITeR nr. 28: J.E.J. Prins e.a., *De universiteitsbibliotheek in het databankenrecht. Een juridisch perspectief op de vraag naar de noodzaak en wenselijkheid van een bibliotheek als informatieproducent*, Deventer: Kluwer 2000. [ISBN 90-268-3645-7]
- ITeR nr. 29: Judica I. Krikke, *Het bibliotheekprivilege in de digitale omgeving*, Deventer: Kluwer 2000. [ISBN 90-268-3644-9]
- ITeR nr. 30: Leonie Siemerink, *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het Internet*, Deventer: Kluwer 2000. [ISBN 90-268-3629-5]
- ITeR nr. 31: Bert-Jaap Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000. [ISBN 90-268-3655-4]
- ITeR nr. 32: Babette Aalberts & Simone van der Hof, *Digital Signature Blindness. Analysis of legislative approaches toward electronic authentication*, Deventer: Kluwer 2000. [ISBN 90-268-3656-2]
- ITeR nr. 33: H.S.M. Kruijer, *De exoneratieclausules in de algemene voorwaarden van de Federatie van Nederlandse ondernemingen in de Informatietechnologie (FENIT)*, Deventer: Kluwer 2000. [ISBN 90-268-3640-6]
- ITeR nr. 34: Luuk Matthijssen, *Jurisprudentiedatabanken. Een internationaal vergelijkende studie naar de publicatie van rechterlijke uitspraken met behulp van informatietechnologie*, Deventer: Kluwer 2000. [ISBN 90-268-3658-9]
- ITeR nr. 35: Joop Verbeek, Theo de Roos & Jaap van den Herik, *Interceptie van vertrouwelijke communicatie. De institutionele kansen en bedreigingen van het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9259-9]

- ITeR nr. 36: A.R. Lodder, A. Oskamp & M.J.A. Duker, *Informatietechnologische ondersteuning binnen het strafprocesrecht*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9263-7]
- ITeR nr. 37: D.W.F. Verkade, D.J.G. Visser & L.D. Bruining, *Ruimere octrooiëring van computerprogramma's: technicality of revolutie?*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9267-X]
- ITeR nr. 38: Pascal Kolkman, Robert van Kralingen & Sjaak Nouwt, *Privacy in bits en bytes. Privacyaspecten van electronic monitoring in netwerkomgevingen*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-540-9268-8]
- ITeR nr. 39: Bert-Jaap Koops e.a., met medewerking van Tomas Oudejans, *Overheden over internationalisering en ICT-recht. De standpunten van Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-5409-270-X]
- ITeR nr. 40: Mirjam Lips, Simone van der Hof & Kees Schalken, *Multiformity in information provision in a new media age. Challenged responsibilities for governments in Europe*, Den Haag: Sdu Uitgevers 2000. [ISBN 90-5409-271-8]
- ITeR nr. 41: Tina van der Linden-Smith, *Een duidelijk geval: geautomatiseerde afhandeling*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-5409-278-5]
- ITeR nr. 42: Jan Holvast, *Het gebruik van persoonlijkheidsprofielen in de publieke sector*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09260-4]
- ITeR nr. 43: Arno R. Lodder, Anja Oskamp & Aernout H.J. Schmidt (eds.), *IT support of the Judiciary in Europe*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09284-1]
- ITeR nr. 44: Clara Sander, *Consumentenbescherming bij transacties op afstand*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09285-X]
- ITeR nr. 45: Bert-Jaap Koops & Anton Vedder, met bijdragen van Jos Mensink & Stephan Raaijmakers, *Opsporing versus privacy: de beleving van burgers*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09343-0]
- ITeR nr. 46: Nirmala Sitompoel e.a., *(Zelf)regulering van nummers en domeinnamen*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09348-1]
- ITeR nr. 47: Tom van Dijk, *Elektronische aanbesteding*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09349-X]
- ITeR nr. 48: Eric Schreuders, *Data mining, de toetsing van beslisregels & privacy. Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09350-3]
- ITeR nr. 49: Christiaan Alberdingk Thijm, *Privacy vs. auteursrecht in een digitale omgeving*, Den Haag: Sdu Uitgevers 2001. [ISBN 90-12-09451-8]
- ITeR nr. 50: Hans de Bruijn e.a., *Samenloop bij toezicht*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09461-5]
- ITeR nr. 51: Corrette Ploem, *Wetenschapsbeoefening en belemmerende privacywetgeving: de wetgever in balans?*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09471-2]
- ITeR nr. 52: Edward Peeman, *Electronic Commerce en de Europese omzetbelasting*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09472-0]

- ITeR nr. 53: Justin Broeders e.a., *Vergunningen op Internet: meer dan gokken op een handhaafbaar stelsel*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09501-8]
- ITeR nr. 54: Babette Aalberts, *Beelddatabanken: stilstaand beeld in beweging?*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09502-6]
- ITeR nr. 55: Ruben Sietsma, Joop Verbeek & Jaap van den Herik, *Datamining en opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: strafprocesrecht versus recht op privacy*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09503-4]
- ITeR nr. 56: Georges van den Eshof e.a., *Opsporing van verborgen informatie. Technische mogelijkheden en juridische beperkingen*, Den Haag: Sdu Uitgevers 2002. [ISBN 90-12-09504-2]
- ITeR nr. 57: Kamiel Koelman, *Auteursrecht en technische voorzieningen. Juridische en rechtseconomische aspecten van de bescherming van technische voorzieningen*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-12-09505-0]
- ITeR nr. 58: Alexander Tsoutsanis, *Domeinnaamgeschillen: inbreuk, onrechtmatige daad of kwade trouw? Stand van zaken-onderzoek voor een geschillenregeling in het .nl-domein*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-12-09506-9]
- ITeR nr. 59: Jelle Arts, *Toegang tot publiek gefinancierde data*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-5409-373-0]
- ITeR nr. 60: Hein Dries, Serge Gijrath & Paul Knol, *Openbaarheid van netwerken en diensten in de Telecommunicatiewet*, Den Haag: Sdu Uitgevers 2003. [ISBN 90-5409-374-9]
- ITeR nr. 61: Kristianne Horrevorts & Rob van Esch, *De rol van zelfregulering bij de juridische erkenning van elektronische documenten en elektronische handtekeningen*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-335-8]
- ITeR nr. 62: Marjolijn van Gool & Rob van Esch, *Betalingen via Internet en faillissement*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-382-X]
- ITeR nr. 63: Hans Franken e.a., *Zeven essays over informatietechnologie en recht*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-391-9]
- ITeR nr. 64: Bart Schermer, *Opsporing vs. privacy in peer-to-peer netwerken*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-390-0]
- ITeR nr. 65: Harry Bouwman e.a., *Interconnectie: het vaste telefoonnet, het mobiele net en internet*, Den Haag, Sdu Uitgevers 2003. [ISBN 90-5409-393-4]
- ITeR nr. 66: Anne-Wil Duthler, *Digitale identiteit en pseudonieme digitale certificaten*, Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-395-1]
- ITeR nr. 67: Sophie van Loon, *Databankenrecht en mededinging, ontwikkelingen vanaf 1996 en evaluatie*, Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-407-9]
- ITeR nr. 68: Arno R. Lodder e.a., *Spam, spammer, …, analyse van het recht en de techniek rond elektronische ongevraagde commerciële communicatie, in het bijzonder via email*, Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-425-7]
- ITeR nr. 69: Joop Verbeek, *Politie en de Nieuwe Internationale Informatiemarkt, Grensregionale politiële gegevensuitwisseling en digitale expertise*, Den Haag, Sdu Uitgevers 2004. [ISBN 90 5409 424 9]

- ITeR nr. 70: Bert-Jaap Koops, Hanneke van Schooten en Merel Prinsen, *Recht naar binnen kijken: een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag, Sdu Uitgevers 2004. [ISBN 90 5409 430 3]
- ITeR nr. 71: Colette Cuijpers, *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn,* Den Haag, Sdu Uitgevers 2004. [ISBN 90-5409-435-4]
- ITeR nr. 72: Marga Groothuis, *Beschikken en digitaliseren. Over normering van de elektronische overheid*, Den Haag, Sdu Uitgevers 2004. [ISBN 90 5409 448 6]
- ITeR nr. 73: Sjaak Nouwt, *Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet*, Den Haag, Sdu Uitgevers 2005. [ISBN 90-1210-913-2]
- ITeR nr. 74: Marieke Berghuis, *Informatielicenties. Een analyse van UCITA en de rechtspraktijk in Nederland en de Verenigde Staten*, Den Haag, Sdu Uitgevers 2005. [ISBN 90-1210-956-6]
- ITeR nr. 75: Bart Lenselink, *De verlening van exploitatiebevoegdheden in het auteursrecht*, Den Haag, Sdu Uitgevers 2005. [ISBN 90-1211-104-8]
- ITeR nr. 76: Anton Ekker, *Anoniem communiceren: van drukpers tot weblog,* Den Haag, Sdu Uitgevers 2006. [ISBN: 90-1211-256-7]