COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 22.01.2004
COM(2004) 28 definitief

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

inzake ongevraagde commerciële communicatie of "spam"

INHOUDSOPGAVE

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

inzake ongevraagde commerciële communicatie of "spam"

(Voor de EER relevante tekst)

SAMENVATTING

Ongevraagde commerciële communicatie via e-mail, ook wel "spam" genoemd, heeft zorgwekkende proporties aangenomen. Geschat wordt dat wereldwijd meer dan 50% van het e-mailverkeer uit spam bestaat. Nog verontrustender is de snelheid waarmee dit percentage groeit: in 2001 was het nog maar 7%.

Spam is om diverse redenen een probleem: privacy, misleiding van consumenten, bescherming van minderjarigen en de menselijke waardigheid, extra kosten voor het bedrijfsleven en productiviteitsverlies. Breder gezien is spam ondermijnend voor het vertrouwen van de consument, dat onmisbaar is voor het succes van e-handel, e-diensten, en de informatiemaatschappij in het algemeen.

De EU is op dit gevaar vooruitgelopen en is in juli 2002 gekomen met Richtlijn 2002/58/EG, een richtlijn betreffende privacy en elektronische communicatie, waarmee in de gehele EU het principe is ingevoerd dat voor marketing via elektronische post (met inbegrip van mobiele SMS- en MMS-berichten) toestemming nodig is (opt-in regeling). De uiterste termijn voor de omzetting van deze richtlijn in nationale wetgeving was 31 oktober 2003. Er zijn inmiddels inbreukprocedures ingeleid tegen een aantal lidstaten die geen omzettingsmaatregelen aan de Commissie hebben doorgegeven.

De invoering van wetgeving is weliswaar een eerste, noodzakelijke stap, maar zeker niet de gehele oplossing. In deze mededeling worden maatregelen genoemd die nodig zijn om de EU-voorschriften aan te vullen en zo het spamverbod in de praktijk te brengen.

Er bestaat evenwel geen wondermiddel tegen spam. De in deze mededeling voorgestelde maatregelen zijn vooral toegespitst op een doeltreffende handhaving door de lidstaten en de autoriteiten, op technische oplossingen en zelfregulering door de industrie, en op voorlichting van de consument. Ook wordt bijzondere aandacht geschonken aan de internationale dimensie want veel spam is van buiten de EU afkomstig.

Ofschoon deze maatregelen in grote trekken de consensus weerspiegelen die in de loop van 2003 is ontstaan en op een openbare workshop van oktober 2003 tot uitdrukking is gekomen, is een consensus over de tenuitvoerlegging ervan eveneens van groot belang. Alleen indien alle betrokkenen - van de lidstaten en de openbare autoriteiten via het bedrijfsleven tot en met de consumenten en de gebruikers van internet en elektronische communicatie - hun steentje bijdragen, kan de verspreiding van spam worden ingedamd.

Aan sommige van deze maatregelen hangt natuurlijk een prijskaartje. Maar dat is de prijs die moet worden betaald om e-mail en e-diensten als efficiënte communicatiemiddelen te behouden. Met de tenuitvoerlegging van de in deze mededeling beschreven maatregelen kan de hoeveelheid spam sterk worden verlaagd, hetgeen de informatiemaatschappij, de burger en de economie ten goede zal komen.

Achtergrond en doel

Ongevraagde commerciële communicatie via elektronische post[1], ook wel "spam" genoemd, wordt door velen gezien als een van de grootste problemen waar internet momenteel mee geconfronteerd wordt. De spamproblematiek heeft zorgwekkende proporties aangenomen. Inmiddels bestaat het gevaar dat e-mail- en SMS-gebruikers niet langer van e-mail - een van de populairste internettoepassingen - of mobiele diensten gebruik wensen te maken, of in ieder geval veel minder dan zij zouden willen. Afgezien daarvan verdient spam nog meer de aandacht omdat internet en andere elektronische communicatiemiddelen (bijv. breedbandtoegang, draadloze toegang en mobiele communicatie) naar verwachting een belangrijke factor zullen vormen voor de groei van de productiviteit in moderne economieën.

Er bestaat weliswaar een consensus over de noodzaak van ingrijpen voordat de voordelen van e-mail en andere e-diensten weer teniet worden gedaan door een overvloed aan spam, maar het is niet evident hoe spam het best kan worden bestreden. Belangrijker nog: er bestaat geen wondermiddel tegen spam. Alleen indien alle betrokkenen, van de lidstaten en de bevoegde autoriteiten, via het bedrijfsleven tot en met de consumenten en de gebruikers van internet en elektronische communicatie, hun steentje bijdragen, bestaat de kans dat spam doeltreffend kan worden aangepakt.

In deze mededeling wordt een inventarisatie gemaakt van de diverse wettelijke, technische en bewustmakingsactiviteiten op basis van Richtlijn 2002/58/EG die samen de (op toestemming gebaseerde) "opt-in"-regeling vormen welke de lidstaten uiterlijk op 31 oktober 2003[2] hadden moeten invoeren.

Daarbij ligt de nadruk in de eerste plaats op de feitelijke tenuitvoerlegging en handhaving van deze richtlijn door de lidstaten, technische maatregelen, zelfregulering door de industrie, bewustmaking van de consument en internationale samenwerking. De internationale dimensie is trouwens cruciaal, want spam blijkt vaak afkomstig van buiten de Europese Unie, vooral uit Noord-Amerika[3].

---

1 Deze mededeling heeft geen betrekking op andere ongevraagde communicatie, zoals ongevraagde (brief)post.

2 Zie in het bijzonder artikel 13 van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (zie punt 2 hieronder).

3 Zo lijken de uit 2002 stammende "spambox"-initiatieven van de Franse "Commission Nationale Informatique et Libertés (CNIL)" en de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) te bevestigen dat de Verenigde Staten en in mindere mate ook Canada de belangrijkste bronnen van spamberichten zijn. De CBPL-conclusies zijn te vinden op http://www.privacy.fgov.be/publicaties/spam_4-7-03_nl.pdf; het CNIL-verslag is te raadplegen op het volgende webadres: http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf. Zie ook: UNCTAD, E-Commerce and Development Report 2003, New York en Genève, 2003, blz. 27.

Deze activiteiten weerspiegelen in grote lijnen de consensus die in de loop van 2003 is ontstaan en op de openbare workshop van oktober 2003[4] tot uitdrukking is gebracht.

Een consensus hierover is des te belangrijker omdat het juist in de eerste plaats de taak van die belanghebbende partijen is om, zo mogelijk met steun van de Commissie, de geïnventariseerde maatregelen in het belang van de informatiemaatschappij, de industrie en de gebruikers ten uitvoer te leggen.

Opzet van het document

In dit document wordt ingegaan op de specifieke aspecten van de spamproblematiek en worden per aspect specifieke maatregelen voorgesteld. Waar nuttig wordt ook de aandacht gevestigd op de beste praktijken.

De voorstellen worden in onderstaande volgorde gepresenteerd:

– **Uitvoerings- en handhavingsmaatregelen** voor in het bijzonder overheden en openbare autoriteiten met betrekking tot onderwerpen zoals rechtsmiddelen en sancties, klachtenmechanismen, grensoverschrijdende klachten, samenwerking met derde landen en toezicht (hoofdstuk 3)

– **Zelfregulerende en technische maatregelen** die in het bijzonder bestemd zijn voor marktspelers op gebieden zoals contractuele afspraken, gedragscodes, aanvaardbare marktpraktijken, etikettering, alternatieve geschillenregelingen en technische oplossingen zoals filtering en veiligheid (hoofdstuk 4)

– **Bewustmakingsacties** van overheden, openbare autoriteiten, marktdeelnemers, consumentenverenigingen, enz. met betrekking tot preventie, consumentenvoorlichting, en indiening van klachten (hoofdstuk 5)

Een tabel aan het einde van deze mededeling biedt een overzicht van al deze acties. De diverse acties hangen op verschillende wijzen met elkaar samen. Daarom moeten zij zoveel mogelijk parallel en op geïntegreerde wijze ten uitvoer worden gelegd.

Alvorens hier nader op in te gaan, wordt in de volgende hoofdstukken een korte analyse gemaakt van spam als zodanig (hoofdstuk 1) en een beschrijving gegeven van de nieuwe voorschriften die sinds 31 oktober 2003 van toepassing zijn (hoofdstuk 2).

[4] Vóór de workshop werd een discussienota over ongevraagde communicatie of spam verspreid. Deze discussienota was gebaseerd op eerdere besprekingen in het kader van het Comité voor communicatie (COCOM) en de Groep gegevensbescherming artikel 29. Naar aanleiding van een vragenlijst werd informatie verstrekt door leden van het COCOM en de Groep gegevensbescherming artikel 29. Ook heeft een aantal industriële organisaties en afzonderlijke bedrijven gereageerd, van ISP's en exploitanten van (mobiele en vaste) communicatienetwerken via direct marketing-bedrijven en adverteerders tot computer- en softwarefabrikanten.

1. DE SPAMPROBLEMATIEK

Wat is nu eigenlijk spam?

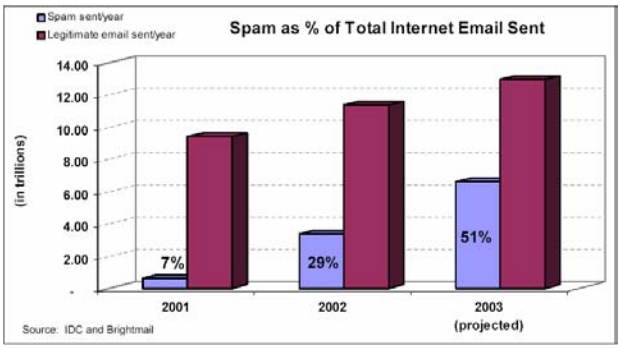
"Spam" is een term die vaker gebruikt dan gedefinieerd wordt. Het is een gangbare aanduiding voor ongevraagde, vaak in groten getale verzonden e-mails. In de nieuwe richtlijn wordt de term spam niet gedefinieerd, noch gebruikt. In plaats daarvan wordt het concept "ongewenste communicatie" via "elektronische post" gebruikt voor de doeleinden van "direct marketing", waarmee eigenlijk de meeste vormen van spam wel worden gedekt. Daarom wordt in deze mededeling de term spam gebruikt voor ongewenste (ongevraagde) commerciële elektronische post.

Wel zij erop gewezen dat onder de term "elektronische post" niet alleen traditionele SMTP-gebaseerde "e-mail" moet worden verstaan, maar ook SMS, MMS en elke andere vorm van elektronische communicatie waaraan de zender en de ontvanger niet gelijktijdig hoeven deel te nemen (zie hoofdstuk 2).

1.1. De omvang van de problematiek

Ongevraagde commerciële e-mail of spam heeft zorgwekkende proporties aangenomen. Ofschoon de statistieken niet volledig overeenstemmen, wordt algemeen aangenomen dat meer dan 50% van het e-mailverkeer wereldwijd uit spam bestaat.

Het groeitempo is bovendien nog verontrustender. In 2000 kwam naar schatting "slechts" 7% van het wereldwijde e-mailverkeer voor rekening van spam. In 2002 werd dit aandeel al op 29% geraamd. En de prognoses voor 2003 voorspellen een aandeel van 51%.



Figuur 1: Spam als aandeel in het totaal aantal via internet verzonden e-mails

Er bestaan grote verschillen tussen de diverse categorieën gebruikers en regio's in de wereld. (Zo wordt geschat dat ongeveer 30% van de door de Europese Commissie ontvangen externe e-mailberichten spam is.) In het algemeen zijn de recente EU-cijfers evenwel niet minder verontrustend van de wereldwijde gegevens[5].

En ook al lijkt ongevraagde communicatie of spam via mobiele netwerken, bijvoorbeeld met tekstberichten via de Short Message Service (SMS), nog een relatief gering probleem, verwacht mag worden dat het spamaandeel dankzij ontwikkelingen zoals de verzending van e-mail via mobiele netwerken zal groeien. De ervaringen in landen (bijv. Japan) waren veel gebruik wordt gemaakt van i-mode, hebben dit bevestigd.

[5] Het spamaandeel in de EU wordt voor september 2003 geraamd op 49%, vergeleken met circa 54% wereldwijd voor dezelfde maand (bron: Brightmail, 2003).

1.2. Waarom vormt spam een probleem?

Gezien vanuit het standpunt van het individu is spam een inbreuk op de privacy. Deze overweging staat aan de basis van de nieuwe voorschriften inzake ongevraagde communicatie die in het volgende hoofdstuk worden beschreven. Bovendien is spam dikwijls misleidend of bedrieglijk. Een groot deel van de spam lijkt te zijn ingegeven door een behoefte om de klant geld af te troggelen met misleidende of bedrieglijke beweringen[6]. Helaas reageren maar al teveel consumenten op deze misleidende of bedrieglijke spam[7]. Pornografische berichten kunnen bovendien ook nog schokkende informatie bevatten[8]. Het verwijderen van spam uit postvakken is tijdrovend voor de gebruiker en brengt kosten met zich mee wanneer de gebruiker filter- en andere software moet aanschaffen.

Wie ergert zich eraan?

Het aantal klachten is een van de indicaties voor de ontevredenheid van de gebruikers. In drie maanden heeft de Franse spambox maar liefst 325.000 meldingen ontvangen. In België zijn de ervaringen met 50.000 klachten in 2½ maand van vergelijkbare orde. De permanente spambox van de FTC, de UCE-database genoemd, ontving begin 2003 130.000 meldingen per dag.

Spam is nu op een punt gekomen waarop ook aanzienlijke kosten ontstaan voor het bedrijfsleven. In termen van directe kosten gaat het om een verlies aan efficiency/productiviteit op het werk omdat ook de werknemers hun postvak moeten schoonmaken. Ook moeten IT-afdelingen tijd en geld aan de oplossing van de problemen spenderen. Internet Service Providers (ISP's) en E-mail Service Providers (ESP's) moeten meer bandbreedte en opslagcapaciteit aanschaffen voor ongevraagde e-mailberichten. Ook bestaat het gevaar dat spam aansprakelijkheidsproblemen oplevert voor de ontvanger (bijvoorbeeld schadelijke inhoud op de pc van een werknemer) of de - onwetende - doorzender

---

6 Volgens een recent verslag van de FTC bevatte 22% van de geanalyseerde spam onjuiste informatie in de betreft-regel; 42% bevatte misleidende betreft-regels waarin ten onrechte werd beweerd dat de afzender een zakelijke of persoonlijke relatie met de ontvanger had; 44% van de spam bevatte onjuiste informatie in de van- of betreft-regel; meer dan de helft van de financieel getinte spam bevatte onjuiste informatie in de van- of betreft-regel; 40% van alle spam bevatte aanwijzingen voor valse informatie in het bericht; in 90% van alle berichten werden vermoedelijk valse beweringen gedaan omtrent investeringsmogelijkheden of commerciële kansen; 66% van de spam bevatte onjuiste informatie in the van- of betreft-regel of het bericht zelf. (False Claims in Spam, een verslag van de Division of Marketing Practices van de FTC, 30 april 2003, verkrijgbaar op: http://www.ftc.gov/reports/spam/030429spamreport.pdf).

7 Volgens Pew Internet zegt 7% van de e-mail-gebruikers een bestelling te hebben geplaatst na een ongewenst e-mailbericht en 33% van gebruikers op een link in een ongewenst e-mailbericht te hebben geklikt om meer informatie te krijgen. Ofschoon het percentage consumenten dat is opgelicht relatief laag is, hebben de enorme schaalvoordelen die dubieuze handelaars kunnen bereiken met misleidende of bedrieglijke spam, het probleem van dit consumentenbedrog op een nieuw plan getild. Zie: "Spam – How It Is Hurting Email and Degrading Life on the Internet, October 2003", verslag van Deborah Fallows in opdracht van het Pew Internet & American Life Project. Dit verslag is beschikbaar op het volgende webadres: http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. Een verzender van bulk e-mail heeft onlangs op het FTC Spam Forum van april-mei 2003 verklaart dat hij zelfs nog winst kan maken als hij in minder dan 0,0001% van de gevallen een reactie ontvangt. (Opmerkingen van Timothy J. Muris Chairman, Federal Trade Commission, Aspen Summit, Cyberspace and the American Dream, The Progress and Freedom Foundation, augustus 19, 2003 Aspen, Colorado).

8 Spamberichten tonen soms ook zinloos geweld of zetten aan tot haat op grond van ras, geslacht, geloofsovertuiging of nationaliteit.

(bijvoorbeeld ongerechtvaardigde opname op de zwarte lijst, aantasting van de reputatie). Er zijn ook indirecte kosten: soms worden rechtmatige commerciële of zakelijke e-mailberichten niet bezorgd als gevolg van de huidige spamfilters ("vals-positieven") of gewoonweg niet gelezen vanwege associaties met spam. Spam wordt steeds vaker gebruikt voor het verspreiden van virussen, hetgeen hoge kosten met zich meebrengt voor het bedrijfsleven.

Het bepalen van de kosten van spam is een moeilijke zaak, vooral voor particulieren, niet in het minst omdat het moeilijk is de veroorzaakte schade in geld uit te drukken. De ramingen zijn doorgaans echter onrustbarend. Ter illustratie kan worden vermeld dat spam het Europese bedrijfsleven volgens een raming van Ferris Research in 2002 € 2,5 miljard heeft gekost, alleen al in termen van productiviteitsverlies[9]. En, zoals hierboven al is aangegeven, is de hoeveelheid spam sinds 2002 nog enorm toegenomen. De softwareleverancier MessageLabs Ltd heeft de kosten van spam voor het Europese bedrijfsleven in juni 2003 op ongeveer £ 3,2 miljard geraamd[10]. Spam heeft ook diverse implicaties voor de betrokken bedrijven, afhankelijk van de sector. Zo is de juridische sector bijzonder kwetsbaar voor de gevolgen van spam, gezien het vertrouwelijke en gevoelige karakter van de informatie waar deze mee omgaat.

Een van de meest verontrustende gevolgen van spam is dat deze afbreuk doet aan het vertrouwen van de gebruiker, dat onmisbaar is voor het succes van elektronische handel en de informatiemaatschappij als geheel. Het beeld dat een verkoopkanaal wordt beheerst door malafide handelaars kan ernstige gevolgen hebben voor de reputatie van bonafide handelaren in dezelfde sector. Recente cijfers uit de VS, waar meer ervaring is opgedaan met spam dan in de EU, bevestigen dat veel mensen minder vertrouwen hebben in e-mail omdat zij zoveel spam ontvangen[11].

Meer in het algemeen worden internet en andere elektronische-communicatiekanalen - breedbandtoegang, draadloze toegang - beschouwd als sleutelfactoren voor de groei van de productiviteit in de moderne economie. Een aantal aantrekkelijke kenmerken van dergelijke diensten, zoals de permanente verbinding en draadloze toegang, kunnen de hoeveelheid ontvangen of doorgegeven spam aanmerkelijk verhogen, als niet de juiste veiligheidsvoorzieningen worden getroffen. Jammer genoeg kan de groei van dergelijke diensten daarom leiden tot een toename van spam, tenzij snel doeltreffende maatregelen worden genomen.

2. DE VOORSCHRIFTEN INZAKE ONGEVRAAGDE COMMERCIËLE COMMUNICATIE IN HET KORT

2.1. De toestemmingsregeling

Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (uiterste datum van omzetting 31 oktober 2003) bepaalt dat de lidstaten het verzenden van ongevraagde commerciële berichten via e-mail of andere elektronische berichtensystemen zoals SMS

---

9 Bron: FerrisResearch, 2003.

10 Dit cijfer en andere ramingen zijn afkomstig uit '"Spam"; Report of an Inquiry by the All Party Internet Group', Londen, oktober 2003, blz. 8; dit rapport kan worden geraadpleegt op de volgende website: http://www.apig.org.uk.

11 Volgens het reeds aangehaalde recente onderzoek van Pew Internet, maakt 25% van de ondervraagden minder vaak gebruik van e-mail omdat zij zoveel spam ontvangen.

en MMS (Multimedia Messaging Service) moeten verbieden, behalve wanneer vooraf toestemming is verkregen van degene die op deze elektronische communicatiediensten geabonneerd is (artikel 13, lid 1, van de richtlijn)[12]. Deze toestemmingsregeling (opt-in-regeling) gold tot dusver enkel voor faxberichten en geautomatiseerde kiessystemen[13].

De drie basisregels van de nieuwe regeling:

Regel nr. 1: Voor marketing via e-mail is voorafgaande toestemming van de abonnee nodig. Er geldt een beperkte uitzondering voor het verzenden van e-mail- (en SMS-)berichten aan bestaande klanten van een aanbieder met betrekking tot soortgelijke diensten of producten. Deze regeling geldt voor natuurlijke personen, maar de lidstaten mogen besluiten deze ook toe te passen op rechtspersonen.

Regel nr. 2: Het is verboden de identiteit van de afzender namens wie het bericht wordt verzonden, te verhullen of te verbergen.

Regel nr. 3: Alle e-mailberichten dienen een geldig retouradres te bevatten waar men zich kan uitschrijven.

Niet alle ongevraagde e-mail-berichten zijn evenwel verboden. Een uitzondering op de regel is het geval waarin de contactgegevens voor het verzenden van e-mail- of SMS-berichten in het kader van een verkooptransactie zijn verkregen. Dit scenario wordt ook wel "soft opt-in" genoemd. In het kader van een dergelijke bestaande klantrelatie mag het bedrijf de van zijn klanten ontvangen gegevens gebruiken voor de marketing van soortgelijke producten of diensten als die welke hij al aan de betrokken klant heeft verkocht. Deze uitzondering is op het niveau van de Gemeenschap geharmoniseerd en de lidstaten zijn verplicht deze toe te passen. Aan de voorwaarden voor deze uitzondering dient evenwel strikt de hand te worden gehouden om te voorkomen dat de toestemmingsregeling in feite wordt ondermijnd. Maar zelfs in dit geval dient het bedrijf al bij de eerste keer dat hij de gegevens verzamelt duidelijk te maken dat deze voor direct marketing kunnen worden gebruikt (en eventueel dat deze voor zulke doeleinden aan derden kunnen worden doorgegeven) en de mogelijkheid te bieden voor de klant om hier "kosteloos en op gemakkelijke wijze" bezwaar tegen te maken. Bovendien moet elk volgend marketing-bericht een gemakkelijke manier voor de klant bieden om kosteloos en op gemakkelijke wijze verdere berichten te stoppen (opt-out).

De opt-in-regeling is verplicht voor alle aan individuele (natuurlijke) personen gerichte e-mail- en SMS-berichten ten behoeve van direct marketing. De lidstaten kunnen besluiten het opt-in-systeem ook toe te passen op aan bedrijven (rechtspersonen) gerichte communicatie. Lidstaten die voor een bezwaarregeling met opt-out-lijsten voor business-to-business marketing hebben gekozen, mogen dit blijven doen. Het toepassen van een gedifferentieerde regeling die afhankelijk is van de aard van de abonnee op een e-maildienst, kan voor de verzenders specifieke moeilijkheden opleveren bij het maken van onderscheid tussen rechtspersonen en natuurlijke personen.

De richtlijn verbiedt voor alle categorieën geadresseerden, dus zowel rechtspersonen als natuurlijke personen, direct marketing waarbij de identiteit van de afzender wordt gemaskeerd of verborgen.

---

12 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), PB L 201 van 31.7.2002.

13 Voor marketing-gesprekken met spraaktelefonie maar niet met geautomatiseerde apparatuur hebben de lidstaten de keuze tussen een toestemmingsregeling en een bezwaarregeling.

Bovendien moeten de betrokken berichten een geldig retouradres bevatten waaraan de ontvanger een verzoek om beëindiging van dergelijke communicatie kan richten[14].

De Groep gegevensbescherming artikel 29, die de Commissie moet adviseren en waarin de gegevensbeschermingsautoriteiten van de EU zijn vertegenwoordigd, buigt zich momenteel over een aantal van deze concepten teneinde tot een uniforme toepassing van Richtlijn 2002/58/EG te komen[15]. Door over deze punten consensus te bereiken kunnen interpretatieverschillen worden vermeden die schadelijk zijn voor de goede werking van de interne markt. Andere aspecten van ongevraagde communicatie zijn al aan de orde gekomen in voorgaande documenten van de Groep[16].

2.2. Handhavingsbepalingen

De bepalingen inzake beroep op de rechter, aansprakelijkheid en sancties van de "algemene" Gegevensbeschermingsrichtlijn zijn eveneens van toepassing op de bepalingen van de Richtlijn betreffende privacy en elektronische communicatie, met inbegrip van de voorschriften ten aanzien van ongevraagde communicatie[17].

In het kort moeten de lidstaten ervoor zorgen dat er in geval van inbreuk sancties kunnen worden getroffen en rechtsmiddelen beschikbaar zijn. Bij elke inbreuk op de krachtens de nationale wetgeving verleende rechten dient een individuele juridische voorziening mogelijk te zijn.

---

14 Artikel 13, lid 4, van Richtlijn 2002/58/EG.

15 Overeenkomstig artikel 15, lid 3, van Richtlijn 2002/58/EG, juncto artikel 30 van Richtlijn 95/46/EG.

16 Zie bijvoorbeeld Advies 7/2000 over het door de Europese Commissie ingediende voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie van 12 juli 2000 en Aanbeveling 2/2001 inzake bepaalde minimumeisen voor het online verzamelen van persoonsgegevens in de Europese Unie. Zie ook "harvesting", een thema dat is besproken in het werkdocument van 21 november 2000 met de titel "Privacy op internet" – Een geïntegreerde EU-aanpak van online-gegevensbescherming". Dit document kan worden geraadpleegd op het volgende webadres: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm.

17 Artikel 15 van Richtlijn 2002/58/EG verwijst naar hoofdstuk III van Richtlijn 95/46/EG inzake beroep op de rechter, aansprakelijkheid en sancties:
Artikel 22 - Beroep
Onverminderd de administratieve voorziening die met name bij de in artikel 28 bedoelde toezichthoudende autoriteit kan worden getroffen voordat de zaak aanhangig wordt gemaakt voor de rechter, bepalen de lidstaten dat een ieder zich tot de rechter kan wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden.
Artikel 23 - Aansprakelijkheid
1. De lidstaten bepalen dat een ieder die schade heeft geleden ten gevolge van een onrechtmatige verwerking of van enige andere daad die onverenigbaar is met de ter uitvoering van deze richtlijn vastgestelde nationale bepalingen het recht heeft van de voor de verwerking verantwoordelijke vergoeding van de geleden schade te verkrijgen.
2. De voor de verwerking verantwoordelijke kan geheel of gedeeltelijk van deze aansprakelijkheid ontheven indien hij bewijst dat de schade hem niet kan worden toegerekend.
Artikel 24 - Sancties
De lidstaten nemen passende maatregelen om de onverkorte toepassing van de bepalingen van deze richtlijn te garanderen en stellen met name de sancties vast die gelden bij inbreuk op de ter uitvoering van deze richtlijn vastgestelde bepalingen.

En ofschoon een dergelijke rechtsmiddel eventuele (zo mogelijk voorafgaande) administratieve procedures onverlet laat, bestaat er ook geen geharmoniseerde verplichting in dergelijke administratieve procedures te voorzien. Er moet een individueel recht op schadevergoeding bestaan voor eventuele schade als gevolg van een onrechtmatige verwerking of daad. Bij een inbreuk moeten er sancties kunnen worden opgelegd die garanderen dat de richtlijn volledig wordt nageleefd.

Met andere woorden, ook al hebben de lidstaten blij de tenuitvoerlegging van de richtlijn vanwege het specifieke karakter van een richtlijn een zekere manoeuvreerruimte bij het kiezen van de maatregelen - rechtsmiddelen en sancties inbegrepen - , toch zijn dergelijke maatregelen noodzakelijk om de "de volledige tenuitvoerlegging" van de bepalingen inzake ongevraagde commerciële communicatie te waarborgen.

Zoals doorgaans het geval is bij richtlijnen, is de handhaving van de bepalingen in de eerste plaats een taak van de lidstaten, niet van de Commissie. Het is dus niet aan de Commissie om degenen die zich niet houden aan de rechten en plichten van de richtlijn te vervolgen of te beboeten[18].

2.3. Overige bepalingen ten aanzien van spam

Een praktijk die vaak samenhangt met spamming is e-mail harvesting, dat wil zeggen het automatisch verzamelen van persoonsgegevens op openbare internet-gerelateerde plaatsen, zoals het web, chatrooms, enz. Een dergelijke praktijk is op grond van de "algemene" Gegevensbeschermingsrichtlijn 95/46/EG onrechtmatig, ongeacht of deze inzameling al dan niet automatisch met behulp van software geschiedt[19].

Frauduleuze en bedrieglijke spam kan bijzonder veel schade aanrichten. Deze praktijken zijn al illegaal op grond van de huidige EU-voorschriften inzake misleidende reclame en oneerlijke handelspraktijken (zoals Richtlijn 84/450/EEG inzake misleidende reclame)[20]. Nationale regelgeving voorziet voor de zwaardere gevallen meestal ook in strengere straffen, met inbegrip van strafrechtelijke sancties.

Sommige categorieën spam kunnen ronduit schokkend zijn, zoals pornografische spam of spam met zinloos geweld, vooral wanneer kinderen hiermee in aanraking komen[21]. Ofschoon de inhoud van dergelijke berichten schadelijk, maar niet per se illegaal is, is de ongedifferentieerde verspreiding ervan zonder onderscheid te maken tussen jong en oud volgens de nationale wet meestal niet toegestaan en staan daar soms zware straffen op.

---

18 Dit in tegenstelling tot instanties zoals de Amerikaanse Federal Trade Commission.

19 Zie ook het werkdocument van de Groep gegevensbescherming artikel 29 met de titel "Privacy op internet – Een geïntegreerde EU-aanpak van on-linegegevensbescherming" (document WP nr. 37 van 21 november 2000).

20 Richtlijn 84/450/EEG van de Raad van 10 september 1984 betreffende het nader tot elkaar brengen van de wettelijke en bestuursrechtelijke bepalingen der lidstaten inzake misleidende reclame, PB L 250, 19.9.1984, blz. 17-20. De Commissie is onlangs met een voorstel gekomen om deze richtlijn te actualiseren en te vervangen (COM(2003) 356 def.).

21 Op 24 september 1998 heeft de Raad een aanbeveling gedaan betreffende de ontwikkeling van de concurrentiepositie van de Europese industrie van audiovisuele en informatiediensten door de bevordering van nationale kaders teneinde een vergelijkbaar en doeltreffend niveau van bescherming van minderjarigen en de menselijke waardigheid te bereiken (98/560/EG). Deze aanbeveling was het eerste wettelijke instrument op EU-niveau met betrekking tot de inhoud van audiovisuele en informatiediensten dat alle kanalen van afgifte bestrijkt, van omroep tot en met internet.

Spamberichten bevatten soms ook illegale inhoud, zoals materiaal dat tot haat op grond van ras, geslacht, geloofsovertuigingen of nationaliteit aanzet. Hoe dan ook, zodra dergelijke berichten worden verspreid in het kader van direct marketing - hetgeen vaak het geval is - vallen zij onder het "spamverbod" dat ook voor andere categorieën ongevraagde e-mailberichten geldt.

Voorts dient ook melding te worden gemaakt van de eis van Richtlijn 2000/31/EG betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel (Richtlijn elektronische handel) dat "commerciële communicatie" duidelijk als zodanig herkenbaar dient te zijn (zie artikel 6, onder a), van de Richtlijn elektronische handel)[22].

Ook vinden activiteiten zoals hacking of identiteitsroof dikwijls plaats ter ondersteuning van spamactiviteiten, bijvoorbeeld om spam te verzenden of om toegang te krijgen tot adreslijsten of computers. Een groot deel van dergelijke activiteiten wordt gedekt door het kaderbesluit van de Raad over aanvallen op informatiesystemen, dat strafrechtelijke sancties in het vooruitzicht stelt. Over dit kaderbesluit, dat op een voorstel van de Commissie berust, is in februari 2003 een politiek akkoord bereikt en het zal vermoedelijk binnenkort officieel worden goedgekeurd[23]. In veel lidstaten is het nu al mogelijk illegale toegang tot of misbruik van servers of personal computers als misdrijf te vervolgen.

3. DOELTREFFENDE TENUITVOERLEGGING EN HANDHAVING DOOR DE LIDSTATEN EN DE OPENBARE AUTORITEITEN

In dit hoofdstuk over doeltreffende tenuitvoerlegging en handhaving wordt ingegaan op de vooral op overheden en openbare autoriteiten gerichte maatregelen op gebieden zoals rechtsmiddelen en sancties, klachtenmechanismen, grensoverschrijdende klachten, samenwerking met derde landen en toezicht.

Alvorens echter in te gaan op de handhaving, wijst de Commissie erop dat een aantal lidstaten de Richtlijn betreffende privacy en elektronische communicatie nog niet heeft omgezet, inclusief de bepalingen ten aanzien van ongevraagde commerciële e-mailberichten, dat deel uitmaakt van een nieuw, breder regelgevingskader voor elektronische communicatie[24].

---

22 Richtlijn van het Europees Parlement en van de Raad van 8 juni 2000, PB L 178 van de 17.7.2006. In de regel dient "commerciële communicatie" in overeenstemming te zijn met de geldende voorschriften van de lidstaat waarin de service provider is gevestigd. Dit geldt evenwel niet voor de toelaatbaarheid van ongevraagde communicatie via elektronische post (zie artikel 3 van de Richtlijn elektronische handel en de bijlage daarvan). In (het beperkte aantal) gevallen waarin natuurlijke personen niet door Richtlijn 2002/58/EEG worden beschermd tegen ongevraagde commerciële communicatie (zoals bij natuurlijke personen die geen abonnee zijn), dienen de lidstaten er op grond van de Richtlijn elektronische handel eveneens voor te zorgen dat service providers die ongevraagde commerciële communicatie via elektronische post verspreiden, regelmatig the opt-out-registers raadplegen waar natuurlijke personen die dergelijke commerciële communicatie niet langer wenst te ontvangen zichzelf kunnen aanmelden (zie artikel 7 van de Richtlijn elektronische handel), en deze respecteren.

23 Voorstel voor een kaderbesluit van de Raad over aanvallen op informatiesystemen, COM(2002) 173 def. van 19.4.2002.

24 Zie het negende verslag van de Commissie over de tenuitvoerlegging van het pakket telecommunicatieregelgeving, dat kan worden geraadpleegd op het volgende webadres:

Het Europees Parlement heeft zich onlangs bezorgd uitgelaten over deze vertraging[25]. Na het verstrijken van de uiterste omzettingstermijn voor de Richtlijn betreffende privacy en elektronische communicatie op 31 oktober 2003 heeft de Commissie in november 2003 inbreukprocedures ingeleid tegen een aantal lidstaten dat nog geen omzettingsmaatregelen heeft doorgegeven[26].

3.1. Inleiding

Ofschoon een deel van de spam met wetgeving kan worden tegengehouden, is wetgeving alleen niet voldoende. Een doeltreffende handhaving van de toestemmingsregeling moet in alle lidstaten prioriteit krijgen. Dit impliceert niet alleen voldoende personeel en middelen, maar ook adequate handhavingsmechanismen, ook over de grenzen heen. Voorts is de samenwerking met landen buiten de EU van groot belang. Toezicht is eveneens belangrijk, alleen al om de handhavingsprioriteiten te bepalen.

Een aantal factoren lijkt invloed te hebben op de doeltreffendheid van de handhavingsmechanismen:

– de mogelijkheid om de regelgeving te handhaven met behulp van adequate boetes en andere sancties; sommige regelgevingsinstanties beschikken kennelijk nog niet over voldoende (doeltreffende) handhavingsbevoegdheden;

– de aard van de klachtenmechanismen en de rechtsmiddelen die voor particulieren en bedrijven beschikbaar zijn;

– de behoefte aan duidelijkheid en coördinatie tussen nationale autoriteiten, gelet op de elkaar soms overlappende bevoegdheden op dit terrein;

– het niveau van kennis onder de gebruikers omtrent hun rechten en de wijze waarop zij deze kunnen afdwingen; de gebruikers moeten worden voorgelicht over waar ze met hun klachten terecht kunnen, wat wel en wat niet wordt onderzocht, hoe de nakoming kan worden afgedwongen en welke informatie zij dienen te verstrekken opdat de autoriteiten een onderzoek kunnen instellen;

– coördinatie en samenwerking tussen lidstaten en tussen lidstaten en derde landen op het gebied van de nationale wetgeving die in bepaalde gevallen van toepassing is;

– de middelen die ter beschikking staan om "spammers" op te sporen die in de EU of daarbuiten actief zijn en hun identiteit verbergen, onder meer door gebruik te maken van de identiteit, adressen of servers van anderen.

Een beschrijving van de handhavingsbepalingen ten aanzien van de voorschriften voor ongevraagde communicatie is al gegeven in punt 2.2.

---

http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/9threport/index_en.htm.

[25] Op het belang van een volledige, doeltreffende en tijdige tenuitvoerlegging van het nieuwe regelgevingskader voor elektronische communicatie, met inbegrip van deze richtlijn, is al door de Commissie de nadruk gelegd in haar "Mededeling over Elektronische communicatie: De weg naar de kenniseconomie" (COM(2003) 65 van 11 februari 2003).

[26] De schriftelijke aanmaningen zijn op 25 november 2003 verzonden (zie IP/03/1663).

De manier waarop de procedures inzake ongevraagde commerciële e-mail ingericht en afgehandeld worden, verschilden tot dusver vaak aanzienlijk[27]. Ofschoon het karakter van een EU-richtlijn impliceert dat de lidstaten enige manoeuvreerruimte behouden bij de tenuitvoerlegging van de bepalingen ervan, is een doeltreffende handhaving noodzakelijk, ongeacht de gekozen methode.

Verschillen tussen de lidstaten

De handhaving van de bepalingen inzake ongevraagde commerciële communicatie gebeurt niet in alle lidstaten door dezelfde instantie. In de meeste lidstaten is het in eerste instantie de gegevensbeschermingsautoriteit die met de handhaving van de voorschriften is belast. In andere landen is het juist de taak van de nationale regelgevingsinstantie voor elektronische communicatie (NRI). In weer andere landen is de handhaving dan weer vooral een zaak van de consumentenbeschermingsautoriteiten (of de ombudsman). Vaak speelt meer dan één autoriteit een rol bij de handhaving van de voorschriften inzake ongevraagde communicatie. Bovendien gaat spam veelal samen met misleidende of frauduleuze praktijken. (In een minderheid van lidstaten is er geen consumentenbeschermingsautoriteit en wordt de handhaving overgelaten aan de consumentenverenigingen of de consumenten zelf.) Spam wordt vaak in verband gebracht met inbreuken op de gegevensbescherming, zoals "harvesting", of zelfs internetcriminaliteit, zoals "computervredebreuk". De handhaving van de desbetreffende voorschriften gebeurt niet altijd door dezelfde autoriteiten, zeker niet over de grenzen heen.

Behalve in een paar lidstaten worden klachten niet altijd ook onderzocht. Soms worden vóór de start van een officiële procedure eerst, met wisselend succes, andere wegen bewandeld, zoals het verstrekken van instructies en richtsnoeren aan bedrijven. Soms wordt deze voorbereidende fase aan de consument overgelaten, die dan contact moet opnemen met het bedrijf alvorens een klacht in te dienen. In sommige landen wordt aan zelfregulering gedaan (bijvoorbeeld in het VK) om deze eerste fase van het optreden te organiseren. In sommige lidstaten heeft de industrie in het kader van zelfregulering reeds een aantal klachtenregelingen ingevoerd. Vaak nemen de autoriteiten ook zelf het initiatief. Als een zaak aan de administratieve autoriteiten wordt overgelaten betekent dit meestal niet dat de directe gang naar de rechter geblokkeerd wordt.

Niet alle gegevensbeschermingsautoriteiten hebben de bevoegdheid om op te treden tegen rechtspersonen. Ook kunnen (nog) niet alle gegevensbeschermingsautoriteiten boetes opleggen. Dergelijke autoriteiten zijn genoodzaakt een juridische procedure aangespannen. In Frankrijk heeft het experiment met de spambox de gegevensbeschermingsautoriteit ertoe gebracht een aantal specifieke gevallen te selecteren om deze voor de rechter te brengen, zij het met weinig succes. Een soortgelijke experiment in België heeft geleid tot een gedachtewisseling met de verdachte verzenders en, in internationale kwesties, tot doorverwijzing naar hun tegenhangers in andere EU-lidstaten of de Amerikaanse FTC.

Een uitgebalanceerde aanpak in de sfeer van regelgeving, handhaving en zelfregulering wordt dikwijls gezien als de meest effectieve methode om de toestemmingsregeling te handhaven. Van de lidstaten wordt verlangd dat zij de doeltreffendheid van hun handhavingsmechanismen evalueren, met name in het licht van de diverse, hieronder voorgestelde maatregelen (zie de punten 3.2 tot en met 3.6).

De lidstaten wordt ook verzocht nationale strategieën te ontwikkelen teneinde de samenwerking tussen de gegevensbeschermingsautoriteiten, de consumentenbeschermingsautoriteiten en de nationale regelgevingsinstanties (NRI's)

[27] Klachten hebben vaak ook betrekking op aanverwante kwesties, zoals het recht op toegang tot persoonsgegevens of het recht om bezwaar te maken tegen de verwerking van gegevens.

voor elektronische communicatie te garanderen en overlapping van bevoegdheden en dubbel werk te voorkomen.

Om de uitwisseling van informatie en beste praktijken op het gebied van doeltreffende handhaving (bijvoorbeeld klachten, rechtsmiddelen, sancties, internationale samenwerking) te bevorderen en te coördineren hebben de diensten van de Commissie met steun van de lidstaten en de gegevensbeschermingsautoriteiten een **informele internetgroep voor ongevraagde commerciële communicatie** opgericht. Deze groep zal eveneens de andere in deze mededeling genoemde activiteiten stimuleren en coördineren, zoals op het gebied van bewustmaking en technische oplossingen.

De naar aanleiding van groepsbesprekingen opgestelde documenten zullen doorgaans worden voorgelegd aan het Comité voor communicatie (COCOM), dat uit hoofde van het regelgevingskader voor elektronische communicatienetwerken en -diensten is opgericht, en/of aan de Groep gegevensbescherming artikel 29, zodat deze hier passende gevolgen aan kunnen geven. In het bijzonder zou de groep benchmarking-criteria kunnen opstellen voor de diverse nog voor te stellen maatregelen.

Aangesloten bij deze internetgroep zijn de nationale overheden en gegevensbeschermingsautoriteiten, alsmede de diensten van de Commissie. De internetgroep zal bepalen hoe de andere belanghebbende partijen kunnen deelnemen.

3.2. Doeltreffende rechtsmiddelen en sancties

3.2.1. Bespreking

Bij rechtsmiddelen gaat het op dit moment meestal om boetes of een bevel om de onrechtmatige verwerking van gegevens te staken, soms ook om het "blokkeren" van de betrokken websites. In sommige lidstaten gaat zo'n "dwangbevel" vooraf aan of samen met boetes in geval van niet-naleving. Niet alle instanties zijn evenwel bevoegd voor het volledige scala van inbreuken in verband met spam en evenmin beschikken zij alle over dezelfde instrumenten. Vaak worden gevallen ook doorverwezen naar de rechterlijke macht. Niet in alle lidstaten bestaan er strafrechtelijke sancties op inbreuken.

Niet alle lidstaten hebben voorzien in rechtsmiddelen en boetes/sancties uit hoofde van bestuursrechtelijke of strafrechtelijke bepalingen. De strafrechtelijke sancties variëren, net als de mogelijkheid van een gevangenisstraf in bepaalde lidstaten. Bovendien bestaat in het algemeen ook de mogelijkheid om langs civiele weg een schadevergoeding te eisen.

Ofschoon er dikwijls onderscheid wordt gemaakt tussen "lichte" en "zware" overtredingen (bijvoorbeeld grootschalige mailings, misleidende of frauduleuze reclame en handelspraktijken), verschillen de straffen tussen de diverse lidstaten sterk.

Veelal kan bij spamactiviteiten ook worden opgetreden krachtens de algemene gegevensbeschermingswetgeving (bijvoorbeeld inbreuk op de kennisgevingsplicht, het recht op toegang, de verplichting tot aanwijzing van een vertegenwoordiger in een EU-lidstaat, enz.) of uit hoofde van specifieke wetgeving (bijvoorbeeld misleidende reclame, frauduleuze handelspraktijken, enz.). Vóór de invoering van de toestemmingsregeling is van verschillende rechtsgronden gebruik gemaakt om bepaalde vormen van spam aan te pakken (zoals grootschalige e-mailcampagnes, onrechtmatig gebruik van persoonsgegevens, netwerkverstoring, misbruik van e-mail accounts, bedrog en onjuiste uitleg van contracten).

Doorgaans wordt gerechtelijk optreden niet gezien als een afdoende methode van handhaving. In het algemeen kan een administratieve boete worden opgelegd door de gegevensbeschermingsautoriteiten, de consumentenbeschermingsautoriteiten en/of de NRI's, zij het dat de hoogte daarvan varieert. Lidstaten waarin deze mogelijkheid nog niet bestaat, overwegen meestal deze alsnog in te voeren. Vergeleken met justitiële rechtsmiddelen, lijken administratieve sancties bijzonder geschikt voor zo'n dynamische sector. De gegevensbeschermingsautoriteiten, consumentenbeschermingsautoriteiten en NRI's verschaffen zichzelf vaak extra handhavingsinstrumenten. Administratieve procedures zijn zowel goedkoop als snel (volgens de Italiaanse gegevensbeschermingsautoriteiten maximaal 50 dagen).

3.2.2. Voorgestelde maatregelen

Als randvoorwaarde dringt de Commissie er bij de lidstaten die de richtlijn en in het bijzonder de bepalingen inzake ongevraagde communicatie nog niet hebben omgezet, op aan dit alsnog zonder verder uitstel te doen. De diensten van de Commissie zijn bereid de lidstaten daarbij zonodig te helpen.

De lidstaten wordt verzocht de doeltreffendheid van hun systeem van rechtsmiddelen en sancties voor inbreuken te evalueren en slachtoffers een adequate manier te bieden om schadevergoeding te eisen.

De lidstaten en de bevoegde instanties die niet over administratieve instrumenten beschikken, dienen te overwegen dergelijke instrumenten tegen spam in te voeren, aangezien zij een snel, betaalbaar en doeltreffend hulpmiddel zijn om de toestemmingsregeling te doen naleven.

De Commissie zal erop toezien dat de nationale omzettingsmaatregelen in werkelijke sancties voorzien, zonodig onder meer in de vorm van boetes en strafrechtelijke sancties, voor het geval dat de betrokken eisen niet door marktspelers worden nageleefd.

In dit verband zal de Commissie eveneens onderzoeken in hoeverre de bevoegde autoriteiten over de noodzakelijke onderzoek- en handhavingsbevoegdheden beschikken.

3.3. Klachtenmechanismen

3.3.1. Bespreking

Voor een doeltreffende handhaving zijn adequate klachtenmechanismen noodzakelijk. Sommige gegevensbeschermingsautoriteiten hebben e-mailboxen opgezet waarnaar de gebruikers ongevraagde commerciële e-mailberichten kunnen doorsturen en hebben zichzelf ertoe verbonden in gerichte gevallen actie te ondernemen.

Sommige lidstaten lijken de voorkeur te geven aan gewone administratieve procedures en/of contacten met ISP's of CERT's (computercalamiteitenteams) in geval van netwerkverstoring. Andere lidstaten hebben weer een voorkeur voor traditionele procedures (civiel- of bestuursrechtelijke schadeclaims). Coregulering of zelfregulering wordt soms gebruikt als beter alternatief voor directe handhaving.

Beste praktijken

Frankrijk en België hebben in het najaar van 2002 gebruikgemaakt van speciale e-mailboxen voor de ontvangst van specifieke klachten over spam en de resultaten daarvan zijn vrij interessant. De verslagen over deze initiatieven zijn toegankelijk voor het publiek[28]. Verwacht wordt dat Frankrijk een permanente e-mailbox zal opzetten op basis van de nieuwe voorschriften ter omzetting van de Richtlijn betreffende privacy en elektronische communicatie. De Amerikaanse Federal Trade Commission (FTC) beschikt over een soortgelijke mailbox en gebruikt deze in het kader van de vervolging op basis van de bestaande wetgeving inzake oneerlijke en bedrieglijke handelspraktijken[29].

Mailboxen hebben onder meer als voordeel dat zij de consument blijken te stimuleren om overtredingen te rapporteren en zo de vastgestelde wetgeving doeltreffender maken. Bovendien kunnen zij essentiële statistische gegevens verschaffen over de aard en de omvang van de problemen in een bepaald land of in een bepaalde regio, aan de hand waarvan de autoriteiten een duidelijke indruk krijgen zodat zij handhavingsprioriteiten kunnen vaststellen of aanpassen. Bovendien kunnen preventieve acties worden opgezet op basis van de verworven kennis. Ter illustratie, de CNIL, d.w.z. de Franse gegevensbeschermingsautoriteit heeft de via haar spambox verzamelde informatie gebruikt om op gebruikers en marketeers gerichte preventieve informatiepakketten samen te stellen.

Het nut van een elektronische mailbox voor het bewaken en meten van de schaal en omvang van spam hangt begrijpelijkerwijs af van het vermogen om de klachten op zinvolle en snelle wijze te onderzoeken.

Er bestaat algemene belangstelling voor het leren van de ervaringen van andere lidstaten met elektronische mailboxen, maar slechts enkele lidstaten zijn van plan of overwegen een speciale elektronische mailbox op te zetten.

---

28 Het verslag van 24 oktober 2002 van de "Commission National Informatique et Libertés" (CNIL), de Franse gegevensbeschermingsautoriteit, is beschikbaar op het volgende webadres: http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm
Het van juli 2003 daterende verslag van de "Commissie voor de bescherming van de persoonlijke levenssfeer" (CBPL), de Belgische gegevensbeschermingsautoriteiten, kan worden gevonden op het volgende adres: http://www.privacy.fgov.be/publicaties/spam_4-7-03_nl.pdf.

29 Zie bijvoorbeeld http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf. Ongevraagde of bedrieglijke berichten kunnen naar het volgende e-mailadres worden gestuurd: uce@ftc.gov.

Meestal worden daarvoor de volgende redenen genoemd: de bestaande mogelijkheid om een klacht in te dienen via bijvoorbeeld de website van de autoriteit, de behoefte aan extra personeel en apparatuur, of de noodzaak om de bestaande juridische procedures te wijzigen.

3.3.2. Voorgestelde maatregelen

De lidstaten en de bevoegde instanties dienen na te gaan of hun rechtsstelsel doeltreffend genoeg is om in te spelen op klachten van de gebruiker of dat eventuele aanpassingen nodig zijn.

De lidstaten en de bevoegde autoriteiten worden ertoe opgeroepen speciale elektronische mailboxen en voorlichtingscampagnes daarvoor op te zetten.

Deze speciale elektronische mailboxen dienen zo te worden ontworpen dat zij met het oog op een beter inzicht in de problematiek en de vaststelling van handhavingsprioriteiten gemakkelijk kunnen worden doorzocht en geanalyseerd.

De diensten van de Commissie zullen met de uitwisseling van informatie over experimenten met elektronische mailboxen bevorderen.

3.4. Grensoverschrijdende klachten en EU-samenwerking bij de handhaving

3.4.1. Bespreking

Een doeltreffende behandeling van grensoverschrijdende klachten is van belang voor een goede bescherming van de consument op dit terrein. Het is essentieel ervoor te zorgen dat de nationale klachtenmechanismen, ongeacht de wijze waarop deze zijn opgezet, op elkaar aansluiten zodat ook klachten van gebruikers in een bepaalde lidstaat over berichten uit een andere lidstaat op doeltreffende wijze worden behandeld (zie voor samenwerking met derde landen punt 3.5).

Op dit moment beschikken nog niet alle lidstaten over een formele procedure voor de behandeling van grensoverschrijdende klachten. Gangbare oplossingen daarvoor zijn onder meer het aanknopen van contacten met de desbetreffende autoriteit in de andere lidstaat en het eventueel doorleiden van de klacht naar de relevante autoriteit in het land van herkomst van de berichten.

De gegevensbeschermingsautoriteiten ontplooien momenteel initiatieven op Europees niveau (de EER en de kandidaatlidstaten inbegrepen) om informatie uit te wisselen over grensoverschrijdende klachten in het kader van de "workshop klachtenafhandeling", een werkgroep die in het kader van de Europese Conferentie van gegevensbeschermingsfunctionarissen is opgericht. De mogelijkheid bestaat om deze te gebruiken voor grensoverschrijdende klachten over spam, onder meer om te bepalen welk recht in een gegeven geval van toepassing is. Maar niet alle gegevensbeschermingsautoriteiten werken actief mee aan de handhaving van de voorschriften ten aanzien van ongevraagde communicatie.

Wat consumentenbescherming betreft, is de Commissie onlangs met een voorstel gekomen voor een verordening betreffende samenwerking met betrekking tot consumentenbescherming, op basis waarvan een netwerk van overheidsinstanties op het

gebied van consumentenbescherming moet worden opgericht dat zich met grensoverschrijdende problemen zal bezighouden[30]. Hiermee worden procedures voor wederzijdse bijstand in het leven roepen en wordt voorzien in intensieve operationele samenwerking tussen nationale autoriteiten. De voorgestelde regeling zou moeten gelden voor misleidende of bedrieglijke spam of spam die in strijd is met de consumentenbeschermingsvoorschriften, maar niet voor alle spam die door de Richtlijn betreffende privacy en elektronische communicatie wordt verboden. Deze verordening is momenteel in behandeling bij de Raad en het Parlement.

3.4.2. Voorgestelde maatregelen

De lidstaten en de bevoegde instanties wordt verzocht na te gaan of hun bestaande procedures voor de behandeling van grensoverschrijdende klachten (zoals overeenkomsten inzake wederzijdse bijstand) doeltreffend genoeg zijn.

Ook wordt coördinatie tussen de bevoegde nationale autoriteiten aangemoedigd. Dit omvat coördinatie en informatie-uitwisseling tussen de handhavingsautoriteiten op het gebied van de nieuwe voorschriften en tussen deze en andere autoriteiten die bevoegd zijn voor bepaalde vormen van spam (bijvoorbeeld frauduleuze spam of "scams", pornografische spam, berichten over illegaal verspreide gezondheidsproducten).

In verband met frauduleuze en bedrieglijke spam wordt er bij de Raad en het Parlement op aangedrongen om zo snel mogelijk overeenstemming te bereiken over het voorstel voor een verordening betreffende samenwerking met betrekking tot consumentenbescherming om ervoor te zorgen dat de consumentenbeschermingsautoriteiten in de EU volledig klaar zijn om op te treden tegen misleidende en bedrieglijke spam. Hun wordt ook verzocht de mogelijkheid te bekijken om het toepassingsgebied van deze verordening uit te breiden tot dat van de Richtlijn betreffende privacy en elektronische communicatie.

De lidstaten wordt gevraagd te onderzoeken hoe de huidige belemmeringen voor informatie-uitwisseling en samenwerking uit de weg kunnen worden geruimd en hoe het mogelijk kan worden gemaakt hun tegenhangers in andere lidstaten te verzoeken op te treden. In praktische termen zou het nuttig kunnen zijn over een verbindingsmechanisme te beschikken (zie bovengenoemd initiatief van de gegevensbeschermingsautoriteiten) op basis waarvan de nationale regelgevers zouden kunnen samenwerken op het punt van grensoverschrijdende handhaving. Bij de oprichting van een samenwerkingsnetwerk zou kunnen worden geprofiteerd van bestaande programma's van de Commissie zoals IDA[31].

De Commissie is voornemens dergelijke coördinatiepogingen van bevoegde nationale autoriteiten te bevorderen, met name door middel van de pas opgerichte informele internetgroep voor ongevraagde commerciële communicatie. De diensten van de Commissie zijn samen met de lidstaten en de bij de handhaving betrokken nationale autoriteiten een onderzoek gestart naar de concrete actie die moet worden ondernomen om de behandeling van grensoverschrijdende klachten te verbeteren. De besprekingen met de nationale autoriteiten zullen in de rest van 2004 worden voortgezet.

---

30 COM (2003) 443 def.

31 Informatie over het programma IDA is te vinden op het volgende webadres: http://europa.eu.int/comm/enterprise/ida/index.htm.

3.5. Samenwerking met derde landen

3.5.1. Bespreking

De nieuwe voorschriften gelden voor de verwerking van persoonsgegevens in relatie met de levering van openbaar toegankelijke elektronische communicatiediensten via openbare communicatienetwerken in de EU (en de EER). Dientengevolge is artikel 13 van Richtlijn 2002/58/EG, waarmee de toestemmingsregeling is ingevoerd, van toepassing op alle ongevraagde commerciële communicatie die ontvangen wordt door of verzonden wordt vanaf netwerken in de EU (en de EER). Dit impliceert dat ook berichten die uit derde landen afkomstig zijn in overeenstemming met de EU-voorschriften moeten zijn, net als berichten die vanuit de EU naar geadresseerden in derde landen worden verstuurd.

De feitelijke handhaving van de voorschriften met betrekking tot uit derde landen afkomstige berichten is natuurlijk veel gecompliceerder dan bij vanuit de EU afkomstige berichten. Toch gaat het om een belangrijk aspect, aangezien veel spam van buiten de EU afkomstig is.

Ofschoon een brede waaier van instrumenten noodzakelijk is, zoals preventieve filtertechnieken, zelfregulering, contracten en internationale samenwerking, wordt in dit punt vooral ingegaan op internationale samenwerking. Het voornaamste doel van internationale samenwerking is het bevorderen van de vaststelling van doeltreffende wetgeving in derde landen. Een tweede doel is de samenwerking met derde landen op het gebied van een doeltreffende handhaving van de toepasselijke voorschriften.

Er is nog niet veel ervaring opgedaan met de handhaving van opt-in- of opt-out-voorschriften voor communicatie die van buiten de EU afkomstig is. Afgezien van het feit dat spam een nog betrekkelijk jong verschijnsel is, wordt dikwijls gewezen op belemmeringen zoals de moeilijkheid van het opsporen van de spammers of de enorme inspanning die dit vergt, het gebrek aan (adequate) internationale samenwerkingsmechanismen,, alsmede het ontbreken van de bevoegdheid van sommige autoriteiten over internationale aangelegenheden.

Wat frauduleuze en bedrieglijke spam betreft, voorziet het voorstel van de Commissie voor een verordening betreffende samenwerking met betrekking tot consumentenbescherming tevens in samenwerking met derde landen bij de handhaving. De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) heeft in 2003 een aanbeveling gedaan die de consumenten tegen frauduleuze en bedrieglijke grensoverschrijdende handelspraktijken moet beschermen[32].

3.5.2. Voorgestelde maatregelen

Op multilateraal niveau hebben sommige lidstaten al actief deelgenomen aan fora zoals de OESO, die initiatieven ten aanzien van spam zijn gestart. Actieve deelname aan dit werk wordt aangemoedigd, met name wat betreft de uitwerking van oplossingen in internationaal verband.

---

[32] OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OESO, 2003.

De Commissie zal in februari 2004 gastvrouwe zijn voor een OESO-workshop over spam die meer inzicht moet verschaffen in de door spam veroorzaakte problematiek en moet bijdragen tot de ontwikkeling van oplossingen in internationaal verband. Bij concrete vervolgactiviteiten in OESO-verband zal worden voortgebouwd op de resultaten van die workshop. De diensten van de Commissie zijn op dit moment bezig deze vervolgactiviteiten met de lidstaten te bespreken, waarbij ook wordt ingegaan op de pogingen van de OESO om de vaststelling van doeltreffende wetgeving, bewustmaking, ontwikkeling van technische oplossingen, zelfregulering en internationale samenwerking op het gebied van handhaving internationaal te bevorderen.

In VN-verband wordt er in de slotverklaring van de Wereldtop over de informatiemaatschappij (Genève, 10-12 december 2003) en het bijbehorende actieplan nadrukkelijk op gewezen dat spam moet worden aangepakt op de daarvoor geschikte nationale en internationale fora. De Commissie zal nagaan hoe een zo goed mogelijk vervolg kan worden gegeven aan de resultaten van de Wereldtop van 2003 in de EU, rekening houdende met de wereldtop van Tunis, die in 2005 zal plaatsvinden.

Bovendien zullen de lidstaten en de bevoegde instanties worden verzocht de bilaterale samenwerking met derde landen te versterken of te initiëren. Dit heeft niet alleen betrekking op de bevordering van doeltreffende wetgeving, maar ook op samenwerking bij de handhaving, inclusief waar nodig ook op politionele en justitiële samenwerking.

Ook zal de samenwerking worden bevorderd tussen de autoriteiten en de particuliere sector, met name ISP's en ESP's, teneinde de spammers op te sporen met inachtneming van de nodige wettelijke garanties.

De diensten van de Commissie zullen actief blijven op internationale fora, waaronder de OESO en de OESO-workshop die de Commissie in februari 2004 in Brussel zal organiseren. Zij zal ook bilaterale vergaderingen en besprekingen met derde landen blijven houden, onder meer om deze landen te stimuleren doeltreffend op te treden tegen spam, vooral de meest aanstootgevende vormen daarvan, en om de samenwerking op het gebied van de handhaving te bevorderen.

De diensten van de Commissie zijn samen met de lidstaten en de bij de handhaving betrokken nationale autoriteiten een onderzoek gestart naar de manier waarop de internationale samenwerking, met name bij de behandeling van grensoverschrijdende klachten, kan worden geoptimaliseerd. Deze contacten met de nationale autoriteiten zullen in de rest van 2004 worden voortgezet.

3.6. Toezicht

3.6.1. Bespreking

Om te evalueren hoe de toestemmingsregeling in de praktijk werkt en specifieke problemen met geschikte maatregelen aan te pakken, hebben de lidstaten behoefte aan objectieve en actuele gegevens over de ontwikkelingen op het gebied van spam, klachten van de gebruikers en moeilijkheden waar de service providers mee te maken krijgen. Mogelijke informatiebronnen en –types zijn onder meer: trends op het gebied van de aard van spam, herkomst en volume van ongevraagde commerciële e-mail zoals die door filtersoftware, service providers en nationale (wetgevings)autoriteiten worden bepaald, en statistische gegevens die, waar relevant, uit het gebruik van spamboxen naar voren komen.

De OESO heeft in 2003 een begin gemaakt met het meten van ongevraagde elektronische berichten op internationaal niveau en zal hiermee in 2004 doorgaan.

Artikel 18 van de Richtlijn betreffende privacy en elektronische communicatie bepaalt dat in 2006 verslag dient te worden uitgebracht over de tenuitvoerlegging van de richtlijn en de gevolgen daarvan voor de exploitanten en consumenten. Bij de samenstelling van het rapport dient de Commissie informatie in te winnen bij de lidstaten, onder meer relevante statistische gegevens.

3.6.2. Voorgestelde maatregelen

De lidstaten dienen ervoor te zorgen dat zij de beschikking krijgen over de informatie en statistische gegevens die nodig zijn om, zonodig in samenwerking met de industrie en rekening houdende met de lopende OESO-werkzaamheden op het gebied van de analyse van ongevraagde elektronische berichten, richting te geven aan hun handhavingsactiviteiten.

De Commissie zal een beroep doen op de onlangs opgerichte informele internetgroep voor ongevraagde commerciële communicatie om de uitwisseling van informatie en beste praktijken op het gebied van trends en statistische gegevens inzake spam te bevorderen en coördineren.

4. TECHNISCHE MAATREGELEN EN ZELFREGULERING DOOR DE INDUSTRIE

In dit hoofdstuk over zelfregulering en technische aspecten wordt ingegaan op voorstellen voor maatregelen die de marktspelers zelf kunnen treffen, met name op gebieden zoals contractuele afspraken, gedragscodes, aanvaardbare marktpraktijken, etikettering en alternatieve geschillenregelingen. Het heeft ook betrekking op een aantal technische oplossingen, zoals filteren en veiligheid van servers.

4.1. Doeltreffende toepassing van de toestemmingsregeling

4.1.1. Bespreking

De bestrijding van spam is een zaak van alle betrokken partijen. De industrie kan hierbij een duidelijke rol spelen door de toestemmingsregeling te vertalen in de dagelijkse praktijk. Daaronder moeten niet alleen de voorwaarden voor eindgebruikers worden verstaan, maar ook de afspraken met zakenpartners.

In veel gevallen is een betere coördinatie door industriële verenigingen en de betrokkenheid van sectorspecifieke zelfreguleringinstanties en consumenten-/gebruikersverenigingen, zoals gegevensbeschermingsautoriteiten of andere bevoegde nationale instanties, noodzakelijk.

Beste praktijken

Ter illustratie: In Nederland fungeert het Electronic Commerce Platform (ECP.NL) sinds 2002 als gastheer voor een ander platform dat zich bezig houdt met de uitgangspunten voor reclame per e-mail en waarin verschillende branchеverenigingen (direct marketing en ISP's) vertegenwoordigd zijn, evenals de Consumentenbond. De bedoeling is tot een praktische uitwerking te komen van het opt-in-beginsel. Deze praktijkregeling zal in samenwerking met de gegevensbeschermingsautoriteit worden getest[33].

Contracten kunnen nuttig zijn bij de bestrijding van spam, mits er garanties komen met betrekking tot de rechten van het individu. Vele internet service providers (ISP's) en e-mail service providers (ESP's) hebben in hun contracten met klanten al een verbod opgenomen op het gebruik van hun diensten voor het versturen van spam.

Deze ISP's en ESP's hebben het verzenden van ongevraagde e-mail en bulk e-mail vanaf hun e-mail accounts al verboden[34].

De concepten die in oudere contracten tussen ISP's en hun klanten werden gebruikt, verschillen waarschijnlijk van die welke in de nieuwe richtlijn en de nationale omzettingsmaatregelen daarvoor worden gehanteerd.

In termen van klantenservice is er ook behoefte aan een actiever beleid inzake filtering door informatie te verstrekken over spamfilters of door eventueel ook filterdiensten of -voorzieningen aan abonnees te verstrekken.

Dit geldt ook wanneer ISP's of mobiele exploitanten contracten met derde partijen afsluiten, in het bijzonder met direct-marketingbedrijven. Dit beperkt zich trouwens niet tot de directe relaties met bedrijven die "value added services" aanbieden. Het geldt ook voor exploitanten waarmee een bepaalde service provider interconnectie-overeenkomsten heeft gesloten, bijvoorbeeld in het geval van mobiele diensten.

De nieuwe toestemmingsregeling heeft ook gevolgen voor diverse direct marketing-activiteiten, zoals:

- het verzamelen van e-mailadressen en andere elektronische contactgegevens op basis van de nieuwe regeling (zoals hierboven al werd opgemerkt is het "harvesten" van e-mail-adressen in strijd met het Gemeenschapsrecht);

- de aanpassing van bestaande lijsten;

- het verbod op het gebruik van gegevens zonder toestemming en op de verkoop van niet-conforme lijsten.

---

33 Zie http://www.ecp.nl/projecten.php#32.

34 Dergelijke clausules zijn soms gebaseerd op de noodzaak om alle nodige maatregelen te treffen om misbruik van hun diensten te voorkomen. Soms verwijzen zij naar bestaande gedragscodes voor bulk e-mail of naar zelfreguleringsbeginselen (zoals de "de netiquette").

4.1.2. Voorgestelde maatregelen

De rol van de industrie en van zelfregulering, of zelfs coregulering, dient te worden bevorderd, met name op gebieden waarop wetgevingen en handhaving door de openbare autoriteiten alleen niet volstaat. Alle betrokken partijen moeten op dit gebied een rol spelen, ook de consumentenverenigingen en/of gebruikersverenigingen.

Contractuele praktijken van service providers ten opzichte van abonnees en zakenpartners

In de eerste plaats zal de industrie moeten beoordelen of haar huidige contracten verenigbaar zijn met de nieuwe voorschriften en, als dit niet het geval is, deze daarmee in overeenstemming brengen.

Dit impliceert een aanpassing van de contractvoorwaarden voor de abonnees. Dit geldt niet alleen voor ISP's en ESP's, maar ook voor de aanbieders van mobiele diensten. Als aanvulling hierop zouden zij als extra klantenservice informatie kunnen verstrekken over filters, en filtersoftware en/of –diensten kunnen verstrekken (zie ook punt 4.3 met betrekking tot filtering). Voorts dienen ook de bepalingen in contracten met zakenpartners (bijvoorbeeld mobiele interconnectie, "value-added services") te stipuleren dat hun marketingpraktijken in overeenstemming dienen te zijn met de toestemmingsregeling en te voorzien in adequate straffen in geval van inbreuk.

De eigen praktijken van de direct-marketingbedrijven

In de tweede plaats kan het noodzakelijk zijn de praktijken van direct-marketingbedrijven aan te passen aan de toestemmingsregeling. Deze bedrijven zouden in het bijzonder overeenstemming kunnen bereiken over specifieke, wettige methoden om persoonsgegevens te verzamelen (bijvoorbeeld op basis van dubbele of herhaalde toestemming).

Gedragscodes

In de derde plaats hebben de brancheorganisaties al diverse initiatieven aangekondigd, zoals de aanpassing of invoering van gedragscodes en de verspreiding van goede marketingpraktijken[35]. De Commissie zal zich inzetten voor pan-Europese online-gedragscodes voor direct-marketingbedrijven. Gedragscodes en andere zelfreguleringsinitiatieven dienen evenals contracten in overeenstemming te zijn met de toestemmingsregeling. De bevoegde regelgevingsinstantie kan hierin een zinvolle rol spelen. Er zij in dit verband aan herinnerd dat de Groep gegevensbescherming artikel 29 haar goedkeuring kan hechten aan communautaire gedragscodes (zie artikel 30 van de "algemene" Gegevensbeschermingsrichtlijn 95/46/EG).

Zoals dikwijls het geval is, hebben zelfreguleringsinitiatieven alleen kans van slagen als er een structuur is opgezet waarmee toezicht kan worden gehouden op de naleving van de afgesproken regels en doeltreffende sancties kunnen worden vastgesteld.

---

[35] De European Federation of Direct Marketing (FEDMA) heeft een specifieke online-gedragscode aangekondigd voor direct-marketingbedrijven.

Labels

In de vierde plaats kan gebruik worden gemaakt van hulpmiddelen zoals labels (of keurmerken), vooral wanneer betrouwbare derde partijen erop toezien en certificeren dat de marktspelers zich aan gedragscodes houden.

Dankzij zichtbare labels kunnen de gebruikers zien welke ISP's, ESP's en andere industriële spelers zich aan de EU-voorschriften en/of erkende gedragscodes voor de implementatie daarvan houden. Zij kunnen ook helpen filtersystemen doeltreffender te maken.

Ook kan worden gedacht aan het toekennen van labels aan databases van gebruikers die zich aan de toestemmingsregeling houden, alsmede aan e-mailberichten die in overeenstemming zijn met de toestemmingsregeling (bijvoorbeeld door het gebruik van het "ADV"-label in the betreft-regel van een e-mailbericht om aan te geven dat dit reclame bevat).

Dankzij labels kunnen de ontvangers dergelijke commerciële communicatie duidelijk herkennen, zoals dat verlangd wordt door de Richtlijn elektronische handel (zie artikel 6, onder a), van Richtlijn 2000/31/EG, alsmede punt 2 van dit document).

4.2. Alternatieve geschillenregelingen

4.2.1. Bespreking

Voor inbreuken op de privacy, zoals het verzenden van ongevraagde e-mail, kan een buitengerechtelijke geschillenregeling nuttig zijn om een betere naleving van de nieuwe voorschriften te bereiken. Zowel op nationaal als op EU-niveau zijn diverse initiatieven ontplooid ten aanzien van alternatieve regelingen voor de behandeling van geschillen over online-transacties en elektronische communicatie. De Commissie heeft in 1998 en 2001 aanbevelingen gedaan inzake alternatieve geschillenregelingen, waarin de uitgangspunten voor dergelijke regelingen zijn beschreven. Diverse initiatieven zijn genomen met betrekking tot alternatieve geschillenregelingen op het gebied van consumentenbescherming (zoals EEJ-NET)[36]. Ook op grond van artikel 17 van de Richtlijn elektronische handel dient de ontwikkeling van dergelijke mechanismen te worden bevorderd.

In sommige landen bestaan buitengerechtelijke geschillenregelingen, die soms een wettelijke basis hebben, maar in diverse opzichten ook verschillen, zoals wat betreft domein (branchespecifiek, zoals direct marketing, e-mail marketing), jurisdictie, bevoegdheden een sancties (bijvoorbeeld schadeclaims), de rol van specifieke autoriteiten (zoals gegevensbeschermingsautoriteiten, reclamecodecommissies), enz.

Dergelijke regelingen kunnen alleen doeltreffend genoeg zijn als aan bepaalde voorwaarden is voldaan, bijvoorbeeld ten aanzien van de wijze waarop zij georganiseerd en gepromoot worden of waarop de overeenstemming met de voorschriften wordt gegarandeerd. Voor de invoering ervan is doorgaans ook samenwerking tussen de autoriteiten en industrie noodzakelijk.

---

[36] Meer informatie is te vinden op: http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm.

4.2.2. Voorgestelde maatregelen

De invoering en toepassing van doeltreffende zelfreguleringsmechanismen en alternatieve geschillenregelingen wordt aangemoedigd, waarbij zo mogelijk moet worden voortgebouwd op bestaande initiatieven (zoals EEJ-NET). Zij kunnen vooral nuttig zijn in gevallen waarin internationale samenwerking moeilijker te realiseren is.

4.3. Technische kwesties

4.3.1. Bespreking

Op technisch gebied worden uiteenlopende oplossingen gekozen ter bestrijding van spam. De internetgemeenschap (bijv. RIPE en IETF) neemt de spamproblematiek eveneens serieus[37]. Initiatieven op langere termijn, zoals de nieuwe technische normen voor e-mail, komen in dit document niet aan de orde. ISP's en ESP's blokkeren dikwijls inkomende post van servers die voor de verzending van spam worden gebruikt (en daarom op de zwarte lijst zijn gezet), totdat de bron van de spam is opgespoord en van de server wordt geweerd. Daarnaast kunnen individuele gebruikers hun eigen eindapparatuur van filtersoftware voorzien en kunnen de aanbieders van elektronische-communicatiediensten deze op hun servers installeren.

Maar niet alle filtermethoden en -technieken bieden dezelfde mate van controle voor de gebruiker. En evenmin bieden zij dezelfde mate van garantie voor de bescherming van gegevens en de privacy, zoals de inachtneming van de vertrouwelijkheid van het communicatieverkeer. Zij zijn ook niet altijd al aangepast aan de nieuwe toestemmingsregeling voor marketingberichten die in de EU landen is ingevoerd (voorafgaande toestemming voor zowel bulk- als niet-bulk-berichten ten behoeve van marketing). Bovendien kan door een sterkere differentiatie tussen rechtmatige marketing (d.w.z. met inachtneming van de toestemmingsregeling) en ongevraagde commerciële communicatie mogelijk doeltreffender filtersoftware worden ontwikkeld.

Hoewel de nieuwe wettelijke bepalingen inzake ongevraagde commerciële e-mail de gebruiker extra waarborgen bieden en de service providers meer garanties bieden om desgevraagd tegen "spammers" op te treden, kunnen af en toe toch rechtmatige e-mailberichten worden tegengehouden ("vals-positieven") of spamberichten worden doorgelaten ("vals-negatieven"). De kans bestaat dan dat hetzij de afzender, hetzij de geadresseerde wettelijke stappen onderneemt tegen een ISP/ESP. Sommige ISP's/ESP's bieden het filteren daarom als alternatieve dienst aan de gebruikers aan en vragen hun eerst toestemming deze te activeren.

Ofschoon het buiten het bestek van deze mededeling valt om hierop in te gaan, kleven er nog andere aspecten aan het gebruik van filtertechnieken in de strijd tegen spam, zoals de afweging filteren versus de vrijheid van meningsuiting en filteren versus de contractuele verplichting van de ISP's/ESP's e-mail berichten door te leiden naar de klanten van hun abonnees.

---

[37] Zo is de werkgroep spambestrijding van RIPE (Réseaux IP Européens) sinds 1998 actief (zie het document "Good Practice for combating Unsolicited Bulk Email" op de website van RIPE (http://www.ripe.net)). In een minder ver verleden heeft de IRTF (Internet Research Task Force) een onderzoeksgroep spambestrijding opgericht (zie http://www.irtf.org/charters/asrg.html). Deze groep houdt zich bezig met de ontwikkeling van bepaalde technologieën die als vertrekpunt kunnen dienen voor een harmonisatie in het kader van de IETF (Internet Engineering Task Force).

Voor het filteren bij mobiele diensten zijn eventueel andere oplossingen gerechtvaardigd, gezien de afwijkende "business model"-omgeving bij mobiele diensten vergeleken met vaste internetdiensten. Bij het eerste soort diensten worden doorgaans afleveringskosten per bericht aangerekend, hetgeen spam duurder maakt. Bij sommige nieuwe diensten worden evenwel kosten in rekening gebracht voor het opvragen van berichten, hetgeen betekent dat door spam juist de ontvanger op kosten wordt gejaagd. Bovendien kan e-mail nu ook naar mobiele eindapparatuur worden gestuurd. In dit geval zouden de abonnees filter- en inzagevoorzieningen moeten kunnen krijgen om mobiele spam te controleren.

Ook dient aandacht te worden geschonken aan open relay servers. Dit zijn SMTP-servers die kunnen worden gebruikt voor het verzenden van berichten door andere gebruikers dan de lokale gebruikers van de server. In het verleden waren de meeste relay servers vrij toegankelijk. Open relay servers kunnen evenwel gemakkelijk door spammers worden gebruikt voor de verzending van ongevraagde berichten. Met eenvoudige preventieve maatregelen zouden de mogelijkheden voor dergelijk misbruik kunnen worden gereduceerd. Hetzelfde geldt voor open proxies, servers waarop software draait die rechtstreekse interactie met internet mogelijk maakt.

4.3.2. Voorgestelde maatregelen

De lidstaten en de bevoegde instanties wordt verzocht duidelijkheid te scheppen over de wettelijke voorwaarden, zoals ten aanzien van de privacy, waaronder in hun land de verschillende soorten filtersoftware kunnen functioneren.

Aanbieders van filtersoftware dienen te garanderen dat hun filtersystemen in overeenstemming zijn met de toestemmingsregeling en met andere EU-voorschriften, waaronder die in verband met de vertrouwelijkheid van het communicatieverkeer.

De gebruikers dienen de mogelijkheid te krijgen invloed uit te oefenen op de manier waarop binnenkomende spam wordt behandeld, afhankelijk van hun individuele behoeften. De aanbieders van filtersoftware moeten rekening houden met de gevolgen van "vals-positieven", "vals-negatieven" en bepaalde vormen van filtering van inhoud, alsmede met de mogelijkheid van eventuele daarmee samenhangende aansprakelijkheidsproblemen.

Filterbedrijven dienen met belanghebbende partijen samen te werken bij de ontwikkeling van technieken voor de herkenning van reclame e-mails die beantwoorden aan aanvaarde marketing-praktijken op basis van het Gemeenschapsrecht, met inbegrip van keurmerken, labels en dergelijke.

De aanbieders van e-maildiensten (en eventueel die van mobiele diensten) dienen op verzoek filtervoorzieningen of -diensten aan hun klanten aan te bieden, evenals informatie over filterdiensten en -producten voor eindgebruikers van derde partijen.

De eigenaars van mailservers dienen ervoor te zorgen dat hun servers afdoende beveiligd zijn zodat zij niet als open relay servers kunnen functioneren (voorzover dit niet gerechtvaardigd is). Hetzelfde geldt ook voor open proxies.

5. BEWUSTMAKINGSACTIVITEITEN

In dit hoofdstuk over bewustmakingsactiviteiten wordt ingegaan op voorgestelde maatregelen op gebieden zoals preventie, consumentenvoorlichting en rapportage.

5.1. Bespreking

De EU-lidstaten dienen de nieuwe toestemmingsregeling voor ongevraagde e-mail uiterlijk op 31 oktober 2003 in nationale wetgeving te hebben omgezet. Ofschoon in de pers vrij veel aandacht is geschonken aan deze nieuwe regeling, blijft het voor de marktspelers en de burgers toch enigszins onduidelijk wat deze toestemmingsregeling in de praktijk nu eigenlijk inhoudt[38].

De nieuwe benadering is erop gebaseerd de gebruiker assertief genoegen te maken om al dan niet toestemming te geven voor de ontvangst van commerciële communicatie. Daartoe dienen zij evenwel goed op de hoogte zijn van de basisvoorschriften ten aanzien van ongevraagde communicatie en te weten waar zij problemen kunnen melden.

Beste praktijken

De Britse "Information Commissioner" (de gegevensbeschermingsautoriteit van het VK) heeft enkele weken voor de inwerkingtreding van de nieuwe uitvoeringsbepalingen voor de richtlijn een gids over de nieuwe Britse voorschriften gepubliceerd, met daarin een apart gedeelte over marketing met elektronische middelen. De Information Commissioner heeft voorts aangekondigd klachtenformulieren online en via zijn kantoren beschikbaar te stellen zodra de nieuwe voorschriften in werking treden en daarbij aan te geven welke informatie waarschijnlijk noodzakelijk is[39].

Voorts moeten de gebruikers beseffen welke risico's zijn verbonden aan het verstrekken van persoonsgegevens via internet (bijvoorbeeld door deze op websites of nieuwsgroepen achter te laten en hun gedrag op grond daarvan aanpassen.

Tenslotte behoren zij te weten welke filtersoftware op de markt is en op welke servers en software providers (bijv. ISP's, ESP's) zij een beroep kunnen doen.

Beste praktijken

De "Commission National Informatique et Libertés" (CNIL), d.w.z. de Franse gegevensbeschermingsautoriteit, heeft een omvangrijk informatiepakket op haar website gezet met betrekking tot de diverse aspecten van spam: de resultaten van haar spambox-experiment en de zaken die voor de rechter zijn gebracht (zie onder), basisrichtsnoeren over hoe spam te voorkomen, informatie over hoe spam te melden, de contactgegevens van gebruikersverenigingen die op dit terrein actief zijn, enz.

Hoewel in de meeste lidstaten bewustmakingsactiviteiten met betrekking tot de nieuwe toestemmingsregeling zijn ontplooid of worden overwogen, verschillen deze sterk van elkaar in termen van tijdsplanning, aard van de verstrekte informatie, doelgroep en betrokken partijen. Sommige lidstaten wachten totdat hun wetgeving is goedgekeurd. Een openbare raadpleging over de tenuitvoerlegging van Richtlijn 2002/58/EG heeft tot een zekere bewustwording van de gebruikers geleid.

---

38 Achtergrondinformatie over de voorschriften voor ongevraagde communicatie in het kader van Richtlijn 2002/58/EG is te vinden op het volgende webadres: http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited.

39 Zie: http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_2002/58/EC.html#guidance

Diverse autoriteiten kunnen met deze activiteiten worden belast, afhankelijk van de bevoegdheden waarover zij in de betrokken lidstaat beschikken (bijvoorbeeld de gegevensbeschermingsautoriteiten, de nationale regelgevingsinstanties, de consumentenverenigingen of de ombudsman).

Er vindt nog niet in alle lidstaten coördinatie plaats tussen de verschillende bevoegde instanties. In sommige lidstaten is het tevens een taak van de ministeries. Ook de brancheverenigingen worden er dikwijls bij betrokken. En soms nemen ook de consumenten- of gebruikersverenigingen deel aan deze activiteiten.

Sommige sectoren van de industrie hebben eveneens bewustmakingsactiviteiten op nationaal, EU- of wereldwijd niveau ontplooid, al geldt ook nu weer dat deze activiteiten soms sterk uiteenlopen. Het gaat onder meer om:
- praktijkgidsen voor direct-marketingbedrijven of speciaal voor de communicatiesector bestemde campagnes;
- algemene instructies voor klanten inzake gedragscodes, klachtenregelingen en filtering;
- platforms/werkgroepen voor de ontwikkeling van beste reclamepraktijken.

5.2. Voorgestelde maatregelen

Om een gedegen inzicht te krijgen in wat wel en niet mag op het gebied van commerciële e-mail, dient op korte termijn in alle lidstaten breed opgezette duurzame actie te worden ondernomen, zowel op het gebied van preventie als op dat van handhaving. Er dient praktische informatie te worden verstrekt over preventie, aanvaardbare marktpraktijken, en technische en wettige oplossingen voor de gebruikers.

Alle partijen worden uitgenodigd om aan de bewustmakingsactiviteiten deel te nemen, van de lidstaten en de bevoegde instanties via het bedrijfsleven tot de consumenten-/gebruikersverenigingen. Lidstaten en bevoegde instanties die dit nog niet hebben gedaan, wordt verzocht begin 2004 alsnog voorlichtingscampagnes te starten of te ondersteunen.

Wat de aard van de verstrekte informatie betreft, dienen de op het bedrijfsleven en/of de consumenten gerichte activiteiten vooral betrekking te hebben op:

- het garanderen van een wijde verspreiding van basiskennis over de nieuwe voorschriften en de door deze voorschriften verleende rechten;

- praktische informatie over aanvaardbare marketingpraktijken in het kader van de toestemmingsregeling, met inbegrip van een uitleg over het rechtmatig verzamelen van persoonsgegevens;

Het Actieplan voor een veilige internet en spam

De Europese Commissie heeft in het kader van het Actieplan voor een veiliger internet (Safer Internet) een uitnodiging gepubliceerd in het kader waarvan projectvoorstellen kunnen worden ingediend op het gebied van spambestrijding op diverse fronten, zoals bewustmaking. Projecten die bij de eerste beoordelingsronde zijn geselecteerd zouden in mei 2004 van start kunnen gaan.

De Commissie werkt momenteel aan een voorstel voor een vervolgprogramma Safer Internet *plus*, waarmee nieuwe maatregelen in de strijd tegen illegale en schadelijke inhoud, evenals onwenselijke inhoud zoals spam kunnen worden gefinancierd.

http://europa.eu.int/information_society/programmes/iap/call/2002/index_en.htm

– praktische informatie voor consumenten over de wijze waarop zij spam kunnen voorkomen (bijv. over het gebruik van persoonsgegevens, enz.);

– praktische informatie voor consumenten over producten en diensten ter bestrijding van spam (bijv. filters, beveiliging);

– informatie over wat moet worden gedaan bij ontvangst van spam, zoals over klachtenregelingen en alternatieve geschillenregelingen, voorzover deze bestaan.

Deze activiteiten dienen op de volgende doelgroepen te zijn gericht:
a) bedrijven die betrokken zijn bij of gebruik maken van direct marketing,
b) consumenten die geabonneerd zijn op e-maildiensten, SMS-diensten inbegrepen, en
c) aanbieders van e-maildiensten, met inbegrip van de exploitanten van mobiele diensten.

Voor de bewustmakingsactiviteiten dient gebruikt worden gemaakt van verschillende kanalen (niet alleen internet) zodat de verschillende doelgroepen ook werkelijk worden bereikt. In dit verband is ook de rol van de industrie en de consumentenverenigingen van belang. En moet worden gezorgd voor coördinatie van de verschillende initiatieven.

De genoemde activiteiten dienen ook te zijn gericht op doeltreffende gedragscodes van de industrie, klachtenregelingen, labels (bijvoorbeeld keurmerken) en, voorzover beschikbaar, certificatiesystemen.

De diensten van de Commissie verschaffen al basisinformatie over de toestemmingsregeling via de EUROPA-website[40]. Met behulp van hyperlinks zullen zij ook doorverwijzen naar informatie over de nationale uitvoeringsaspecten en waar mogelijk ook naar basisgegevens en -trends op het gebied van spam. De diensten van de Commissie zullen voor de verspreiding van informatie over de nieuwe voorschriften tevens een beroep doen op de euro-infocentra.

CONCLUSIE

Spam is een van de grootste uitdagingen waar internet momenteel mee geconfronteerd wordt. De bestrijding van spam vereist actie op diverse fronten, niet alleen op het gebied van een doeltreffende handhaving en internationale samenwerking, maar ook op dat van zelfregulering, technische maatregelen van de industrie en voorlichting van de consument. De diverse maatregelen die in deze mededeling zijn genoemd, zijn in onderstaand overzicht samengevat.

Ofschoon de Commissie deze activiteiten zoveel mogelijk zal steunen, zijn het in de eerste plaats de EU-lidstaten en de bevoegde autoriteiten, de industrie, de consumenten en de gebruikers van internet en elektronische communicatiediensten die hierbij zowel op nationaal als op internationaal niveau een rol hebben te spelen.

Een geïntegreerde en parallelle tenuitvoerlegging van de in deze mededeling genoemde maatregelen, die brede steun genieten van alle betrokken partijen, kan een bijdrage leveren tot een aanzienlijke verlaging van de enorme hoeveelheid spam die momenteel de voordelen van e-mail en andere vormen van elektronische communicatie voor onze samenleving en onze economie weer in gevaar brengt.

40 http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm

De Commissie zal in de loop van 2004 toezicht gehouden op de tenuitvoerlegging van deze acties, onder meer via de informele internetgroep voor ongevraagde communicatie. Uiterlijk eind 2004 zal zij nagaan of aanvullende of corrigerende maatregelen noodzakelijk zijn.

OVERZICHT VAN DE IN DEZE MEDEDELING GENOEMDE MAATREGELEN

In onderstaande tabel staan de maatregelen die in deze mededeling zijn genoemd. De maatregelen van de Commissie/diensten van de Commissie zijn afzonderlijk vermeld. Zoals gezegd hangen de diverse activiteiten op verschillende manieren met elkaar samen en dienen zij daarom zoveel mogelijk parallel en op geïntegreerde wijze te worden uitgevoerd.

I - Doeltreffende tenuitvoerlegging en handhaving door de lidstaten en de bevoegde autoriteiten

Het is onmisbaar dat de lidstaten de Richtlijn betreffende privacy en elektronische communicatie, in het bijzonder de voorschriften ten aanzien van ongevraagde communicatie, zonder verdere vertraging in nationale wetgeving omzetten.

De lidstaten en bevoegde instanties dienen na te gaan of de handhavingsmechanismen doeltreffend zijn, in termen van rechtsmiddelen en sancties, klachtenregelingen, intra-Europese samenwerking en samenwerking met derde landen, en toezicht. De lidstaten dienen ook nationale strategieën te ontwikkelen om de samenwerking met de gegevensbeschermingsautoriteiten, consumentenbeschermingsautoriteiten en nationale regelgevingsinstanties te waarborgen en overlapping van bevoegdheden en dubbel werk te voorkomen.

Lidstaten en bevoegde instanties dienen in het bijzonder:

a) Doeltreffende rechtsmiddelen en sancties

- adequate mogelijkheden te creëren voor slachtoffers om schadeclaims te eisen en te voorzien in werkelijke straffen, zoals boetes en waar nodig ook strafrechtelijke sancties;

- in lidstaten zonder bestuurlijke procedures de mogelijkheid te overwegen alsnog in dergelijke procedures voor de handhaving van de nieuwe voorschriften te voorzien;

- de bevoegde instanties adequate onderzoeks- en handhavingsbevoegdheden te verlenen;

b) Klachtenregelingen

- adequate klachtenmechanismen in te voeren, zoals speciale mailboxen waar de gebruikers met hun klachten terecht kunnen;

- de activiteiten van de diverse bevoegde nationale instanties te coördineren;

c) Grensoverschrijdende klachten en EU-samenwerking bij de handhaving

- gebruik te maken van bestaande of zonodig nieuwe verbindingsmechanismen op basis waarvan de nationale autoriteiten kunnen samenwerken in hun streven naar grensoverschrijdende handhaving (informatie-uitwisseling, wederzijdse bijstand) in de EU. Wat frauduleuze en bedrieglijke spam betreft dient er in dit verband bij de Raad en het Parlement op aangedrongen te worden zo snel mogelijk overeenstemming te bereiken over het voorstel voor een verordening betreffende samenwerking met betrekking tot consumentenbescherming en te onderzoeken in hoeverre het mogelijk is om het toepassingsgebied van deze verordening uit te breiden tot dat van de Richtlijn betreffende privacy en elektronische communicatie;

d) Samenwerking met derde landen

- actief deel te nemen aan multilaterale fora (zoals de OESO) om in internationaal verband tot oplossingen te komen;

- de bilaterale samenwerking met derde landen te versterken of te initiëren;

- samen met de Commissie te onderzoeken welke specifieke initiatieven kunnen worden ontplooid om de internationale samenwerking te bevorderen;

- samen te werken met de particuliere sector bij het traceren van spammers met inachtneming van de nodige wettelijke garanties;

e) Toezicht

- ervoor te zorgen dat zij de beschikking krijgen over de informatie en statistische gegevens die nodig zijn om, zonodig in samenwerking met de industrie en rekening houdende met de lopende analysewerkzaamheden van de OESO, richting te geven aan hun handhavingsactiviteiten.

II – Zelfregulering en technische maatregelen van de industrie

De marktspelers (zoals de ISP's, ESP's, mobiele exploitanten, softwarebedrijven en direct-marketingbedrijven) dienen ernaar te streven de toestemmingsregeling in samenwerking met de consumenten-/gebruikersverenigingen en waar relevant ook de bevoegde instanties te vertalen naar de dagelijkse praktijk, en in het bijzonder:

a) Zelfregulering

- de contractuele praktijken van de service providers (ISP's, ESP's en mobiele exploitanten) ten opzichte van abonnees en zakenpartners te evalueren en zo nodig bij te sturen; als aanvullende dienst voor de klant informatie te verstrekken over filters en eventueel filtersoftware en/of –diensten aan te bieden;

- de direct-marketingpraktijken aan de toestemmingsregeling aan te passen en zo mogelijk overeenstemming te bereiken over specifieke, wettige methoden om persoonsgegevens te verzamelen (bijvoorbeeld op basis van dubbele of herhaalde toestemming);

- doeltreffende praktijkcodes te ontwikkelen en verspreiden (zoals het initiatief van de FEDMA) die aan de toestemmingsregeling beantwoorden, in samenwerking met de Groep gegevensbescherming artikel 29 of, waar relevant, de bevoegde nationale autoriteiten;

- overwegen labels te gaan gebruiken voor e-mails en databases die in overeenstemming met de toestemmingsregeling zijn, om de gebruikers (en de filters) te helpen deze te herkennen, conform de Richtlijn elektronische handel;

- doeltreffende zelfreguleringsmechanismen en alternatieve geschillenregelingen te gebruiken of te creëren, waarbij zo mogelijk moet worden voortgebouwd op bestaande initiatieven (zoals EEJ-NET);

b) Technische maatregelen

- (aanbieders van filtersoftware dienen) te garanderen dat hun filtersystemen in overeenstemming zijn met de toestemmingsregeling en met andere EU-voorschriften, waaronder die in verband met de vertrouwelijkheid van het communicatieverkeer. De lidstaten en de bevoegde instanties wordt verzocht duidelijkheid te scheppen in de wettelijke voorwaarden, zoals ten aanzien van de privacy, waaronder in hun land de verschillende soorten filtersoftware kunnen functioneren;

- (aanbieders van filtersoftware dienen) rekening te houden met de gevolgen van "vals-positieven", "vals-negatieven" en bepaalde vormen van filtering van inhoud, alsmede met de mogelijkheid van eventuele daarmee samenhangende aansprakelijkheidsproblemen. De gebruikers dienen de mogelijkheid te krijgen invloed uit te oefenen op de manier waarop binnenkomende spam wordt behandeld, afhankelijk van hun individuele behoeften;

- (aanbieders van filtersoftware dienen) met belanghebbende partijen samen te werken bij de ontwikkeling van technieken voor de herkenning van reclame e-mails die beantwoorden aan aanvaarde marketing-praktijken op basis van het Gemeenschapsrecht, zoals labels;

- (aanbieders van e-mail-diensten en eventueel die van mobiele diensten dienen) op verzoek filtervoorzieningen of -diensten aan hun klanten aan te bieden, evenals informatie over filterdiensten en -producten voor eindgebruikers van derde partijen;

- (eigenaars van mail-servers dienen) ervoor te zorgen dat hun servers afdoende beveiligd zijn zodat zij niet als open relay servers kunnen functioneren (voorzover dit niet gerechtvaardigd is). Hetzelfde geldt ook voor open proxies.

III – Bewustmakingsacties van de lidstaten, de industrie en de consumenten-/gebruikersverenigingen

Lidstaten en bevoegde instanties die dit nog niet hebben gedaan, wordt verzocht begin 2004 alsnog voorlichtingscampagnes te starten of te ondersteunen.

Alle partijen, van de lidstaten en de bevoegde instanties via het bedrijfsleven tot de consumenten-/gebruikersverenigingen, dienen deel te nemen aan voorlichtingscampagnes over de preventie van spam, aanvaardbare marktpraktijken, en technische en wettige oplossingen voor alle gebruikers, en in het bijzonder dienen zij:

- hun acties te richten op a) bedrijven die betrokken zijn bij of gebruik maken van direct marketing, b) consumenten die geabonneerd zijn op e-maildiensten, SMS-diensten inbegrepen, en c) aanbieders van e-maildiensten, met inbegrip van de exploitanten van mobiele diensten;

- ervoor te zorgen dat bedrijven en/of consumenten beschikken over:
- een ruim verspreide basiskennis over de nieuwe voorschriften en de door deze voorschriften verleende rechten,
- praktische informatie over aanvaardbare marketingpraktijken in het kader van de toestemmingsregeling, met inbegrip van een uitleg over het rechtmatig verzamelen van persoonsgegevens,
- praktische informatie voor consumenten over de wijze waarop zij spam kunnen voorkomen (bijvoorbeeld over het gebruik van persoonsgegevens, enz.),
- praktische informatie voor consumenten over producten en diensten ter bestrijding van spam (bijv. filters, beveiliging),
- informatie over wat moet worden gedaan bij ontvangst van spam, zoals over klachtenregelingen en alternatieve geschillenregelingen, voorzover deze bestaan;

- te verwijzen naar doeltreffende gedragscodes van de industrie, klachtenregelingen, labels (bijv. keurmerken) en, voorzover beschikbaar, certificatiesystemen;

- deze bewustmakingsactiviteiten via verschillende kanalen (niet alleen internet) te laten plaatsvinden zodat de verschillende doelgroepen daadwerkelijk worden bereikt.

In dit verband is ook de rol van de industrie en de consumentenverenigingen van belang. Er moet worden gezorgd voor coördinatie van de verschillende initiatieven.

IV – Activiteiten van de Commissie/diensten van de Commissie

De Commissie zal in de loop van 2004 toezicht houden op de uitvoering van deze maatregelen, onder meer via de informele internetgroep voor ongevraagde communicatie, en zal uiterlijk eind 2004 beoordelen of aanvullende of corrigerende maatregelen noodzakelijk zijn.

De Commissie zal toezicht blijven houden op de tenuitvoerlegging van de richtlijn. In het bijzonder zal zij zich ervan vergewissen dat de nationale omzettingsmaatregelen in werkelijke sancties voorzien, zonodig onder meer in de vorm van boetes en strafrechtelijke sancties, voor het geval de betrokken eisen niet door de marktspelers worden nageleefd. (De Commissie heeft in november 2003 inbreukprocedures ingeleid tegen een aantal lidstaten die geen omzettingsmaatregelen hadden doorgegeven.) De diensten van de Commissie zijn bereid de lidstaten daarbij zonodig te helpen.

De diensten van de Commissie hebben met steun van de lidstaten en de gegevensbeschermingsautoriteiten een informele internetgroep voor ongevraagde commerciële communicatie opgericht. Deze groep zal de activiteiten die op een doeltreffende handhaving zijn gericht (zoals klachten, rechtsmiddelen, sancties, internationale samenwerking) en de overige in deze mededeling genoemde activiteiten bevorderen.

De diensten van de Commissie zullen we de Groep gegevensbescherming artikel 29 verzoeken zo snel mogelijk advies uit te brengen over een aantal concepten dat in de Richtlijn betreffende privacy en elektronische communicatie wordt gebruikt teneinde bij te dragen tot een uniforme toepassing van de nationale maatregelen die het kader van de richtlijn zijn genomen.

De diensten van de Commissie zijn samen met de lidstaten en de bij de handhaving betrokken nationale autoriteiten een onderzoek gestart naar de manier waarop de internationale samenwerking, met name bij de

behandeling van grensoverschrijdende klachten, kan worden geoptimaliseerd. Deze contacten met de nationale autoriteiten zullen in de rest van 2004 worden voortgezet.
De Commissie zal zich inzetten voor de totstandkoming van pan-Europese online gedragscodes voor direct marketing en voorzover toepasselijk de Groep gegevensbescherming artikel 29 verzoeken deze goed te keuren.
De diensten van de Commissie zullen in februari 2004 gastheer zijn voor een OESO-workshop en zullen de vervolgactiviteiten met de lidstaten te bespreken, onder meer de werkzaamheden van de OESO die erop gericht zijn de vaststelling van doeltreffende wetgeving, bewustmaking, ontwikkeling van technische oplossingen, zelfregulering en internationale samenwerking op het gebied van handhaving internationaal te bevorderen. De Commissie zal tevens nagaan hoe een zo goed mogelijk vervolg kan worden gegeven aan de resultaten van de Wereldtop van 2003 in de EU, rekening houdende met de wereldtop van Tunis, die in 2005 zal plaatsvinden. De Commissie heeft in het kader van het Actieplan voor een veiliger internet een uitnodiging gepubliceerd in het kader waarvan projectvoorstellen konden worden ingediend op het gebied van spambestrijding op diverse fronten. De Commissie werkt momenteel aan een voorstel voor een vervolgprogramma Safer Internet *plus*, waarmee nieuwe maatregelen in de strijd tegen onder meer spam kunnen worden gefinancierd. De diensten van de Commissie blijven basisinformatie verstrekken over de toestemmingsregeling via de EUROPA-website. Met behulp van hyperlinks zullen zij ook doorverwijzen naar informatie over de nationale uitvoeringsaspecten en waar mogelijk ook naar basisgegevens en -trends op het gebied van spam. De diensten van de Commissie zullen voor de verspreiding van informatie over de nieuwe voorschriften tevens een beroep doen op de euro-infocentra.