KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 22.01.2004
KOM(2004) 28 endgültig

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

über unerbetene Werbenachrichten (Spam)

INHALTSVERZEICHNIS

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

über unerbetene Werbenachrichten (Spam)

(Text von Bedeutung für den EWR)

ZUSAMMENFASSUNG

Unerwünschte Werbung über elektronische Post, auch als „Spam“ bezeichnet, hat besorgniserregende Ausmaße angenommen. Schätzungen zufolge bestehen über 50 % des weltweiten E-Mail-Aufkommens nun aus Spam. Noch beunruhigender ist die Wachstumsrate: 2001 waren es „lediglich“ 7 %.

Spam ist aus zahlreichen Gründen problematisch: Bedrohung der Privatsphäre, Enttäuschung der Verbraucher, Gefährdung Minderjähriger und der Menschenwürde, Zusatzkosten für Unternehmen, Produktivitätsverlust. Generell untergräbt diese Praxis das Verbrauchervertrauen, das Voraussetzung für den Erfolg des elektronischen Handels, elektronischer Dienste und nicht zuletzt der Informationsgesellschaft ist.

Die EU erkannte diese Gefahr und erließ im Juli 2002 die Richtlinie 2002/58/EG über den Datenschutz in der elektronischen Kommunikation, mit der EU-weit der Grundsatz der zustimmungsbedürftigen Werbung über elektronische Post einschließlich SMS- oder MMS-Nachrichten (Opt-in-Regelung) eingeführt und Verbraucherschutzmaßnahmen verstärkt wurden. Die Datenschutzrichtlinie sollte bis zum 31. Oktober 2003 umgesetzt sein. Gegen mehrere Mitgliedstaaten, die der Kommission keine Umsetzungsmaßnahmen notifiziert hatten, wurden Verstoßverfahren eingeleitet.

Der Erlass von Rechtsvorschriften ist ein erster, notwendiger Schritt, aber nur teilweise eine Antwort. In dieser Mitteilung werden verschiedene Maßnahmen aufgezeigt, die notwendig sind, um die EU-Vorschriften abzurunden und das Spamverbot in die Praxis umzusetzen.

Es gibt jedoch kein Patentrezept gegen Spam. Die hier aufgezeigten Maßnahmen sind vor allem auf die effiziente Umsetzung durch Mitgliedstaaten und staatliche Behörden, technische Lösungen und Selbstregulierung der Industrie und Verbraucheraufklärung ausgerichtet. Auch die internationale Dimension wird berücksichtigt, da Spam großenteils aus Drittländern stammt.

Diese Maßnahmen entsprechen weitgehend dem Konsens, der sich im Laufe des Jahres 2003 herauskristallisierte und auf einem öffentlichen Workshop im Oktober 2003 bestätigt wurde, doch muss auch Einigkeit über ihre Durchführung herrschen. Nur wenn alle, von den Mitgliedstaaten über staatliche Behörden und Unternehmen bis hin zu Verbrauchern und Nutzern des Internet und der elektronischen Kommunikation, ihre Aufgabe dabei wahrnehmen, lässt sich die Ausbreitung des Spam eindämmen.

Einige dieser Maßnahmen sind mit spürbaren Kosten verbunden. Dies muss jedoch in Kauf genommen werden, wenn E-Mail und elektronische Dienste als effiziente Kommunikationswerkzeuge fortbestehen sollen. Die Durchführung der hier dargelegten

Maßnahmen wird wesentlich zur Eindämmung des Spam-Phänomens beitragen und somit der Informationsgesellschaft, unseren Bürgern und Wirtschaftssystemen zugute kommen.

Hintergrund und Ziel

Unerbetene Werbung über elektronische Post[1], auch als „Spam" bezeichnet, wird weithin als eines der größten Probleme im heutigen Internet anerkannt. Spam hat besorgniserregende Ausmaße erreicht. Derzeit besteht die Gefahr, dass E-Mail- oder SMS-Nutzer diese beliebte Internet-Anwendung bzw. ihren Mobilfunkdienst einfach aufgeben oder nicht in dem Umfang nutzen, wie sie es sonst tun würden. Da das Internet und andere elektronische Kommunikationsdienste (wie Breitbandzugang, Drahtloszugang, Mobilkommunikation) voraussichtlich ein wesentlicher Faktor des Produktivitätswachstums in modernen Wirtschaftssystemen sein werden, ist dem Spam noch mehr Aufmerksamkeit zu widmen.

Es besteht zwar Einigkeit darin, dass etwas geschehen muss, ehe die Vorteile, die Unternehmen und Bürgern aus E-Mail und anderen elektronischen Diensten erwachsen, durch die Ausbreitung des Spam zunichte gemacht werden, doch ist keineswegs klar ersichtlich, wie sich dieses Phänomen am besten bekämpfen lässt. Es gibt keine Patentlösung in diesem Kampf. Nur wenn alle, von den Mitgliedstaaten über die zuständigen Behörden und Unternehmen bis hin zu Verbrauchern und Nutzern des Internet und der elektronischen Kommunikation, ihre Aufgabe dabei wahrnehmen, gibt es eine Möglichkeit, Spam wirksam zu bekämpfen.

Ausgehend von der Richtlinie 2002/58/EG[2], mit der ein (zustimmungsbedürftiges) „Opt-in" System für Werbenachrichten eingeführt wurde, das die Mitgliedstaaten bis zum 31. Oktober 2003 umsetzen mussten, werden in dieser Mitteilung verschiedene rechtliche, technische und Aufklärungsmaßnahmen aufgezeigt.

Im Mittelpunkt dieses Maßnahmenkatalogs stehen die Umsetzung und Durchsetzung der Richtlinie durch die Mitgliedstaaten, technische Maßnahmen, Selbstregulierung der Industrie, Verbraucheraufklärung und internationale Zusammenarbeit. Der internationalen Dimension kommt maßgebende Bedeutung zu, da Spam großenteils aus Drittländern stammt, insbesondere aus Nordamerika[3].

Diese Maßnahmen entsprechen weitgehend dem Konsens, der sich im Laufe des Jahres 2003 herauskristallisierte und auf einem öffentlichen Workshop im Oktober 2003 bestätigt wurde[4]. Einigkeit ist umso wichtiger, als die betreffenden Stellen, soweit möglich mit Unterstützung

---

1 Die vorliegende Mitteilung bezieht sich nicht auf unerwünschte Offline-Werbung, z.B. auf dem normalen Postweg.

2 Vgl. insbesondere Artikel 13 der Richtlinie 2002/58/EG über den Datenschutz in der elektronischen Kommunikation (s. Abschnitt 2).

3 Die 2002 von der französischen "Commission Nationale Informatique et Libertés (CNIL)" und der belgischen "Commission de la Protection de la Vie Privée (CPVP)" eingeleiteten "Spambox-Initiativen" scheinen zu bestätigen, dass Spam-Nachrichten überwiegend aus den Vereinigten Staaten, und in geringerem Umfang aus Kanada stammen. Die Ergebnisse der CPVP sind unter http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf abrufbar. Der CNIL-Bericht kann eingesehen werden unter http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf. S. auch: UNCTAD, E-Commerce and Development Report 2003, New York und Genf, 2003, S. 27.

4 Ein Papier über unerbetene Werbung (Spam) wurde vor dem Workshop verteilt. Es knüpfte an vorangehende Diskussionen im Rahmen des Kommunikationsausschusses (COCOM) und der Datenschutzgruppe nach Artikel 29 an. Die Mitglieder des COCOM und der Datenschutzgruppe beantworteten einen Fragebogen. Auch verschiedene Industrieverbände und Einzelunternehmen reagierten, darunter Internet-Anbieter, (Mobil- und Fest-) Kommunikationsbetreiber, Direktmarketing- und Werbeagenturen, Computer- und Softwarehersteller.

durch die Kommission, die aufgezeigten Maßnahmen zugunsten der Informationsgesellschaft, der Industrie und der Nutzer durchführen müssen.

Aufbau des Papiers

Es werden spezielle Aspekte des Spam-Phänomens angesprochen und zu jedem Aspekt spezifische Maßnahmen vorgeschlagen. Auch empfehlenswerte Verfahren werden aufgezeigt, wo sich dies anbietet.

Vorgeschlagenen werden folgende Maßnahmen:

– **Umsetzungs- und Durchsetzungsmaßnahmen**, insbesondere für Regierungen und Behörden, z.B. Abhilfen und Sanktionen, Rechtsschutzmechanismen, grenzüberschreitende Beschwerden, Zusammenarbeit mit Drittländern, Überwachung (Abschnitt 3).

– **Selbstregulierung und technische Maßnahmen,** insbesondere für Marktteilnehmer, z.B. vertragliche Vereinbarungen, Verhaltenskodizes, zulässige Marketing-Praktiken, Kennzeichnungen, alternative Streitbeilegungsverfahren, technische Lösungen wie Filter- und Sicherheitsfunktionen (Abschnitt 4).

– **Aufklärungsmaßnahmen** für Regierungen und Behörden, Marktteilnehmer, Verbraucherverbände u.a. Dazu gehören z.B. Vorbeugungs-, Verbrauchererziehungs- und Berichterstattungsverfahren.

Diese Maßnahmen sind am Ende der Mitteilung zusammengefasst. Sie sind auf verschiedene Weise miteinander verknüpft. Nach Möglichkeit sollten sie parallel und integriert durchgeführt werden.

Zunächst wird in den folgenden Abschnitten das Spamming-Phänomen untersucht (Abschnitt 1) und ein Überblick über die seit dem 31. Oktober 2003 geltenden Vorschriften vermittelt (Abschnitt 2).

1. DIE PROBLEMATIK

Was ist Spam?

Der Begriff „Spam“ wird häufiger gebraucht als definiert. Er bezeichnet, kurz gesagt, unerbetene E-Mails, häufig in Form von Massenpost. In der neuen Richtlinie wird dieser Begriff weder definiert noch verwendet. Sie spricht von „unerbetenen Nachrichten“ über „elektronische Post“ „für Zwecke der Direktwerbung“, womit praktisch die meisten Arten von „Spam“ erfasst sind. Daher wird in dieser Mitteilung kurz der Begriff „Spam“ für unerbetene Werbung über elektronische Post verwendet.

Man beachte, dass der Begriff „elektronische Post“ eigentlich nicht nur herkömmliche E-Mails bezeichnet, sondern auch SMS, MMS und jegliche Form elektronischer Kommunikation, bei der die gleichzeitige Teilnahme von Sender und Empfänger nicht erforderlich ist (s. Abschnitt 2).

1.1. Tragweite des Problems

Unerbetene Werbung über elektronische Post oder Spam hat ein beängstigendes Ausmaß angenommen. Trotz statistischer Abweichungen bestehen Schätzungen zufolge über 50 % des gesamten E-Mail-Aufkommens aus Spam.

Noch beunruhigender ist die Wachstumsrate. 2001 wurde das Spam-Aufkommen auf „lediglich“ 7 % des gesamten E-Mail-Verkehrs geschätzt, 2002 auf 29 %, und die Prognosen für 2003 lauten auf 51 %.

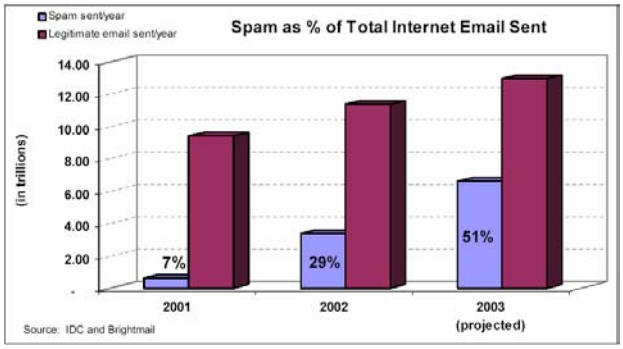

Abb. 1: Anteil des Spam am gesamten E-Mail-Verkehr

Es kann erhebliche Abweichungen zwischen Nutzerkategorien und Weltregionen geben. (Bei der Europäischen Kommission beispielsweise sind ca. 30 % der von außen eingehenden E-Mail Spam.) Generell sind jedoch die jüngsten EU-Zahlen nicht weniger besorgniserregend als die weltweiten Statistiken[5].

Spam über Mobilfunknetze, z.B. in Form von Textnachrichten als SMS (Short Messaging Service), scheinen derzeit weniger problematisch zu sein; Entwicklungen wie E-Mail per Mobilfunk dürften jedoch das Spam-Volumen noch erhöhen. Diese Annahme wird durch Erfahrungen in Ländern mit weit verbreiteter I-Mode-Kommunikation (z.B. Japan) bestätigt.

1.2. Warum ist Spam ein Problem?

Aus der Sicht des Einzelnen stellt Spam ein Eindringen in die Privatsphäre dar. Diese Befürchtung liegt den neuen Vorschriften über unerbetene E-Mail zugrunde, die im folgenden Abschnitt beschrieben werden. Ferner enthält Spam häufig irreführende oder betrügerische Angaben. Ein erheblicher Spam-Anteil scheint von dem Wunsch bestimmt, die Verbraucher auf diese Weise „auszunehmen“[6]. Leider reagieren nur allzu viele Verbraucher auf

Fühlt sich der Bürger betroffen?

Die Zahl der Beschwerden ist ein Anzeichen für die Befürchtungen der Nutzer. Innerhalb von 3 Monaten gingen bei der französischen Spambox 325.000 Zuschriften ein. Ein ähnlicher Versuch in Belgien ergab 50.000 Beschwerden in 2,5 Monaten. Anfang 2003 verzeichnete die permanente Spambox der FTC, die sog. UCE-Datenbank, täglich 130 000 Nachrichten.

5 Im September 2003 betrug der Spam-Anteil in der EU etwa 49 %, gegenüber 54 % weltweit im gleichen Zeitraum (Quelle : Brightmail, 2003).

6 Einem kürzlichen Bericht der FTC zufolge enthalten 22 % der geprüften Spams falsche Angaben in der Betreffzeile; 42 % enthielten irreführende Betreffzeilen, die fälschlich behaupteten, der Absender unterhalte eine geschäftliche oder persönliche Beziehung zum Empfänger; 44 % enthielten falsche Angaben in der Absender- oder Betreffzeile; über die Hälfte der Finanzwerbungen enthielten falsche Absender- oder Betreffzeilen; bei 40 % der Spams gab es Anzeichen für Fälschung in der Nachricht; 90 % der Investitions- und Geschäftsangebote enthielten vermutlich falsche Behauptungen; 66 % enthielten falsche Angaben in der Absender-, der Betreffzeile oder dem Text der Nachricht. (Quelle: “False Claims in Spam, A report by the FTC’s Division of Marketing Practices”, 30. April 2003, s. http://www.ftc.gov/reports/spam/030429spamreport.pdf)

diese irreführende oder betrügerische Werbung[7]. Auch pornografische Nachrichten können ebenfalls sehr belästigend sein[8] Das Löschen von Spam-Nachrichten aus der Mailbox ist für den Nutzer zeitraubend und kostspielig, wenn Filter- und anderweitige Software benötigt wird.

Spam hat ein Ausmaß erreicht, das Unternehmen auch beträchtliche Kosten verursacht. Direkte Kosten entstehen dadurch, dass die Angestellten ihre Briefkästen aufräumen müssen, was die Effizienz und Produktivität am Arbeitsplatz beeinträchtigt. Die IT-Abteilungen investieren Zeit und Geld in die Lösung des Problems. Internet-Diensteanbieter und E-Mail-Betreiber müssen mehr Bandbreite und Speicherkapazität für unerwünschte E-Mails erwerben. Darüber hinaus besteht die Gefahr, dass Spam ein Problem für den Empfänger darstellt (z.B. durch dubiose Inhalte auf den PCs der Angestellten) oder nach sich zieht (z.B. durch falsche schwarze Listen, Rufschädigung).Indirekte Kosten werden dadurch verursacht, dass einige legitime geschäftliche Nachrichten bedingt durch derzeitige Filtertechniken (sog. „falsche Positive“) nicht zugestellt oder einfach nicht mehr gelesen werden, weil man sie mit Spam in Verbindung bringt. Spam wird zunehmend als Träger zur Verbreitung von Viren genutzt, was sich für Unternehmen als sehr kostspielig erweisen kann.

Die Kosten des Spam-Phänomens zu ermessen ist ein schwieriges Unterfangen, insbesondere für Einzelne, nicht zuletzt weil das angerichtete Unheil nur schwer in Geldwert auszudrücken ist. Schätzungen sind jedoch besorgniserregend. Nach Angaben von Ferris Research verursachte Spam europäischen Unternehmen allein durch Produktivitätsverlust Kosten in Höhe von 2,5 Mrd. €[9]. Und das Phänomen hat, wie bereits erwähnt, seit 2002 erheblich an Umfang zugenommen. Der Software-Anbieter MessageLabs Ltd. schätzte im Juni 2003 die Spam-Kosten für britische Unternehmen auf ca. 3,2 Mrd. £[10]. Je nach Branche kann Spam unterschiedliche Auswirkungen haben. Das Rechtswesen beispielsweise kann angesichts der vertraulichen und sensiblen Informationen, mit denen es umgeht, besonders empfindlich betroffen sein.

Eine der bedenklichsten Folgen des Spam ist, dass das Verbrauchervertrauen untergraben wird, das Voraussetzung für den Erfolg des elektronischen Handels und der Informationsgesellschaft insgesamt ist. Der Eindruck, dass ein Einzelhandelsträger von Gaunern beherrscht wird, kann weitreichende Folgen für den Ruf redlicher Geschäftsleute derselben Branche haben. Neuere Zahlen der USA, die über umfangreichere Erfahrungen mit

---

7 Pew Internet zufolge berichteten 7 % der Nutzer, auf unerbetene E-Mail hin eine Bestellung aufgegeben zu haben; 33 % klickten ein Link in einem Spam an, um weitere Informationen zu erhalten. Selbst wenn der Prozentsatz der geschröpften Verbraucher relativ niedrig ist, hat das Problem angesichts der phänomenalen Skaleneffekte, die sich mit irreführenden oder betrügerischen Spams erzielen lassen, eine neue Dimension erreicht. Vgl. „Spam–How It Is Hurting Email and Degrading Life on the Internet“, Oktober 2003’, ein Bericht von Deborah Fallows im Auftrag von Pew Internet & American Life Project. Dieser Bericht ist abrufbar unter http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. Ein Versender von Massenpost bezeugte kürzlich auf dam Spam-Forum der FTC vom April-Mai 2003, er könne Gewinne erzielen, selbst wenn die Antwortrate unter 0,0001 % liege. (Anmerkungen von Timothy J. Muris, Vorsitzender, auf dem Aspen-Gipfel der Federal Trade Commission über „Cyberspace and the American Dream, The Progress and Freedom Foundation“, 19. August 2003 Aspen, Colorado).

8 Spam-Nachrichten beinhalten zuweilen sinnlose Gewalt oder hetzen zum Hass aufgrund der Rasse, des Geschlechts, der Religion oder der Staatsangehörigkeit auf.

9 Quelle: Ferris Research, 2003.

10 Diese Zahlen und andere Schätzungen sind dem Bericht „“Spam”; Report of an Inquiry by the All Party Internet Group“, London, Oktober 2003, S.8, zu entnehmen. Der Bericht ist über die URL http://www.apig.org.uk abrufbar.

Spam verfügen als die EU, bestätigen, dass das Vertrauen in elektronische Post angesichts der zahlreichen Spams gesunken ist[11].

Internet und andere elektronische Kommunikationsdienste (wie Breitbandzugang, Drahtloszugang) werden voraussichtlich eine wesentliche Rolle beim Produktivitätswachstum in modernen Wirtschaftssystemen spielen. Einige attraktive Merkmale dieser Dienste – „permanenter Anschluss", Drahtloszugang – können jedoch die Zahl der eingehenden oder weitergeleiteten Spam-Nachrichten wesentlich erhöhen, wenn keine geeigneten Sicherheitsmaßnahmen getroffen werden. Paradoxerweise könnte daher die Ausbreitung dieser Dienste zu einer Zunahme des Spam-Phänomens führen, wenn nicht umgehend effiziente Maßnahmen getroffen werden.

2. KURZÜBERSICHT ÜBER DIE REGELUNGEN FÜR UNERBETENE WERBENACHRICHTEN

2.1. Opt-in-System

Aufgrund der Richtlinie 2002/58/EG über Datenschutz in der elektronischen Kommunikation[12] (Umsetzungstermin: 31. Oktober 2003) müssen die Mitgliedstaaten unerwünschte Werbung per E-Mail oder über andere elektronische Nachrichtensysteme wie SMS (Short Messaging Service) und MMS (Multimedia Messaging Service) untersagen, sofern nicht der Teilnehmer zuvor seine Zustimmung erteilt hat (Artikel 13 Absatz 1). Diese Opt-in-Regelung galt bislang nur für Faxgeräte und automatische Anrufsysteme[13].

Das neue System umfasst drei Grundregeln:

Regel Nr. 1: Elektronische Werbung bedarf der vorherigen Zustimmung des Teilnehmers. Ausgenommen hiervon sind lediglich E-Mails (oder SMS) über vergleichbare Produkte oder Dienste ein und derselben Person an ihre Kunden. Dieses Verfahren gilt für natürliche Personen, die Mitgliedstaaten können es jedoch auf Rechtspersonen ausdehnen.

Regel Nr. 2: Die Identität des Absenders der Nachricht darf nicht verschleiert oder verborgen werden.

Regel Nr. 3: Alle elektronischen Nachrichten müssen eine gültige Rückadresse enthalten, bei der sich der Teilnehmer abmelden kann.

Allerdings sind nicht alle unerbetenen elektronischen Nachrichten verboten. Eine Ausnahme besteht, wenn Kontaktadressen für E-Mail oder SMS bei einem Kauf angegeben wurden. Dieser Vorgang wird auch als „Soft Opt-in" bezeichnet. Im Rahmen einer solchen Kundenbeziehung kann das Unternehmen die von seinen Kunden angegebenen Daten zur Werbung für Produkte oder Dienste verwenden, die mit den bereits verkauften vergleichbar sind. Diese Ausnahme wurde gemeinschaftsweit harmonisiert, und den Mitgliedstaaten bleibt keine andere Wahl, als sie umzusetzen. Sie ist jedoch klar abzugrenzen, um zu vermeiden, dass das Opt-in-System in der Praxis unterlaufen wird. Dennoch muss das Unternehmen auch dann bereits bei der Erfassung der Daten klarstellen, dass diese für Direktwerbung verwendet (und gegebenenfalls zu diesem Zweck an Dritte weitergegeben) werden können, und dem

---

[11] Einer kürzlichen Umfrage von Pew Internet zufolge nutzen 25 % der Befragten E-Mail weniger, weil sie sehr viel Spam erhalten.

[12] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12 .Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002

[13] Bei Werbeanrufen über das normale Sprachtelefon können die Mitgliedstaaten zwischen einem Opt-in- und einem Opt-out-Verfahren wählen.

Kunden die Möglichkeit einräumen, dies „gebührenfrei und problemlos abzulehnen“. Auch muss es jede anschließende Werbenachricht dem Kunden gestatten, weitere Nachrichten kostenlos und ohne Schwierigkeiten abzuweisen.

Das Opt-in-System ist für alle E-Mails und SMS Vorschrift, die als Direktwerbung an Einzelne (natürliche Personen) gerichtet werden. Die Mitgliedstaaten können das System auf Mitteilungen an Unternehmen (Rechtspersonen) ausdehnen. Wenn sie sich für ein Opt-out-System für Werbung von Unternehmen zu Unternehmen entschieden haben, können sie dies beibehalten. Ein differenziertes System für einen E-Mail-Dienst je nach Teilnehmergruppe kann Schwierigkeiten für den Absender mit sich bringen, wenn es gilt, juristische von natürlichen Personen zu unterscheiden.

Nachrichten zum Zweck der Direktwerbung, die die Identität des Absenders verheimlichen oder verschleiern, sind jedoch grundsätzlich (bei allen Empfängerkategorien) verboten. Ferner müssen Werbenachrichten eine gültige Adresse angeben, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann[14].

Die „Datenschutzgruppe nach Artikel 29“, die die Kommission berät und in der die Datenschutzbehörden der EU vertreten sind, prüft einige dieser Konzepte näher, um zu einer einheitlichen Anwendung der einzelstaatlichen Maßnahmen aufgrund der Richtlinie 2002/58/EG beizutragen[15]. Durch Einigkeit in diesen Fragen lassen sich abweichende Auslegungen vermeiden, die das Funktionieren des Binnenmarktes beeinträchtigen würden. Weitere Aspekte unerbetener Mitteilungen[16] wurden in früheren Papieren der Arbeitsgruppe behandelt.

2.2. Durchsetzungsbestimmungen

Die Bestimmungen der „allgemeinen“ Datenschutzrichtlinie über Rechtsbehelfe, Haftung und Sanktionen gelten auch für die Vorschriften der Datenschutzrichtlinie für elektronische

---

14 Artikel 13 Absatz 4 der Richtlinie 2002/58/EWG.

15 Gemäß Artikel 14 Absatz 3 der Richtlinie 2002/58/EG in Verbindung mit Artikel 30 der Richtlinie 95/46/EG.

16 Vgl. Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000. Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union; Arbeitspapier vom 21. November 2000 mit dem Titel „Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz“. Diese Unterlagen können eingesehen werden unter:
http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm

Kommunikation[17], einschließlich der Vorschriften über unerwünschte Nachrichten.

Kurz, die Mitgliedstaaten müssen dafür sorgen, dass bei Verstößen Sanktionen und Abhilfen zur Verfügung stehen. Jede Person muss bei der Verletzung der Rechte, die sie aufgrund der einzelstaatlichen Vorschriften genießt, Rechtsbehelf einlegen können. Dies gilt unbeschadet etwaiger (vorheriger) Verwaltungsverfahren, allerdings sind letztere nicht gemeinschaftsweit vorgeschrieben. Der Einzelne muss Anspruch auf Schadenersatz für jeglichen Nachteil haben, der ihm aus einer unrechtmäßigen Verarbeitung oder Handlung entsteht. Bei Verstößen sind solche Sanktionen zu verhängen, die die uneingeschränkte Umsetzung der Richtlinie gewährleisten.

Somit lässt die Richtlinie den Mitgliedstaaten die Wahl der Maßnahmen zur Umsetzung der Richtlinie – auch der Abhilfen und Sanktionen -, sofern die uneingeschränkte Umsetzung der Bestimmungen über unerbetene Werbenachrichten gewährleistet ist.

Für die Durchsetzung der Vorschriften sind wie bei allen Richtlinien zunächst die Mitgliedstaaten zuständig, nicht die Kommission. Zum Beispiel ist es nicht Aufgabe der Kommission, diejenigen, die gegen die in der Richtlinie vorgesehenen Rechte und Pflichten verstoßen, strafrechtlich zu verfolgen oder mit Geldbußen zu belegen[18].

2.3. Sonstige Bestimmungen gegen Spam

Eine häufig mit Spam einhergehende Praxis ist das „Ernten“ von E-Mail- Adressen, d.h. das automatische Einsammeln persönlicher Daten von öffentlichen Internetanwendungen wie E-Mail, Web, Chaträumen u.a. Dies ist gemäß der „allgemeinen“ Datenschutzrichtlinie 95/46/EG rechtswidrig, gleichgültig, ob das Einsammeln über eine Software automatisch erfolgt oder nicht[19].

Betrügerische Spam-Nachrichten können ein besonderes Ärgernis sein. Diese Praktiken sind bereits nach den derzeitigen EU-Vorschriften über irreführende Werbung und unlautere

---

[17] Artikel 15 der Richtlinie 2002/58/EG verweist auf Kapitel III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen:
Artikel 22 – Rechtsbehelf
Unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens, das vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 28 genannten Kontrollstelle eingeleitet werden kann, sehen die Mitgliedstaaten vor, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann.
Artikel 23 – Haftung
1) Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadenersatz zu verlangen.
2) Der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.
Artikel 24 – Sanktionen
Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen, und legen insbesondere die Sanktionen fest, die bei Verstößen gegen die zur Umsetzung dieser Richtlinie erlassenen Vorschriften anzuwenden sind.

[18] Damit unterscheidet sie sich von Behörden wie der amerikanischen Federal Trade Commission (FTC).

[19] Vgl. Arbeitspapier der Datenschutzgruppe nach Artikel: „Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz“ (WP 37 vom 21. November 2000).

Geschäftspraktiken verboten (Richtlinie 84/450/EWG über irreführende Werbung)[20]. Auch die einzelstaatlichen Gesetze werden für schwerere Fälle in der Regel strengere Strafen einschließlich strafrechtlicher Sanktionen vorsehen.

Noch lästiger können bestimmte Arten von Spam sein, die z.B. Pornographie oder sinnlose Gewalt beinhalten, vor allem, wenn Kinder betroffen sind[21]. Der Inhalt solcher Nachrichten kann zwar jugendgefährdend, muss aber als solcher nicht rechtswidrig sein; die wahllose Verbreitung unter Erwachsenen und Kindern gleichermaßen ist jedoch nach einzelstaatlichem Recht illegal und zieht zuweilen schwere Strafen nach sich. Spam-Nachrichten können auch illegale Inhalte umfassen und z.B. zum Hass aufgrund der Rasse, des Geschlechts, der Religion oder der Staatsangehörigkeit aufhetzen. Sobald solche Nachrichten einen Direktwerbungszweck verfolgen – was häufig der Fall ist – unterliegen sie wie andere Arten unerbetener E-Mail dem Spamverbot.

Ferner sei auf die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, verwiesen, wonach kommerzielle Nachrichten klar als solche zu erkennen sein müssen (Artikel 6 Buchstabe a))[22].

Hacking und Identitätsdiebstahl dienen häufig dazu, Spam zu versenden oder Zugang zu Adressdatenbanken oder Computern zu erhalten. Viele derartige Aktivitäten fallen unter den Rahmenbeschluss des Rates über Angriffe auf Informationssysteme, der strafrechtliche Sanktionen vorsieht. Dieser Rahmenbeschluss basiert auf einem Vorschlag der Kommission, erhielt im Februar 2003 die politische Zustimmung und dürfte in Kürze offiziell verabschiedet werden[23]. Viele Mitgliedstaaten können bereits den rechtswidrigen Zugriff auf Server oder Personal Computer oder deren Missbrauch als Straftat verfolgen.

---

20 Richtlinie 84/450/EWG des Rates vom 10. September 1984 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über irreführende Werbung, ABl. L 250 vom 19.9.1984, S. 17-20. Die Kommission hat kürzlich einen Vorschlag zur Ablösung und Aktualisierung der Richtlinie über irreführende Werbung unterbreitet (KOM (2003) 356 endgültig).

21 Am 24. September 1998 verabschiedete der Rat eine Empfehlung zur Steigerung der Wettbewerbsfähigkeit des europäischen Industriezweiges der audiovisuellen Dienste und Informationsdienste durch die Förderung nationaler Rahmenbedingungen für die Verwirklichung eines vergleichbaren Niveaus in Bezug auf den Jugendschutz und den Schutz der Menschenwürde (98/560/EG). Diese Empfehlung war das erste Rechtsinstrument auf EU-Ebene, das sich mit dem Inhalt von audiovisuellen und Informationsdiensten befasste und alle Übertragungsarten, vom Fernsehen bis zum Internet, berücksichtigte.

22 Richtlinie des Europäischen Parlaments und des Rates vom 8. Juni 2000, ABl. L 178 vom 17.7.2000. In der Regel müssen Werbenachrichten die Vorschriften des Mitgliedstaates erfüllen, in dem der Diensteanbieter seinen Sitz hat. Dies gilt jedoch nicht für unerbetene elektronische Nachrichten (s. Artikel 3 der Richtlinie über elektronischen Geschäftsverkehr und deren Anhang). Für den (seltenen) Fall, dass eine natürliche Person nicht durch die Richtlinie 2002/58/EG gegen unerbetene elektronische Werbung geschützt ist (weil sie z.B. kein Teilnehmer ist) müssen die Mitgliedstaaten aufgrund der Richtlinie über elektronischen Geschäftsverkehr gewährleisten, dass Diensteanbieter, die unerbetene Werbenachrichten versenden, regelmäßig die Listen einsehen und beachten, in denen sich natürliche Personen eintragen lassen können, die keine derartige Werbung zu erhalten wünschen (Artikel 7 der Richtlinie über elektronischen Geschäftsverkehr).

23 Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme, KOM (2002) 173 endgültig vom 19.4.2002.

3. UMSETZUNG UND DURCHSETZUNG DURCH MITGLIEDSTAATEN UND STAATLICHE BEHÖRDEN

Nachstehend werden Umsetzungs- und Durchsetzungsmaßnahmen erörtert, insbesondere für Regierungen und staatliche Behörden, z.B. Abhilfen und Sanktionen, Rechtsschutzmechanismen, grenzüberschreitende Beschwerden, Zusammenarbeit mit Drittländern und Überwachung.

Bevor auf die Durchsetzungsmaßnahmen eingegangen wird, ist jedoch zu bemerken, dass einige Mitgliedstaaten die Datenschutzrichtlinie für elektronische Kommunikation noch nicht umgesetzt haben, einschließlich der Bestimmungen über unerbetene Werbenachrichten, die Teil eines neuen, umfassenderen Rechtsrahmens für elektronische Kommunikation[24] ist. Das Europäische Parlament hat unlängst seiner Besorgnis über diese Verzögerung Ausdruck verliehen[25]. Nach Ablauf der Umsetzungsfrist für die Datenschutzrichtlinie für elektronische Kommunikation am 31. Oktober 2003 leitete die Kommission im November 2003 Vertragsverletzungsverfahren gegen mehrere Mitgliedstaaten ein, die keine Umsetzungsmaßnahmen notifiziert hatten[26].

3.1. Einleitung

Rechtsvorschriften können Spamming teilweise verhindern, reichen aber allein nicht aus. Der Durchsetzung des Opt-in-Systems ist in allen Mitgliedstaaten Vorrang einzuräumen. Dies erfordert nicht nur genügend Personal und Ressourcen, sondern auch angemessene Durchsetzungsverfahren einschließlich grenzüberschreitender Mechanismen. Auch der Zusammenarbeit mit Drittländern kommt maßgebende Bedeutung zu. Überwachung ist ebenfalls entscheidend, sei es auch nur, um Durchsetzungsprioritäten zu ermitteln.

Verschiedene Faktoren scheinen die Wirksamkeit der Durchsetzungsverfahren zu beeinflussen:

– die Möglichkeit, Rechtsvorschriften mit wirksamen Geldbußen oder Sanktionen durchzusetzen. Einige Regulierungsbehörden verfügen offenbar noch nicht über (effektive) Durchsetzungsbefugnisse;

– die Art der Rechtsschutzmechanismen und Abhilfen, die Einzelnen und Unternehmen zur Verfügung stehen;

– das Bedürfnis nach Klarheit und Koordinierung zwischen den einzelstaatlichen Behörden angesichts ihrer sich gelegentlich überschneidenden Verpflichtungen auf diesem Gebiet;

– der Grad der Aufklärung der Nutzer über ihre Rechte und die Möglichkeiten, sie durchzusetzen. Die Nutzer müssen darüber informiert werden, wo sie sich beschweren können, was untersucht wird und was nicht, welche Arten von Durchsetzungsmaßnahmen

---

24 Vgl. 9. Bericht über die Umsetzung des Telekom-Reformpakets unter: http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/9threport/index_en.htm

25 Auf die Bedeutung der uneingeschränkten, effizienten und fristgerechten Umsetzung des neuen Rechtsrahmens für elektronische Kommunikation wies die Kommission in ihrer Mitteilung „Elektronische Kommunikation: der Weg zu einer wissensbestimmten Wirtschaft“ hin (KOM (2003) 65 vom 11. Februar 2003).

26 Die Aufforderungsschreiben wurden am 25. November 2003 versandt (s. IP/03/1663).

getroffen werden können und welche Informationen sie den Behörden liefern müssen, um eine Untersuchung einzuleiten;

– Koordinierung und Zusammenarbeit zwischen den Mitgliedstaaten sowie zwischen diesen und Drittländern hinsichtlich der für bestimmte Fälle geltenden nationalen Gesetze;

– die verfügbaren Mittel zum Aufspüren von „Spammern“, die innerhalb oder außerhalb der EU ihr Unwesen treiben und ihre Identität verbergen, indem sie u.a. die Identität, Adressen oder Server anderer benutzen.

Die Durchsetzungsmaßnahmen zu den Bestimmungen über unerbetene Nachrichten sind unter Punkt 2.2 erläutert. Die Verfahren gegen unerbetene elektronische Werbung wurden bislang sehr unterschiedlich organisiert und gehandhabt[27]. Eine EU-Richtlinie als Instrument lässt den Mitgliedstaaten einen gewissen Handlungsspielraum bei der Umsetzung ihrer Bestimmungen; diese sind jedoch ungeachtet des gewählten Verfahrens durchzusetzen.

Ein ausgewogenes Verhältnis von Rechtsetzung, Durchsetzung und Selbstregulierung wird

Abweichungen zwischen den Mitgliedstaaten

Für die Durchsetzung der Bestimmungen über unerbetene Werbung ist nicht in allen Mitgliedstaaten die gleiche Behörde zuständig. In den meisten Ländern nimmt an erster Stelle die Datenschutzbehörde (DSB) diese Aufgabe wahr, in anderen hingegen die nationale Regulierungsbehörde (NRB) für elektronischen Kommunikation. In wieder anderen ist vor allem die Verbraucherschutzbehörde (und der Verbraucherschutzbeauftragte) für die Durchsetzung verantwortlich. Häufig ist mehr als eine Behörde beteiligt. Spam beinhaltet vielfach irreführende und betrügerische Praktiken. (Nur in einigen Mitgliedstaaten gibt es keine Verbraucherschutzbehörde; hier bleibt die Durchsetzung den Verbraucherverbänden oder den Verbrauchern selbst überlassen.). Spamming geht oft mit Verstößen gegen den Datenschutz wie Sammeln von Adressen einher, oder gar mit cyberkriminellen Aktivitäten wie Eindringen in PCs oder Server. Die diesbezüglichen Bestimmungen werden möglicherweise nicht von den gleichen Behörden durchgesetzt, ganz abgesehen vom grenzüberschreitenden Verkehr.

Außer in einigen Mitgliedstaaten führen Beschwerden nicht zwangsläufig zu Ermittlungen. Gelegentlich werden mit gewissem Erfolg Kontakte geknüpft, ehe es zu einem Verstoß kommt. So werden Anweisungen und Leitlinien an Unternehmen verteilt. Zuweilen bleibt es dem Verbraucher überlassen, Verbindung mit dem inkriminierten Unternehmen aufzunehmen, ehe er eine Beschwerde einreicht. In einigen Ländern (z.B. dem VK) unterliegt diese erste Phase der Selbstregulierung. In mehreren Mitgliedstaaten hat die Industrie bereits von sich aus Rechtsschutzmechanismen eingeführt. Die Behörden handeln häufig auch aus Eigeninitiative. Das Einschalten einer Verwaltungsbehörde schließt in der Regel den unmittelbaren Zugang zur Justiz nicht aus.

Nicht alle DSB sind befugt, gegen Rechtspersonen vorzugehen. Auch können (bislang) nicht alle DSB Sanktionen verhängen. In diesem Fall müssen sie ein Verfahren bei den Justizbehörden anstrengen. In Frankreich sah sich die DSB im Zusammenhang mit Ihren Erfahrungen mit der e-Mailbox veranlasst, den Justizbehörden einige spezifische Fälle vorzulegen, ohne nennenswerten Erfolg. In Belgien führte ein ähnliches Vorgehen zu einem Meinungsaustausch mit den verdächtigen Absendern; und in grenzüberschreitende Fällen wurden diese den der amerikanische FTC entsprechenden Behörden in der EU vorgelegt.

häufig als wirksamstes Mittel zur Durchsetzung des Opt-in-Systems genannt. Den Mitgliedstaaten wird empfohlen, die Effizienz ihrer Durchsetzungsverfahren zu prüfen, insbesondere anhand der nachstehend vorgeschlagenen Maßnahmen (Punkt 3.2 – 3.6).

[27] Man beachte, dass Beschwerden häufig auch verwandte Aspekte betreffen, z.B. das Recht auf Zugang zu personenbezogenen Daten und auf Einspruch gegen deren Verarbeitung.

Ferner wird angeregt, nationale Strategien zu entwickeln, um die Zusammenarbeit zwischen den Datenschutzbehörden, (DSB), Verbraucherschutzbehörden (VSB) und nationalen Regulierungsbehörden (NRB) für elektronische Kommunikation zu gewährleisten und Überschneidungen und Doppelarbeit zwischen den Behörden zu vermeiden.

Um den Austausch von Informationen und empfehlenswerten Durchsetzungsverfahren (z.B. Beschwerden, Abhilfen, Sanktionen, internationale Zusammenarbeit) zu fördern, haben die Dienststellen der Kommission mit Unterstützung der Mitgliedstaaten und der Datenschutzbehörden eine **informelle Online-Gruppe für unerbetene Werbung** eingesetzt. Die Gruppe wird auch die Arbeiten im Rahmen anderer hier aufgezeigter Maßnahmen wie Aufklärung und Erarbeitung technischer Lösungen fördern.

Die im Anschluss an die Beratungen der Gruppe erstellten Dokumente werden in der Regel dem aufgrund des Rechtsrahmens für elektronische Kommunikationsnetze und Dienste eingesetzten Kommunikationsausschuss und/oder der Datenschutzgruppe nach Artikel 29 zur weiteren Veranlassung vorgelegt. Insbesondere kann die Gruppe Benchmarking-Kriterien für die vorzuschlagenden Maßnahmen festlegen.

Dieser Gruppe gehören Vertreter der zuständigen nationalen Verwaltungen und Datenschutzbehörden sowie der Kommissionsdienststellen an. Sie wird entscheiden, wie die Mitwirkung anderer Betroffener und Interessenten gewährleistet werden kann.

3.2. Abhilfen und Sanktionen

3.2.1. Diskussion

Zu den derzeitigen Abhilfen gehören Geldbußen oder die Verfügung, die unrechtmäßige Datenverarbeitung einzustellen, gelegentlich auch das „Blockieren“ der betreffenden Websites. In einigen Mitgliedstaaten werden bei Verstößen diese Verfügungen vor oder gleichzeitig mit der Auferlegung von Geldbußen erlassen. Jedoch haben nicht alle Behörden Entscheidungsbefugnis für die gesamte Palette der mit Spam einhergehenden Rechtsverletzungen, auch verfügen sie nicht alle über die gleichen Instrumente.Häufig werden Fälle an die Justizbehörden weitergeleitet. Nicht alle Mitgliedstaaten verfügen über gerichtliche Sanktionen gegen Gesetzesverstöße.

Nicht alle Mitgliedstaaten sehen Abhilfen bzw. Geldbußen/Geldstrafen im Verwaltungs- oder im Strafrecht vor. Die strafrechtlichen Sanktionen sind unterschiedlich; in einigen Mitgliedstaaten werden sogar Freiheitsstrafen verhängt. Ferner besteht in der Regel nach dem Zivilrecht die Möglichkeit, auf Schadenersatz zu klagen.

Häufig wird zwischen „leichten“ und „schweren“ Verstößen (Massenpost, irreführende oder betrügerische Werbe- bzw. Handelspraktiken) unterschieden; und auch die Strafen selbst variieren stark zwischen den Mitgliedstaaten.

Vielfach kann auch nach dem allgemeinen Datenschutzrecht (z.B. bei Verletzung der Notifizierungspflicht, des Rechts auf Zugang, der Verpflichtung, einen Vertreter in einem EU-Staat zu benennen u.a.) oder nach spezifischen Rechtsvorschriften gegen Spam vorgegangen werden (z.B. bei irreführender Werbung, betrügerischen Vertriebspraktiken u.a.). Insbesondere vor Einführung des Opt-in-Systems sind viele verschiedene Rechtsgrundlagen herangezogen worden, um bestimmten Formen des Spam entgegenzuwirken (z.B. Massenemailkampagnen, rechtswidriger Verwendung

personenbezogener Daten, Netzabschaltung, Missbrauch von E-Mail-Konten, Betrug und Falschauslegung von Verträgen).

Generell wird das Vorhandensein von Rechtsmitteln nicht als hinreichende Durchsetzungsmaßnahme angesehen. In der Regel kann die DSB, die VSB oder die NRB administrative Geldstrafen auferlegen, die Beträge sind jedoch unterschiedlich. Die Mitgliedstaaten, in denen diese Möglichkeit nicht besteht, erwägen überwiegend deren Einführung. Im Vergleich zu gerichtlichen Abhilfemaßnahmen scheinen Verwaltungssanktionen für einen so dynamischen Bereich angemessener. Die DSB, VSB und NRB bedienen sich häufig zusätzlicher Durchsetzungsinstrumente. Verwaltungsverfahren können sowohl kostengünstig als auch zeitsparend sein.

3.2.2. Vorgeschlagene Maßnahmen

Zunächst fordert die Kommission diejenigen Mitgliedstaaten, die die Richtlinie, insbesondere die Bestimmungen über unerbetene Nachrichten, noch nicht umgesetzt haben, dringend auf, dies unverzüglich zu tun. Ihre Dienststellen sind bereit, sie bei Bedarf zu unterstützen.

Den Mitgliedstaaten wird empfohlen, die Wirksamkeit ihrer Abhilfen und Sanktionen für Rechtswidrigkeiten zu prüfen und für die Opfer angemessene Möglichkeiten zu schaffen, Schadenersatz zu fordern.

Mitgliedstaaten und Behörden, die keine Verwaltungsverfahren gegen Spam vorgesehen haben, sollten diese als rasche, erschwingliche und wirksame Maßnahme zur Durchsetzung des Opt-in-Systems in Erwägung ziehen.

Die Kommission wird darauf achten, dass die nationalen Umsetzungsmaßnahmen echte Sanktionen bei Verstößen von Marktteilnehmern gegen die einschlägigen Vorschriften und gegebenenfalls finanzielle und strafrechtliche Sanktionen vorsehen.

In diesem Zusammenhang wird die Kommission auch prüfen, inwieweit die zuständigen Behörden die notwendigen Ermittlungs- und Durchsetzungsbefugnisse besitzen.

3.3. Rechtsschutzmechanismen

3.3.1. Diskussion

Eine effiziente Durchsetzung erfordert angemessene Rechtsschutzmechanismen. Einige DSB haben Mailboxen eingerichtet, an die die Nutzer unerbetene Werbenachrichten weiterleiten können, und zugesagt, in bestimmten Fällen Maßnahmen zu treffen.

Mehrere Mitgliedstaaten scheinen normale Verwaltungsverfahren und Kontakte zu den Internet-Diensteanbietern oder Computer-Notfallteams vorzuziehen. Andere bevorzugen herkömmlichere Verfahren (Schadenersatzforderung nach dem Bürgerlichen Recht oder Verwaltungsverfahren). Gelegentlich wird auf Mitregulierung oder Selbstregulierung als Alternative zu direkten Umsetzungmaßnahmen verwiesen.

Empfehlenswerte Verfahren

Frankreich und Belgien haben Ende 2002 spezielle E-Mailboxen für Beschwerden über Spamming eingerichtet. Die Ergebnisse sind recht interessant. Berichte über diese Initiativen sind öffentlich verfügbar[28]. Frankreich wird voraussichtlich nach den neuen Umsetzungsvorschriften zur Datenschutzrichtlinie für elektronische Kommunikation eine permanente Mailbox unterhalten. Die amerikanische Federal Trade Commission (FTC) betreibt eine ähnliche Mailbox und nutzt die Zuschriften zur strafrechtlichen Verfolgung aufgrund bestehender Gesetze gegen unlautere und betrügerische Geschäftspraktiken[29].

E-Mailboxen bieten unter anderem den Vorteil, dass sie offenbar die Verbraucher motivieren, über Verstöße zu berichten und damit die Durchsetzung der erlassenen Rechtsvorschriften erleichtern. Ferner können sie wesentliches Zahlenmaterial über Art und Umfang der in einem bestimmten Land oder einer Region aufgetretenen Probleme liefern und so einen klaren Überblick vermitteln, der ein wertvolles Instrument für die Behörden darstellt, die Durchsetzungsprioritäten zuweisen oder anpassen müssen. Auch können anhand der erworbenen Kenntnisse Vorbeugungsmaßnahmen entwickelt werden. o hat die französische DSB, die während ihrer Spambox-Aktion gesammelten Informationen dazu verwendet, zur Vorbeugung Informationspakete für Nutzer und Geschäftsleute zu erstellen.

Eine E-Mailbox zur Überwachung und Ermittlung des Spam-Ausmaßes ist verständlicherweise nur sinnvoll, wenn den eingereichten Beschwerden sachgerecht und rasch nachgegangen werden kann.

Generell besteht ein Interesse daran, aus den Erfahrungen anderer Mitgliedstaaten mit E-Mailboxen zu lernen, allerdings scheinen nur einige die Einrichtung einer speziellen Mailbox zu planen oder erwägen. Begründet wird dies in der Regel mit der bestehenden Möglichkeit, sich per E-Mail zu beschweren - in der Regel über die Website der Behörde -, mit dem Bedarf an zusätzlichen Mitarbeitern und Geräten oder der Notwendigkeit, bestehende Verfahren zu ändern.

3.3.2. Vorgeschlagene Maßnahmen

Die Mitgliedstaaten und die zuständigen Behörden sollten die Effizienz ihres Rechtssystems bei der Behandlung von Nutzerbeschwerden prüfen und bei Bedarf Anpassungen erwägen.

Empfohlen wird, dass Mitgliedstaaten bzw. zuständige Behörden spezielle E-Mailboxen einrichten, begleitet durch Informationskampagnen.

Diese sind so auszulegen, dass eine einfache Suche und Analyse zum besseren Verständnis der Problematik möglich ist und Durchsetzungsprioritäten zugewiesen werden können.

Die Dienststellen der Kommission werden den Austausch von Informationen über Erfahrungen mit E-Mailboxen unterstützen.

---

28 Der Bericht der französischen Datenschutzbehörde, „Commission Nationale Informatique et Libertés (CNIL)“, vom 24. Oktober 2002, ist abrufbar unter: http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm
Der Bericht der belgischen Datenschutzbehörde, „Commission de Protection de la Vie Privée“, vom Juli 2003 kann unter folgender URL eingesehen werden: http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf

29 Vgl. http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf. Unerwünschte oder betrügerische E-Mails können an folgende Aderesse weitergeleitet werden: uce@ftc.gov.

3.4. Grenzüberschreitende Beschwerden und Zusammenarbeit bei der Durchsetzung in der EU

*3.4.1. Diskussion*Die Bearbeitung grenzüberschreitender Beschwerden ist Bestandteil eines erfolgreichen Verbraucherschutzes auf diesem Gebiet. Es muss unbedingt gewährleistet sein, dass die nationalen Rechtsschutzmechanismen ungeachtet ihrer Modalitäten verknüpft werden können, damit Beschwerden von Nutzern eines Mitgliedstaates über Nachrichten aus einem anderen effizient bearbeitet werden (vgl. Punkt 3.5, „Zusammenarbeit mit Drittländern).

Zum gegenwärtigen Zeitpunkt gibt es nicht in allen Mitgliedstaaten ein offizielles Verfahren zur Bearbeitung grenzüberschreitender Beschwerden. Derzeit kann Verbindung zur zuständigen Behörde eines anderen Mitgliedstaates aufgenommen oder die Beschwerde an die zuständige Behörde des Landes weitergeleitet werden, aus dem die Nachricht stammt.

Auf europäischer Ebene (einschließlich der EWR- und Beitrittsländer) tauschen die DSB Informationen über grenzüberschreitende Beschwerden über eine Beschwerdestelle aus, die von der Europäischen Konferenz der Datenschutzbeauftragten geschaffen wurde. Sie kann bei grenzüberschreitenden Spam-Beschwerden hinzugezogen werden, um u.a. zu ermitteln, welches Recht auf einen bestimmten Fall anwendbar ist. Jedoch setzen nicht alle DSB die Bestimmungen über unerbetene Nachrichten durch.

Im Bereich des Verbraucherschutzes hat die Kommission kürzlich eine Verordnung über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden[30] vorgeschlagen, um grenzüberschreitende Probleme in den Griff zu bekommen. Damit werden Verfahren zur gegenseitigen Hilfeleistung und eine intensive Zusammenarbeit zwischen den nationalen Behörden eingeführt. Das vorgeschlagene Verfahren würde zwar für Spam-Nachrichten gelten, die irreführend oder betrügerisch sind oder gegen die Verbraucherschutzvorschriften verstoßen, nicht aber für alle Spams, die durch die Datenschutzrichtlinie für elektronische Kommunikation verboten sind. Der Vorschlag liegt dem Rat und dem Parlament zur Beratung vor.

3.4.2. Vorgeschlagene Maßnahmen

Den Mitgliedstaaten und den zuständigen Behörden wird empfohlen, ihre derzeitigen Verfahren zur Bearbeitung grenzüberschreitender Beschwerden (z.B. Vereinbarungen über gegenseitige Hilfeleistung) auf ihre Wirksamkeit zu überprüfen.

Die Koordinierung zwischen den zuständigen nationalen Behörden wird unterstützt. Dazu gehören die Koordinierung und der Informationsaustausch zwischen den Behörden, die die neuen Bestimmungen durchsetzen, sowie zwischen diesen und anderen Behörden, die sich mit speziellen Arten von Spam befassen (wie betrügerischen Spam-Nachrichten, Pornografie, Nachrichten über illegal vertriebene Gesundheitspräparate).

Um betrügerischen Spam-Nachrichten entgegenzuwirken, wird dem Rat und dem Parlament dringend nahe gelegt, die vorgeschlagene Verordnung über die Zusammenarbeit beim Verbraucherschutz so rasch wie möglich zu verabschieden, damit gewährleistet ist, dass die Verbraucherschutzbehörden für die Bekämpfung irreführender und betrügerischer Spam-Nachrichten gewappnet sind. Ferner wird ihnen empfohlen die Einbeziehung der

[30] KOM(2003) 443 endgültig.

Datenschutzrichtlinie für elektronische Kommunikation in den Geltungsbereich dieser Verordnung zu prüfen.

Die Mitgliedstaaten werden ersucht, Wege zum Abbau bestehender Hindernisse für den Informationsaustausch und die Zusammenarbeit sowie die Möglichkeit zu prüfen, Maßnahmen der Behörden anderer Mitgliedstaaten zu fordern. In der Praxis könnte sich eine Kontaktstelle als sinnvoll erweisen (vgl. vorgenannte Initiative der DSB), über die die nationalen Regulierungsbehörden die grenzüberschreitende Durchsetzung gemeinsam anstreben. Beim Aufbau eines Netzes zur Unterstützung der Zusammenarbeit könnten Gemeinschaftsprogramme wie IDA herangezogen werden[31].

Die Kommission gedenkt die Maßnahmen zur Koordinierung der zuständigen nationalen Behörden zu fördern, insbesondere durch die neue Online-Gruppe für unerbetene Werbenachrichten. Ihre Dienststellen haben begonnen, zusammen mit den Mitgliedstaaten und den mit der Durchsetzung beauftragten nationalen Behörden zu prüfen, welcher konkreter Maßnahmen es bedarf, um die Bearbeitung grenzüberschreitender Beschwerden zu verbessern. Die Gespräche mit den nationalen Behörden werden 2004 andauern.

3.5. Zusammenarbeit mit Drittländern

3.5.1. Diskussion

Die neuen Vorschriften gelten für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste über öffentliche Netze in der Europäischen Union (und dem EWR). Daher gilt Artikel 13 der Richtlinie 2002/58/EG (Opt-in-Regelung) für alle unerbetenen Werbenachrichten, die in Netzen der EU eingehen oder aus diesen versandt werden. Dies bedeutet, dass derartige Nachrichten aus Drittländern die EU-Vorschriften ebenso erfüllen müssen wie Nachrichten aus der EU, die an Adressen in Drittländern versandt werden.

Die Durchsetzung wird in der Praxis bei Nachrichten aus Drittländern eindeutig schwieriger sein als bei denen, die aus der EU stammen. Dennoch ist sie von Bedeutung, da viele Spam-Nachrichten aus Drittländern eingehen.

Es wird eine Kombination verschiedener Instrumente erforderlich sein, zu denen Vorbeugung, Filtertechniken, Selbstregulierung, Verträge und internationale Zusammenarbeit gehören, mit der sich dieser Abschnitt befasst. Hauptziel der internationalen Zusammenarbeit ist die Förderung effizienter Rechtsvorschriften in Drittländern. Das nächste Ziel ist die Zusammenarbeit mit diesen, um die geltenden Bestimmungen durchzusetzen.

Es gibt nicht viel Erfahrungen mit der Durchsetzung der bestehenden Opt-in- und Opt-out-Regelungen bei Nachrichten aus Drittländern. Abgesehen davon, dass Spam ein relativ neues Phänomen ist, wird häufig auf Hindernisse hingewiesen wie die Schwierigkeit, die Absender dieser Nachrichten zu ermitteln oder den hierfür erforderlichen Aufwand, den Mangel an (geeigneten) Verfahren zur internationalen Zusammenarbeit und den Mangel an Rechtsprechung in internationalen Angelegenheiten bei einigen Behörden.

Was betrügerische Spam-Nachrichten betrifft, sieht der Vorschlag der Kommission für eine Verordnung über die Zusammenarbeit beim Verbraucherschutz auch die Kooperation mit Drittländern bei der Durchsetzung vor. Die Organisation für wirtschaftliche Zusammenarbeit

---

[31] Nähere Einzelheiten zum Programm IDA s. http://europa.eu.int/comm/enterprise/ida/index.htm.

und Entwicklung (OECD) verabschiedete 2003 eine Empfehlung zum Schutz der Verbraucher gegen grenzüberschreitende betrügerische Geschäftspraktiken[32].

3.5.2. Vorgeschlagene Maßnahmen

Auf multilateraler Ebene wirken einige Mitgliedstaaten bereits tatkräftig in Foren wie der OECD mit, wo die Bekämpfung des Spam ihren Ausgang nahm. Eine rege Beteiligung an diesen Tätigkeiten wird insbesondere im Hinblick auf die Erarbeitung von Lösungen auf internationaler Ebene empfohlen.

Die Kommission wird im Februar 2004 einen OECD-Workshop über Spam veranstalten, der zu einem besseren Verständnis des Spam-Problems führen und zur Erarbeitung von Lösungen auf internationaler Ebene beitragen soll. Konkrete Folgemaßnahmen auf OECD-Ebene werden auf den Ergebnissen des Workshops aufbauen. Die Dienststellen der Kommission erörtern derzeit mit den Mitgliedstaaten diese Maßnahmen. Dazu gehören Arbeiten der OECD zur Förderung der Gesetzgebung auf internationaler Ebene, Aufklärungsmaßnahmen, technische Lösungen, Selbstkontrolle und internationale Zusammenarbeit bei der Durchsetzung.

Auf UN-Ebene wird in der Erklärung des Weltgipfels Informationsgesellschaft (Genf, 10.-12. Dezember 2003) und dem zugehörigen Aktionsplan betont, dass Spam auf den entsprechenden nationalen und internationalen Ebenen zu bekämpfen ist. Die Kommission wird unter Berücksichtigung des Gipfels, der 2005 in Tunis stattfinden wird, prüfen, welche Maßnahmen aufgrund der Ergebnisse des Weltgipfels 2003 in der EU zu treffen sind.

Den Mitgliedstaaten und zuständigen Behörden wird empfohlen, die bilaterale Zusammenarbeit mit Drittländern zu verstärken oder aufzunehmen. Sie betrifft nicht nur die Förderung einer effizienten Gesetzgebung, sondern auch deren Durchsetzung, gegebenenfalls in polizeilicher und gerichtlicher Zusammenarbeit.

Auch die Zusammenarbeit zwischen Behörden und der Privatwirtschaft wird empfohlen, insbesondere Anbietern von Internet- und elektronischen Diensten, um entsprechend angemessener rechtlicher Vorkehrungen Spammer aufzuspüren.

Die Dienststellen der Kommission werden weiterhin in internationalen Foren mitwirken, u.a. in der OECD und anlässlich des Workshops, den die Kommission im Februar 2004 in Brüssel veranstalten wird. Sie wird ferner die bilateralen Sitzungen und Gespräche mit Drittländern fortsetzen, um diese u.a. zu bewegen, wirksame Maßnahmen gegen Spam, insbesondere in seiner aggressivsten Form, zu ergreifen und die Zusammenarbeit bei der Durchsetzung zu fördern.

Die Dienststellen der Kommission haben begonnen, zusammen mit den Mitgliedstaaten und den mit der Durchsetzung beauftragten Behörden zu prüfen, wie die internationale Zusammenarbeit am besten gewährleistet werden kann, damit vor allem Beschwerden über Spam aus Drittländern bearbeitet werden können. Diese Arbeit wird 2004 zusammen mit den nationalen Behörden fortgesetzt.

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

3.6. Überwachung

3.6.1. Diskussion

Um zu beurteilen, wie das Opt-in-System in der Praxis funktioniert und spezifischen Problemen mit geeigneten Maßnahmen zu begegnen, benötigen die Mitgliedstaaten objektive, aktuelle Informationen über die Tendenzen beim Spam, über Nutzerbeschwerden und über Schwierigkeiten, mit denen sich Diensteanbieter konfrontiert sehen. Dazu gehören Informationen über Tendenzen hinsichtlich der Art, der Herkunft und des Umfangs unerbetener elektronischer Werbung, die von den Filtersoftware-Anbietern, Diensteanbietern und nationalen (rechtlichen) Initiativen ermittelt werden, sowie gegebenenfalls Statistiken aufgrund einer E-Mailbox für Beschwerden.

Die OECD hat 2003 mit der Erfassung des Ausmaßes unerbetener elektronischer Nachrichten auf internationaler Ebene begonnen und wird diese Arbeit 2004 fortsetzen.

Gemäß Artikel 18 der Datenschutzrichtlinie für elektronische Kommunikation ist 2006 ein Bericht über die Durchführung der Richtlinie und ihre Auswirkungen auf Marktteilnehmer und Verbraucher zu erstellen, wobei ein besonderer Schwerpunkt auf unerbetenen Nachrichten liegt. Zur Erstellung dieses Berichts muss die Kommission Informationen der Mitgliedstaaten, darunter einschlägige Statistiken, einholen.

3.6.2. Vorgeschlagene Maßnahmen

Die Mitgliedstaaten müssen dafür sorgen, dass die benötigten Informationen und Statistiken über ihre Durchsetzungsmaßnahmen vorliegen. Hierzu müssen sie soweit angemessen mit der Industrie zusammenarbeiten und die laufenden OECD-Maßnahmen zur Erfassung des Umfangs unerbetener elektronischer Nachrichten berücksichtigen.

Die Kommission wird über die Online-Gruppe für unerbetene Werbenachrichten den Austausch von Informationen und empfehlenswerten Verfahren im Zusammenhang mit Spam-Tendenzen und –Statistiken fördern und koordinieren.

4. TECHNISCHE UND SELBSTREGULIERUNGSMASSNAHMEN DER WIRTSCHAFT

Dieser Abschnitt über Selbstregulierung und technische Fragen umfasst Maßnahmen, die den Marktbeteiligten insbesondere in Bereichen wie vertragliche Vereinbarungen, Verhaltenskodizes, zulässige Werbepraktiken, Kennzeichnungen und alternative Streitbeilegungsverfahren vorgeschlagen werden. Auch werden einige technische Lösungen angesprochen, z. B. die Filterung und die Sicherheit von Servern.

4.1. Tatsächliche Anwendung der Zustimmungsregelung

4.1.1. Diskussion

Die Bekämpfung von Spam ist Angelegenheit aller interessierten Parteien. Die Industrie kann eine besondere Rolle spielen, da sie die Zustimmungsregelung („Opt-In“) zur täglichen Geschäftspraxis machen kann. Zur täglichen Praxis gehören nicht nur die Geschäftsbedingungen für Endnutzer, sondern auch die Beziehungen mit Geschäftspartnern.

In vielen Fällen ist eine bessere Koordinierung über Industrieverbände und die Einbeziehung branchenspezifischer Selbstregulierungsgremien sowie von Verbraucher- bzw. Nutzerverbänden erforderlich, sowie die Mitarbeit von Datenschutzbehörden oder anderen zuständigen nationalen Behörden.

Empfehlenswerte Verfahren

Beispielsweise ist in den Niederlanden seit 2002 die ‚Elektronische Handelsplattform' Gastgeber eines Forums ‚Grundsätze für die E-Mail-Werbung', auf dem verschiedene Wirtschaftszweige (Direktwerber und Internetanbieter) mit dem niederländischen Verbraucherverband zusammenkommen. Dort soll besprochen werden, wie der Grundsatz der vorherigen Zustimmung praktisch umzusetzen ist. Diese praktische Umsetzung wird zusammen mit der Datenschutzbehörde erprobt.[33]

Verträge können beim Kampf gegen Spam helfen, wenn Vorkehrungen zum Schutz der Rechte des Einzelnen eingebaut sind. Viele Internetanbieter und E-Mail-Anbieter haben in die Verträge mit ihren Kunden bereits das Verbot der Nutzung ihrer Dienste für das Senden von Spam aufgenommen. Solche Anbieter verbieten bereits das Senden unerwünschter elektronischer Post oder von elektronischer Massenpost von ihren E-Mail-Konten aus.[34]

Die Ansätze in bisherigen Verträgen zwischen Internetanbietern und ihren Kunden dürften sich von denen der neuen Richtlinie und den nachfolgenden Gesetzen zu deren Umsetzung in den Mitgliedstaaten unterscheiden.

Im Hinblick auf den Dienst am Kunden besteht auch Bedarf an einem aktiveren Vorgehen in Bezug auf die Filterung, z. B. durch Information über Spam-Filter und durch ein Angebot an Filterdiensten oder Filterfunktionen, aus denen die Kunden wählen können.

Das Gleiche gilt, wenn Internetanbieter oder Mobilfunkbetreiber Verträge mit Dritten - insbesondere mit Direktwerbern - eingehen. Dies betrifft nicht etwa nur die direkten

---

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

34 Solche Klauseln basieren manchmal auf der Notwendigkeit, alle Maßnahmen zur Verhinderung unangemessener Nutzung ihrer Dienste zu treffen . Andere Klauseln verweisen auf bestehende Verhaltenskodizes in Bezug auf elektronische Massenpost oder auf Grundsätze der Selbstregulierung (z. B. die ‚Netiquette').

Beziehungen mit Unternehmen, die ‚Mehrwertdienste' anbieten. Es gilt auch für Betreiber, mit denen ein bestimmter Diensteanbieter Zusammenschaltungsvereinbarungen geschlossen hat, was bei mobilen Diensten der Fall ist.

Die neue Zustimmungsregelung wirkt sich auch auf mehrere Aspekte der Direktwerbung aus, wie etwa

- die Methoden für die Sammlung von E-Mail-Adressen und anderer Daten für elektronische Kontakte (wie oben erwähnt, ist die Einsammlung von E-Mail-Adressen mit dem Gemeinschaftsrecht unvereinbar);

- die Anpassung bestehender Listen;

- das Verbot der Nutzung von Daten ohne Zustimmung und des Verkaufs illegaler Listen.

4.1.2. Vorgeschlagene Maßnahmen

Die Beteiligung der Wirtschaft und die Selbstregulierung oder, besser, die Koregulierung, sollten insbesondere in den Bereichen gefördert werden, in denen Rechtsvorschriften und deren Durchsetzung durch die Behörden vielleicht nicht ausreichen. Alle interessierten Parteien sollten hier ihre Aufgabe übernehmen, einschließlich der Verbraucherverbände und/oder Nutzerverbände.

Vertragspraktiken der Diensteanbieter gegenüber Kunden und Geschäftspartnern

Zunächst muss die Wirtschaft vor allem untersuchen, inwieweit ihre bestehenden Verträge mit den neuen Regelungen vereinbar sind, und sie gegebenenfalls anpassen.

Dies betrifft die Anpassung der Allgemeinen Geschäftsbedingungen in den Verträgen mit den Kunden. Dies gilt nicht nur für Internetanbieter und E-Mail-Anbieter, sondern auch für Anbieter mobiler Dienste. Als ergänzende Maßnahme könnten den Kunden Informationen über Filter und Filtersoftware geliefert oder den Kunden könnten entsprechende Dienste optional angeboten werden (die Filterung wird auch im nachfolgenden Abschnitt 4.3 behandelt). Klauseln in Verträgen mit Geschäftspartnern (z. B. mobile Zusammenschaltung, Mehrwertdienste) sollten mit der Zustimmungsregelung vereinbare Werbepraktiken widerspiegeln und angemessene Sanktionen bei Verstößen vorsehen.

Praktiken der Direktwerber

Zum zweiten kann eine Anpassung der Praktiken der Direktwerber an die Zustimmungsregelung erforderlich werden. Insbesondere könnten sich die Direktwerber mit speziellen, legalen Verfahren zur Sammlung persönlicher Daten (z. B. Regelungen der ‚doppelten' oder ‚bestätigten' Zustimmung) einverstanden erklären.

Verhaltenskodizes

Drittens haben Wirtschaftsverbände bereits verschiedene Initiativen angekündigt, wie die Anpassung oder Annahme von Verhaltenskodizes und die Verbreitung guter Werbepraktiken.[35] Die Kommission wird europaweite Online-Verhaltenskodizes für die Direktwerbung unterstützen. Verhaltenskodizes und andere Initiativen zur Selbstregulierung sowie Verträge müssen mit der Zustimmungsregelung in Einklang stehen. Dabei könnte die

[35] Der europäische Fachverband für Direktwerbung (FEDMA) hat einen speziellen Online-Verhaltenskodex für Direktwerber angekündigt.

Einbeziehung der zuständigen Regulierungsbehörde hilfreich sein. Hier sollte darauf hingewiesen werden, dass die Datenschutzgruppe nach Artikel 29 europaweite Verhaltenskodizes billigen kann (siehe Artikel 30 der ‚allgemeinen' Datenschutzrichtlinie 95/46/EG).

Wie in den meisten Fällen wird eine wirksame Anwendung von Selbstregulierungsmaßnahmen davon abhängen, welche Strukturen für die Einhaltung der vereinbarten Regeln sorgen müssen und ob spürbare Strafen vorgesehen sind.

Kennzeichnungen

Viertens könnten, um die Nutzer besser aufzuklären, Instrumente wie Kennzeichnungen (u. a. auch bekannt als ‚Gütesiegel' oder ‚Websiegel') verwandt werden, insbesondere dort, wo vertrauenswürdige Dritte die Einhaltung der Verhaltenskodizes durch die Marktbeteiligten überwachen und bestätigen.

Sichtbare Kennzeichnungen können den Nutzern dabei helfen, Internetanbieter, E-Mail-Anbieter und andere Kräfte der Wirtschaft zu finden, die sich an die EU-Regeln und/oder anerkannte Verhaltenskodizes halten, die die EU-Regeln umsetzen. Auch könnten sie helfen, die Filtersysteme effizienter zu machen.

Erwägenswert wäre auch eine Kennzeichnung von Nutzerdatenbanken, die der Zustimmungsregelung entsprechen, sowie von solchen elektronischen Nachrichten (z. B. ein Kennzeichen ‚ADV' in der Betreffzeile einer E-Mail, um anzudeuten, dass sie Werbung enthält).

Durch solche Kennzeichnungen könnten die Empfänger derartige Werbemitteilungen im Einklang mit der Richtlinie über den elektronischen Geschäftsverkehr (vgl. Artikel 6 Buchstabe a) der Richtlinie 2000/31/EG) eindeutig erkennen; siehe hierzu auch Abschnitt 2).

4.2. Alternative Streitbeilegungsverfahren (ADR)

4.2.1. Diskussion

Bei Verletzungen der Privatsphäre wie dem Senden unerwünschter elektronischer Post kann ein außergerichtliches Verfahren zu einer besseren Einhaltung der neuen Regeln beitragen. Auf nationaler und auf EU-Ebene wurden mehrere Initiativen für alternative Streitbeilegungsverfahren (ADR) eingeleitet, um Streitigkeiten in Bezug auf Online-Transaktionen und elektronische Kommunikation zu beheben. 1998 und 2001 verabschiedete die Kommission Empfehlungen zu ADR, in denen sie Grundsätze für solche Systeme festlegte. Derzeit laufen mehrere Initiativen zu ADR-Systemen in Bezug auf den Verbraucherschutz (z. B. EEJ-NET)[36]. Auch Artikel 17 der Richtlinie über den elektronischen Geschäftsverkehr regt zur Entwicklung solcher Verfahren an.

Außergerichtliche Streitbeilegungsverfahren - manchmal gesetzlich vorgeschrieben - gibt es in einigen Ländern. Sie unterscheiden sich jedoch in vielerlei Beziehung, wie ihrem Ursprung (z. B. branchenspezifisch für die Direktwerbung oder die E-Mail-Werbung), der ‚Rechtsprechung', der Befugnisse und Sanktionen (z. B. Schadensersatzansprüche), der Mitwirkung spezieller Stellen (z. B. Datenschutzbehörden, Gremien für Werbungsnormen) usw.

[36] Nähere Informationen siehe: http://europa.eu.int/comm/consumers/redress/out_of_court/index_de.htm.

Damit diese Verfahren ausreichende Wirkung erzielen, sind bestimmte Voraussetzungen erforderlich, etwa hinsichtlich ihrer Organisation und Unterstützung sowie der Durchsetzung der Schiedssprüche. Ihre Einrichtung erfordert außerdem eine Zusammenarbeit zwischen den Behörden und der Wirtschaft.

4.2.2. Vorgeschlagene Maßnahmen

Die Schaffung und Anwendung wirksamer Selbstregulierungs-Rechtsschutzmechanismen sowie alternativer Streitbeilegungsverfahren (ADR) wird gefördert, wobei so weit wie möglich auf bestehenden Initiativen (z. B. EEJ-NET) aufzubauen ist. Nützlich könnten solche Verfahren vor allem in Fällen sein, in denen eine internationale Zusammenarbeit schwieriger zu erreichen wäre.

4.3. Technische Fragen

4.3.1. Überlegungen

Spam lässt sich auf unterschiedliche Weise technisch bekämpfen. Die Internetgemeinde (z. B. RIPE, IETF) nimmt das Problem Spam ernst.[37] Langfristigere Initiativen wie neue technische Normen für die elektronische Post werden im vorliegenden Papier nicht behandelt. Internetanbieter und E-Mail-Anbieter sperren oft eingehende Post von Servern, die für das Versenden von Spam benutzt werden (schwarze Liste), bis die Quelle des Spam ermittelt ist und an der Nutzung des Servers gehindert wird. Zusätzlich können der einzelne Nutzer in seinem Endgerät oder die Anbieter elektronischer Kommunikation in ihren Servern Filterprogramme einsetzen.

Nicht alle Filterverfahren und -techniken geben dem Nutzer das gleiche Maß an Kontrolle. Auch bieten sie nicht die gleichen Garantien für den Datenschutz und den Schutz der Privatsphäre, wie etwa die Beachtung der Vertraulichkeit von Nachrichten. Auch entsprechen sie nicht immer der neuen, in den Ländern der EU für Werbemitteilungen geltenden Zustimmungsregelung (auf vorheriger Zustimmung beruhend; in Verbindung mit Werbung stehend; Massenpost und andere Post). Auch könnte eine genauere Unterscheidung zwischen zulässiger Werbung (z. B. im Einklang mit der Zustimmung) und unerwünschter Werbung die Entwicklung wirksamerer Filterprogramme ermöglichen.

Zwar bieten die neuen Rechtsvorschriften zu unerwünschter Werbung per E-Mail dem Nutzer zusätzlichen Schutz und den Diensteanbietern eine größere Sicherheit, wenn sie auf Antrag Maßnahmen gegen ‚Spammer' unternehmen, doch kann die Filterung gelegentlich rechtmäßige E-Mail abblocken (‚falsche Positive') oder Spam durchlassen (‚falsche Negative'). In einigen Fällen riskieren Internet- bzw. E-Mail-Anbieter auf diese Weise, von einem Absender oder einem beabsichtigten Empfänger gerichtlich verklagt zu werden. Daher bieten manche dieser Anbieter die Filterung ihren Nutzern wahlweise an und aktivieren sie nur auf deren Wunsch hin.

---

[37] So ist etwa die Anti-Spam-Arbeitsgruppe von RIPE (Réseaux IP Européens) seit 1998 tätig (siehe das Dokument „Good Practice for combating Unsolicited Bulk Email" auf den RIPE-Webseiten: http://www.ripe.net). Auch die IRTF (Internet Research Task Force) hat kürzlich eine Forschungsgruppe zur Bekämpfung von Spam eingerichtet (http://www.irtf.org/charters/asrg.html). Diese Gruppe kann bestimmte Technologien entwickeln, die als Ausgangspunkt für Standardisierungsbemühungen im Rahmen der IETF (Internet Engineering Task Force) dienen könnten.

Obwohl diese Mitteilung diese Themen nicht behandelt, wirft die Nutzung von Filtertechniken zur Bekämpfung von Spam auch andere Fragen auf, wie etwa Filterung vs. freie Meinungsäußerung und Filterung vs. die vertragliche Verpflichtung von Internet- bzw. E-Mail-Anbietern zur Übermittlung elektronischer Nachrichten an die Kunden ihrer Abonnenten.

Für die Filterung bei mobilen Diensten könnten wegen der unterschiedlichen geschäftlichen Umfelder für mobile Dienste und feste Internetdienste unterschiedliche Lösungen gerechtfertigt sein. Insbesondere würde das Geschäftsmodell für mobile Dienste normalerweise ein Zustellungsentgelt pro Nachricht enthalten, was Spam teurer macht. Bei einigen neuen Diensten wird jedoch ein Entgelt für den Empfang erhoben, und auf diese Weise treibt Spam die Kosten für den Empfänger in die Höhe. Außerdem kann elektronische Post jetzt auch an mobile Endgeräte zugestellt werden. Dann könnten den Teilnehmern Filter und Vorschaufunktionen zur Bekämpfung ‚mobilen Spams' angeboten werden.

Zu beachten sind auch offene Mailserver. Kurz gesagt, sind offene Mailserver SMTP-Server, die zur Weiterleitung von Nachrichten genutzt werden können, welche von anderen als lokalen Nutzern des Servers gesendet wurden. Früher standen die meisten weiterleitenden Server offen. So konnten sich die Spammer ihrer bedienen, um recht leicht unerwünschte Nachrichten zu senden. Die Möglichkeiten für einen solchen Missbrauch lassen sich durch einfache Abhilfemaßnahmen verringern. Das Gleiche gilt für offene Proxyserver, also für Server, die über ihre Software ein direkte Verbindung mit dem Internet herstellen.

4.3.2. Vorgeschlagene Maßnahmen

Die Mitgliedstaaten und die zuständigen Behörden werden aufgefordert, die rechtlichen Bedingungen - einschließlich der Erfordernisse bezüglich des Schutzes der Privatsphäre - zu klären, unter denen in ihrem Land verschiedene Arten von Filterprogrammen eingesetzt werden können.

Die Anbieter von Filterprogrammen müssen sicherstellen, dass ihre Systeme mit der Zustimmungsregelung und anderen Anforderungen des EU-Rechts - auch solcher in Bezug auf die Vertraulichkeit von Nachrichten - vereinbar sind.

Die Nutzer sollten die Möglichkeit erhalten, je nach ihren eigenen Bedürfnissen selbst zu bestimmen, wie eingehende Spam-Nachrichten behandelt werden. Die Anbieter von Filterprogrammen müssen die Auswirkungen berücksichtigen, die ‚falsche Positive' oder ‚falsche Negative' sowie gewisse Formen der Filterung aufgrund von Inhalten für die Nutzer haben und welche Haftungsfragen sich daraus ergeben können.

Filteranbieter sollten mit interessierten Parteien zusammenarbeiten, um Techniken zur Erkennung elektronischer Werbenachrichten zu entwickeln, die vom Gemeinschaftsrecht anerkannten Werbepraktiken entsprechen, wie etwa Websiegel, Kennzeichnungen usw.

Die Anbieter von E-Mail-Diensten (und ggf. mobiler Dienste) sollten ihren Kunden Filterfunktionen oder -dienste als Option anbieten, die sie anfordern können, und sie auch über Filterdienste und -produkte Dritter informieren, die Endnutzern zur Verfügung stehen.

Die Eigentümer von Mailservern sollten für eine ordnungsgemäße Sicherung ihrer Servers sorgen, so dass diese nicht zur Weiterleitung offen stehen (sofern dies nicht gerechtfertigt ist). Das Gleiche gilt für offene Proxyserver.

5. AUFKLÄRUNGSMASSNAHMEN

Dieser Abschnitt über Fragen der Aufklärung umfasst vorgeschlagene Maßnahmen in Bereichen wie Vorbeugung, Aufklärung der Verbraucher, Berichterstattung.

5.1. Diskussion

Die EU-Mitgliedstaaten sollten die neue Zustimmungsregelung für unerwünschte elektronische Post bis spätestens 31. Oktober 2003 in ihr nationales Recht umgesetzt haben. Dieses neue Konzept fand zwar einigen Widerhall in der Presse, doch ist den Marktbeteiligten und den Bürgern vielleicht immer noch nicht ganz deutlich, was die Zustimmung in der Praxis tatsächlich bedeutet.[38]

Das neue Konzept stützt sich darauf, dass der Nutzer selbst entscheiden kann, ob er Werbemitteilungen erhalten will oder nicht. Damit er dies kann, muss er jedoch die für unerwünschte Mitteilungen geltenden Grundregeln kennen und wissen, wo er Probleme melden kann.

Empfehlenswerte Verfahren

Die ‚Information Commission' des VK (die Datenschutzbehörde des VK) hat wenige Wochen vor Inkrafttreten der neuen Verordnungen zur Umsetzung der Richtlinie einen Leitfaden veröffentlicht, in dem die neuen, im VK geltenden Regeln erläutert werden und der auch einen Sonderteil über die Werbung auf elektronischem Wege enthält. Die Information Commission kündigte auch an, Beschwerdeformulare würden online und in ihrem Amt zur Verfügung stehen, sobald die neuen Vorschriften in Kraft treten, und die wahrscheinlich erforderlichen Informationen erläutern.[39]

Alle Nutzer müssen die Risiken verstehen, die mit dem Hinterlassen ihrer persönlichen Daten im Internet (z. B. nach dem Verlassen von Webseiten, Usenet) verbunden sind, und sollten ihr Verhalten entsprechend anpassen.

Schließlich müssen sie auch wissen, welche Filterprogramme auf dem Markt sind und was Dienste- und Softwareanbieter (z. B. Internet- und E-Mail-Anbieter) für sie tun können.

Empfehlenswerte Verfahren

Die ‚Commission National Informatique et Libertés' (‚CNIL'), die französische Datenschutzbehörde, hat auf ihren Webseiten umfangreiche Informationen zu verschiedenen Aspekten von Spam veröffentlicht: Ergebnisse ihrer Erfahrungen mit E-Mail-Briefkästen und Fälle, die an Gerichte weiterverwiesen wurden (siehe weiter unten), einfache Leitlinien zur Spam-Vorbeugung, Informationen über das Melden von Spam, Hinweise auf einschlägige Nutzerverbände usw.

Zwar wurden in den meisten Mitgliedstaaten Aufklärungsmaßnahmen bezüglich der neuen Zustimmungsregelung durchgeführt oder sind geplant, doch diese unterscheiden sich stark in Bezug auf die zeitliche Planung, die Art der gelieferten Informationen, die Zielgruppen und die beteiligten Parteien. Einige Mitgliedstaaten warten jedoch ab, bis ihre Gesetze

---

[38] Hintergrundinformationen zu den Regeln, die nach der Richtlinie 2002/58/EG für unerwünschte Nachrichten gelten, sind im Internet zu finden unter http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited.

[39] Siehe: http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html#guidance.

verabschiedet sind. Wo sie stattfand, trug die öffentliche Konsultation zur Umsetzung der Richtlinie 2002/58/EG zu einer gewissen Aufklärung bei.

Je nach ihren Befugnissen im jeweiligen Mitgliedstaat können verschiedene Stellen für diese Aktivitäten verantwortlich sein (z. B. Datenschutzbehörden, NRB, Verbraucherschutzbehörden, Ombudsmänner). Eine Koordinierung zwischen den verschiedenen zuständigen Behörden besteht (noch) nicht in allen Mitgliedstaaten. In einigen Mitgliedstaaten scheinen Ministerien beteiligt zu sein. Wirtschaftsverbände sind häufig beteiligt, und manchmal beteiligen sich auch Verbraucher- oder Nutzerverbände an diesen Aktivitäten.

Auch Teile der Wirtschaft haben Aufklärungsmaßnahmen auf nationaler, europäischer oder weltweiter Ebene durchgeführt, obwohl auch hier große Unterschiede bestehen können. Dazu gehören:

– praktische Leitfäden für Direktwerber oder Kampagnen, die sich speziell an die Kommunikationsbranche richten;

– allgemeine Informationen für Verbraucher über Verhaltenskodizes, Beschwerdeverfahren und Filterung;

– Foren bzw. Arbeitsgruppen zur Entwicklung empfehlenswerter Verfahren für Werbepost.

5.2. Vorgeschlagene Maßnahmen

Damit der neue Knigge für elektronische Werbepost wirklich gut verstanden wird, sind kurzfristig in allen Mitgliedstaaten umfassende und anhaltende Maßnahmen in Bezug auf Vorbeugung und Durchsetzung nötig. Es sollten praktische Informationen über Vorbeugung, annehmbare Werbepraktiken sowie technische und rechtliche Abhilfen für die Nutzer gegeben werden.

Alle Parteien - von Mitgliedstaaten und zuständigen Behörden über Unternehmen bis zu Verbraucher- und Nutzerverbänden - werden aufgefordert, ihre Aufgabe bei Aufklärungsmaßnahmen zu übernehmen. Diejenigen Mitgliedstaaten und zuständigen Behörden, die dies bisher noch nicht tun, werden aufgefordert, Anfang 2004 Kampagnen einzuleiten oder zu unterstützen.

Was die Art der zu liefernden Informationen betrifft, so sollten die an Unternehmen und/oder Verbraucher gerichteten Maßnahmen Folgendes umfassen:

- Gewährleistung eines grundlegenden, aber weit verbreiteten Verständnisses der neuen Regeln und der Rechte nach diesen Regeln;
- praktische Informationen über zulässige Werbepraktiken nach der Zustimmungsregelung, einschließlich einer Klärung der rechtmäßigen Sammlung persönlicher Daten;
- praktische Informationen, wie Verbraucher Spam vermeiden können (z. B. bezüglich der Verwendung persönlicher Daten);
- praktische Informationen, welche Produkte und Dienste Verbrauchern zur Verfügung stehen, um Spam zu vermeiden (z. B. Filterung, Sicherheit);
- Informationen über praktische Schritte, die Verbraucher unternehmen können, wenn sie mit Spam konfrontiert werden, darunter ggf. auch über Rechtsschutzmechanismen und ADR-Regelungen.

Das Programm „Sicheres Internet“ und Spam

Im Rahmen des Programms Sicheres Internet veröffentlichte die Europäische Kommission eine Aufforderung zur Einreichung von Vorschlägen für Projekte, die sich unter mehreren Leitthemen, z. B. dem Thema Sensibilisierung, mit Spam befassen. Nach der ersten Bewertung im Rahmen dieser Aufforderung ausgewählte Projekte könnten im Mai 2004 anlaufen.

Derzeit erarbeitet die Kommission einen Vorschlag für ein Nachfolgeprogramm, Mehr Sicherheit im Internet, das weitere Maßnahmen fördern soll, die sich mit illegalen und schädlichen Inhalten sowie mit unerwünschten Inhalten wie Spam befassen.

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

Diese Maßnahmen sollten folgende Zielgruppen erreichen:
a) Unternehmen, die an Direktwerbung beteiligt sind oder diese einsetzen,
b) Verbraucher, die E-Mail-Dienste, auch SMS-Dienste, nutzen und
c) Anbieter von E-Mail-Diensten, auch Anbieter mobiler Dienste.

Aufklärungsmaßnahmen sollten über verschiedene Kanäle (nicht nur über das Internet) laufen, damit die unterschiedlichen Zielgruppen auch wirklich erreicht werden. In dieser Hinsicht ist die Einbeziehung der Wirtschaft und der Verbraucherverbände wichtig. Es muss für eine Koordinierung zwischen den verschiedenen möglichen Initiativen gesorgt werden.

Die genannten Maßnahmen sollten sich ggf. auch auf wirksame Verhaltenskodizes für die Wirtschaft, Rechtsschutzmechanismen, Kennzeichnungen (z. B. ‚Gütesiegel') und Zertifizierungssysteme erstrecken.

Die Kommissionsdienststellen informieren auf dem EUROPA-Server bereits über die Grundlagen der Zustimmungsregelung.[40] Sie wird auch Querverweise auf Aspekte der Umsetzung in den Mitgliedstaaten setzen sowie, soweit verfügbar, auf grundlegende Zahlen und Trends in Bezug auf Spam. Die Kommissionsdienststellen werden sich außerdem der Euro-Info-Zentren zur Verbreitung von Informationen über die neuen Regeln bedienen.

SCHLUSSFOLGERUNG

Spam gehört heute zu den wichtigsten Herausforderungen, denen das Internet gegenübersteht. Spam muss an mehreren Fronten bekämpft werden, nicht nur durch eine wirksame Durchsetzung und eine internationale Zusammenarbeit, sondern auch durch Selbstregulierung und technische Lösungen der Wirtschaft sowie durch Aufklärung der Verbraucher. Die in der vorliegenden Mitteilung aufgeführten Maßnahmen sind in der nachstehenden Aufstellung zusammengefasst.

Zwar wird die Kommission diese Bemühungen so weit wie möglich unterstützen, doch obliegt es hauptsächlich den EU-Mitgliedstaaten und deren zuständigen Behörden, der Wirtschaft, den Verbrauchern und Nutzern des Internet und der elektronischen Kommunikationsdienste, auf nationaler und internationaler Ebene ihre Aufgabe zu übernehmen.

Eine integrierte und gleichzeitige Umsetzung der in dieser Mitteilung genannten Maßnahmen, die breite Unterstützung der interessierten Parteien genießen, kann sehr zur Verringerung der Menge an Spam beitragen, der derzeit die Vorteile der elektronischen Post und anderer elektronischer Kommunikationsmittel für unsere Gesellschaft und Wirtschaft untergräbt.

Die Kommission wird - unter anderem über die informelle Arbeitsgruppe zu unerwünschten Mitteilungen - die Durchführung dieser Maßnahmen im Laufe des Jahres 2004 überwachen. Spätestens Ende 2004 wird sie überprüfen, ob zusätzliche oder Korrekturmaßnahmen erforderlich sind.

---

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

ÜBERSICHT ÜBER DIE IN DER MITTEILUNG GENANNTEN MASSNAHMEN

In nachstehender Aufstellung sind die in dieser Mitteilung genannten Maßnahmen zusammengefasst. Maßnahmen der Kommission bzw. der Kommissionsdienststellen sind darin getrennt aufgeführt. Wie bereits angedeutet, hängen die Maßnahmen miteinander auf verschiedene Weise zusammen und sollten so weit wie möglich parallel und integriert durchgeführt werden.

I – Wirksame Umsetzung und Durchsetzung durch die Mitgliedstaaten und zuständigen Behörden

Als Voraussetzung sollten die Mitgliedstaaten die Datenschutzrichtlinie für elektronische Kommunikation, insbesondere die Bestimmungen über unerwünschte Werbung, unverzüglich umsetzen.

Die Mitgliedstaaten und zuständigen Behörden sollten die Wirksamkeit ihrer Durchsetzungsverfahren (Abhilfen und Sanktionen, Rechtsschutzmechanismen, Zusammenarbeit innerhalb der EU sowie mit Drittländern und Überwachung) bewerten. Außerdem sollten die Mitgliedstaaten nationale Strategien entwickeln, um die Zusammenarbeit zwischen Datenschutz- und Verbraucherschutzbehörden sowie NRB sicherzustellen und Überlappungen und Doppelarbeit zwischen einzelnen Behörden zu vermeiden.

Wichtige Maßnahmen der Mitgliedstaaten und zuständigen Behörden in einzelnen Bereichen:

a) Wirksame Abhilfen und Sanktionen

- Schaffung angemessener Möglichkeiten für Spam-Opfer, auf Schadenersatz zu klagen, und Einführung empfindlicher Sanktionen, ggf. einschließlich finanzieller und strafrechtlicher Sanktionen.

- in Mitgliedstaaten ohne verwaltungsrechtliche Abhilfen sollte die Einführung solcher Abhilfen zur Durchsetzung der neuen Regeln erwogen werden;

- Ausstattung der zuständigen Behörden mit den erforderlichen Ermittlungs- und Durchsetzungsbefugnissen.

b) Rechtsschutzmechanismen

- Einführung angemessener Rechtsschutzmechanismen, einschließlich spezieller elektronischer Briefkästen für die Beschwerden der Nutzer;

- Koordinierung der Maßnahmen der verschiedenen beteiligten zuständigen nationalen Behörden.

c) Grenzüberschreitende Beschwerden und Zusammenarbeit bei der Durchsetzung innerhalb der EU

- Nutzung des vorhandenen oder, falls erforderlich, Schaffung eines neuen Verbindungsmechanismus, über den die nationalen Behörden zwecks grenzüberschreitender Durchsetzung innerhalb der EU (Informationsaustausch, gegenseitige Hilfe) zusammenarbeiten können. In diesem Zusammenhang werden der Rat und das Parlament insbesondere in Bezug auf betrügerischen und irreführenden Spam dringend aufgefordert, sich so schnell die möglich auf die vorgeschlagene Verordnung über die Zusammenarbeit beim Verbraucherschutz zu einigen und zu prüfen, inwieweit die Datenschutzrichtlinie für elektronische Kommunikation in den Anwendungsbereich der Verordnung aufgenommen werden sollte.

d) Zusammenarbeit mit Drittländern

- aktive Zusammenarbeit in multilateralen Foren (z. B. OECD) zur Erarbeitung von Lösungen auf internationaler Ebene;

- Stärkung oder Aufnahme bilateraler Zusammenarbeit mit Drittländern;

- Prüfung, zusammen mit der Kommission, welche speziellen Initiativen zur Erleichterung der internationalen Zusammenarbeit möglich sind;

- Zusammenarbeit mit der Privatwirtschaft, um Spammer unter Einhaltung von Rechtsgarantien aufzuspüren.

e) Überwachung

- Gewährleistung, dass sie über alle Informationen und Statistiken verfügen, die sie zur gezielten Ausrichtung ihrer Durchsetzungsbemühungen benötigen, ggf. in Zusammenarbeit mit der Wirtschaft und unter Berücksichtigung der laufenden OECD-Arbeiten zu Messungen

II – Selbstregulierung und technische Maßnahmen der Wirtschaft

Die Marktbeteiligten (z. B. Internet- und E-Mail-Anbieter, Mobilfunkbetreiber, Softwarehäuser, Direktwerber) sollten sich, ggf. in Zusammenarbeit mit Verbraucher- bzw. Nutzerverbänden und zuständigen Behörden, bemühen, die Zustimmungsregelung zur alltäglichen Praxis werden zu lassen. Insbesondere bieten sich folgende Maßnahmen an:

a) Maßnahmen der Selbstregulierung

- Beurteilung und erforderlichenfalls Anpassung der Vertragspraktiken der Diensteanbieter (Internet- und E-Mail-Anbieter, Mobilfunkbetreiber) gegenüber Kunden und Geschäftspartnern; Information der Kunden über Filterung und optional zur Verfügung stehende Filterprogramme oder -dienste

- Anpassung der Praktiken der Direktwerber an die Zustimmungsregelung und möglichst Einverständnis mit speziellen, legalen Verfahren zur Sammlung persönlicher Daten (z. B. Regelungen der ‚doppelten' oder ‚bestätigten' Zustimmung)

- Entwicklung und Verbreitung wirksamer Verhaltenskodizes (z. B. FEDMA-Initiative) im Einklang mit der Zustimmungsregelung, ggf. in Zusammenarbeit mit der Datenschutzgruppe nach Artikel 29 oder den zuständigen nationalen Behörden

- möglicherweise Verwendung von Kennzeichnungen für der Zustimmungsregelung entsprechende elektronische Post oder Datenbanken, damit Nutzer (und Filter) diese besser erkennen können, im Einklang mit der Richtlinie über den elektronischen Geschäftsverkehr

- Anwendung oder erforderlichenfalls Schaffung wirksamer Selbstregulierungs-Rechtsschutzmechanismen und alternativer Streitbeilegungsverfahren (ADR), wobei so weit wie möglich auf bestehenden Initiativen (z. B. EEJ-NET) aufzubauen ist

b) Technische Maßnahmen

- (Die Anbieter von Filterprogrammen) müssen sicherstellen, dass ihre Systeme mit der Zustimmungsregelung und anderen Anforderungen des EU-Rechts - auch solcher in Bezug auf die Vertraulichkeit von Nachrichten - vereinbar sind. Die Mitgliedstaaten und die zuständigen Behörden werden aufgefordert, die rechtlichen Bedingungen - einschließlich der Erfordernisse bezüglich des Schutzes der Privatsphäre - zu klären, unter denen in ihrem Land verschiedene Arten von Filterprogrammen eingesetzt werden können.

- (Die Anbieter von Filterprogrammen) müssen die Auswirkungen berücksichtigen, die ‚falsche Positive' oder ‚falsche Negative' sowie gewisse Formen der Filterung aufgrund von Inhalten für die Nutzer haben und welche Haftungsfragen sich daraus ergeben können. Die Nutzer sollten die Möglichkeit erhalten, je nach ihren eigenen Bedürfnissen selbst zu bestimmen, wie eingehende Spam-Nachrichten behandelt werden.

- (Die Anbieter von Filterprogrammen) sollten mit interessierten Parteien zusammenarbeiten, um Techniken zur Erkennung legitimer elektronischer Werbenachrichten (die vom Gemeinschaftsrecht anerkannten Werbepraktiken entsprechen) zu entwickeln, wie etwa Kennzeichnungen.

- (Die Anbieter von E-Mail-Diensten und ggf. mobiler Dienste) sollten ihren Kunden Filterfunktionen oder -dienste als Option anbieten, die sie anfordern können, und sie auch über Filterdienste und -produkte Dritter informieren, die Endnutzern zur Verfügung stehen.

- (Die Eigentümer von Mailservern) sollten für eine ordnungsgemäße Sicherung ihrer Servers sorgen, so dass diese nicht zur Weiterleitung offen stehen (sofern dies nicht gerechtfertigt ist). Das Gleiche gilt für offene Proxyserver.

III – Aufklärungsmaßnahmen durch Mitgliedstaaten, Wirtschaft und Verbraucher- bzw. Nutzerverbände

Diejenigen Mitgliedstaaten und zuständigen Behörden, die dies bisher noch nicht tun, werden aufgefordert, Anfang 2004 Kampagnen einzuleiten oder zu unterstützen.

Alle Parteien - von Mitgliedstaaten und zuständigen Behörden über Unternehmen bis zu Verbraucher- und Nutzerverbänden – sollten aktiv praktische Informationen über Vorbeugung, zulässige Werbepraktiken sowie technische und rechtliche Abhilfen für die Nutzer geben. Insbesondere sollten sie

- gezielte Maßnahmen durchführen für a) Unternehmen, die an Direktwerbung beteiligt sind oder diese einsetzen, b) Verbraucher, die E-Mail-Dienste, auch SMS-Dienste, nutzen und c) Anbieter von E-Mail-Diensten, auch Anbieter mobiler Dienste;

- Unternehmen und/oder Verbrauchern Folgendes vermitteln:

– ein grundlegendes, aber weit verbreitetes Verständnis der neuen Regeln und der Rechte nach diesen Regeln;

– praktische Informationen über zulässige Werbepraktiken nach der Zustimmungsregelung, einschließlich einer Klärung der rechtmäßigen Sammlung persönlicher Daten;

– praktische Informationen, wie Verbraucher Spam vermeiden können (z. B. bezüglich der Verwendung persönlicher Daten);

– praktische Informationen, welche Produkte und Dienste Verbrauchern zur Verfügung stehen, um Spam zu vermeiden (z. B. Filterung, Sicherheit);

– Informationen über praktische Schritte, wenn sie mit Spam konfrontiert werden, darunter ggf. auch über Rechtsschutzmechanismen und ADR-Regelungen.

- ggf. auf wirksame Verhaltenskodizes für die Wirtschaft, Rechtsschutzmechanismen, Kennzeichnungen (z. B. ‚Gütesiegel') und Zertifizierungssysteme hinweisen;

- diese Aufklärungsmaßnahmen über verschiedene Kanäle (online und offline) laufen lassen, damit die unterschiedlichen Zielgruppen auch wirklich erreicht werden.

In dieser Hinsicht ist die Einbeziehung der Wirtschaft und der Verbraucherverbände wichtig. Es muss für eine Koordinierung zwischen den verschiedenen möglichen Initiativen gesorgt werden.

IV – Maßnahmen der Kommission bzw. der Kommissionsdienststellen

Die Kommission wird - unter anderem über die informelle Arbeitsgruppe zu unerwünschten Mitteilungen - die Durchführung dieser Maßnahmen im Laufe des Jahres 2004 überwachen und spätestens Ende 2004 überprüfen, ob zusätzliche oder Korrekturmaßnahmen erforderlich sind.

Ganz allgemein wird die Kommission die Umsetzung der Richtlinie weiterhin genau überwachen. Insbesondere wird sie darauf achten, dass die nationalen Umsetzungsmaßnahmen empfindliche Strafen vorsehen, ggf. einschließlich finanzieller Sanktionen und strafrechtlicher Maßnahmen. (Im November 2003 hat die Kommission Verstoßverfahren gegen mehrere Mitgliedstaaten eingeleitet, die keine nationalen Umsetzungsmaßnahmen gemeldet haben.) Die Kommissionsdienststellen sind bereit, den Mitgliedstaaten erforderlichenfalls zu helfen.

Die Kommissionsdienststellen haben mit Unterstützung der Mitgliedstaaten und der Datenschutzbehörden eine informelle Online-Arbeitsgruppe zu unerwünschten Mitteilungen ins Leben gerufen. Diese Gruppe wird die Bemühungen um eine wirksame Durchsetzung (z.B. Beschwerden, Abhilfen, Sanktionen, internationale Zusammenarbeit) vereinfachen und die anderen, in dieser Mitteilung genannten Maßnahmen erleichtern.

Die Kommissionsdienststellen werden die Datenschutzgruppe nach Artikel 29 auffordern, so rasch wie möglich zu einigen Konzepten Stellung zu nehmen, die in der Datenschutzrichtlinie für elektronische Kommunikation verwandt werden, um zu einer einheitlichen Anwendung der nach dieser Richtlinie getroffenen nationalen Maßnahmen zu kommen.

Die Kommissionsdienststellen haben damit begonnen, zusammen mit den Mitgliedstaaten und den nationalen Strafverfolgungsbehörden zu untersuchen, wie die Vorschriften am besten grenzüberschreitend innerhalb der EU und in Drittländern durchgesetzt werden können. Diese Zusammenarbeit mit den nationalen Behörden wird 2004 fortgesetzt.

Die Kommission wird europaweite Online-Kodizes für die Direktwerbung und ggf. ihre Billigung durch die Datenschutzgruppe nach Artikel 29 unterstützen.

Weiter wird die Kommission im Februar 2004 eine OECD Arbeitstagung über Spam veranstalten und mit den Mitgliedstaaten Nachfolgemaßnahmen erörtern, einschließlich Arbeiten im Rahmen der OECD zur Förderung international wirksamer Rechtsvorschriften, zur allgemeinen Kenntnis der Probleme, zu technischen Lösungen, zur Selbstregulierung und zur internationalen Zusammenarbeit bei der Durchsetzung.

Auch wird die Kommission prüfen, wie sie die Ergebnisse des 2003 abgehaltenen Weltgipfels über die Informationsgesellschaft im Hinblick auf den 2005 in Tunis geplanten Gipfel am besten umsetzen kann.

Im Rahmen des Programms Sicheres Internet veröffentlichte die Kommission eine Aufforderung zur Einreichung von Vorschlägen für Projekte, die sich unter mehreren Leitthemen mit Spam befassen. Derzeit erarbeitet sie einen Vorschlag für ein Nachfolgeprogramm, Mehr Sicherheit im Internet, das weitere Maßnahmen fördern soll, die sich unter anderem mit Spam befassen.

Die Kommissionsdienststellen werden auf dem EUROPA-Server weiter grundlegend über die Zustimmungsregelung informieren. Sie wird auch Querverweise auf Aspekte der Umsetzung in den Mitgliedstaaten setzen sowie, soweit verfügbar, auf grundlegende Zahlen und Trends in Bezug auf Spam. Die Kommissionsdienststellen werden sich außerdem der Euro-Info-Zentren zur Verbreitung von Informationen über die neuen Regeln bedienen.