

JURIDISCHE ASPECTEN VAN SPAM**

INLEIDING

Het is 12 april 1994, een gewone dag op Usenet. Totdat Laurence Canter en Martha Siegel, twee advocaten uit Arizona, daar verandering in brengen. Met behulp van een speciaal computer script overspoelen ze de duizenden nieuwsgroepen van Usenet met berichten waarin ze hun diensten als immigratie-advocaten aanbieden. Lawrence Siegel zou zijn actie later tegenover de nieuwssite CNET als volgt omschrijven: “For what we were doing back then -- selling immigration services -- the Internet seemed like a logical source because at that time it was still pretty much the domain of techies and people in academia. And a lot of them, at least in the United States, happened to be foreign born and were our target audience.”¹

De “techies” vonden het internet een minder voor de hand liggende keuze om advertenties te verspreiden. De gebruikers van Usenet reageerden woedend op het commerciële gebruik van de nieuwsgroepen. Canter en Siegel werden gebombardeerd met hate-mail en -faxen, ontvingen dreig-telefoontjes en werden vergeleken met ingeblikt varkensvlees. Spam – zo noemden de netizens de lawine commerciële berichten van Canter en Siegel.

WAT IS SPAM?

Spam is van origine verblijkt vleesbeleg van de Amerikaanse firma Hormel. De naam is een afkorting van de ingrediënten van zijn product: *shoulder of pork and ham*. Van spam wordt wel gezegd dat het alleen maar vult en geen enkele voedingswaarde of culinaire kwaliteit bezit. Tegenwoordig wordt de merknaam van het ingeblikte varkensvlees vooral geassocieerd met ongevraagde e-mail. Dat is net als het originele product slechts loze vulling zonder waarde.

Internet spam is altijd ongevraagd, meestal commercieel en wordt meestal ook in grote hoeveelheden verzonden. Een e-mail is *ongevraagd* als je geen al dan niet impliciete toestemming hebt verleend voor de ontvangst ervan. Daarom pleiten tegenstanders van spam ervoor dat verzending van commerciële e-mail alleen is toegestaan indien van te voren expliciet toestemming is verleend, de zogenaamde opt-in. Een *commercieel* e-mailbericht hoeft overigens niet per definitie afkomstig te zijn van een commerciële instelling. Ook liefdadigheidsmail kan gekwalificeerd worden als commercieel. Privacyorganisatie Bits of Freedom noemde een charitatieve mailing voor de nationale Help India-actie eens zelfs de “grootste verzending van ongevraagde e-mail (spam) in de Nederlandse geschiedenis”.

* Mr Chr.A. Alberdingk Thijm, advocaat te Amsterdam bij SOLV Advocaten (thijm@solv.nl)

** Dit artikel is een bewerking van een lezing voor de Eerste Nationale E-mail Marketing Conferentie (DENEK) d.d. 11 september 2002 te Amsterdam.

Het versturen van ongevraagde, commerciële bulk e-mail kan een interessante marketingtool zijn: de kosten zijn immers erg laag en het potentiële bereik groot. Voor een paar euro kan je al snel duizenden e-mailadressen kopen. De adressen worden overal op het net geoogst of “geharvest”: van nieuwsgroepen of discussielijsten, uit de WHOIS-database van de Stichting Internet Domeinnaam Registratie (SIDN) of verkregen van “gratis” dienstverleners, zoals een gratis internet provider. Het is niet altijd duidelijk dat een bericht spam is dus zal het dikwijls toch deels gelezen worden. En dat is natuurlijk precies wat de adverteerder wil. Eén van de grootste spammers ter wereld, de Amerikaan Ronald Scelton, beschrijft het eenvoudige business model als volgt: “I can send out 80 million e-mails offering vacation packages. More than 99.9 percent of the recipients may ignore that come-on. But if the e-mails go out by the millions, only a small fraction need respond to make the job pay off big.”²

Er zijn echter ook belangrijke *nadelen* verbonden aan het verzenden van spam. Het tast het vertrouwen van het internet aan. Mensen zijn bijvoorbeeld minder snel geneigd hun e-mailadres af te staan, waardoor de vrije communicatie op het net onder druk komt te staan. Internetjournalist Francisco van Jole voorspelt zelfs dat eens de situatie zal ontstaan dat men slechts nog e-mail wil ontvangen van bekenden.³ Daarnaast nemen spammers netwerkcapaciteit zoals bandbreedte in beslag. De kosten daarvan worden door de spammers op anderen afgewenteld. De Europese Commissie heeft eens uitgerekend dat het ophalen van spamberichten de consument jaarlijks 10 miljard euro kost.

Spammers vormen bovendien ook een risico voor internet beveiliging. Zo maken spammers dikwijls gebruik van zogenaamde open relays van mail servers van derden. Er wordt dan als het ware ingebroken op de server van een ander van waaruit vervolgens de berichten worden verzonden. Voor spammers heeft dit een aantal voordelen: het wordt moeilijk de afkomst van de boodschap te traceren, spam-filters worden omzeild en er kunnen grotere hoeveelheden berichten worden verstuurd. Ten slotte dreigt ook commerciële e-mail voor legitieme doeleinden met het “spam badwater” weggespoeld te worden. Zoals Van Jole terecht signaleert: “Gebruikers worden steeds minder kieskeurig in het verwijderen van ongewenste e-mail en gooien alles wat met commercie te maken heeft linea recta in de prullenbak, inclusief de aanbiedingen van bedrijven waar ze zelf om gevraagd hebben.”⁴

Naast deze meer praktische nadelen verbonden aan spam, is er ook een veelgehoord *principeel* argument. Veel mensen ervaren spam als hinderlijk en daardoor mede als een inbreuk op de privacy van de ontvangers. Ongevraagd wordt men benaderd met veelal controversiële, aanstootgevende boodschappen. Dikwijls gaat het om porno, anti-abortus teksten, religieuze boodschappen, dubieuze detectivebureautjes,

¹ Sharael Feist, “The Father of Modern Spam Speaks”, *CNET News.com* 26 maart 2002, <<http://news.com.com/2008-1082-868483.html>>

² John M. Moran, Spam King Living High In The Bayou, *CTNow* 30 juni 2002 <<http://www.ctnow.com/technology/hc-sp1sceltonjun30.story?coll=hc-headlines-home>>

³ *De Volkskrant* 10 maart 2002.

⁴ *De Volkskrant* 10 maart 2002.

pyramidespelen en word-snel-rijk acties. Dit principiële bezwaar tegen spam zal ik hieronder in meer detail bespreken.

SPAM EN PRIVACY

Waarom is het ontvangen van ongevraagde e-mail een inbreuk op de privacy? De consument wordt toch al jaren lastiggevalen met reclame via de gewone post? Al die reclame via radio en televisie, is dat soms ook een inbreuk op de privacy?

Het zijn geen eenvoudige vragen, die de verdedigers van een privacy-benadering van spam moeten beantwoorden. Het probleem zit hem in het recht op privacy zelf. Dat is heel ruim en daardoor bijzonder vaag. “Privacy is een van de leegste woorden die ik ken. Het circuleert frequent en iedereen weet dat het iets is wat geschonden of beschermd kan worden, zeker op het internet. Maar vraag eens om je heen om een definitie. Vaagheid alom.”, schrijft Marianne van den Boomen.⁵

Privacy wordt vaak omschreven als het recht om met rust gelaten te worden (relationele privacy). Dan is ieder telefoontje van mijn moeder op zondagochtend een inbreuk op mijn privacy. Zo makkelijk is het helaas niet. Het recht op privacy is geen absoluut recht en zal altijd moeten worden afgewogen tegen de rechten en belangen van anderen. De journalist Kuitenbrouwer heeft dat eens treffend een “conflict tussen ik en mezelf” genoemd: ik wil zoveel mogelijk van u weten maar scherm mezelf liever voor u af.⁶ Daarom is privacybescherming dan ook steeds een “afwegingsproces”. Factoren die daarbij in overweging kunnen worden genomen zijn: het *doel* van de inbreukmaker, de *aard* van de inbreuk en de mogelijkheden om de inbreuk te voorkomen.

Privacy is bovendien een *relationeel* begrip: de relatie en hoedanigheid waarin partijen tegenover elkaar staan is van belang. De inhoud en omvang van het begrip zijn afhankelijk van het antwoord op de vraag door wie en tegenover wie het recht wordt ingeroepen. Het is bijvoorbeeld van belang of privacybescherming wordt geclaimd door een patiënt ten opzichte van zijn arts, een werknemer ten opzichte van zijn werkgever of een consument ten opzichte van een grootgrutter. Omgekeerd maakt het uit of een beroep op privacy wordt gedaan ten opzichte van de overheid of de pers. De pers zal zich in het belang van vrije nieuwsgaring verdergaande inperkingen van andermans privacy mogen veroorloven dan een nieuwsgierige ambtenaar.

Daarbij geldt ook dat niet iedereen recht heeft op dezelfde mate van privacybescherming. Mensen die vanwege hun beroep publieke bekendheid genieten, hebben vrijwillig een deel van hun privacy opgegeven en hebben dus ook een minder vergaand recht op bescherming daarvan. Hoge bomen vangen veel wind, is een in dit verband een veel geciteerd gezegde.

⁵ M. van den Boomen, “Privacy is raar spul”, *Netkwesties* 19 juli 2002, <<http://www.netkwesties.nl/editie41/column1.html>>

⁶ *NRC Handelsblad* 25 maart 1999.

Mogelijk is het verspreiden van spam onder omstandigheden ook strijdig met de zogenaamde *informationele privacy*. Bij de *relationele privacy* gaat het om de controle over de eigen ruimte of omgeving, waardoor het individu tot op zekere hoogte zelf kan bepalen of het met rust gelaten wil worden of niet. Het is het recht op selectieve contactlegging, met als meest extreme variant het recht om met rust gelaten te worden. *Informationele privacy* is het recht op selectieve openbaarmaking. De nadruk ligt hier op de controle over de eigen gegevens, informatie en de beslissingen die daarop zijn gebaseerd. Een wet die uiting geeft aan de *informationele privacy* is de Wet bescherming persoonsgegevens (Wbp).

DE WET BESCHERMING PERSOONSGEGEVENS

Op 1 september 2001 is de Wet bescherming persoonsgegevens (Wbp) in werking getreden. De Wbp is opvolger van de Wet persoonsregistraties uit 1989. De belangrijkste aanleiding voor de nieuwe wet is gelegen in de omzetting van een Europese Privacyrichtlijn.⁷

Er is nogal wat kritiek op de Wbp gekomen, met name ten aanzien van de ‘overregulering’ van de wet. De Wbp tracht de omgang van persoonsgegevens tot in de finesses te regelen.⁸ Een monsterverbond van werkgeversorganisatie VNO-NCW en de Consumentenbond waarschuwde in 1998 al voor de verstrekende gevolgen. De wet zou doorslaan in haar goede bedoelingen en het verwerken van persoonsgegevens tot in de puntjes willen regelen. Volgens VNO-NCW en de Consumentenbond zal de wet het bedrijfsleven jaarlijks f 859 miljoen gaan kosten. Ook het Rathenau-instituut in Den Haag waarschuwde dat de WBP haar doel voorbij schiet. De wet zou enkel zijn gericht op het verwerken van persoonsgegevens, terwijl ze burgers juist zou moeten beschermen tegen de *gevolgen* daarvan. Bij de analyse van de Wbp past ook een waarschuwing: gezien de jonge leeftijd van de wet bestaat er weinig ervaring met de toepassing ervan. Afgewacht moet worden of een aantal ogenschijnlijk rigide regels ook in de praktijk stringent zullen worden toegepast.

De reikwijdte van de Wbp wordt bepaald door de centrale begrippen ‘persoonsgegeven’ en ‘verwerken’. Het object van de regelgeving is de verwerking van persoonsgegevens. Beide begrippen worden bijzonder ruim gedefinieerd. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke (levende) persoon. Een persoon kan worden aangemerkt als identificeerbaar, indien de identiteit zonder onevenredige inspanning kan worden vastgesteld. Ook zonder direct identificeerbare gegevens zoals naam, adres, woonplaats kan identificatie mogelijk zijn. Een e-mail adres maakt soms directe identificatie mogelijk, namelijk als het adres de gehele naam van de houder van het adres bevat. Meestal zal het echter om een indirect identificerend gegeven gaan: via tussenkomst van de internet service provider kan de betreffende houder van het adres worden geïdentificeerd.

⁷ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995, PbEG 1995 L 281/31.

⁸ J.E.J. Prins en J.M.A. Berkvens, ‘De wet bescherming persoonsgegevens’, in: J.E.J. Prins en J.M.A. Berkvens, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2002, p. 77.

Onder ‘verwerking’ wordt iedere handeling of elk geheel van handelingen met betrekking tot persoonsgegevens verstaan. Daarmee valt praktisch iedere handeling ten aanzien van persoonsgegevens onder het bereik van de wet. In de Wbp worden onder meer expliciet genoemd: het verzamelen, vastleggen, ordenen, bijwerken, wijzigingen, raadplegen, gebruiken, samenbrengen en verstrekken door middel van doorzending. De materiële normen van de Wbp zijn van toepassing op iedere verwerking die plaatsvindt, ook al zijn het opeenvolgende handelingen. Daarnaast wordt het begrip verwerking gebruikt om het samenhangend geheel van handelingen aan te duiden. Opvallend is dat de mogelijke relevantie van de verwerking voor de persoonlijke levenssfeer niet terzake doet; ook zuiver technisch vereiste handelingen vallen onder het bereik van de Wbp.

Zoals gezegd, zal een e-mailadres doorgaans wel te kwalificeren zijn als een persoonsgegeven. De restricties die de Wbp stelt aan het verwerken van persoonsgegevens zijn dan onverkort van toepassing. Zo bepaalt artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Het is het eerste artikel van het hoofdstuk ‘Voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens’ en kan wel als het ‘moederartikel’ van de wet worden beschouwd.⁹ Iedere verwerking kan aan de open geformuleerde normen ‘behoorlijk’ en ‘zorgvuldig’ worden getoetst.

Daarnaast bevat artikel 8 Wbp een limitatieve opsomming van de gronden die een gegevensverwerking rechtvaardigen, waarvan er twee in casu van belang zijn: de betrokkene heeft zijn *ondubbelzinnige* toestemming voor het gebruik van zijn e-mailadres gegeven (artikel 8 sub a Wbp) of degene die het e-mailadres gebruikt heeft een gerechtvaardigd bedrijfsbelang bij het verwerken van het persoonsgegeven (artikel 8 sub f Wbp).

In het geval van toestemming moet deze ‘ondubbelzinnig’ zijn, dat wil zeggen, dat er geen twijfel mag bestaan over de vraag of deze is gegeven. Daarvan is geen sprake indien de betrokkene slechts de mogelijkheid van bezwaar tegen de verwerking openstaat. Als een dergelijke opt-out mogelijkheid is geboden, kan men immers uit het uitblijven van een reactie niet afleiden dat men toestemt in het gebruik voor bijvoorbeeld direct marketing. Bovendien moet de reikwijdte van de toestemming duidelijk zijn en moet de toestemming op basis van de juiste informatie zijn gegeven. De toestemming kan ook altijd weer worden ingetrokken, maar een dergelijke intrekking heeft geen terugwerkende kracht. Indien er twijfel over de toestemming bestaat, rust er op degene die het e-mailadres wil gebruiken een verificatieplicht.

Verder kan het verzamelen en gebruiken van e-mailadressen toegestaan zijn indien de gegevensverwerking: “noodzakelijk is voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke of een derde aan wie de gegevens worden verstrekt, tenzij het belang of de

⁹ E. Schreuders, *Data mining, de toetsing van beslisregels & privacy*, Sdu Uitgevers: Den Haag 2001, p. 100.

fundamentele rechten van de vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.”¹⁰

Deze grondslag biedt een vangnet voor de gevallen die niet gerechtvaardigd zijn op grond van de andere grondslagen van artikel 8. Het is dus een soort restbepaling, wat mede geïllustreerd wordt door het gebruik van veel open geformuleerde begrippen. Zo moet de verwerking allereerst “noodzakelijk” zijn. Deze noodzakelijkheid moet in verhouding tot het doel worden beoordeeld: een gegevensverwerking is niet noodzakelijk voor het behartigen van het belang van de verantwoordelijke als dit belang op een minder ingrijpende of eenvoudiger manier kan worden gediend.¹¹ Bovendien moet er sprake zijn van een “gerechtvaardigd belang”. Het doen van een mailing om een nieuw product onder de aandacht van de bestaande klanten te brengen, kan bijvoorbeeld gezien worden als een gerechtvaardigd belang.¹²

Een e-mailadres mag op grond van de Wbp slechts worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat hierbij om de eerste fase van verwerken: het verzamelen. Het daaropvolgende, *secundair* gebruik van e-mailadressen zal alleen zijn toegestaan indien dit gebeurt op een wijze die verenigbaar is met de doeleinden waarvoor ze in eerste instantie zijn verkregen. Bij de beoordeling of een secundaire verwerking verenigbaar is met het primaire doel, moet met een aantal verschillende factoren rekening worden gehouden, waaronder: a) de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen; b) de aard van de betreffende gegevens; c) de gevolgen van de beoogde verwerking voor de betrokkene; d) de wijze waarop de gegevens zijn verkregen en e) de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Dat betekent dat een belangenafweging uitwijst of een e-mailadres voor spam mag worden gebruikt. Wat betreft de mogelijke gevolgen van de verwerking wordt in de Memorie van Toelichting het volgende opgemerkt: “Het gebruik van persoonsgegevens voor [direct marketing] doeleinden heeft geen invloed op iemands mogelijkheden tot maatschappelijke ontplooiing, noch leidt dit ertoe dat iemand het voorwerp [wordt] van bijzondere aandacht van overheidsorganen. Ieder is vrij de aan hem geadresseerde informatie al dan niet gelezen weg te werpen zonder dat dit enige gevolgen voor hem heeft.” Daarmee geeft de wetgever dus aan de inbreuk op de privacy gering te achten.

Wanneer e-mailadressen voor direct mail doeleinden worden gebruikt, dienen de betrokkenen actief te worden geïnformeerd over de identiteit van degene die de persoonsgegevens gebruikt, de doeleinden van de verwerking en over nadere aspecten voorzover dat nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen.¹³ De wijze waarop de e-mailadressen worden verkregen, zijn van belang voor de informatieplicht. Indien de gegevens van de betrokkenen zelf worden verkregen, moeten deze

¹⁰ Artikel 8 sub f Wbp.

¹¹ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 87.

¹² *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 87.

voorafgaand aan verkrijging worden geïnformeerd. Als de e-mailadressen van derden worden verkregen, moeten de betrokkenen in beginsel op het moment van vastlegging worden geïnformeerd. Indien het individueel informeren onevenredige inspanning vergt, kan hiervan worden afgeweken. Wel zal dan bijvoorbeeld via de krant informatie moeten worden verstrekt. Ook is men verplicht de herkomst van de e-mailadressen vast te leggen.

De Wbp bepaalt verder dat indien gegevens worden verwerkt voor direct marketing doeleinden de betrokkene daartegen te allen tijde kosteloos verzet moet kunnen aantekenen. Bovendien moet in iedere e-mail die gezonden wordt op de mogelijkheid van dit verzet worden gewezen.

XS4ALL VS. AB.FAB

De mogelijkheden om op basis van de Wbp en andere wet- en regelgeving op te treden tegen spammers zijn getest in een procedure tussen enerzijds XS4ALL en een aantal van haar abonnees en anderzijds Ab.Fab. XS4ALL is een internet service provider, die de privacybescherming van haar abonnees hoog in haar vaandel heeft staan. Ab.Fab houdt zich bezig met direct marketing via e-mail. Zij zendt op verzoek van opdrachtgevers als NRC Handelsblad grote aantallen commerciële e-mails, ook als de geadresseerden daarvoor geen toestemming hebben gegeven. Ab.Fab biedt een opt-out mogelijkheid. De vraag die in deze procedure centraal stond, is of dat voldoende is.

Het Hof Amsterdam, dat de zaak in tweede instantie behandelde, merkt eerst op dat e-mailadressen vaak aan te merken zijn als persoonsgegevens. Volgens het hof rechtvaardigt “de wijze waarop met name vele particuliere consumenten hun e-mailadres plegen in te richten” de veronderstelling dat een aanzienlijk deel van de e-mailadressen waarover Ab.Fab beschikt bescherming verdient op basis van de Wet bescherming persoonsgegevens. Het hof is dus van mening dat de wijze waarop een e-mailadres wordt ingericht relevant is voor de beoordeling of er sprake is van een persoonsgegeven. Dat lijkt mij onjuist. Zoals hierboven is aangegeven, zullen gegevens die indirect, via nadere stappen, in verband kunnen worden gebracht met een bepaald persoon kwalificeren als persoonsgegeven. Dat is het geval met een e-mailadres. Slechts indien doeltreffende maatregelen zijn genomen waardoor daadwerkelijke identificatie redelijkerwijs is uitgesloten, zal er geen sprake zijn van een persoonsgegeven.¹⁴

De analyse van het hof of het gebruik van de e-mailadressen door Ab.Fab is toegestaan, vindt louter plaats onder de vangnet bepaling van artikel 8 sub f Wbp. Het hof komt op grond daarvan tot de slotsom dat de gegevensverwerking door Ab.Fab noodzakelijk is voor de behartiging van haar gerechtvaardigde commerciële belang als marketeer, gespecialiseerd in direct marketing per e-mail. Vervolgens bespreekt het hof de vraag of Ab.Fab het belang en de bescherming van de persoonlijke levenssfeer van haar geadresseerden voldoende respecteert, zowel uit oogpunt van proportionaliteit als uit oogpunt van subsidiariteit. Er dient dus een afweging van het belang van Ab.Fab en dat van haar geadresseerden plaats

¹³ Artikelen 33 en 34 Wbp.

¹⁴ Zie *Kamerstukken II 1997/98*, 25 892, nr. 3, pp. 48-49.

te hebben. Bij die afweging betreft het hof de *aard* van de persoonsgegevens, het *gebruik* van de persoonsgegevens en de wijze waarop Ab.Fab rekening houdt met de *belangen* van de geadresseerden.

Het hof oordeelt dat een e-mailadres niet een persoonsgegeven is van gevoelige aard. Een gewoon adres vindt het hof schijnbaar een gevoeliger gegeven. Ontdekking van een e-mailadres dat verborgen had moeten blijven, heeft volgens het hof in het algemeen minder ingrijpende gevolgen dan ontdekking van een reëel adres. Dit omdat iemand meestal relatief gemakkelijk van e-mailadres kan veranderen zonder sporen na te laten en zonder al te veel kosten of nadelige gevolgen. Ik vraag me af of dit juist is.

De inbreuk op de privacy in het geval van spammen is kwalijker dan in het geval van direct marketing via de gewone post. Een e-mailadres is persoonlijker. Daarmee wordt iemand direct bereikt: veelal op de werkplek of via de mobiele telefoon of PDA, waarmee e-mail kan worden opgehaald. Het ontvangen van ongevraagde e-mail is verder moeilijk te negeren, zoals een reclamefolder op de deurmat dat wel is. Niet altijd is direct duidelijk dat het om reclame gaat en zal de e-mail eerst geopend worden. Bovendien kan een e-mailadres volstrekt waardeloos worden door een stortvloed van spam, terwijl dat met de deurmat wel mee zal vallen. Ten slotte zal het meestal niet eenvoudig zijn om van e-mailadres te veranderen, vooral niet binnen een onderneming waar iedereen hetzelfde type e-mailadres hanteert, zoals voornaam@bedrijfsnaam.nl.

In de tweede plaats oordeelt het hof dat de aard, inhoud, omvang en frequentie van het gebruik van de e-mailadressen door Ab.Fab niet buiten proporties is. De reclame van Ab.Fab is volgens het hof van een aanvaardbaar niveau zonder obscure herkomst. Verder is het dataverkeer waarmee Ab.Fab de geadresseerden opzadelt relatief bescheiden van omvang (maximaal 20 tot 25 Kb) en frequentie. Het binnenhalen van haar berichten levert voor de geadresseerden daarom weinig tijdsverlies en, als er al afzonderlijke kosten aan verbonden zijn, zeer geringe kosten op. Ten slotte voorziet Ab.Fab al haar berichten van een kenmerk, waardoor de berichten al in de inbox van de ontvanger herkenbaar zijn als reclameboodschap.

In de derde plaats merkt het hof op dat Ab.Fab iedere geadresseerde in elk van haar e-mailberichten de mogelijkheid aanbiedt om te laten weten verder niet van dergelijke reclame gediend te zijn. Dat betekent volgens het hof dat zij ervan blijk geeft de persoonlijke levenssfeer van haar geadresseerden in de toekomst te willen respecteren.

Het bovenstaande afwegende komt het hof tot de slotsom dat tegenover het belang van Ab.Fab als gespecialiseerde e-marketeer geen zwaarder wegende belangen van haar geadresseerden staan: “Vanwege haar specialisatie heeft Ab.Fab geen ander medium ter beschikking dan elektronische post. De wijze waarop zij haar berichtenverkeer inricht, is niet buiten proportie. De “overlast” die zij bij geadresseerden veroorzaakt alsmede de inbreuk op hun persoonlijke levenssfeer is relatief gering.”, aldus het hof.

Zoals het hof zelf erkent, is de houdbaarheid van het arrest gering. Uiterlijk op 31 oktober 2003 moet in alle lidstaten van de Europese Unie een verbod op spam gelden op grond van de richtlijn Privacy in de sector elektronische communicatie.

RICHTLIJN PRIVACY IN DE SECTOR ELEKTRONISCHE COMMUNICATIE

Na een verhitte strijd tussen de Europese Commissie en het Europese Parlement is medio 2002 uiteindelijk een Europese richtlijn aangenomen die het verzenden van ongevraagde, commerciële e-mail aan banden legt. Het verzenden van e-mail met het oog op direct marketing is alleen toegestaan aan degenen die daar van te voren uitdrukkelijk hun toestemming voor hebben gegeven.

De Europese Commissie was altijd al groot voorstander van een opt-in regime en had daartoe in juli 2000 een voorstel voor een richtlijn ingediend. Onder druk van diverse lobbygroepen uit de direct marketing-branche heeft het Europese Parlement zich daartegen echter fel verzet. Volgens het Parlement moesten de lidstaten zelf bepalen of ze opt-in of opt-out zouden invoeren. De Commissie zag daarin echter een belemmering voor de totstandkoming van de interne markt.¹⁵ Als verschillende landen een ander regime zouden toepassen, zou het direct marketeers in landen met een opt-in regime nog steeds toegestaan zijn spam te versturen naar landen met een opt-out stelsel. Bovendien zou het tot een onwerkbaar situatie leiden, aangezien niet altijd duidelijk is vanuit welk land de spam wordt verzonden.

Uiteindelijk hebben Commissie en Parlement een compromis bereikt door bedrijven toe te staan hun bestaande klanten met aanbiedingen te benaderen voor “eigen gelijkaardige producten of diensten”, mits deze klanten de gelegenheid wordt geboden bezwaar te maken tegen het gebruik van hun e-mailadressen.

Hoofregel is dat het gebruik van automatische oproepsystemen zonder menselijke tussenkomst (automatische oproepapparaten), fax of e-mail met het oog op direct marketing alleen zijn toegestaan met betrekking tot abonnees die daarin vooraf hebben toegestemd, met andere woorden, opt-in. Die toestemming kan on-line door middel van een vinkje in een daartoe bestemd hokje worden gegeven. Niet duidelijk is wanneer er precies sprake is van toestemming. De toestemming hoeft niet “ondubbelzinnig” te zijn, zoals op grond van de Wbp. Er worden overigens geen vereisten gesteld ten aanzien van de hoeveelheid berichten die worden verstuurd. Ook het verzenden van een enkele commerciële e-mail kan dus in strijd zijn met de richtlijn, indien deze ongevraagd en commercieel zijn.

Belangrijk is dat de richtlijn alleen *commerciële* spam verbiedt. Er moet sprake zijn van “direct marketing”. Dat is opvallend, omdat de kwalijke gevolgen van spam zullen intreden ongeacht de inhoud van het bericht. Veel spam is religieus, politiek of filosofisch van aard. Zoals John Gilmore terecht opmerkt: “What is objectionable about "spam" is that it is uninteresting to the recipient and sent in bulk. Whether it is an ad, a plea for charitable donations, a call for political action, a request for votes, a patriotic declaration during a national emergency, or an incomprehensible rant, people don't want to see it

¹⁵ Overweging 40.

in their mailbox.”¹⁶ En dan zijn er ook nog de berichten die je niet iets willen verkopen, maar er alleen op uit zijn je op te lichten. Denk aan de beroemde Nigeriaanse e-mails: wij willen graag 152 miljoen dollar op uw bankrekening storten. Dat is dus geen spam, maar slechts scam.

Wat onder “direct marketing” moet worden verstaan, is niet duidelijk. De richtlijn geeft geen definitie van het begrip. Mogelijk zou hierbij aansluiting kunnen worden gezocht bij de Wet bescherming persoonsgegevens, waarin het begrip is gedefinieerd als verwerking “in verband met de totstandkoming of instandhouding van een directe relatie tussen de verantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële of charitatieve doelen”.¹⁷

De vraag of bepaalde spam als “commercieel” moet worden aangemerkt, kwam ook aan de orde in een recente procedure bij de rechter te Almelo. De gedaagde in deze zaak is Dr Matthias Rath, een handelaar in vitaminepreparaten, die zich verzet tegen bepaalde regelgeving ter regulering van onder meer de handel in vitaminepreparaten. Via de website van Rath konden internetgebruikers e-mails naar leden van de Tweede Kamer zenden om te protesteren tegen de op handen zijnde wetgeving. In totaal zijn 604 miljoen e-mails naar de Kamerleden verzonden. De rechter zoekt bij zijn beslissing aanknopingspunt bij de richtlijn Privacy in de elektronische sector. Hij oordeelt dat de e-mails “commercieel” zijn, aangezien de onderneming van Dr Mathias Rath er belang bij heeft dat de wetgeving op dat gebied van vitaminepreparaten soepel blijft dan wel wordt. Er bestaat volgens de rechter een rechtstreeks verband tussen de verkoop van vitaminepillen en de e-mail die via de websites van gedaagden naar de Staat wordt gestuurd. Hiermee is naar het oordeel van de voorzieningenrechter het commerciële karakter van de spam voldoende aannemelijk.

WETGEVING GESCHIKT OM SPAM TE BESTRIJDEN?

Het is de vraag of deze specifieke wetgeving geschikt is om spam effectief te bestrijden. De meeste spam komt uit derde landen, waar men immuun is voor de Europese wetgeving. Ook staat dergelijke wetgeving op gespannen voet met de vrijheid van meningsuiting, die ook commerciële berichten beschermt. “Anti-spam is to Internet freedom as anti-terrorism is to Constitutional rights. The most ridiculous justifications are routinely accepted and believed. The lemmings all cheer when somebody restricts our freedom to communicate "because of spam".”, schrijft scepticus Gilmore.¹⁸

Beter lijkt het technische middelen in te roepen om spam tegen te gaan. Sommige mail application zoals SpamAssassin kunnen spam herkennen en vernietigen. Ook is het mogelijk met behulp van blacklists spam tegen te gaan. XS4ALL is hier in Nederland toe overgegaan. SpamCop, SPEWS en Spamhaus zijn

¹⁶ John Gilmore, *What to do about spam? Use smarter mail readers*, Politechbot.com 28 februari 2002 <<http://www.politechbot.com/p-03204.html>>

¹⁷ Artikel 41 Wbp. Zie ook C.W. Noorda, ‘Nieuwe Europese regels voor cookies en spam’, *Mediaforum* 2002/9, p. 274.

¹⁸ John Gilmore, *Earthlink's anti-spam censorship*, Politechbot.com 8 september 2002 <<http://www.politechbot.com/p-03967.html>>

voorbeelden van dergelijke blacklists. Een ander aardig initiatief is Habeas, waarmee mail een keurmerk kan krijgen, dat het “the e-mail you want” is.

Ten slotte zijn de wetten van de markt hopelijk behulpzaam in het tegengaan van spam. In de Verenigde Staten bestaat op federaal niveau geen algemene privacy of anti-spam wet. Wel hebben achttien individuele Staten anti-spam wetgeving aangenomen. Deze kennen doorgaans een opt-out regime. Daarnaast gelden in de Verenigde Staten gewoon de wetten van de markt. Opvallend is dat op grond daarvan een opt-in stelsel wordt bepleit. Volgens marketinggoeroe Seth Godin, schrijver van het boek *Permission Marketing*, zijn opt-in e-mailcampagnes vele malen effectiever dan spam: “E-mailadressen zijn op zichzelf niets waard. Je kunt tegenwoordig 600 miljoen e-mailadressen kopen voor 600 dollar. Maar als je die mensen een e-mail stuurt, zullen ze je haten. Je hebt meer nodig dan alleen een e-mailadres; je hebt het recht of de toestemming nodig om te corresponderen.”

CONCLUSIE

Direct e-mail gaat volgens de gerenommeerde onderzoeksbureaus een gouden toekomst tegemoet. Het Amerikaanse bureau Jupiter voorspelt zelfs dat de markt voor reclame-mail de komende jaren gaat verveertigvoudigen tot 7,3 miljard e-mails in 2005. Dat betekent een jaarlijkse stijging van 40 tot 1600 e-mails per jaar, oftewel meer dan 30 mails per week. Hopelijk vergeten de verzenders van de mails niet van te voren even toestemming te vragen. Dat is niet alleen beter voor de consument, maar ook voor de marketeer. Ook de aartsvader van de moderne spam, de advocaat Canter lijkt deze gedachte tegenwoordig te huldigen. In een interview met CNET News.com uit hij zijn twijfels over de effectiviteit van spam: “[S]omething does have to be done to eliminate the unbelievable volume (of spam) that many people get. One would think that it would lessen itself because it's not as effective.”