Privacy & Informatie 2002/6, pp. 250-259

Christiaan Alberdingk Thijm[*]

HET EINDE VAN SPAM?[**]

Regulering van ongevraagde e-mail

In toenemende mate wordt spam gereguleerd door wetgeving, met name wetgeving ter bescherming van de privacy. De juridische regulering van spam vormt het onderwerp van dit artikel. Bijzondere aandacht zal worden besteed aan de Wet bescherming persoonsgegevens en de Europese richtlijn Privacy in de sector elektronische communicatie.[1] Laatstgenoemde richtlijn beoogt specifiek spam aan banden te leggen. Geconcludeerd zal worden met de behandeling van de vraag of dergelijke specifieke wet- en regelgeving geschikt is om spam te bestrijden.

INLEIDING

Op 12 april 1994 schrijven twee advocaten uit Arizona internetgeschiedenis. Op die dag overspoelen Martha Canter en Lawrence Siegel de duizenden discussiegroepen van Usenet met advertenties.[2] Met behulp van een speciaal computer script vervuilen zij de discussiegroepen 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."[3]

De "techies" vonden het internet een minder voor de hand liggend medium voor advertenties. Commercieel gebruik van het net was pas sinds een jaar toegestaan. Adverteren op internet was als vloeken in de kerk. De gebruikers van Usenet reageerden woedend op de vervuiling van hun discussiegroepen. Het zelfregulerend vermogen van de internetgemeenschap werd voor het eerst op de proef gesteld. De netizens namen hun toevlucht tot een krachtig wapen: massale wraak. Canter en Siegel werden gebombardeerd met hate-mail en -faxen, ontvingen dreig-telefoontjes en werden vergeleken met ingeblikt varkensvlees. Spam – zo noemde men de lawine commerciële berichten van Canter en Siegel.

---

[*] 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 (DENEC) d.d. 11 september 2002 te Amsterdam.

[1] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van de Europese Unie 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.

[2] Usenet is het gedeelte van het internet dat bestaat uit een verzameling discussie- of nieuwsgroepen, waarbinnen over de meest uiteenlopende onderwerpen kan worden gediscussieerd. In de nieuwsgroep <nl.juridisch> wordt bijvoorbeeld over Nederlandse juridische kwesties gediscussieerd en in <misc.int-property> over intellectueel eigendomsrecht.

Nog steeds wordt "spammen" beschouwd als één van de grootste taboes op internet. Veel internet service providers hebben nadrukkelijk in hun algemene voorwaarden opgenomen dat hun netwerk niet mag worden gebruikt voor het verspreiden van spam. Een saillant voorbeeld daarvan is HavenCo, dat zijn diensten aanbiedt vanaf een voormalig anti-geschutsplatform, net buiten de territoriale wateren van Engeland. Een gepensioneerde majoor is er in de jaren zestig neergestreken en heeft er zijn koninkrijk gesticht, the principality of Sealand. HavenCo is gespecialiseerd in het "hosten" van controversiële diensten die in de meeste jurisdicties verboden zullen zijn. Sealand onttrekt zich naar eigen zeggen aan iedere wet- en regelgeving. Op grond van de Acceptable Use Policy van HavenCo zijn echter twee zaken verboden: spammen en kinderporno – in die volgorde.

WAT IS SPAM?

Van origine is spam verblikt vleesbeleg van de Amerikaanse firma Hormel. Het verwierf grote populariteit bij de Britten, nadat het in de Tweede Wereldoorlog in het kader van een hulpprogramma de Atlantische Oceaan was overgestoken. De naam is afgeleid van de ingrediënten van het 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.

De term "spam" is geen juridisch begrip, maar *internetspeak*. Discussies over spam worden bemoeilijkt doordat dikwijls verschillende definities van het begrip worden gehanteerd. Over de vraag of spam ook altijd commercieel is of in grote hoeveelheden moet zijn verzonden, bestaat onenigheid.[4] De belangrijkste gemene deler in de verschillende definities is dat spam ongevraagd is. 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.

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 betreft, 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.

---

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

[4] Zo noemde Privacyorganisatie Bits of Freedom een charitatieve mailing voor de nationale Help India-actie eens de "grootste verzending van ongevraagde e-mail (spam) in de Nederlandse geschiedenis".

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."[5]

Er zijn echter ook belangrijke *nadelen* verbonden aan het verzenden van spam. In de eerste plaats wordt het vertrouwen van het medium internet aangetast. Mensen zullen minder snel geneigd zijn 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 op den duur men nog slechts e-mail wil ontvangen van bekenden.[6] 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 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. Voor de nietsvermoedende derde betekent dit dat gebruik wordt gemaakt van zijn faciliteiten en dat zijn mail server mogelijk ook op een black list terecht komt en zijn eigen mail geblokkeerd zal worden.

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."[7]

Naast deze meer praktische nadelen verbonden aan spam, is er ook een veelgehoord *principieel* argument tegen spam. Veel mensen ervaren de ontvangst van spam als hinderlijk, en daardoor mede als een inbreuk op hun privacy. Ongevraagd wordt men benaderd met niet zelden controversiële, aanstootgevende boodschappen, variërend van aanbiedingen voor penis-verlengers, porno en pyramidespelen tot anti-abortus teksten en religieuze boodschappen van fanatici. De ratio om spam te reguleren in wet- en regelgeving, is dan ook gelegen in de bescherming van de privacy. Voordat ik deze privacywetgeving in meer detail zal bespreken, zal ik eerst het een en ander over deze ratio opmerken.

SPAM EN PRIVACY

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

[5] John M. Moran, Spam King Living High In The Bayou, *CTNow* 30 juni 2002 <http://www.ctnow.com/technology/hc-sp1scelsonjun30.story?coll=hc-headlines-home>

[6] *De Volkskrant* 10 maart 2002.

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.[8]

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 Frank 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.[9] Daarom is privacybescherming 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 veel geciteerd gezegde.

Het verspreiden van spam kan onder omstandigheden ook strijdig zijn 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

---

[7] *De Volkskrant* 10 maart 2002.
[8] M. van den Boomen, "Privacy is raar spul", *Netkwesties* 19 juli 2002, <
http://www.netkwesties.nl/editie41/column1.html>
[9] *NRC Handelsblad* 25 maart 1999.

de eigen gegevens, informatie en de beslissingen die daarop zijn gebaseerd. Een wet die de informationele privacy reguleert 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.[10]

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.[11] Een monsterverbond van werkgeversorganisatie VNO-NCW en de Consumentenbond waarschuwde in 1998 al voor de verstrekkende gevolgen. Volgens VNO-NCW en de Consumentenbond zal de wet het bedrijfsleven jaarlijks 859 miljoen gulden ofwel 390 miljoen euro gaan kosten. De wet zou doorslaan in haar goede bedoelingen en iedere verwerking van persoonsgegevens willen reguleren, waarbij de daadwerkelijke relevantie van de verwerking voor de persoonlijke levenssfeer niet altijd terzake doet; ook zuiver technisch vereiste handelingen vallen onder het bereik van de Wbp. Ook het Rathenau-instituut in Den Haag waarschuwde dat de WBP haar doel voorbijschiet door geen onderscheid te maken tussen verwerkingen en geen bescherming te bieden tegen de *gevolgen* daarvan.

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.

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.

[10] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995, PbEG 1995 L 281/31.
[11] 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.

Zoals gezegd, zal een e-mailadres doorgaans wel te kwalificeren zijn als een persoonsgegeven. Dat betekent dat de restricties die de Wbp stelt aan het verwerken van persoonsgegevens onverkort van toepassing zijn. Zo mag een e-mailadres op grond van de Wbp slechts worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7 Wbp). Als het adres nu in eerste instantie voor een ander doel dan e-mail marketing is verzameld, is er niet per definitie een man overboord. Het is toegestaan een e-mailadres voor een ander doeleinde te verwerken, mits dit verenigbaar is met de doeleinden waarvoor het adres in eerste instantie is verkregen (artikel 9 Wbp). Bij de beoordeling of dergelijke secundaire verwerking verenigbaar is met het primaire doeleinde waarvoor het e-mailadres is verkregen, 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.

Niet iedere verwerking van e-mailadressen zal zijn toegestaan. Artikel 8 Wbp bevat een limitatieve opsomming van de gronden die een gegevensverwerking rechtvaardigen. In het geval van de verwerking van e-mailadressen, komen twee gronden in het bijzonder in aanmerking: de betrokkende 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 belang 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. Opt-out is dus onvoldoende. Bovendien moet de reikwijdte van de toestemming duidelijk zijn, en moet de toestemming op basis van de juiste informatie zijn gegeven. Toestemming kan 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.

De meeste gevallen van e-mailverwerking zullen hun rechtvaardiging vinden in artikel 8 sub f Wbp, namelijk indien de verwerking "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 fundamentele rechten van de vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert."[12]

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

[12] Artikel 8 sub f Wbp.

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.[13] 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.[14] Een gerechtvaardigd belang zal in de regel aanwezig zijn indien de gegevensverwerking plaatsvindt in het kader van de normale bedrijfsvoering van de verantwoordelijke.

Net als bij artikel 9 Wbp vereist toepassing van artikel 8 sub f Wbp een belangenafweging. Wat dat betreft, valt het dus wel mee met het vermeend rigide karakter van de Wbp. Uiteindelijk zullen verschillende factoren uitwijzen of een e-mailadres voor spam mag worden gebruikt.

Wanneer e-mailadressen voor direct mail doeleinden worden gebruikt, wat dikwijls het geval zal zijn bij spam, geldt nog een aantal bijzondere verplichtingen. De betrokkenen dienen 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.[15] Overigens is voor deze informatieplicht de wijze waarop de e-mailadressen worden verkregen van belang. Indien de gegevens van de betrokkenen zelf worden verkregen, moeten deze 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. Er moet dus altijd een opt-out mogelijkheid geboden worden.

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 XS4ALL en een aantal van haar abonnees enerzijds en het bedrijf Ab.Fab anderzijds. XS4ALL is een bekende internet service provider die de privacybescherming van haar abonnees hoog in het vaandel heeft staan. Gedaagde Ab.Fab houdt zich bezig met direct marketing via e-mail. Zij verzendt op verzoek van opdrachtgevers als NRC Handelsblad grote aantallen commerciële e-mails, ook als de geadresseerden daarvoor geen toestemming hebben gegeven. Ab.Fab biedt slechts een opt-out mogelijkheid. Op grond van de netiquette, de ongeschreven gedragscode van het internet, is

[13] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 87.
[14] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 87.

Ab.Fab daarom een spammer. De vraag is of de handelwijze van Ab.Fab ook in strijd is met de Wet bescherming persoonsgegevens.

Het Hof Amsterdam, dat de zaak in tweede instantie behandelde, merkt allereerst 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 ook 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.[16]

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 moet dus een afweging van het belang van Ab.Fab en dat van haar geadresseerden gemaakt worden. Bij die afweging betrekt 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 fysiek 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 mij af of dit juist is.

De inbreuk op de privacy in het geval van spammen is mijns inziens 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

[15] Artikelen 33 en 34 Wbp.
[16] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, pp. 48-49.

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.

De mogelijkheden om op grond van de Wbp tegen spammers op te treden, lijken met het arrest van het hof gering. Wie zijn diensten inricht zoals Ab.Fab zal op grond van de Wbp weinig te vrezen hebben. Of de e-mailactiviteiten de grens van het geoorloofde overschrijden, zal uiteindelijk afhankelijk zijn van de omstandigheden van het specifieke geval, waarbij de belangen van verzender en geadresseerde tegenover elkaar afgewogen zullen moeten worden. In de toekomst lijkt echter weinig ruimte meer voor een dergelijke belangenafweging. De Europese wetgever heeft de balans inmiddels doorgeslagen in het belang van de geadresseerde. 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 eindelijk een Europese richtlijn aangenomen die het verzenden van ongevraagde[17], commerciële e-mail aan banden legt. Hoofdregel is dat het verzenden van e-mail met het oog op direct marketing alleen is toegestaan aan degenen die daar van te voren hun toestemming voor hebben gegeven.

[17] De Nederlandse vertaling spreekt van “ongewenste” communicatie; “ongevraagde” is mijns inziens echter een betere vertaling van het Engelse “unsolicited”.

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 daar echter fel tegen 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. [18] Als verschillende landen een ander regime zouden toepassen, zou het direct markeeters 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 onwerkbare situatie leiden, aangezien niet altijd duidelijk is vanuit welk land de spam wordt verzonden.

Uiteindelijk hebben Commissie en Parlement een compromis bereikt door bedrijven bij wijze van uitzondering 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. Dit wordt ook wel de soft opt-in genoemd. De vraag is wanneer er sprake is van eigen producten of diensten. Mag bedrijf X zijn eigen klanten berichten over de gelijkaardige producten of diensten van bedrijf Y waar X mee samenwerkt?

Zoals gezegd, is de hoofdregel 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. Dit is dus een opt-in systeem. De richtlijn biedt weinig houvast hoe de toestemming moet worden verkregen. Is het bijvoorbeeld toegestaan potentiële geïnteresseerden per e-mail om hun toestemming te vragen? Strikt genomen zou die e-mail ook een ongevraagde e-mail zijn, en dus niet zijn toegestaan.

Onduidelijk is bovendien wat voor een vereisten aan de toestemming zijn verbonden. Artikel 2 sub f van richtlijn verwijst voor de definitie van toestemming naar de vorige Privacyrichtlijn, waar toestemming wordt gedefinieerd als elke vrije, specifieke en op informatie berustende wilsuiting. De tekst van de richtlijn creëert echter enige verwarring omtrent de vereisten die aan deze wilsuiting zijn verbonden. Toepassing van artikel 13 van de richtlijn vereist geen "ondubbelzinnige" toestemming, zoals op grond van artikel 8 sub a van de Wbp. Daarentegen bevat overweging 40 de toevoeging dat de toestemming "uitdrukkelijk" moet zijn. In de Wbp komt dit vereiste terug in de paragraaf over gevoelige persoonsgegevens. Deze mogen slechts worden verwerkt met de uitdrukkelijke toestemming van de betrokkene (artikel 23 lid 1 sub a Wbp). Het bijvoeglijk naamwoord "uitdrukkelijke" geldt hier als een verzwaring ten opzichte van de "ondubbelzinnige" toestemming van artikel 8 sub a. Een stilzwijgende of impliciete toestemming is onvoldoende: de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking.[19]

[18] Overweging 40.
[19] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 123.

Opvallend is dat geen vereisten worden 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 is. De hierboven beschreven praktische nadelen verbonden aan spam worden met name veroorzaakt door het grote volume. Een enkel spam-bericht neemt een te verwaarlozen hoeveelheid netwerkcapaciteit in beslag. In dit opzicht lijkt de Europese wetgever dus te hebben gekozen voor een principiële benadering van spam. Voor de privacy-inbreuk van de ontvanger maakt het immers niet uit of de e-mail die hij ongevraagd ontvangt in bulk verzonden is of niet. Dat de Europese wetgever de bestrijding van spam op privacy-argumenten baseert, blijkt ook wel uit de naam van de richtlijn en de overwegingen daarbij.[20]

Vreemd genoeg wordt deze principiële benadering weer verlaten voor wat betreft de inhoud van het spam-bericht. De richtlijn lijkt slechts *commerciële* spam te verbieden. Er moet sprake zijn van "direct marketing". De inhoud van de boodschap is dus bepalend voor de vraag of de verzending daarvan is toegestaan. 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 in their mailbox."[21]

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".[22] Dan valt tevens charitatieve spam onder het bereik van de richtlijn. De definitie die de richtlijn Elektronische handel hanteert van "commerciële communicatie" is weer wat ruimer.[23] Daar wordt commerciële communicatie -- kortweg – omschreven als elke vorm van communicatie voor het direct of *indirect* promoten van de goederen, diensten of het imago van een onderneming organisatie of persoon.

De vraag of bepaalde spam als "commercieel" kan worden aangemerkt, kwam ook aan de orde in een recente kort geding-procedure bij de voorzieningenrechter te Almelo.[24] Dr Matthias Rath, een handelaar in vitaminepreparaten, had internetgebruikers aangezet tot het verzenden van e-mails aan leden van de Tweede Kamer. Doel van de actie was te protesteren tegen op handen zijnde wetgeving ter regulering van

[20] Zie bijvoorbeeld overweging 40.
[21] John Gilmore,*What to do about spam? Use smarter mail readers*, Politechbot.com 28 februari 2002 <http://www.politechbot.com/p-03204.html>
[22] Artikel 41 Wbp. Zie ook C.W. Noorda, 'Nieuwe Europese regels voor cookies en spam', *Mediaforum* 2002/9, p. 274.
[23] Richtlijn 2000/31/EG, *PbEG* L178.
[24] Vzr Rb Almelo 13 september 2002, *Mediaforum* 2002/11-12, nr. 44 m.nt. Noorda.

onder meer de handel in vitaminepreparaten. Om het de internetgebruikers makkelijk te maken had Rath een programmaatje op zijn site geplaatst waarmee automatisch e-mails kunnen worden verzonden. Als gevolg waren de Tweede Kamerleden de gelukkige ontvangers van maar liefst 604 miljoen e-mails.

Bij zijn oordeel dat deze verzending ongeoorloofd is jegens de Staat zoekt de rechter aansluiting 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. Op grond van een dergelijke redenering heeft bijna iedere e-mail indirect een commercieel karakter, zonder dat er sprake is van een direct wervend of aanprijzend karakter van de e-mail.

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, met name China en Zuid Korea, waar men immuun is voor de Europese wetgeving. De meest kwaadaardige spammers zullen hun ongewenste praktijken dus gewoon voortzetten, ondanks een Europees verbod. Wat dat betreft, creëert de richtlijn schijnveiligheid. Overigens zullen direct marketeers die daadwerkelijk geïnteresseerd zijn in een langdurige relatie relatie met hun klanten ook zonder deze specifieke wetgeving geen ongewenste e-mail versturen. 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."

Mogelijk worden juist deze legitieme marketeers de dupe van de stringente richtlijn. Doordat de richtlijn onvoldoende duidelijkheid verschaft over wanneer sprake is van toestemming en op welke wijze die kan zijn verkregen, zal het voor hen lastiger worden om e-mail te gebruiken voor hun uitingen. Dit geldt helemaal voor nieuwkomers op de markt, die niet al een bestaande klanten database hebben opgebouwd. E-mail verliest met dit alles deels zijn waarde als communicatiemiddel.

Daarnaast kan men zich afvragen of een rigide regeling van spam recht doet aan het genuanceerde karakter van de privacybescherming. Zoals gezegd, is de mate van privacybescherming afhankelijk van verschillende factoren. Ook op grond van de vermeend stringente Wet bescherming persoonsgegevens zagen we dat er dikwijls ruimte is voor een belangenafweging. Grote spammers zouden ook nu al op grond van het leerstuk van onrechtmatige daad kunnen worden aangesproken, hetgeen ook werd geoordeeld door de voorzieningenrechter te Almelo in de Dr Rath-zaak: "In beginsel hoeft hinder niet onrechtmatig te zijn. Dit verandert echter wanneer hinder een zodanige vorm en inhoud aanneemt dat het niet langer kan worden aanvaard. (…) De voorzieningenrechter is van oordeel dat gezien de aard en omvang van de e-mail alsmede gezien de omvang van de schade die de Staat hierdoor lijdt het verzenden

van de e-mail via de websites van gedaagden thans als onrechtmatig dient te worden aangemerkt."[25] Daar is dus geen specifieke wetgeving ter voorkoming van spam voor nodig. Het is spijtig dat niet voldoende ervaring is opgedaan met het huidige instrumentarium van het Nederlands recht.

Een volgend bezwaar is dat deze specifieke regulering van spam op gespannen voet staat met de vrijheid van meningsuiting. Deze beschermt ook commerciële berichten, zij het dat deze minder bescherming toekomen dan politieke uitspraken.[26] Niet alleen de inhoud van e-mails wordt echter aan beperkingen onderhevig gemaakt, maar ook de vrijheid om een communicatiemiddel te gebruiken. Dit kan eveneens opgevat worden als een beperking van de vrijheid van meningsuiting.[27] Scepticus Gilmore hierover: "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'."[28]

Gezien deze nadelen verbonden aan de juridische regulering van spam, was het wellicht verstandig geweest nog even te wachten met deze specifieke wetgeving totdat meer ervaring was opgedaan met andere middelen. De richtlijn lijkt strijdig met de beginselen van proportionaliteit en subsidiariteit. Mijns inziens verdient het de voorkeur ongevraagde e-mail technisch te bestrijden. Daarvoor worden op de markt tal van mogelijkheden geboden. Sommige mail applications 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 voorbeelden van dergelijke blacklists. Een ander aardig initiatief is Habeas, waarmee mail een keurmerk kan krijgen, dat het "the e-mail you want" is.

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 en het internet in het algemeen, maar uiteindelijk 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." Was hij er maar nooit aan begonnen.

---

[25] Vzr Rb Almelo 13 september 2002, *Mediaforum* 2002/11-12, nr. 44 m.nt. Noorda.
[26] J.M. de Meij e.a., *Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief*, Amsterdam: Otto Cramwinckel Uitgever 2000, pp. 244-247.
[27] Vgl HR 26 februari 1999, *NJ* 1999, 716 m.nt EJD en EHRM 22 mei 1990, *NJ* 1991, 740, m.nt. EAA.
[28] John Gilmore, *Earthlink's anti-spam censorship*, Politechbot.com 8 september 2002 <http://www.politechbot.com/p-03967.html>