DEUTSCHER BUNDESTAG Ausschussdrucksache 15(9)**1848**
Ausschuss für
Wirtschaft und Arbeit 15. April 2005
15. Wahlperiode

Materialien

zur öffentlichen Anhörung in Berlin am 18. April 2005 zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Zusammenstellung der schriftlichen Stellungnahmen

Deutscher Bundestag
15. Wahlperiode
Ausschuss für Wirtschaft und Arbeit
(9. Ausschuss)

13. April 2005

Sekretariat des Ausschusses: ☎32487
Sitzungssaal: ☎31487, 31483
Fax: 30487

Mitteilung

Tagesordnung

89. Sitzung des
Ausschusses für Wirtschaft und Arbeit
am Montag, dem 18. April 2005, 13.00 – 15.00 Uhr
10557 Berlin, Marie-Elisabeth-Lüders-Haus, Sitzungssaal 3.101

Vorsitz: Abg. Dr. Rainer Wend

Einziger Punkt der Tagesordnung

Öffentliche Anhörung von Sachverständigen

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN **Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz)** (BT-Drucksache 15/4835) Hierzu Ausschussdrucksachen/BT-Drucksachen: 15/2655, 15(9)1722	***Ausschuss für Wirtschaft und Arbeit*** *(federführend)* *Innenausschuss* *Rechtsausschuss* *Ausschuss für Verbraucherschutz, Ernährung und Landwirtschaft* *Ausschuss für Kultur und Medien*
b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU **Spam effektiv bekämpfen** (BT-Drucksache 15/2655) Hierzu Ausschussdrucksachen/BT-Drucksachen: 15/4835	***Ausschuss für Wirtschaft und Arbeit*** *(federführend)* *Innenausschuss* *Rechtsausschuss* *Haushaltsausschuss* *Ausschuss für Verbraucherschutz, Ernährung und Landwirtschaft* *Ausschuss für Kultur und Medien*

Dr. Rainer Wend
Vorsitzender

A n l a g e

Teilnehmer

- Verbraucherzentrale Bundesverband
- AOL Deutschland GmbH & Co. KG
- T-Online International AG
- eco Electronic Commerce Forum – Verband der deutschen Internetwirtschaft e. V.
- Deutscher Industrie- und Handelskammertag, Frau Rechtsanwältin Reppelmund
- Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e. V.
- Heise Zeitschriften Verlag GmbH & Co. KG
- Frau RA'in Dr. Irini E. Vassilaki, Deutsche Gesellschaft für Recht und Informatik e. V., Universität Karlsruhe, Sachverständige für Strafrecht
- Herr Rechtsanwalt Niko Härting, Kanzlei Härting
- Herr Rechtsanwalt Matthias Hartmann, HK2 Rechtsanwälte

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1849**

8. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Verbraucherzentrale Bundesverband vzbv

Zusammenfassung:

Der vzbv begrüßt die Initiative der Bundestagsfraktionen von SPD und Bündnis 90/ Die Grünen, einen erweiterten gesetzlichen Regelungsrahmen gegen die weiter zunehmende Versendung unerwünschter kommerzieller Werbung per elektronischer Post zu schaffen.

Die Einführung eines Ordnungswidrigkeitentatbestandes nur für den Fall einer Verschleierung der Absenderinformationen oder des kommerziellen Charakters einer Nachricht wird nach Auffassung des vzbv jedoch nicht zu einer wirksameren Verfolgung von Spammern und zum besseren Schutz der Nutzer führen.

Vielmehr sollte jegliches Übersenden unverlangter kommerzieller Werbung per elektronischer Post als Ordnungswidrigkeit eingestuft werden.

Das Versenden von Spam-Mails, bei denen Angaben zur Absenderidentifikation oder zum Charakter der Nachricht in Kopf- und Betreffzeile vorsätzlich so gestaltet sind, dass der Empfänger über die wahre Identität des Absenders oder den Charakter der Nachricht keine oder irreführende Angaben erhält, sollten als Straftatbestand qualifiziert werden. Dies gilt ganz besonders für solche Nachrichten oder Angebote in Telediensten, bei denen die Empfänger über den wahren Absender oder Anbieter getäuscht und dadurch verleitet werden, geheime Informationen preiszugeben, die von Dritten zur Täuschung im Rechtsverkehr genutzt werden können (sog. Phishing und Spoof-Attacken).

Des weiteren sollte eine im Gesetz klar bezeichnete, mit entsprechenden Kompetenzen und Sanktionsmöglichkeiten ausgestattete zentrale Stelle auf der Bundesebene für die Verfolgung und Ahndung von Verstößen gegen dieses Gesetz beauftragt werden.

Schließlich sollte zur Bekämpfung der Ursachen von Spam die Sammlung persönlicher Daten durch Unternehmen durch eine Reform des Teledienstedatenschutzgesetzes an strengere Voraussetzungen geknüpft werden. Jede Zusendung kommerzieller elektronischer Werbung muss an eine freiwillige und ausdrückliche Einwilligung des Adressaten gebunden sein (Opt-In). Die Einschränkung des § 7 Abs. 3 UWG sollte daher aufgehoben werden.

I. Vorbemerkung

Das Versenden unverlangter kommerzieller Werbung in Form von E-Mails (sog. Mail-Spamming) ist nicht nur ein lästiges Übel. Es wird mittlerweile als ernsthafte Bedrohung für die auch politisch gewünschte breitere Nutzung des elektronischen Rechts- und Geschäftsverkehrs angesehen. Hierauf deuten nicht zuletzt die vielfältigen Bemühungen auf internationaler, europäischer und nationaler Ebene hin, eine möglichst gemeinsame Basis für wirksamere Gegenmaßnahmen zu schaffen.

In diesen Kontext reiht sich auch das vom Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft (BMVEL) initiierte Projekt eines „Aktionsbündnis gegen Werbemüll im Internet“ ein. Das Projekt wurde am 15. März 2005 vom BMVEL gemeinsam mit dem Verbraucherzentrale Bundesverband (vzbv) e.V., der Zentrale zur Bekämpfung unlauteren Wettbewerbs (WBZ) und dem Verband der Deutschen Internetwirtschaft (eco e.V.) der Öffentlichkeit vorgestellt. Im Rahmen dieses Bündnisses sollen das fachliche Wissen und die technischen Möglichkeiten der Internetwirtschaft genutzt werden, um Spam-Mails im Einzelfall bis zu ihrem tatsächlichen Absender zurückzuverfolgen. Der vzbv und die Wettbewerbszentrale werden dann auf der Grundlage die-

ser vom eco e.V. gelieferten Daten juristisch, d.h. insbesondere mit Hilfe der Verbandsklage, zunächst gegen Spam-Versender und ihre Auftraggeber in Deutschland vorgehen. Die Bemühungen des Aktionsbündnisses könnten durch eine verbesserte Gesetzeslage, also auch durch einen auf Spamming erweiterten Ordnungswidrigkeiten- bzw. Straftatbestand, wirksam unterstützt werden.

Trotz der in Deutschland bestehenden gesetzlichen Bestimmungen gegen unverlangte Werbung (UWG) sind die Versuche des vzbv, gegen Spamming im Internet vorzugehen, in der Vergangenheit weitgehend gescheitert. Dies liegt im Wesentlichen daran, dass sich der vzbv in den Fällen, in denen die Absenderangaben verschleiert waren und / oder die Absender aus dem Ausland heraus operierten, nicht in der Lage sah, mit eigenen Mitteln den tatsächlichen Absender der Mails ausfindig zu machen, oder eine Rechtsdurchsetzung im Sitzland des Spammers unmöglich war. Für in Deutschland versandte Mails wird durch das Aktionsbündnis voraussichtlich eine effektivere Verfolgung von Spammern möglich sein.

Für eine grenzüberschreitende Rechtsdurchsetzung fehlt es an entsprechenden internationalen Vereinbarungen und einer wirksamen Kooperation der für die Verfolgung und Durchsetzung zuständigen Behörden und privaten Organisationen.

Erste konkrete Schritte zu einer engeren Zusammenarbeit auf internationaler Ebene sind die entsprechenden Aktivitäten der OECD und der EU. Hierzu zählt zum Beispiel der „London Action Plan“. Dieser wurde Ende 2004 in London unter der Schirmherrschaft des britischen „Office for Fair Trading (OFT)“ und der amerikanischen „Federal Trade Commission (FTC)“ durch Vertreter von Regierungsstellen in 15 Ländern verabschiedet und unterzeichnet. Ziel ist es dabei, internationale Verbindungen aufzubauen, um Spam und die damit verbundenen Probleme gemeinsam besser zu bewältigen. Allerdings sollten auch Verbraucher- und vergleichbare Organisationen, die sich im Kampf gegen Spam engagieren, gleichberechtigt in das Netzwerk eingebunden werden. Das ist bislang nicht der Fall.

Um die Mitarbeit in internationalen Netzwerken zur Bekämpfung von Spam zu verbessern, sollte parallel dazu auf der nationalen (Bundes)Ebene eine zentrale Zuständigkeit zum Beispiel bei der Regulierungsbehörde für Post und Telekommunikation (RegTP) geschaffen werden. Diese könnte dann auch als Ansprechpartner für ausländische Behörden und andere Organisationen dienen.

Zum Gesetzentwurf:

Der aktuelle Gesetzesvorschlag der Koalitionsfraktionen sieht eine Erweiterung der Regelungen des Teledienstegesetzes vor. Er stellt das Verschleiern oder Verheimlichen von Absenderangaben und/ oder des kommerziellen Charakters einer Nachricht unter ein gesetzliches Verbot und führt einen Ordnungswidrigkeitentatbestand für den Fall eines Verstoßes gegen dieses Verbot ein.

Wenngleich der vzbv die Initiative der Bundestagsfraktionen von SPD und Bündnis 90/ Die Grünen von ihrer Zielrichtung her ausdrücklich unterstützt, werden die dort vorgeschlagenen Maßnahmen allein kaum die gewünschte Wirkung entfalten können.

Darüber hinausgehende Änderungs- und Ergänzungsvorschläge des vzbv dazu sind deshalb nachfolgend erläutert und durch Verbesserungsvorschläge konkretisiert.

II. Anmerkungen im Einzelnen

Erweiterter Auskunftsanspruch

Bewertung:

Die Erfahrungen des vzbv und der Wettbewerbszentrale in den vergangenen Jahren haben gezeigt, dass allenfalls in Fällen, in denen ein erkennbarer Absender in Europa involviert ist, eine Chance besteht, gegen diesen auf der Basis des UWG vorzugehen.Diese Voraussetzung ist aber in den wenigsten Fällen gegeben.

So werden oft Relay-Server genutzt und zusätzlich die Herkunft und die Absenderangaben verheimlicht oder verschleiert. Ohne Hilfe der Internet Provider (ISP) und der dort vorliegenden **Verbindungsdaten** sind die wahren Absender aber nicht zu ermitteln, da die ISP aufgrund der in Deutschland geltenden Rechts- und Gesetzeslage im Fall einer Ordnungswidrigkeit diese Daten ohne konkreten Auskunftsanspruch nicht an Dritte weitergeben dürfen. Auch der Auskunftsanspruch nach § 13 Unterlassungsklagengesetz bezieht sich lediglich auf Bestandsdaten.

Vorschlag:

Ergänzend zu den nachfolgenden Vorschlägen zu den §§ 7 und 12 TDG wird vorgeschlagen, im TDG einen erweiterten Auskunftsanspruch gegenüber Internet Service Providern zu schaffen, aufgrund dessen bei der behördlichen Nachforschung nicht nur die Bestands-, sondern erforderlichenfalls auch die Verbindungsdaten abgefragt werden könnten, die ein Spam-Versender im Einzelfall hinterlässt.

Informationspflichten(§ 7 TDG n.F.)

Bewertung:

Die in § 7 TDG n.F. vorgesehene subjektive Tatbestandsseite, wonach die Kopf- oder –Betreffzeile absichtlich im Sinne des Satzes 1 verheimlicht oder verschleiert sein muss, hält der vzbv für kritisch. Laut amtlicher Begründung soll mit dieser Voraussetzung an die subjektive Tatbestandsseite eines absichtsvollen Handelns verhindert werden, dass kleine und mittlere Unternehmen als Spammer sanktioniert werden, wenn sie in ihren kommerziellen Kommunikationen die Kopf- und Betreffzeile lediglich aus Unkenntnis nicht hinreichend deutlich formulieren und somit ohne Verschleierungs- und Verheimlichungsabsicht gehandelt haben.

Wir halten diese Einschränkung für ungerechtfertigt. Denn auch solche Unternehmen dürfen sich nicht der Verpflichtung entziehen können, sich vor dem Versand von elektronischer Werbung entsprechend rechtskundig zu machen. Abgesehen davon dürfte der Nachweis des absichtlichen Handelns in den meisten Fällen gar nicht zu erbringen sein. Es müsste demnach davon ausgegangen werden, dass Spammer oder deren Auftraggeber den Einwand einer fehlenden Absicht als Schutzbehauptung vortragen werden.

Außerdem wäre zum Schutze kleiner oder mittelständischer Unternehmen gem. § 12 Abs. 2 TDG n.F. eine „Entlastung“ in Fällen „weniger sanktionswürdigen

Unrechts“ insoweit möglich, dass die betreffende Ordnungswidrigkeit gar nicht oder mit einer sehr geringen Geldbuße geahndet werden kann.

Schließlich sei auf die Widersprüchlichkeit der vorgeschlagenen Formulierungen zum subjektiven Tatbestand in den §§ 7 und 12 TDG n.F. hingewiesen: So handelt laut § 12 Abs. 1 TDG n.F. auch derjenige ordnungswidrig, der in vorsätzlicher oder fahrlässiger Weise gegen die allgemeinen Informationspflichten nach § 6 Satz 1 verstößt. Hingegen wird in § 7 Nr. 3 Satz 2 des Neuentwurfs eine absichtliche Gestaltung der Kopf- oder Betreffzeile derart vorausgesetzt, dass der Empfänger keine oder irreführende Angaben über die Identität des Anbieters/ Versenders erhält.

Diese unterschiedlichen Vorgaben hätten zur Folge, dass eine Bußgeldbewehrung nach § 12 TDG n.F. an weniger enge subjektive Tatbestandsvoraussetzungen geknüpft wäre als der Tatbestand des § 7 Nr. 3 selbst. Eine Tathandlung kann aber nicht gleichzeitig fahrlässig und absichtlich begangen werden.

Forderung:

Der vzbv hält die Streichung der subjektiven Tatbestandsvoraussetzung in § 7 Ziffer 3, d.h. die Streichung des Wortes „absichtlich“, für dringend erforderlich.

Bußgeldvorschriften (§ 12 TDG n.F.)

Bewertung:

In Erweiterung der bestehenden Regelungen des UWG für unverlangte kommerzielle Wer-bung sieht der Vorschlag zum Teledienstegesetz ein Verbot der Verschleierung oder Verheimlichung des Absenders und/oder des kommerziellen Charakters einer Nachricht vor.

Die negativen Effekte bzw. wirtschaftlichen Schäden durch Spam im Internet entstehen aber schon dadurch, dass Nachrichten eines Absenders zum selben Zeitpunkt in großer Zahl über das Internet versandt werden. Hierdurch werden die Internet Service Provider (ISP) organisatorisch und ggf. kostenmäßig belastet, was wiederum zu einer zusätzlichen Kostenbelastung auf Seiten der Endnutzer führen kann.

Die zunehmende Belästigung durch unverlangte elektronische Werbung aller Art wird nicht zuletzt auch durch die geltende Rechts- und Gesetzeslage erleichtert. Beispielhaft sei die Öffnungsklausel in § 7 Abs. 3 UWG genannt, nach der im Rahmen einer bestehenden Vertragsbeziehung und unter bestimmten Voraussetzungen Kundenwerbung zulässig ist.

Schließlich sehen wir in der Beschränkung des gesetzlichen Verbots auf solche E-Mails mit verschleierten oder verheimlichten Absenderangaben in den Kopf- und Betreffzeilen ein Hindernis für eine breitere und effektivere Spam-Bekämpfung.

Vorschlag:

In Ergänzung des Tatbestands der Wettbewerbswidrigkeit gem. § 7 Abs. 2 UWG sollte jegliche Übersendung unerwünschter kommerzieller Werbung via E-Mail mit einem (abgestuften) Bußgeld mit maximal möglichem Abschreckungseffekt belegt werden, das sich der Höhe nach an der Spannweite orientiert, die innerhalb der Europäischen Union bereits besteht.

Eine Bußgeldbewehrung bis höchstens 50.000 Euro halten wir in ihrer abschreckenden Wirkung gegenüber Spammern und deren Auftraggeber für zu niedrig, zumal die Anti-Spam-Gesetze anderer Mitgliedsstaaten der Europäischen Union unserer Kenntnis nach Sanktionszahlungen zwischen 3.000 bis 450.000 Euro vorsehen. Das Telekommunikationsgesetz in seiner Fassung vom 22. Juni 2004 sieht Bußgelder bis 500.000 Euro vor.

Wir schlagen daher eine Heraufsetzung des maximal möglichen Bußgeldbetrages im TDG auf 450.000 Euro vor.

Konkret sollte der § 12 TDG folgendermaßen formuliert werden:

§ 12 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. **entgegen §6 Satz 1 eine Information nicht, nicht richtig oder nicht vollständig verfügbar hält oder**
2. **kommerzielle Kommunikationen per elektronischer Post (E-Mail) ohne die vorherige ausdrückliche Einwilligung der Adressaten gemäß den Vorschriften des Teledienstedatenschutzgesetzes versendet.**

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 450.000 Euro geahndet werden.

Ergänzend dazu sollte die Öffnungsklausel des § 7 Abs. 3 UWG ersatzlos gestrichen werden.

Einführung eines Straftatbestands

Das Versenden von Spam-Mails, bei denen die Empfänger über den wahren Absender oder Anbieter bewusst getäuscht und dadurch dazu verleitet werden, geheime Informationen preiszugeben, die von Dritten zur Täuschung im Rechtsverkehr genutzt werden können (Beispiel: Phishing und Spoof-Attacken im Bereich des Online-Banking), sollte als Straftatbestand qualifiziert werden. Weil Phishing- und Spoof-Attacken im Vorfeld der nachfolgend beabsichtigten Täuschungsdelikte nach geltender Rechtslage nicht strafbar sind, würde durch die vorgeschlagene Maßnahme eine gefährliche Gesetzeslücke geschlossen.

Vorschlag:

Zur Einführung eine Straftatbestandes im Falle verfälschter oder verschleierter Angaben sollte ein neuer § 13 in das TDG mit folgendem Wortlaut aufgenommen werden:

§ 13 TDG – Strafvorschriften

Wer vorsätzlich oder fahrlässig eine elektronische Nachricht so gestaltet, dass der Empfänger über den wahren Absender oder über den Charakter der Nachricht getäuscht wird oder dadurch verleitet wird, geheime Informationen preiszugeben, die Dritte zur Täuschung im Rechtsverkehr einsetzen können, wird mit einer Freiheitsstrafe bis zu ... oder mit einer Geldstrafe bestraft.

Ausdehnung des Klagerechts auf Internet Service Provider

Da die Internet Service Provider im Rahmen des Wettbewerbsrechts keine Möglichkeit haben, gegen Spammer vorzugehen, wäre es auch aus Sicht des

vzbv überlegenswert, den ISP im Rahmen des TDG ein Sonderklagerecht einzuräumen.

Einheitliche Kennzeichnung elektronischer kommerzieller Nachrichten

Es erscheint sinnvoll, dass kommerzielle elektronische Werbung - ähnlich wie die Werbung in den Print- und elektronischen Medien - vom Absender mit einer Art einheitlichem „elektronischem Kennzeichen“ versehen wird. Mittels eines solchen Kennzeichens wäre es dann zum Beispiel dem Internet Service Provider möglich, vor der Weiterleitung an den Adressaten zu prüfen, welcher Art die ankommende Nachricht ist. Im „Missbrauchsfall“ könnte dann mittels entsprechender Systemeinstellungen die Zustellung der Nachricht abgeblockt werden. Auch dem Adressaten würde durch eine einheitliche Kennzeichnung kommerzieller Nachrichten die Einrichtung eines Filters erheblich erleichtert.

Spannungsverhältnis zwischen dem Post- und Fernmeldegeheimnis und der Filterung von Nachrichten durch Unternehmen und Provider

Aufgrund der Vorschriften des Ordnungswidrigkeitengesetzes (§ 46) sind Auskunftsersuchen, die das Post- und Fernmeldegeheimnis verletzen, nicht zulässig. Darüber hinaus dürfen ISP aus dem gleichen Grund (drohende Verletzung des Post- und Fernmeldegeheimnisses) die Zustellung von elektronischen Nachrichten nicht blockieren.

Zwar sollte das Post- und Fernmeldegeheimnis als hohes verfassungsmäßig garantiertes Rechtsgut auf keinen Fall weiter ausgehöhlt werden als bisher schon geschehen.

Es wäre jedoch überlegenswert, eine Regelung ins TDG dahingehend aufzunehmen, dass auf ausdrücklichen (dokumentierten) Wunsch des Empfängers elektronischer Nachrichten (E-Mails) dessen Provider als solche erkennbare (bzw. gekennzeichnete) Werbemails vor der Ablage in das betreffende Postfach ausfiltern kann, ohne mit dem Post- und Fernmeldegeheimnis in Konflikt zu geraten. Dabei könnte die oben vorgeschlagene einheitliche Kennzeichnung kommerzieller elektronischer (Werbe)Post hilfreich sein.

III. Anmerkungen zum Antrag der CDU/CSU Fraktion (BT DS15/2655) vom 9. März 2005:

Der vzbv unterstützt den Vorschlag der CDU/CSU Fraktion, eine zentrale Melde- bzw. Beschwerdestelle im Gesetz zu benennen, die in Kooperation mit den Internetserviceprovidern effektive Maßnahmen gegen Spam - Attacken ergreifen, gegen die Versender und Auftraggeber vorgehen und wirksame Sanktionen erlassen kann. Diese Stelle sollte sinnvoller Weise auf der Bundesebene eingerichtet werden, da von hier aus die Koordinierung mit entsprechenden Stellen im Ausland einfacher und effizienter gestaltet werden könnte. Nach Möglichkeit sollten bereits vorhandene Zuständigkeiten und Strukturen genutzt werden.

Andererseits lehnen wir den Vorschlag ab, die ordnungsrechtliche Verantwortung und die Bußgeldpflicht auch auf die Beworbenen auszudehnen.

Hierdurch würden Opfer von Spam- und Eindringattacken quasi zu Mittätern gemacht.

Es soll nicht bestritten werden, dass auch Internetnutzer in Einzelfällen aus Unwissenheit über die grundlegenden Wirkungsmechanismen der Internetkommunikation und in Verkennung deren Risiken die Verbreitung von Spam über ihren PC begünstigen. Dennoch wäre es unserer Meinung zu weit gehend, die Nutzer mit denselben Sanktionen zu überziehen wie die ursprünglichen Versender der Nachrichten oder diejenigen, die aus kommerziellem Interesse für eine massenhafte Verbreitung der Nachrichten sorgen.

07.04.2005

DEUTSCHER BUNDESTAG Ausschussdrucksache 15(9)**1863**
Ausschuss für
Wirtschaft und Arbeit 13. April 2005
15. Wahlperiode

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

AOL Deutschland

Positionspapier zu Maßnahmen gegen Spam

E-Mails sind der Kern moderner Kommunikation. Sie sind günstig, weltweit verfügbar und nahezu in Echtzeit beim Empfänger. In den letzten Monaten ist jedoch dieses Kommunikationsmittel zunehmend zur Belastung für Anbieter und Nutzer geworden. Allein in den gegenwärtig bis zu 210 Millionen Postfächern des weltweit größten Online-Dienstes AOL landen zunehmend mehr unerwünschte als erwünschte E-Mails.

AOL hat daher bereits seit einiger Zeit den unerwünschten E-Mails, dem sog. „Spam" den Kampf angesagt. Seither beschäftigen sich eine Vielzahl von Mitarbeitern an den AOL-Standorten mit der Eindämmung des Spam-Problems. Dem durch Spam verursachten Wachstum von E-Mails muss ständig durch neue Investitionen in Technik und Personal entgegen getreten werden.

AOL hat das Internet und damit auch die E-Mail-Kommunikation nie bloß als technischen Vorgang, sondern als unverzichtbares Medium verstanden, das unser Leben erleichtern soll. Daher ist es auch oberstes Ziel, die E-Mail-Kommunikation nicht zur Belastung werden zu lassen – weder beim Nutzer noch beim Anbieter.

Aus diesem Grund hat AOL gemeinsam mit der ComputerBild eine Anti-Spam-Kampagne gestartet und beteiligt sich an der Anti-Spam Task Force unter dem Dach des Eco-Verbandes. Ziel ist es, durch Ermöglichung und Anwendung rechtlicher, technischer und aufklärender Maßnahmen, Spam einzudämmen. Dabei ist vorauszuschicken, dass ein 100-prozentiger Spam-Schutz nicht zu gewährleisten ist.

1. Technische Maßnahmen

Um dem massiven Anstieg an Spam Herr zu werden, bedarf es eines technischen Ansatzes. Dieser kann sowohl serverseitig beim Mail-Host-Provider als auch durch den Nutzer selbst erfolgen.

▪ ***Serverseitige Maßnahmen***

Effektivstes Mittel gegen Spam ist die schlichte „Annahmeverweigerung" wie man sie aus der herkömmlichen Briefpost kennt. Dieses kann aus technischen und wirtschaftlichen Gründen nur der Mail-Provider leisten. Deshalb ist dringend erforderlich, die Mail-Provider in die Lage zu versetzen, die zumeist massenweise Versendung einer inhaltsgleichen Mail, die nach den technischen Umständen (Manipulation am „Header" – den Absender- und Übertragungsinformationen) identifiziert werden, gar nicht erst anzunehmen. AOL hat dazu seit Jahren eindeutige Bestimmungen veröffentlicht, wonach die Benutzung der AOL-Server zur Übertragung von Spam untersagt ist. Auf dieser Grundlage wird die Annahme verweigert und dem Absender der Mail – soweit dieser überhaupt erreichbar ist – kenntlich gemacht.

▪ ***Nutzerseitige Maßnahmen***

Da die Einordnung einer E-Mail als Spam nicht immer möglich ist und die Umgehungsversuche der Spammer stets ausgefeilter werden, ist nicht gänzlich zu verhindern, dass Spam-Mails in den elektronischen Postfächern der AOL-Kunden landen.

Daher gibt es bereits in der Version 8.0 der AOL-Zugangssoftware die Möglichkeit, die Mailbox nach Spam zu sortieren. In der Version 9.0 wurde zudem ein gesonderter Spam-Ordner angelegt, in den potentieller Spam – auch nach vom Nutzer ausgewählten Kriterien – abgelegt wird.

Die vorbeschriebenen Maßnahmenbündel stellen eine sehr aufwändige aber auch effektivere Vorgehensweise gegen Spam dar. Die Experten von AOL sind täglich

damit beschäftigt, die Maßnahmen gegen Spam zu optimieren. Die Nutzerinnen und Nutzer erwarten von einem Online-Dienst eine effektive Bekämpfung dieser digitalen Plage.

▪ ***Informationen über Spam-Schutz***

Zusätzlich zu den vorbenannten Maßnahmen werden die AOL-Nutzer über die Ursachen und Risiken von Spam aufgeklärt. Ein umfassendes, redaktionelles Angebot soll die Nutzer dazu anleiten, den richtigen Umgang mit ihren Mail-Adressen zu pflegen und sich in geeigneter Weise gegen Spam zu schützen. Den Nutzern steht es zudem frei, die anbieterseitigen Anti-Spam-Maßnahmen zu erleichtern, beispielsweise in dem sie verdächtige Mails melden.

2. Rechtliche Maßnahmen

AOL begrüßt das Ziel des Gesetzgebers, geeignete rechtliche Rahmenbedingungen zur besseren Spam-Bekämpfung zu schaffen. Der vorliegende Gesetzentwurf ist vom Ansatz zu begrüßen, jedoch mit Blick auf die Effektivität der Maßnahmen teilweise unzureichend oder präzisierbar. AOL kommentiert die einzelnen Vorschriften wie folgt:

▪ **Zu Artikel 1 Anti-Spam-Gesetz**

§ 3 TDG sollte um die wichtigsten Spam-relevanten Definitionen technologieneutral ergänzt werden.

> „7. „Header-Information“ - die einer elektronischen Post beigefügten oder in ihr enthaltenen Übermittlungsinformationen, insbesondere Informationen zu Herkunft, Ziel und Übermittlungszeit.

Die im Gesetzentwurf genannte Formulierung ist auf den Versand von eMails bezogen (Internet-Domain). Die Definition ist jedoch weiter zu fassen, um beispielsweise SMS oder Instant Messenger zu erfassen.

> 8. „elektronische Post“ - jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die einem Kommunikationsnetz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von dem Empfänger abgerufen wird.“

Diese Definition entspricht Art. 2 lit. h der Richtlinie 2002/58/EC. Der in der RL verwendete Begriff elektronische Post ist - über eMail hinaus - gegenüber anderen Spielarten unaufgeforderter elektronischer Werbung offen (z.B. SMS, MMS, Instant Messenging, Fax) offen.

▪ **Zu Artikel 1 Anti-Spam-Gesetz (§ 7 TDG)**

Die Irreführung über den kommerziellen Charakter der Kommunikation ist bereits jetzt in § 7 Nr. 1 TDG erfasst. Es bedarf keiner weiteren Regelung, zumal gemäß § 7 letzter Satz TDG das Verbot der §§ 3, 4 Nr. 3 UWG eingreift.

Die Täuschung über die Identität des Absenders ist bereits im § 7 Nr. 2 TDG erfasst. Eine Sonderregelung für eMail-Kommunikation ist nicht erforderlich.

Daher schlägt AOL vor, § 7 TDG unverändert zu lassen.

▪ **Zu Artikel 1 Anti-Spam-Gesetz (§ 8 TDG)**

Spam ist nicht nur für die einzelnen Internet-Nutzer, sondern auch für ihre Mail-Provider eine enorme Belastung. Deshalb ist es umso dringlicher, dass gerade auch den Providern Rechtssicherheit im Kampf gegen den „E-Müll“ eingeräumt wird.

Zum Hintergrund: Um Belästigungen für Nutzer abzuwehren und um ihre eigenen Systeme zu schützen, setzen Diensteanbieter Filtersysteme ein, die Viren aus der an sie gerichteten elektronischen Post herausfiltern, elektronische Post von unsicheren Systemen zurückweisen oder anhand objektiver Kriterien vom Nutzer unerwünschte kommerzielle Kommunikation zurückweisen bzw. kennzeichnen. Die Zulässigkeit dieser Schutzmaßnahmen ist im Hinblick auf § 206 StGB noch einmal klarzustellen. Zwar hat das OLG Karlsruhe in seiner Entscheidung vom 17. Januar 2005 (Az.: 1 Ws 152/04) festgestellt, dass etwa die Filterung von Viren ein tauglicher Rechtfertigungsgrund für eine Filterung und Abweisung elektronischer Post sein kann. Ein vergleichbare Klarstellung im Hinblick auf die Spam-Filterung ist geboten.

Im Einzelnen sollte Diensteanbietern daher auch rechtssicher möglich sein:

- Anwendung von Filtern, die auf objektive Kriterien bei der Bewertung elektronischer Post als Spam abstellen (z.B. Bayesian Filter)
- Die Möglichkeit der Diensteanbieter eMail, die von offensichtlich unsicheren Systemen herrühren (z.B. fehlende Reverse DNS-Auflösung) oder bereits wegen des massenhaften Versands unerwünschter elektronischer Post bekannt geworden sind (Blacklists) zurückzuweisen. Die Zurückweisung muss während des Kommunikationsvorgangs oder unverzüglich danach erfolgen (z.B. als Fehlerprotokoll sogenannte „error message“).

Aus diesem Grunde schlägt AOL vor, den § 8 TDG, der die Regeln der Verantwortlichkeit einleitet, um einen Absatz zu ergänzen. So soll klargestellt werden, dass und unter welchen Voraussetzungen Provider berechtigt sein sollen, elektronische Post zurückzuweisen.

> § 8 TDG
>
> (3) Diensteanbieter im Sinne der §§ 9 bis 11 sind berechtigt, aufgrund objektiver Kriterien im Einzelfall die an ihre Nutzer gerichtete elektronische Post gegenüber dem einliefernden Diensteanbieter zurückzuweisen, wenn Tatsachen die Annahme rechtfertigen, dass
>
> a. die Systeme des die elektronische Post einliefernden Diensteanbieter oder Nutzers schädliche Software (Viren, Würmer oder Trojaner) versenden oder diese zur massenhaften Versendung unaufgeforderter kommerzieller Kommunikation genutzt werden können;
>
> b. die elektronische Post unaufgeforderte kommerzielle Kommunikation darstellt.
>
> Der Diensteanbieter ist verpflichtet, den einliefernden Diensteanbieter über die Zurückweisung im Rahmen des Kommunikationsvorgangs oder unverzüglich danach zu informieren.“

Entscheidend sollte dabei sein, dass der Mail-Server bzw. das Mail-Konto, von dem aus die Spam-Nachricht versandt wurde, über die Zurückweisung in Kenntnis gesetzt

wird. Dabei ist jedoch zu berücksichtigen, dass regelmäßig Mail-Server und –Konten zum Versand missbraucht werden und die Inhaber davon keine Kenntnis haben. Deshalb schlagen wir im weiteren vor, gerade diese Handlungen ebenfalls zu sanktionieren, da diese gegenwärtig nicht strafbar sind (s.u.)

▪ **Zu Artikel 1 Anti-Spam-Gesetz (§ 12 TDG)**

AOL begrüßt den Vorschlag des Entwurfs, relevante Handlungsweisen zu sanktionieren. Im Wissen um den Ursprung der Spam-Nachrichten, die in der weit überwiegenden Zahl vom Ausland nach Deutschland versandt werden, empfehlen wir die Strafbewehrung und nicht nur die Bußgeldbewehrung. Hintergrund ist die für die Verfolgung von Spammern erforderliche Rechtshilfe auf internationalem Gebiet, die regelmäßig (vor allem im relevanten Nicht-EU-Ausland) das Vorliegen einer Straftat voraussetzt. Die internationale Zusammenarbeit ermöglicht zudem die Aufdeckung der Geldströme und damit die Ermittlung der tatsächlich für den Spam Verantwortlichen. Die Strafbewehrung hat aber neben der Erleichterung der Strafverfolgung auch eine höhere Präventivwirkung zur Abschreckung von Spam-Versendern.

Eine Vielzahl von computer-relevanten Handlungen ist bereits heute strafbewehrt. Jedoch sollen die bestehen Strafbarkeitslücken, die sich Spam-Versender regelmäßig zu Nutze machen, geschlossen werden:

- Eine von Spammern verwendete Verschleierungstechnik ist, ihre e-Mails unter Nutzung fremder Computer zu versenden. Der Zugang zu solchen Computern kann dabei durch so genannte „Trojanische Pferde“ erschlichen worden sein. Diese Programme bringen Nutzer dazu, sie zu starten, indem sie vorgeben, eine vom Nutzer gewünschte Funktion zu erfüllen. Tatsächlich ermöglichen sie einem Dritten - zusätzlich oder anstelle der vorgegebenen Funktion - vollständigen Zugang zu dem Computer des Nutzers.
- Eine weitere, häufiger genutzte Technik ist, e-Mails durch unsichere Übertragungsmöglichkeit (so genannte „open relays“) und die nicht gesicherte Vorauswahl eines Servers (so genannte „open proxies“) zu versenden. In diesem Szenario versendet der Spammer seine e-Mails durch fehlerhaft konfigurierte e-Mail-Server. Der Server löscht oder überschreibt die ursprüngliche Header-Information der e-Mail - also die Informationen, die über die Herkunft Aufschluss geben - und ersetzt diese mit der eigenen. So erweckt der Spam den Eindruck, von dem fehlerhaft konfigurierten Server zu stammen und nicht von dem Diensteanbieter des Spammers. Die unbefugte Nutzung eines fremden Rechnersystems ist allerdings nach geltendem Recht straflos. Das Versenden über einen nicht gesicherten oder von einem Dritten - etwa durch einen Trojaner von Dritten „geöffneten“ eMail Server (Open Relay) stellt keine Leistungserschleichung im Sinne des § 265a StGB dar, da es an einer Überwindung technischer Hindernisse, etwa von Systemen zur Verifikation der Identität des Anmelders mangelt (vgl. Schönke/Schröder, § 265a Rn. 8 mwN).
- Die Tatbestände der §§ 303a, 303b StGB sind weit formuliert und erfassen Angriffe auf Hard- oder Software und insbesondere den Einsatz von Computerviren und „Würmern“. Soweit die Sicherheitslücke von einem Spammer erzeugt worden ist – etwa durch einen Virus (Open Proxy/Relay) oder durch eine Veränderung von Systemen (Hacking) – ist dieser Straftatbestand verwirklicht. Anders ist es, wenn der Hacker eine bereits bestehende Sicherheitslücke eines Systems ohne weitere Veränderung ausnutzen kann, etwa weil das System falsch konfiguriert war (vgl. Frank, zur strafrechtlichen Bewältigung des Spamming, Würzburg 2004, Seite 162).
- Eine weitere Verschleierungstechnik ist die Registrierung von elektronischen Postkonten unter Verwendung einer verfälschten Identität. Dazu richten Spammer häufig automatisch eine Vielzahl von e-Mail-Konten bei Diensteanbietern ein und nutzen diese Konten (die vorgeblich realen Nutzern gehören), um Spam zu versenden. Zudem führt die Irreführung über die Herkunft des Spams nicht nur zu einer unmittelbaren Täuschung des Nutzers, sondern umgeht auch Spam-Filter, die dann diejenigen Domains nicht mehr herauszufiltern können, von denen bekanntermaßen große Mengen Spam ausgehen. Dieses Verhalten ist unlauter, aber straflos. Denn das Ausnutzen einer Registrierungsmöglichkeit für einen eMail-Dienst stellt lediglich eine Übermaßnutzung eines Angebots dar. Ein Erschleichen im Sinne des § 265a Absatz 1 StGB dürfte regelmäßig nicht in Betracht kommen. Allenfalls bei Überwindung technischer Hindernisse, etwa Systemen zur Verifikation der Identität des Anmelders wäre ein Erschleichen denkbar. Gleichwohl ist bei kostenlosen eMail-Diensten (Freemailern) nach geltendem Recht eine Strafbarkeit regelmäßig auch deswegen zu verneinen, weil diese Dienste unentgeltlich angeboten werden und somit die Absicht, ein Entgelt zu ersparen, entfällt.

▪ **Zu Artikel 1 Anti-Spam-Gesetz (§ 13 TDG)**

AOL schlägt daher vor, nicht den § 12 TDG zu ergänzen, sondern einen § 13 TDG einzuführen.

„§ 13

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

a. sich ohne Genehmigung oder unter Überschreitung der Genehmigung des Berechtigten zu einem fremden Computer oder Datennetz Zugang verschafft,

b. elektronische Postadressen, Nutzerkonten, numerischer Internetprotokoll-Adressen, Telefonnummern oder Domain-Namen unter Verwendung einer erheblich verfälschten Identität registriert;

c. sich gegenüber den Betreibern von Telekommunikations- oder Telediensten fälschlich als der registrierte Nutzer numerischer Internet-Protokoll-Adressen, elektronischer Postadressen, Nutzerkonten oder Domain-Namen oder dessen Rechtsnachfolger ausgibt oder

d. in sonstiger Weise die Absender oder Header-Informationen verändert.

und hierdurch seine Identität bei der Versendung kommerzieller Kommunikation verschleiert.

(2) Ebenso wird bestraft, wer die Handlungen nach Absatz 1 zur Förderung des eigenen Handels oder Gewerbes oder zum Zwecke des Absatzes von Waren oder Dienstleistungen ausnutzt.“

Durch die o.g. Einführung eines Straftatbestandes werden besonders schwerwiegende Verstöße gegen die Verpflichtung aus § 7 Nr. 1 TDG sanktioniert.

Für die Wahl dieser Regelungstiefe spricht auch der Vergleich mit anderen für den Bereich rechtswidriger Werbung einschlägigen Vorschriften. Auch die Versendung unzulässiger Werbung auf dem Post- oder Telekommunikationsweg löst nicht grundsätzlich die (wettbewerbsrechtliche) Strafbarkeit des Handelnden aus. Der Werbende macht sich gemäß § 16 UWG vielmehr nur dann strafbar, wenn zu dem Umstand der Versendung ein weiterer Unwertgehalt hinzutritt, so etwa das wahrheitswidrige Versprechen besonderer Vorteile. Dann liegt neben der Belästigung der Werbeempfänger zusätzlich eine Vermögensgefährdung – und damit eine eigenständige, weitere Rechtsgutsverletzung der Betroffenen – vor, die die Eröffnung des strafrechtlichen Handlungsinstrumentariums rechtfertigt. Dieser erhöhte Unwertgehalt liegt in der Nutzung der in § 13 Abs. 1 TDG beschriebenen Praktiken, die darauf abzielen, eine Verfolgung des Verantwortlich nachhaltig zu erschweren.

Die Einführung des Absatzes 2 trägt dazu bei, dass der vom Spamming profitierende Auftraggeber zur Verantwortung gezogen werden kann. Damit erfasst der neue Straftatbestand über den unmittelbar handelnden Spammer hinaus grundsätzlich auch die Personen, die das Spamming in Auftrag gegeben oder in irgendeiner sonstigen Weise gefördert haben. Mit der Sanktionierung der Auftraggeber werden gerade die Personen einbezogen, die den entscheidenden wirtschaftlichen Anreiz für die Versendung unerwünschter elektronischer Mails liefern.

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1844**

8. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

T-Online International AG

Die T-Online International AG teilt die Ansicht der Entwurfsverfasser, dass unerwünschte eMail-Werbung eine ernstzunehmende Erscheinung darstellt, die langfristig das Vertrauen der Verbraucher in die elektronische Kommunikation gefährden kann. Gleichzeitig entsteht ein hoher volkswirtschaftlicher Schaden, da die Provider zur Bewältigung der eMail-Mengen Ihre Leitungen und Speicherkapazitäten unnötig verstärken müssen. Der Einsatz von Maßnahmen zur Verhinderung der weiteren Verbreitung von Spam-eMails ist daher unerlässlich.

T-Online begrüßt die Möglichkeit, zu dem vorliegenden Gesetzentwurf Stellung nehmen zu können.

1. Allgemeine Bewertung

Aufgrund der gravierenden Belästigung der Konsumenten durch das stetig ansteigende Spam-Aufkommen sowohl im beruflichen als auch privaten Umfeld werden mögliche Lösungsansätze und Bekämpfungsstrategien zunehmend auch in der Öffentlichkeit und in der Politik diskutiert. T-Online unterstützt daher das Engagement der Fraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN, die identifizierten Problemfelder im Rahmen des vorliegenden Gesetzesentwurfs anzugehen.

Hierbei gilt es jedoch zu beachten, dass nicht jede eMail mit kommerziellem Charakter als unerwünscht betrachtet und damit als Spam klassifiziert wird. Werbe-eMails haben sich in der Vergangenheit als unkomplizierte und schnelle Form der Informationsversorgung bewährt und werden vom Kunden als solche akzeptiert und gewünscht. Sie unterstützen die Schaffung von Transparenz und ermöglichen den Verbrauchern eine stets aktuelle Marktübersicht. Um die aus direkten Kundenansprachen resultierenden Umsätze seriöser Unternehmen nicht unnötig zu gefährden, müssen zulässige Formen des eMail-Marketings auch weiterhin möglich sein.

Aus diesem Grund ist es notwendig, sich dem Thema differenziert zu nähern und eine Abgrenzung der gewünschten und vom Kunden angeforderten eMails von den tatsächlichen Spam-eMails vorzunehmen.

2. Widersprüche / Klärungsbedarf

Fahrlässiges vs. absichtliches Handeln

T-Online unterstützt die Auffassung, dass die absichtliche Verheimlichung oder Verschleierung der Identität des Absenders einer eMail die für den Empfänger notwendige Transparenz und Entscheidungsfreiheit bei der Bearbeitung seines eMail-Postfachs unterbindet. Aus diesem Grund ist die Einführung eines Bußgeldtatbestands für entsprechende Verstöße zu begrüßen.

Der Gesetzesentwurf sieht weiterhin vor, auch das Verschleiern oder Verheimlichen des kommerziellen Charakters der eMail in der Betreffzeile mit einem Verbot zu belegen. Dies ist aus Sicht der T-Online zwar nicht unbedingt notwendig. Es bleibt jedoch abzuwarten, inwiefern eine Umsetzung dieser Regelung in der späteren praktischen Anwendung zu einer effizienten Eindämmung des Spam-Volumens beitragen kann.

In beiden Fällen muss das Verbot jedoch zwingend auf jene Fälle begrenzt werden, bei denen eine eindeutige Absicht zur Verheimlichung oder Verschleierung vorliegt. Andernfalls könnten unnötigerweise auch solche Versender kriminalisiert werden, die aus reiner Unkenntnis die Kopf- und Betreffzeile ihrer eMails nicht hinreichend aussagekräftig formulieren. In der Begründung zu § 7 Nr. 3 S. 2 TDG-E wird die-

ser Punkt auch richtigerweise durch die Erläuterung umgesetzt, dass es dem Versender darauf ankommen muss, seine Identität oder den kommerziellen Charakter seiner Nachricht zu verheimlichen oder zu verschleiern.

§ 12 TDG-E sanktioniert dagegen bereits das fahrlässige Verhalten. Danach begeht bereits derjenige eine Ordnungswidrigkeit, der fahrlässig entgegen § 7 Nr. 3 TDG-E in der Kopf- und Betreffzeile den Absender oder den kommerziellen Charakter der Nachricht verschleiert oder verheimlicht.

Um Unstimmigkeiten auszuräumen, ist hier eine eindeutige Eingrenzung der Sanktionierung auf das absichtsvolle Handeln vorzunehmen.

Zulässigkeit von Blocking-Maßnahmen

Auf S. 2 des Gesetzesentwurfs wird unter dem Punkt C/Alternativen erläutert, dass „wirksamere Methoden wie beispielsweise das Prüfen der eingelieferten Mails durch den Service-Provider an dem Post- und Fernmeldegeheimnis [scheitern], dem auch diese unterworfen sind."

Auf S. 6 stellt die Begründung hingegen ausdrücklich fest, welche Bedeutung ebendiese Maßnahmen zum Blocken bei der Spam-Bekämpfung haben: „Neben den gesetzlichen Regelungen spielt vor allem die Wirtschaft eine große Rolle bei der Bekämpfung unerwünschter elektronischer Post. Sie kann durch den konsequenten Ausbau technischer Schutzvorrichtungen einen wichtigen Beitrag zur Eindämmung der Spam-Flut leisten. Besondere Bedeutung kommt dabei dem Einsatz von Filterprogrammen zu, deren Aufgabe darin besteht, Spam-Nachrichten zu blockieren." Hier wird ganz richtig erkannt, dass die technische Blocking-Tools einen elementaren und unverzichtbaren Beitrag zur Verringerung des Spam-Aufkommens leisten.

Demzufolge ist der Gesetzesentwurf in diesem Punkt widersprüchlich.

Prinzipiell ist hier zu beachten, dass die Begriffe des Blockens und des Filterns unterschiedliche technische Methoden bezeichnen und dementsprechend differenziert verwendet werden müssen. Aus Sicht der T-Online steht in diesem Zusammenhang das Blokken von eMails im Vordergrund, also die Nicht-Annahme von unerwünschten Massen-Mailings durch die eMail-Systeme der Provider.

Dies vorausgesetzt, sollte der Gesetzgeber klarstellen, dass das Blocken von Spam-eMails entgegen vereinzelter Stimmen in der Rechtsliteratur rechtmäßig ist.

3. Alternative Lösungsansätze zur Spam-Bekämpfung

Das Engagement zur Bekämpfung der Spam-Problematik anhand des vorliegenden Entwurfs zum Anti-Spam-Gesetz ist grundsätzlich zu begrüßen. Jedoch wird diese Verschärfungen des nationalen Rechts das Problem nicht vollständig lösen können, sondern lediglich einen begrenzten Beitrag dazu leisten können. Aufgrund der internationalen Dimension des Spammings kann eine Bekämpfung mit nationalen Rechtsmitteln nicht ausreichend sein.

Vielmehr müssen dem Kunden zusätzliche Mittel zum eigenverantwortlichen Schutz vor Spam zur Verfügung gestellt werden. Dazu zählen die bereits unter Punkt 2 angeführten Blocking-Tools sowie Filtermöglichkeiten, mit denen der Kunde eigenverantwortlich Regeln zum Schutz seines eMail-Postfaches festlegen kann. Gleichwohl gilt es zu verhindern, dass Kunden ihren eMail-Account für den missbräuchlichen Versand von eMails nutzen.

Einen elementaren Bestandteil in der Bekämpfung von Spam stellt auch die Förderung der Medienkompetenz unserer Nutzer dar. Diese müssen im Umgang mit ihren persönlichen Daten sensibilisiert und auf Fehler bei der Nutzung des Internets hingewiesen werden.

4. Fazit

- Die Bekämpfung von Spam ist eine wichtige Voraussetzung, um Kundenvertrauen zu schaffen und zu erhalten. Dabei ist zu gewährleisten, dass nicht jede eMail mit Werbeinhalten als Spam definiert wird. Um die aus direkten Kundenansprachen resultierenden Umsätze seriöser Unternehmen nicht unnötig zu gefährden, müssen zulässige Formen des E-Mail-Marketings auch weiterhin möglich sein.
- Die in dem vorliegende Entwurf zum Anti-Spam-Gesetz enthaltenen Verbote des Verschleierns und Verheimlichens von Absender und kommerziellem Charakter können einen wertvollen Beitrag zur Verringerung des Spam-Aufkommens leisten. Voraussetzung für eine praktikable und wirkungsvolle Umsetzung ist jedoch, dass der Verbotstatbestand sich lediglich auf jene schwere Begehungsformen beschränkt, denen ein absichtsvolles Handeln zugrunde liegt.
- Es wird festgestellt, dass die Blocking-Angebote der Provider die Spam-Massen wirkungsvoll bekämpfen können. Der Entwurf sollte deshalb um eine Klarstellung erweitert werden, dass das Blokken von unerwünschten Massen-eMails rechtmäßig ist.
- Eine Verschärfung der nationalen Rechtslage wird das Spam-Problem aufgrund seiner internationalen Dimension nicht gänzlich lösen können. Es ist daher unerlässlich, dem Kunden zusätzliche technische Lösungsmöglichkeiten anzubieten. Weitere Abhilfe kann durch die Aufklärung des Kunden zum verantwortungsbewussten Verhalten im Netz geschaffen werden.

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1856**

12. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Eco Electronic Commerce Forum - Verband der deutschen Internetwirtschaft e.V.

Einleitung

Der Verband der deutschen Internetwirtschaft begrüßt ausdrücklich, dass die Spam-Problematik, die damit verbundene erhebliche Belastung für Wirtschaft und Verbraucher sowie insbesondere die Gefahr eines Vertrauensverlustes in die Sicherheit elektronischer Kommunikation seit geraumer Zeit in das Bewusstsein der Bundesregierung gerückt ist.

Die im Verband der deutschen Internetwirtschaft organisierten Unternehmen - insbesondere die Internet-Service-Provider - setzen sich bereits seit mehreren Jahren mit den technischen, wirtschaftlichen und rechtlichen Implikationen des Phänomens Spam auseinander und haben erhebliche Mittel in technische und organisatorische Schutzmaßnahmen investiert.

Auf die von eco etablierten nationalen wie internationalen Selbstregulierungsmechanismen wird in der Gesetzesbegründung erfreulicherweise ausdrücklich verwiesen.

Der Verband der deutschen Internetwirtschaft teilt die Auffassung der Fraktionen, wonach der vielschichtige Problematik Spam nur durch eine Kombination aus gesetzlicher Regelung, Schutzmaßnahmen der Wirtschaft, Selbstverpflichtung, Internationaler Zusammenarbeit und Verbraucheraufklärung begegnet werden kann.

Die Einführung einer weiteren, über die wettbewerbsrechtliche Regelung des § 7 UWG hinausgehenden gesetzlichen Regelung, insbesondere die beabsichtigte Einführung eines Ordnungswidrigkeitentatbestandes, hält der Verband der deutschen Internetwirtschaft in der vorliegenden Form jedoch derzeit weder für erforderlich, noch für zielführend.

Vielmehr sind insbesondere die flankierenden Maßnahmen der Wirtschaft auf nationaler und internationaler Ebene und die Verbraucheraufklärung auszubauen und zu fördern.

Darüber hinaus sind zunächst die innerhalb des derzeitigen Rechtsrahmens bestehenden Regelungen auszuschöpfen.

1. Bestehender Rechtsrahmen

In der Begründung des Gesetzesentwurfes wird ausdrücklich auf die zahlreichen zivil- und strafrechtlichen Rechtsgrundlagen verwiesen, aufgrund derer bereits heute die Verschleierung der Identität des Absenders elektronischer Nachrichten sowie die Werbung mittels elektronischer Post ohne Einwilligung des Adressaten wettbewerbsrechtliche Unterlassungsansprüche begründet. Daneben bestehen Schadensersatz- und Unterlassungsansprüche nach den allgemeinen zivilrechtlichen Regelungen (§§ 823, 1004 BGB). Weiter wird im Gesetzentwurf im Falle von strafrechtlich relevanten Inhalten von Spam auf die zahlreichen Straftatbestände verwiesen, die den Strafverfolgungsbehörden Handlungsmöglichkeiten eröffnen.

Sämtlichen Regelungen ist gemein, dass sie insbesondere wegen der Internationalität des Spam-Problems und der Schwierigkeit der Identifizierung der Versender an Grenzen stoßen.

Dies wird auch für jede neue gesetzliche Regelung gelten.

Generelle Kritik an weiteren gesetzlichen Regelungen gegen Spam

Die Identifizierung der Versender als Grundlage für die Durchsetzung zivilrechtlicher Ansprüche und der Strafverfolgung bereitet erhebliche Schwierigkeiten und ist in vielen Fällen gar nicht möglich. Eine Identifizierung ist oftmals nur durch die Kooperation von Spam-

Empfängern und Providern möglich, wie sie gerade im Rahmen des „Aktionsbündnis gegen Spam“ des eco-Verbands, der Bundeszentrale Verbraucherverbände sowie der Zentrale zur Bekämpfung unlauteren Wettbewerbs initiiert worden ist[1].

Dort wo die Versender identifiziert werden können handelt es sich in der absoluten Mehrzahl der Fälle um Absender aus Nicht-EU-Staaten. Die Durchsetzung von zivilrechtlichen Ansprüchen scheitert jedoch ebenso wie die Strafverfolgung in den Fällen, in denen der Spam-Versand aus Ländern erfolgt, in denen dieses Geschäftsgebaren nicht rechtswidrig, zumindest aber nicht justitiabel ist.

So kann zwar in der Praxis beispielsweise gegen einen ausländischen Spam-Versender durch einen deutschen Mitbewerber vor einem deutschen Gericht eine einstweilige Verfügung erwirkt werden, da deutsches Wettbewerbsrecht für alle auf den deutschen Markt wirkenden Wettbewerbshandlungen Anwendung findet. Die Vollstreckung der einstweiligen Verfügung gegen einen ausländischen Versender ist jedoch oft unmöglich bzw. mit einem unverhältnismäßig hohen Aufwand verbunden. Bleibt jedoch die Vollstreckung aus, so hat der Antragsteller die Gerichts- und Anwaltskosten selbst zu tragen.

Vor diesem Hintergrund besteht die Gefahr, dass sich auch die Schaffung eines Ordnungswidrigkeitentatbestandes als stumpfes Schwert erweisen wird, da die zuständigen Ordnungsbehörden in der absoluten Mehrzahl der Fälle nicht in der Lage sein wird, den Versender zu ermitteln bzw. ein verhängtes Bußgeld zu vollstrecken.

2. Selbstregulierungsmaßnahmen der Wirtschaft

Gegenüber weiteren gesetzlichen Regelungen sind nach Überzeugung des Verbands der deutschen Internetwirtschaft Selbstregulierungsmaßnahmen der Wirtschaft insbesondere vor dem Hintergrund des internationalen Aspektes der Spam-Problematik der Vorzug zu geben.

Die in der Begründung zum Gesetzesentwurf genannte, von eco betriebene Hotline kooperiert mit internationalen Hotlines in 19 Staaten und kann daher bei strafrechtlich relevanten E-Mails oder der damit beworbenen Websites auch auf internationaler Ebene agieren.

Weiter wird mit dem vom Verband der deutschen Internetwirtschaft initiierten Projekt „Spotspam“ insbesondere die internationale Verfolgung von Spammern und die Aggregierung von Beschwerden zur Ermöglichung einer effizienten Verfolgung auch über nationale Grenzen hinweg verfolgt.

Darüber hinaus ist mit dem „Aktionsbündnis gegen Spam“ ein weiteres Instrument auf nationaler Ebene geschaffen worden, mit dem Wirtschaft und Verbraucherverbände (VZBV, WBZ und eco) gemeinsam ihre Kräfte und ihr Know-How bündeln. Nach Auffassung der an diesem Bündnis beteiligten Verbände ist die derzeitige Rechtslage durchaus geeignet, um nach erfolgreicher Identifizierung eines deutschen Spam-Versenders Unterlassungsansprüche und gegebenenfalls Schadensersatzforderungen gerichtlich durchzusetzen.

3. Internationale politische Kooperationen

Auch auf politischer Ebene wird verstärkt die internationale Kooperation als geeignetes Mittel zur effektiven Spam-Bekämpfung erkannt.

So haben die mit der Bekämpfung von Spam befassten Behörden aus 13 EU-Staaten einen Informationsaustausch und die grenzüberschreitende Verfolgung von Beschwerden zur europaweiten Bekämpfung der unerwünschten elektronischen Post vereinbart[2]. Sie wollen bei der Untersuchung von Beschwerden über grenzüberschreitenden Spam innerhalb der EU zusammenarbeiten, um die Urheber leichter ermitteln und verfolgen zu können. Während sich Belgien, Griechenland, Italien, Litauen und Zypern für den Anti-Spam-Bund verpflichtet haben, ist die Bundesrepublik Deutschland noch nicht Mitglied.

4. Konkrete Kritik am Gesetzesentwurf

Unabhängig davon, dass der Verband der deutschen Internetwirtschaft eine weitere gesetzliche Regelung zur Bekämpfung von Spam derzeit nicht für erforderlich hält, weist der vorgelegte Gesetzesentwurf verschiedene Mängel auf, die sowohl handwerklicher Natur sind, als auch erhebliches Potential für Rechtsunsicherheit der betroffenen Wirtschaftszweige wie auch der Verbraucher in sich bergen.

Dies liegt zunächst darin begründet, dass die Anti-Spam-Regelungen in die bestehende Vorschrit des § 7 TDG eingearbeitet werden soll. Diese Norm beschreibt neben § 6 TDG allgemeine Informationspflichten und Informationspflichten für elektronische Kommunikation. Diesen Kriterien ist gemein, dass sie positiv das Vorliegen bestimmter Merkmale regeln, während § 7 Satz 1 Nr. 3 TDG-E ein Verbot ausspricht. Die beabsichtigte Regelung ist daher bereits systematisch zumindest nicht ganz ideal getroffen.

Darüber hinaus sind folgende Punkte kritikwürdig:

4.1.

Der Gesetzesentwurf regelt ausschließlich den Versand unerlaubter E-Mail Werbung. Zukünftig wird unerlaubte Massenwerbung jedoch vermehrt auch über SMS-, MMS-, Chat- und Instant Messaging erfolgen. Es wäre daher eine technologieneutrale Regelung wünschenswert, die auch zukünftige Formen der unerlaubten Massenwerbung über andere elektronische Medien erfasst und sämtliche Dienste und Technologien gleich behandelt. Dem entsprechend bezieht sich auch die Regelung des § 7 Abs. 2 Nr. 4 UWG generell auf " Nachrichten". Es ist nicht nachvollziehbar, warum der Anwendungsbereich des TDG-E hinter dem des UWG zurückbleiben sollte. Vielmehr zeigt sich bereits an diesem Punkt, dass das neue UWG hier weiter gefasst ist und es einer engeren Regelung durch ein geändertes TDG nicht bedarf.

4.2.

Der Entwurf bleibt auch unter einem weiteren Aspekt hinter der Regelung des UWG zu unerwünschter elektronischer Kommunikation zurück.

Die Regelung des § 7 Abs. 1 Ziff. 3 UWG knüpft an das Versenden von elektronischer Post mit werbendem Inhalt an, ohne dass eine Einwilligung des Adressaten vorliegt. Bereits in diesem Fall ist ein Unterlassungsanspruch gegeben, ohne das es zwingend zusätzlich auf die in § 7

[1] Vgl. SPIEGEL-ONLINE, http://www.spiegel.de/netzwelt/politik/0,1518,346548,00.html

[2] http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/146&format=HTML&aged=0&language=DE&guiLanguage=en

Abs. 2 Ziff. 4 UWG geregelte Verschleierung oder Verheimlichung des Absenders ankäme.

Dem gegenübersieht der TDG-E im Vergleich zum UWG als einzigen neuen inhaltlichen Aspekt die „Verschleierung der Betreffzeile“ vor. Durch diese Ergänzung werden jedoch in der Praxis keinerlei Spam-Tatbestände erfasst, die nicht ohnehin durch die Regelung des UWG erfasst werden würden. Denn auch im Falle einer verschleierten Betreffzeile wird der Adressat dem Empfang der Nachricht nicht zugestimmt haben. Hat der Empfänger indes dem Empfang der E-Mail zugestimmt und der Absender ist ordnungsgemäß angegeben, so handelt es sich auch im Falle eines verschleierten Betreffs nicht um Spam. Auch insoweit besteht daher kein rechtspolitischer Bedarf für eine Ausdehnung des Tatbestandes.

4.3.

Die Regelung des § 7 Ziff. 3 TDG-E ist aber auch insgesamt zu unbestimmt und inkonsistent. Sie birgt an verschiedenen Stellen die Gefahr erheblicher Rechtsunsicherheit:

4.3.1.

So ist unklar, was genau unter „Kopfzeile“ verstanden wird. Sofern damit nur der sichtbare „Header“ einer E-Mail gemeint ist, bestehend aus Absender-, Empfänger- und Betreffzeile, so wäre dies klarzustellen. Denn unter „Header“ wird die gesamte Kopfzeile einer E-Mail verstanden, die über Sonderfunktionen des jeweils verwendeten E-Mail Programms angezeigt werden kann und weitere Informationen enthält (verwendeter E-Mail-Server, E-Mail-Programm, Message-ID, etc.)[3]. Gerade diese Angaben werden in vielen Fällen ergänzend zu den Angaben in der Absender- und Betreffzeile gefälscht und erschweren so die Identifizierung des Versenders. Auch diese Angaben lassen sich jedoch unter die „Identität des Absenders“ Im Sinne des § 7 Abs. 2 Ziff. 4 UWG subsumieren, so dass eine weitere Regelung nicht erforderlich ist.

4.3.2.

Gemäß der Vorschrift des § 7 Ziff. 3 Satz 2 TDG-E liegt ein Verschleiern oder Verheimlichen insbesondere dann vor, wenn die Kopf- oder Betreffzeile **absichtlich** irreführend gestaltet ist. Dieses subjektive Merkmal wird in der Praxis zum einen kaum nachzuweisen sein. Zum anderen steht es nicht im Einklang mit den in dem Gesetzesentwurf in § 12 TDG-E normierten Bußgeldbestimmungen, in denen lediglich auf **Vorsatz und Fahrlässigkeit** abgestellt wird.

Darüber hinaus ist in § 7 Ziff. 3 Satz 2 TDG-E die Rede von „Kopf- **oder** Betreffzeile“, während in Satz 1 auf „Kopf- **und** Betreffzeile“ abgestellt wird. Hier sollte klargestellt werden, ob es sich um ein Redaktionsversehen handelt oder im Falle der absichtlichen Verschleierung die kumulativen Voraussetzungen gewollt sind, während bei vorsätzlicher und fahrlässiger Begehung die alternativen Tatbestandsmerkmale ausreichen sollen.

4.3.3.

Sofern die Formulierung „…weder der Absender, noch der kommerzielle Charakter…“ in § 7 Ziff. 3 S. 1 TDG-E sowie der Tatbestand in § 12 Abs. 1 Nr. 2 TDG-E alternativ gemeint sein soll, wird dies zu erheblicher Rechtsunsicherheit bei den zahlreichen seriösen Unternehmen führen, die bestrebt sind ausschließlich rechtmäßiges Direktmarkteing und Kundenkommunikation unter vorheriger Einholung der Zustimmung der Empfänger und unter ordnungsgemäßer Angabe des Absenders zu versenden. Dies gilt für nahezu sämtliche großen deutschen Handelsunternehmen, aber auch für Tausende Online-Shops mittelständischer Handelsbetriebe. Diese Unternehmen verschleiern nicht den Absender.

Wann jedoch ein Verschleiern des kommerziellen Charakters einer E-Mail in der Betreffzeile im Sinne des Gesetzesentwurfes vorliegt bzw. bis wann noch nicht von einem solchen Verschleiern ausgegangen werden kann, wird in vielen Fällen nicht eindeutig beantwortet werden können und würde zu einer erheblichen Rechtsunsicherheit hinsichtlich der Gestaltung der Betreffzeile führen.

In den USA wurde dieses Problem im „CAN-SPAM Act“ mit der Verpflichtung der Anbieter zu einer einheitlichen, ausdrücklichen Kennzeichnung als Werbung versucht zu lösen[4]. Da in den USA das sog. Opt-Out-Prinzip verfolgt wird, d.h. grundsätzlich an jedermann Werbung verschickt werden darf, ohne, dass eine Einwilligung des Nutzers vorliegt, muss in den USA Werbung als solche in der Betreffzeile gekennzeichnet werden. Demgegenüber hat sich die EU für die strengere sog. Opt-In-Regelung entschieden, wonach der Nutzer vor der Versendung der Werbung, dem Erhalt ausdrücklich zugestimmt haben muss.

Eine über das Opt-In-Prinzip hinausgehende ausdrückliche Kennzeichnung würde eine erhebliche Einschränkung der seriösen Verwendung von E-Mail zu Marketing- und Kundenkommunikationszwecken bedeuten und insbesondere die Erbringung von werbefinanzierten und dadurch kostenlosen Diensten gefährden. Auch aus diesem Grund ist eine über die bereits bestehende Regelung des novellierten UWG hinausgehende Sanktionierung einer verschleierten Betreffzeile nicht zielführend.

4.3.4

Auch für unbeteiligte Verbraucher und unbeteiligte E-Mail-Provider birgt die gesetzliche Regelung die Gefahr, wegen einer vermeintlichen Ordnungswidrigkeit in Anspruch genommen zu werden. Denn immer mehr Spam-Versender gehen dazu über, Tausende tatsächlich bestehender E-Mai-Adressen von Privatpersonen als Absender zu verwenden, ohne dass diese Personen tatsächlich an dem Vorgang beteiligt sind bzw. überhaupt davon wüssten.

Dazu werden die bei den E-Mail-Providern eingerichteten Accounts von den Versendern „gehijackt“, um massenhaft Mails über die Dienste der Provider unter Missbrauch der E-Mail-Adressen von ahnungslosen Verbrauchern zu versenden.

Dies darf nicht dazu führen, dass sich die eigentlichen Inhaber der Adressen und die Provider Bußgeldern ausgesetzt sehen bzw. es Sache der Provider oder der in Anspruch genommenen Verbraucher ist, sich im Rahmen eines Ordnungswidrigkeitenverfahrens zu entlasten.

4.4.

Grundsätzlich ist zu berücksichtigen, dass die E-Mail-Provider die Infrastruktur bereitstellen, die durch Spam-

[3] Zum Aufbau eines Headers vgl. http://th-h.de/faq/headerfaq.php3#Section_6

[4] vgl. *heise online* vom 16.12.2003, http://www.heise.de/newsticker/meldung/42995

Versender missbraucht werden kann und in vielen Fällen trotz erheblicher Sicherheitsvorkehrungen der Provider auch missbraucht wird.

4.4.1.

Gerade in Fällen der Nichtidentifizierbarkeit oder Nichterreichbarkeit der Urheber rechtswidriger Inhalte jeglicher Art hat sich in der Vergangenheit trotz der grundsätzlichen Haftungsprivilegierung der Provider die Tendenz abgezeichnet, Unterlassungsansprüche gegen Provider durchzusetzen. Spätestens nach der Entscheidung des BGH „Rolex ./. Ricardo“ ist höchstrichterlich entschieden, dass die allgemeinen Grundsätze der Störerhaftung neben den haftungsprivilegierenden Regelungen der §§ 8 – 11 TDG Anwendung finden[5].

Insbesondere im Hinblick auf die Haftung von E-Mail-Providern für die Versendung von Spam über ihre Infrastruktur bedarf es daher dringend einer gesetzlichen Klarstellung dahingehend, dass die Provider diesbezüglich der Haftungsprivilegierung der §§ 8 – 11 TDG unterfallen.

4.4.2.

Darüber hinaus ist aus Sicht der Provider wie auch der Verbraucher die Einführung eines Ordnungswidrigkeitentatbestandes aus einem weiteren Gesichtspunkt ein ungeeigneter Sanktionsmechanismus:

Nach § 14 OWiG wird nicht zwischen Teilnehmer und Täter unterschieden, sondern nach dem OWiG handelt jeder ordnungswidrig, der sich an einer Bußtat beteiligt. Das OWiG geht dabei von dem so genannten Einheitstäter aus. Dabei ist grundsätzlich gleichgültig, in welcher Weise er zur Verwirklichung des Tatbestandes beiträgt.

Dadurch ist grundsätzlich die Ahndung von vermeintlichen Tatbeteiligten möglich, auch wenn ein anderweitig Beteiligter nicht bekannt oder ihm die Bußtat nicht nachzuweisen ist. Selbst wenn die Bußnorm eine bestimmte Tätereigenschaft verlangt, so muss diese besondere Täterqualität nicht bei allen Beteiligten vorliegen. Es genügt, wenn die von der Bußnorm verlangte persönliche Tätereigenschaft bei einem der Beteiligten vorliegt.

Vor dem Hintergrund der in § 12 Abs. 1 TDG-E vorgesehenen vorsätzlichen und **fahrlässigen** Begehungsform ist daher eine Inanspruchnahme der Provider durch die zuständigen Ordnungsbehörden als „fahrlässige Nebentäter“ zu befürchten, wenn nach Auffassung der Behörde die eigentliche Tat objektiv gefördert wird.

Diese Befürchtung besteht insbesondere angesichts des Umstandes, dass die Ordnungsbehörden in der absoluten Mehrzahl der Fälle nicht in der Lage sein werden, des eigentlichen Versenders oder wirtschaftlichen Nutznießers habhaft zu werden.

Im Falle des oben dargestellten „Hijackings“ ist zudem auch aus Verbrauchersicht zu befürchten, dass Bußgelder gegen Verbraucher verhängt werden, deren E-Mail-Accounts von Spam-Versendern mißbraucht wurden und die dadurch gegenüber dem Empfänger als Absender der E-Mail erscheinen.

Auch vor diesem Hintergrund stellt die geplante Regelung eine erhebliche Rechtsunsicherheit dar. Dem müsste durch eine Haftungsprivilegierung der Provider begegnet werden.

5.

Insgesamt ist festzuhalten, dass nach Auffassung des Verbands der deutschen Internetwirtschaft die mit dem Gesetz beabsichtigte „Anti-Spam“-Wirkung aufgrund der nicht zu realisierenden Durchsetzbarkeit des Gesetzes nicht eintreten wird.

Dem gegenüber sind technischen Lösungen, der Verbraucheraufklärung und den Eigeninitiativen der Wirtschaft der Vorzug zu geben, die auf Grundlage der bereits bestehenden gesetzlichen Regelungen effektiv agieren können.

[5] BGH I ZR 304/01, CR 2004, 763

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1864**

13. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Heise Zeitschriften Verlag GmbH & Co. KG

Zusammenfassung:

Aus Sicht des Heise Zeitschriften Verlags ist der vorliegende Gesetzentwurf nur bedingt geeignet, den angestrebten Zwecken Rechnung zu tragen. Das Ziel, „weltweit zur Abschreckung von Spammern“ beizutragen, ist mit nationaler Gesetzgebung ohnehin kaum zu erreichen. Längst ist Spam nicht mehr ein Problem, welches sich ausschließlich mit juristischen Mitteln lösen lässt.

Dessen ungeachtet unterstützt der Heise Zeitschriften Verlag grundsätzlich die mit dem Gesetz angestrebten Ziele, sieht jedoch noch in einigen Punkten Ergänzungs- und Präzisierungsbedarf:

1. Straftat, nicht Ordnungswidrigkeit

Spam ist längst ein internationales Phänomen, das nicht mehr nur von kleinen Unternehmen geprägt wird, die ohne Kenntnis der Rechtslage mal eben kostengünstig für ihr Angebot werben wollen. Der weit überwiegende Teil versandter Spam-Mails kommt längst von hochprofessionalisierten Anbietern, die sich im kriminellen Bereich bewegen. So wird inzwischen der überwiegende Teil des weltweit versandten Spams über so genannte „Zombie-PCs“ verschickt. Darunter versteht man mit Viren und Trojanern infizierte Rechner, die über diese Schadprogramme von Dritten ferngesteuert werden. Ganze Heere dieser Rechner werden zu so genannten „Botnets“ zusammengefasst und zentral gesteuert. Dabei sind Rechnerverbände von 10.000 bis 50.000 Rechnern keine Seltenheit. Diese so zusammengefassten Ressourcen werden von den Betreibern für alle möglichen kriminellen Aktivitäten wie DDoS-Angriffe, Erpressungen, Ausspähen von Passwörtern oder eben auch den Versand von Spam vermietet.

Daher ist das Ziel, Spammer nicht zu kriminalisieren, angesichts der enormen durch Spam verursachten Kosten ebenso wie angesichts der enormen kriminellen Energie auf Seiten der Spammer rechtspolitisch verfehlt. Vielmehr kann man derartigen Handlungsformen allenfalls noch mit den bei der Verfolgung von Straftaten zur Verfügung stehenden Mitteln begegnen.

Doch nicht nur aus diesem Grund ist es nicht ausreichend, in dem Entwurf nur von einer Ordnungswidrigkeit auszugehen. Wichtigstes Mittel zur Ermittlung der Spammer sind die durch den Versand entstehenden Nutzungsdaten, insbesondere die IP-Adresse. Der Zugriff und die Auswertung solche Daten ist aber nach derzeitiger Rechtslage auf Straftaten beschränkt. Eine Verfolgung von Spammern mit den Mitteln des Ordnungswidrigkeitenrechts ist mithin nur eingeschränkt möglich, ohne wesentliche Vorschriften des OWiG zu ändern.

Ein sinnvoller und gehbarer Weg wäre es, alle elektronischen Nachrichten, die entgegen der entsprechenden Vorschrift des § 7 UWG versandt werden, als Straftaten, wenigstens aber als Ordnungswidrigkeiten zu definieren.

2. Verhältnis fahrlässige Verschleierung – absichtliche Tathandlung

Die Unstimmigkeiten im Verhältnis der §§ 7 und 12 TDG-E sind offensichtlich und erfordern Änderungen. Insoweit sollte auf das Merkmal der „Absicht“ verzichtet werden.

3. Zuständige Behörde

Die nach derzeitigem Stand wohl zuständigen Ordnungsämter haben im Normalfall weder die Kompe-

tenz noch das Personal für eine solche Aufgabe. Häufig mangelt es schon an schnellen Netzanschlüssen oder modernen Rechnern. Auch Schwerpunktbehörden bei den Ländern halte ich für ineffizient, wie die negativen Erfahrungen bei der mangelnden Transparenz (Welche Behörde ist in welchem Land zuständig?) und Durchsetzung von Ordnungswidrigkeiten nach dem TDG hinsichtlich der Impressumspflicht bereits zeigt.

Die Erfahrung in der Bekämpfung von Spam auf rechtlichem Weg zeigt, dass hierfür hohe technische Kompetenz notwendig ist. Daher ist die Einrichtung einer zentralen Anlaufstelle mit entsprechendem Know-How unabdingbar. Dies könnte nach meiner Auffassung die RegTP, aber auch das BSI oder der BfD sein. Um angesichts der neu dort angehäuften Kompetenzen das Entstehen eine „Superbehörde" bei der RegTP zu vermeiden, wäre naheliegendste Stelle für eine Zuständigkeit -- auch aufgrund von Ausrichtung und der technischen Kompetenz -- das BSI.

4. Bisherige Gesetzesregelung im UWG

Das UWG ist ein stumpfes Schwert im Kampf gegen Spam. Die Umsetzung der EU-Richtlinie im Wettbewerbsrecht war weder sinnvoll noch sonderlich hilfreich. Grund dafür ist die Tatsache, dass die unmittelbar von Spam Betroffenen, also die Unternehmen, Verbraucher und Provider, aus dem UWG in aller Regel kein eigenes Klagerecht ableiten können, wenn sie nicht gerade zufällig oder mühsam konstruiert Mitbewerber sind. Die Betroffenen müssen sich daher für eine Rechtsdurchsetzung zwangsweise an die dafür vorgesehenen Verbände wenden. Die Erfahrung zeigt, dass diese – trotz einiger löblicher Initiativen - zumindest bislang nicht einmal ansatzweise in der Lage waren, hier für entsprechende Abhilfe zu sorgen. Leider ist hier im Bereich der Selbstverpflichtung und Eigenregulierung auch in absehbarer Zeit keine Besserung der unbefriedigenden Situation zu erwarten.

Wesentlich effektiver wäre eine entsprechende Umsetzung mit einem eigenen Klagerecht für die einzelnen Empfänger als Ergänzung zu den aus Richterrecht resultierenden Ansprüchen nach §§ 823, 1004 BGB. Für eine solche Umsetzung würde sich angesichts der Bedrohung, die Spam für die TK-Infrastruktur darstellt, das TKG anbieten.

5. Klagerecht für Provider

Erforderlich ist ein eigenständiges Klagerecht für die von der Plage stark betroffenen Provider. Nach meiner Meinung kann eine Ausdehnung des Kreises der Klagebefugten ohne Systembruch kaum im Rahmen des UWG erfolgen. Daher wäre eine o.g. „Anti-Spam-Klausel" im TKG oder TDG wünschenswert. Diese sollte entsprechende Unterlassungsansprüche der betroffenen Unternehmen und Verbraucher ebenso regeln wie das spezielle Recht der Provider.

Nachzudenken wäre auch über die Schaffung eines „Direktmarketing-Gesetzes", das verbindlich sowohl für Versender als auch für Verbraucher und Unternehmen Rechtssicherheit nicht nur im Bereich der E-Mail-Werbung schafft.

6. Mail-Filterung

Die Einrichtung von zentralen Spam-Filtern ist juristisch nicht unproblematisch. Neben vielen datenschutz- und telekommunikationsrechtlichen Vorschriften ist vor allem das Strafgesetzbuch zu beachten. Danach ist die Löschung von E-Mails durch Unternehmen und Provider ohne Kenntnis und Zustimmung des Empfängers unter Umständen strafbar nach §§ 206, 303a des Strafgesetzbuchs (StGB). Dies hat jüngst auch noch einmal das OLG Karlsruhe in einer Entscheidung bestätigt (Az: 1 Ws 152/04).

Dies gilt sowohl für die Filterung von Spam als auch für das gezielte Löschen einzelner Mails, nicht dagegen für virenverseuchte Nachrichten. Hier überwiegt das Interesse an dem Erhalt der IT-Infrastruktur das des Empfängers an der Zustellung der Nachricht, sodass eine Strafbarkeit ausscheidet.

Aus meiner Sicht reichen die bestehenden gesetzlichen Regelungen aus und entsprechen vor allem den Interessen der Mail-Empfängern. Gleichzeitig ist es den filternden Providern und Unternehmen vergleichsweise unproblematisch möglich, vorab entsprechende Einwilligungen der Betroffenen einzuholen. Erforderlich könnte allenfalls eine gesetzgeberische Klarstellung sein, dass eine pauschale Zustimmung der Betroffenen per AGB oder Betriebsvereinbarung ausreichend ist. Angesichts der Formerfordernisse der datenschutzrechtlich relevanten Zustimmung der einzelnen Betroffenen könnte es in diesem Bereich einen Regelungsbedarf geben.

7. Werbung in Foren und Gästebüchern sowie per SMS oder MMS

Der Entwurf übersieht andere, aber vom Grad der Belästigung und den entstehenden Kosten vergleichbare Werbeformen, bei denen zivilrechtliche Mittel nicht greifen. So besteht von Umfang und Inhalt her gesetzgeberischer Handlungsbedarf hinsichtlich automatisierter Werbeeinträge in Foren, Gästebüchern und in den Kommentarfunktionen von Blogs. Diese, längst automatisiert vorgenommenen massenhaften Einträge manipulieren zugleich Suchmaschinen und haben sich zu einer neuen digitalen Plage des Netzes entwickelt.

Gegen solche unerwünschten Werbeeinträge ist ein Grossteil der Betreiber nach derzeitiger Rechtslage wohl weitgehend schutzlos. Eine Anspruchsgrundlage könnte sich allenfalls –- für den Betreiber in den meisten Fällen wenig hilfreich – aus Wettbewerbsrecht ergeben. Zweifellos handelt es sich bei derartigen Einträgen um unlautere Wettbewerbshandlungen. Auch eine Übertragung der bisher von der Rechtsprechung zu unerwünschten E-Mails entwickelten Anspruchsgrundlagen auf Basis der §§ 823, 1004 BGB kommt allenfalls bei gewerblichen Betreibern in Betracht. Auch solche Einträge dürften als Eingriff in den Gewerbebetrieb zu werten sein. Bei Privatpersonen als Betreibern dürfte dagegen eine Regelungslükke bestehen, da es sich bei Blogs, Gästebüchern oder Foren kaum um Bereiche handelt, die dem Schutz des allgemeinen Persönlichkeitsrechts unterstehen.

Ebenfalls geregelt werden sollte die Bewerbung mittels SMS oder MMS, die, insoweit ja auch schon ge-

richtlich bestätigt, mit der von E-Mail ohne weiteres vergleichbar ist.

Erforderlich ist die Gleichstellung von unerwünschten Werbeeinträgen in Gästebüchern, Blog-Kommentaren, SMS und Foren mit den Regeln von E-Mail-Spam mit einem entsprechenden Unterlassungsanspruch. Eine solche Umsetzung im UWG wäre nach den o.g. Grundsätzen weitgehend sinnlos und sollte daher etwa im TDG oder TKG erfolgen.

Hannover, den 11. April 2005

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1852**

11. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Bundesverband Informationswirtschaft Telekommunikation und Neue Medien e.V. BITKOM

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder mit ca. 120 Mrd. Euro Umsatz und mehr als 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Mehr als 600 Direktmitglieder gehören dem Mittelstand an. BITKOM setzt sich insbesondere für eine Verbesserung der rechtlichen und politischen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein.

Die Bundestagsfraktionen von SPD und BÜNDNIS 90/ DIE GRÜNEN haben den Entwurf eines Anti-Spam-Gesetzes vorgelegt. BITKOM begrüßt die Möglichkeit, zu diesem wichtigen Thema Stellung beziehen zu können.

- Allgemeines

BITKOM teilt die Ansicht der Entwurfsverfasser, dass die Zahl unerwünschter und störender E-Mails (Spam) stetig steigt und inzwischen einen erheblichen Anteil der elektronischen Kommunikation ausmacht. Die damit einhergehende Belästigung wird zunehmend zu einer messbaren Schädigung. Betroffen sind Nutzer der E-Mail-Kommunikation im privaten Umfeld, aber auch Unternehmen und Behörden. Daneben belastet Spam auch die Anbieter von E-Mail-Kommunikation, die Provider, da sie unnötig ein wesentlich erhöhtes Datenvolumen transportieren, bearbeiten und speichern müssen. Die steigende Zahl an Spam-E-Mails lässt auch die Wahrnehmung für dieses Phänomen in der Öffentlichkeit und in der Politik steigen.

BITKOM begrüßt die Beschäftigung mit diesem Thema, sieht aber auch das wichtige Erfordernis, sich der Thematik differenziert zu nähern und Augenmaß zu bewahren. Wichtig ist vor allem, dass nicht jede E-Mail mit Werbeinhalten als Spam gelten kann. Vielmehr stellt die Nutzung dieses Kommunikationsmittels zur Werbung, etwa mit regelmäßigen Newslettern, individualisierten Angeboten usw. eine gerade auch für den Nutzer sehr bequeme Form der Information über Produkte und Dienstleistungen dar. Die Möglichkeit der Kundenansprache durch Werbung ist elementarer Bestandteil einer freien Marktwirtschaft. Seriöse Werbe-E-Mails von tatsächlichem Spam zu unterscheiden, ist eine zentrale Aufgabe der aktuellen Debatte.

Dies vorausgeschickt, teilen wir grundsätzlich den Ansatz der Entwurfsverfasser, einen sehr eng begrenzten Tatbestand zu schaffen.

Im Einzelnen merken wir dazu an:

- Klare Begrenzung des Tatbestands

Wir begrüßen das Bemühen der Entwurfsverfasser, sich bei dem Verbotstatbestand auf spezifische Begehungsformen zu beschränken, die wesentliche Grundübel der Spamflut sind. Nur so kann gewährleistet werden, dass sich die zuständigen Behörden auf diese besonders verwerflichen Spam-Versender konzentrieren. Unbedingt vermieden werden muss zudem eine verfehlte Kriminalisierung seriöser Werbetreibender in rechtlichen Zweifelsfällen.

Wir teilen die Einschätzung, dass die Verschleierung und Verheimlichung des Absenders oder des kommerziellen Charakters einer Werbe-E-Mail grundsätzlich zu diesen wesentlichen Grundübeln gehören.

Aufgrund der unbestimmten Rechtsbegriffe des „Verschleierns“ und „Verheimlichens“ kommt unserer Ansicht nach der Gesetzesbegründung eine entscheidende Bedeutung zu. Ihr entnehmen wir bereits in der Entwurfsfassung, dass die Rechtsbegriffe des „Verschleierns“ und „Verheimlichens“ eng auszulegen sein sollen.

Wichtig scheinen uns zwei Feststellungen, die noch deutlicher betont werden sollten:

- Keine Pflicht zur ausdrücklichen Kennzeichnung von Werbung

Ein Verschleiern/Verheimlichen des kommerziellen Charakters liegt nicht bereits dann vor, wenn eine Nachricht nicht ausdrücklich als „Werbung“ gekennzeichnet ist. Für Kopf- und Betreffzeile gelten nicht die Anforderungen des § 6 TDG. Dies führt die Gesetzesbegründung auf S. 11 aus.

Für Unklarheit hingegen sorgt der Verweis auf die „Umsetzung der erweiterten Transparenzpflichten bei der Ausgestaltung kommerzieller Kommunikationen für den Bereich der Werbewirtschaft“ auf S. 9. Diese Formulierung sollte gestrichen werden. Der Entwurf will (und sollte) gerade keine zusätzliche Kennzeichnungspflicht statuieren, sondern nur aktive Täuschungshandlungen verbieten.

Insgesamt bringt eine isolierte Betrachtung der Betreffzeile große Angrenzungsschwierigkeiten mit sich. Stellt etwa ein Modeversandhaus seine Frühjahrsmode mit der Betreffzeile „Der Frühling ist da!“ vor, so lässt allein dieser Slogan nicht ohne weiteres auf den kommerziellen Inhalt der Nachricht schließen. Es kann aber nicht Sinn einer Anti-Spam-Gesetzgebung sein, einen – in der Offlinewelt völlig gebräuchlichen – Slogan wie diesen zu verbieten. Die Interessen des Empfängers sind in einem solchen Fall bereits dann vollständig gewahrt, wenn er den Absender – im genannten Fall also „Modeversand XY“ – klar erkennen kann. Auf diese Weise erfasst er mit einem kurzen Blick den kommerziellen Charakter der Nachricht und kann über seinen weiteren Umgang mit der E-Mail eine gut informierte Entscheidung treffen.

Bereits aus Praktikabilitätsgründen sollte daher klargestellt werden, dass die Betreffzeile nicht isoliert betrachtet werden darf. Soweit der Bezug auf die Betreffzeile im Gesetzestext überhaupt aufrechterhalten werden soll, muss es genügen, dass sich der kommerzielle Charakter aus der Zusammenschau von Absender und Betreffzeile ergibt.

- Erfordernis eines subjektiven Tatbestands

Unserer Ansicht nach erfordern die Handlungen des „Verschleierns“ oder „Verheimlichens“ schon vom natürlichen Wortsinn her eine Absichtskomponente. Dies spricht auch die Gesetzesbegründung auf S. 13 an. Als Grund nennt sie zutreffend, dass vermieden werden muss, dass „insbesondere kleine und mittlere Unternehmen als Spammer sanktioniert werden, wenn sie die Kopf- oder Betreffzeile lediglich aus Unkenntnis nicht hinreichend eindeutig formulieren, ohne hiermit eine Verschleierungs- oder Verheimlichungsabsicht zu verfolgen.“

Zusätzlich betont § 12 des Entwurfs noch einmal den allgemeinen Grundsatz des Ordnungswidrigkeitenrechts, dass ein Bußgeld nur bei vorsätzlichem oder fahrlässigem Handeln verwirkt werden kann. In der Praxis wird eine solche Absicht oft anhand objektiver Kriterien nachgewiesen werden können, wie sie der Begründungsentwurf auf S. 11 und 12 aufzählt. Diese Konkretisierungen sind hilfreich und sollten grundsätzlich in der Begründung erhalten bleiben.

Besonders hohe Anforderungen an den Nachweis einer Verschleierungsabsicht müssen insbesondere im Hinblick auf die Betreffzeile gelten. Die Betreffzeile ist bereits Teil des Inhalts der E-Mail und muss auch für seriöse Werbenachrichten grundsätzlich frei gestaltbar bleiben. Alles andere wäre ein schwerer Eingriff in die unternehmerische Freiheit. Nicht nachvollziehen können wir deshalb insbesondere das vierte Beispiel auf S. 12 der Begründung („der Spamversender generiert automatisch eine “persönliche“ Ansprache des Adressaten, wenn Namensbestandteile aus der Empfängeradresse ersichtlich sind (z.B.:„Hello Mr. Schulte!“)“). Auch seriöse Werbetreibende bedienen sich mitunter einer persönlichen Ansprache. Eine solche ist nicht verwerflich und auch kein Indiz für eine absichtliche Täuschungshandlung. Es sollte daher in der Begründung zwingend umgekehrt klargestellt werden, dass die Gestaltung der Betreffzeile grundsätzlich Sache der unternehmerischen Freiheit ist und dass insbesondere personalisierte Werbung an sich nicht von dem Verbot erfasst ist.

- Klare Begrenzung des Täterkreises

Bedenklich stimmt uns die Äußerung auf S. 14 der Begründung, nach dem im Ordnungswidrigkeitenrecht maßgeblichen einheitlichen Täterbegriff erfasse der Bußgeldtatbestand auch alle Personen, die „das Spamming in Auftrag gegeben oder in irgendeiner sonstigen Weise gefördert haben“.

Hier muss unbedingt klargestellt werden, dass Auftraggeber und andere Beteiligte selbstverständlich auch nach § 14 OWiG nur dann haften, wenn auch ihnen hinsichtlich der konkreten Täuschungshandlung eine Absicht nachgewiesen werden kann. Anderenfalls würde ein enormes Missbrauchspotenzial geschaffen, das gerade für exponierte seriöse Unternehmen zu einer Gefahr werden könnte.

- Legalisierung von Filterinstrumenten

Vereinzelt wird vertreten, dass das Filtern von Spam durch Diensteanbieter den Tatbestand des § 206 Abs. 2 Nr. 2 StGB (Unterdrücken von Nachrichten) erfülle (OLG Karlsruhe vom 20.01.2005 - 1 Ws 152/04). Konkret wird auf S. 2 des Gesetzesentwurfs unter dem Punkt C/Alternativen erläutert: „Wirksamere Methoden wie beispielsweise das Prüfen der eingelieferten Mails durch den Service-Provider scheitern an dem Post- und Fernmeldegeheimnis, dem auch diese unterworfen sind.“

Auf S. 6 stellt die Begründung hingegen ausdrücklich fest, welche Bedeutung bei der Spambekämpfung ebendiese Maßnahmen zur Blockade und Filterung von Spam haben: „Neben den gesetzlichen Regelungen spielt vor allem die Wirtschaft eine wichtige Rolle bei der Bekämpfung unerwünschter elektronischer Post. Sie kann durch den konsequenten Ausbau technischer Schutzvorrichtungen einen wichtigen Beitrag zur Eindämmung der Spam-Flut leisten. Besondere Bedeutung kommt dabei dem Einsatz von Filterprogrammen zu, deren Aufgabe darin besteht, Spam-Nachrichten zu blockieren.“

Insoweit ist die Begründung widersprüchlich. Der Gesetzgeber sollte klarstellen, dass die Filterung/Blockierung von Spam-E-Mails rechtmäßig ist.

Berlin, den 11. April 2005

Positionspapier

zur fehlenden Strafbarkeit von Phishing- und Spoof-Attacken im Internet

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BIT-KOM) vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder mit ca. 120 Mrd. Euro Umsatz und mehr als 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Mehr als 600 Direktmitglieder gehören dem Mittelstand an. BITKOM setzt sich insbesondere für eine Verbesserung der rechtlichen und politischen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein.

- Hintergrund zu Phishing- und Spoof-Attacken

In den letzten Monaten tritt eine zunächst aus dem englischsprachigen Raum bekannte Form der Internetkriminalität zunehmend auch im deutschsprachigen Internet auf. Mit so genannten „Phishing-Mails“ (sprachlich abgeleitet von „Password-Fishing“) wird versucht, durch eine täuschende Gestaltung von massenhaft versandten E-Mails die Empfänger dazu zu verleiten, die Zugangsdaten (Benutzername oder Kontonummer und Passwort) für sicherheitsrelevante Anwendungen wie Online-Banking, Online-Shops oder andere E-Commerce-Anwendungen preiszugeben. Meist verlinken die Phishing-Mails auf Webseiten (sog. „Spoof“-Seiten), die in ihrer äußeren Gestaltung das Erscheinungsbild der Originalseiten der jeweiligen Anwendung, wie z.B. von Banken, nachahmen. Die Nutzer werden – oft unter Androhung erheblicher Konsequenzen bei Nichtbefolgung – aufgefordert, ihre Zugangsdaten und gelegentlich sogar weitere sensible Daten (z.B. Kreditkartennummern oder sogar Karten-PINs etc.) auf diesen Seiten anzugeben. Zuletzt wurden Fälle bekannt, in denen ganze Online-Shops täuschend echt nachgeahmt wurden, nur um auf diese Weise an die Zugangsdaten getäuschter Nutzer zu gelangen.

Die gewonnen Daten werden von den Tätern dann zur unbefugten Nutzung der Bank- und Nutzerkonten und damit zur Begehung oft sehr folgenreicher Straftaten missbraucht. Aufgrund der inzwischen erreichten hohen Qualität der täuschenden E-Mails und Webseiten werden trotz aller Aufklärungsbemühungen immer wieder Internetnutzer Opfer dieser Attacken. Hierdurch führt das Phänomen Phishing bzw. Spoof auch über die konkreten Schadensfälle hinaus zu einer wachsenden Verunsicherung der Bürger bei der Nutzung von elektronischen Geschäftsanwendungen und ist damit geeignet, das wirtschaftliche Potenzial dieses Bereichs zu gefährden.

Angesichts der stark zunehmenden Problematik bereitet es nicht nur betroffenen Online-Banken und -Unternehmen, sondern auch den Ermittlungs- und Strafverfolgungsbehörden erhebliche Sorge, dass das Phishing- und Spoof-Phänomen strafrechtlich kaum erfasst werden kann.

- Die bisherige Rechtssituation

In Frage kommen grundsätzlich Strafbarkeiten wegen Betrugs nach § 263 StGB und wegen Ausspähens von Daten nach § 202a StGB. Beim Betrug stellt sich allerdings das Problem, dass die angestrebte Preisgabe der Zugangsdaten wohl weder als Vermögensverfügung (die Zugangsdaten an sich sind keine vermögenswerten Güter) noch als konkrete schadensgleiche Vermögensgefährdung (sie schafft lediglich die Voraussetzungen für die Herbeiführung eines Vermögensschadens in einem weiteren Akt) angesehen werden kann. Auch liegt noch kein unmittelbares Ansetzen zu einer später mit den Daten geplanten Straftat (in den meisten Fällen Computerbetrug nach § 263a StGB) vor. Die Strafbarkeitsschwelle wird damit erst erreicht, wenn die Täter die Daten nach erfolgreichem Datenklau zur wirtschaftlichen Schädigung der Opfer nutzen. Das Versenden der Phishing-E-Mails und das Aufsetzen von Spoof-Seiten, die zunächst die einzigen sichtbaren Handlungen sind, bleiben hingegen derzeit als Vorbereitungshandlungen straffrei.

Hiergegen bietet auch der Tatbestand des § 202a StGB (Ausspähen von Daten) keine Handhabe, da tatbestandlich schon keine Daten im Sinne des Absatzes 2 betroffen sind. Denn Objekt der Ausspähung sind nicht die beim Online-Anbieter elektronisch gespeicherten Daten, sondern die eben nicht elektronisch oder anders gespeicherten bzw. übermittelten Informationen beim Nutzer. Zudem fehlt es insoweit an der besonderen Sicherung gegen den unberechtigten Zugriff. Schließlich fehlt bei § 202a StGB auch eine Versuchsstrafbarkeit, was die Ermittlungsbehörden, die oft nur von der Phishing- bzw. Spoof-Attacke selbst, nicht aber von eventuellen Erfolgsfällen Kenntnis haben, vor Schwierigkeiten stellt.

Auch die aktuell geplante und bereits in den Bundestag eingebrachte Neuregelung zu Spam-E-Mails wird hier keine Abhilfe schaffen können, da diese allein auf „kommerzielle Kommunikationen per elektronischer Post“ abstellt. Diese Beschränkung auf Werbe-E-Mails schließt aber gerade die in betrügerischer Absicht abgefassten Phishing-E-Mails von der Anwendbarkeit aus, obgleich auch sie massenhaft verschickt werden und sogar wesentlich größere Schäden anrichten können. Auch Spoof-Seiten erfasst die gesetzliche Neuregelung nicht.

- Rechtliche Lösungsmöglichkeit

Es erscheint deshalb erforderlich, einen speziellen Straftatbestand zu schaffen. Dieser sollte es mit Strafe bedrohen, elektronische Nachrichten oder Webseiten in betrügerischer Absicht so zu gestalten, dass der Empfänger der Nachricht bzw. der Besucher der Webseite über den wahren Absender bzw. Urheber getäuscht und damit zur Preisgabe geheimer Informationen verleitet wird, die dann zur Täuschung im Rechtsverkehr eingesetzt werden können.

Das Delikt sollte vorzugsweise als abstraktes Gefährdungsdelikt ausgestaltet sein, um nicht im Einzelfall den Nachweis eines Erfolges notwendig zu machen, der für die Ermittlungsbehörden auch bei Kenntnis einer Phishing- bzw. Spoof-Attacke oft nur schwer feststellbar ist. Alternativ müsste bei Ausgestaltung als Erfolgsdelikt zumindest eine Versuchsstrafbarkeit bestehen.

Auch wenn es sich bei Phishing und Spoof – wie auch bei Spam und anderen internetbezogenen Attacken – nicht um nationale, sondern um originär internationale Phänomene handelt, ist dennoch die Einführung einer nationalen Strafvorschrift sinnvoll. Über die Regeln des internationalen Strafrechts wird in vielen Fällen die Anwendbarkeit des deutschen Rechts zu begründen sein. Gerade das zuletzt vermehrte Auftreten deutschsprachiger Phishing-E-Mails und Spoof-Seiten zeigt zudem, dass erkennbar auch gerade der deutsche E-Commerce-Markt im Visier der Täter ist. Diese sind offenbar in vielen Fällen auch in Deutschland ansässig; anderenfalls können sie zumindest über die internationale Rechtshilfe ermittelt und verfolgt werden. Auch andere Länder haben bereits oder diskutieren die Strafbarkeit von Phishing- und Spoof-Attacken, so z.B. die Vereinigten Staaten Strafbarkeiten wegen „Identity Theft“ nach 18 U.S.C. § 1028(a)(7) oder nach dem neuen CAN-SPAM Act (18 U.S.C. § 1037).

BITKOM regt deshalb die Einführung eines Straftatbestands entweder im Fünfzehnten Abschnitt des Besonderen Teils des StGB (Verletzung des persönlichen Lebens- und Geheimnisbereichs, §§ 201ff. StGB) oder – vorzugsweise, da es sich im Regelfall um die Vorbereitung von gegen das Vermögen gerichteten Straftaten handelt – im Bereich der Vermögensdelikte an. Dieser könnte wie folgt formuliert sein:

als abstraktes Gefährdungsdelikt:

Wer eine elektronische Nachricht oder ein Angebot in Tele- und Mediendiensten so gestaltet, dass Empfänger der Nachricht oder Nutzer des Angebots über den wahren Absender oder Anbieter getäuscht und dadurch verleitet werden sollen, geheime Informationen preiszugeben, die zur Täuschung im Rechtsverkehr eingesetzt werden können, wird mit Freiheitsstrafe bis ... oder mit Geldstrafe bestraft.

als Erfolgsdelikt mit Versuchsstrafbarkeit:

(1) Wer sich fremde Informationen, die zur Täuschung im Rechtsverkehr eingesetzt werden können, dadurch verschafft, dass er elektronische Nachrichten oder Angebote in Tele- und Mediendiensten so gestaltet, dass der Empfänger der Nachricht oder der Nutzer des Angebots über den wahren Absender oder Anbieter getäuscht und dadurch zur Preisgabe der Information verleitet wird, wird mit Freiheitsstrafe bis ... oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Berlin, den 22. März 2005

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1845**

8. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Deutscher Industrie- und Handelskammertag DIHK

I. Vorbemerkung

Die Verbreitung unerwünschter E-Mails oder „Spam" hat einen Punkt erreicht, der ein wesentliches Problem für die Entwicklung des elektronischen Handels und der Informationsgesellschaft darstellt. Nach Angaben der EU-Kommission wird der Anteil von Spam am weltweiten E-Mail-Verkehr auf 50 % und am E-Mail-Verkehr innerhalb der EU auf 46 % geschätzt. Dies stellt einen dramatischen Anstieg dar, denn im April 2001 belief sich Schätzungen zufolge der Anteil von Spam am weltweiten E-Mail-Verkehr auf "nur" 7 %. Neben einer zunehmenden Belästigung der Verbraucher führt das Zusenden unerwünschter E-Mails zu großem finanziellen Schaden bei den Unternehmen. Die EU-Kommission geht davon aus, dass der Produktivitätsverlust für Unternehmen in der EU im Jahr 2002 ca. 2,5 Mrd. € betrug. Der hohe volkswirtschaftliche Schaden entsteht u. a. durch die erheblichen Kosten beim Empfänger als Unternehmer sowie als Privater und beim Internet Service Provider (ISP) durch die blockierte Speicherkapazität und Prozessorleistung, die aufgewendete Zeit zum Aussortieren der E-Mails, die Bearbeitung von Beschwerden, die Online-Zeit zum Abrufen der E-Mails und den Erwerb von Filtersoftware. Darüber hinaus führt die Flut unverlangt zugesendeter E-Mails zu einem Vertrauensverlust in die elektronische Kommunikation und die damit verbundene Leistungsfähigkeit der Informationstechnologie.

Das Problem „Spam“ ist nur durch ein gemeinsames Vorgehen von Industrie, Politik und Verbrauchern sowohl auf nationaler und als auch auf internationaler Ebene zu lösen. Die dabei erforderlichen Maßnahmen erstrecken sich insbesondere auf folgende Bereiche:

1. Selbstregulatorischer und technischer Lösungsansatz

Die selbstregulatorischen Initiativen der Internetwirtschaft sind zu begrüßen. Gesetzliche Vorgaben zum Einsatz von technischen Schutzmaßnahmen erscheinen dabei wenig sinnvoll, da gerade in einem offenen Wettbewerb die Anbieter die besten Angebote entwickeln, um der Kundennachfrage gerecht werden. Wirksamer Spam-Schutz wird zu einem entscheidenden Kriterium im Wettbewerb.

2. Aufklärerischer Lösungsansatz

Sehr wichtig ist zudem die gezielte Aufklärung der Nutzer. Der Empfänger einer E-Mail ist ein wichtiger Partner der ISPs im Kampf gegen Spam. Durch bestimmte Verhaltensregeln kann er sich selber vor Spam schützen. Aus diesem Grund sind Medienkompetenz sowie die Fähigkeit zum Selbstschutz zu stärken. Eine aktive Informationspolitik von Wirtschaft, Politik und Verbänden spielt somit eine zentrale Rolle.

3. Internationale Zusammenarbeit/Aktivitäten

Der Kampf gegen Spam kann erst durch eine internationale Zusammenarbeit und Übereinkommen gewonnen werden. Auf EU-Ebene gibt es hierzu immerhin bereits eine gemeinsame Vereinbarung von 13 Mitgliedstaaten, wonach die Behörden dieser Länder bei der Bekämpfung unerwünschter Werbemails künftig eng zusammenarbeiten wollen. Ziel der Vereinbarung ist es vor allem, Urheber von Spam in Europa leichter zu ermitteln und zu verfolgen. Grundlage für diese Vereinbarung war ein Beschluss des EU-Rates vom Dezember 2004. Deutsche Behör-

den haben sich der Vereinbarung bislang erstaunlicherweise nicht angeschlossen. Über eine Zusammenarbeit in Europa hinaus ist es aber besonders wichtig, auch mit Drittländern sowohl bilateral als auch in internationalen Foren, wie z. B. der OECD und der Internationalen Fernmeldeunion, Spam zu bekämpfen. Die besondere Bedeutung der internationalen Zusammenarbeit wird auch in dem Antrag der CDU/CSU-Fraktion betont.

4. Gesetzgeberischer Lösungsansatz

Im Gegensatz zu anderen europäischen Ländern hat Deutschland bisher keinerlei spezielle straf- oder ordnungsrechtliche Maßnahmen gegen Spam ergriffen. In § 7 UWG wurde Artikel 13 der EU-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) umgesetzt. Demnach ist die Werbung mittels E-Mails nur in zwei Fällen zulässig: Grundsätzlich muss der Empfänger vorher sein Einverständnis erklärt haben. Im Interesse der Pflege bestehender Geschäftsbeziehungen dürfen Unternehmen ihre Kunden unter engen Voraussetzungen über weitere Angebote informieren. Alle anderen Werbe-E-Mails sind unzulässig.

Diskutiert wird sei längerem, ob Ordnungswidrigkeiten oder gar Straftatbestände eingeführt werden sollen. Diese Diskussion wurde in dem nun vorliegenden Fraktionsentwurf mit der Einführung eines Ordnungswidrigkeitentatbestands aufgegriffen. Bereits vorher hatte die CDU/CSU-Fraktion sich dafür ausgesprochen, eine ordnungsrechtliche Verantwortung und Bußgeldpflicht einzuführen und auch auf die durch Spam Beworbenen auszudehnen.

Zwingende europäische Vorgaben für die Einführung eines Straftatbestands oder einer Ordnungswidrigkeit gibt es nicht. Fraglich ist zudem, ob überhaupt ein rechtspolitisches Bedürfnis nach einem neuen Anti-Spam-Gesetz besteht oder ob nicht das klassische Computerstrafrecht bzw. geltende Strafrecht und internationale Übereinkommen genügen. Betroffene sollten vielmehr verstärkt dazu ermuntert werden, ihre bestehenden Rechte zivil- und wettbewerbsrechtlicher Art - ggf. mit Hilfe von Verbraucher- bzw. Wettbewerbsvereinen - durchzusetzen.

Der vorliegende Gesetzentwurf schießt an seinem Ziel vorbei, als Anti-Spam-Gesetz den Mail-Missbrauch zu bekämpfen. Die Regelungen bringen in Wirklichkeit keine Verbesserungen, sondern erzeugen nur Kosten und Aufwand in der Wirtschaft und verstärken zudem die Rechtsunsicherheit.

II. Argumentation im Einzelnen

1. Weitaus größter Teil der Spam-Mails wird nicht erfasst

Wie die Gesetzesbegründung an verschiedenen Stellen treffend ausführt, wird das Gesetz sich bei 90 % der Fälle als zahnlos herausstellen. Denn dies ist der Anteil der Werbenachrichten, die aus dem EU-Ausland verschickt werden, in dem es keine vergleichbar strengen Regelungen zur Bekämpfung von Spam gibt. Damit aber sind nicht einmal 10 % der Versender innerhalb der Europäischen Union ansässig, so dass sich erst recht die Frage stellt, wie viele dieser Versender letztlich überhaupt der deutschen Gebietshoheit und somit dem deutschen Ordnungswidrigkeitenrecht unterfallen würden. Diese Zahlen machen mehr als deutlich, dass die Bekämpfung von Spam-Mails nur durch verstärkte internationale Zusammenarbeit in dem rechtspolitisch gewünschtem Umfang zu erreichen wäre, sei es nun auf der Ebene der Europäischen Union oder weiter gehender zwischenstaatlicher Mechanismen.

Solange diese fehlen, wird es aufgrund des weltweiten Zugangs zum Internet auch in Zukunft selbst bei einer verbesserten Rechtslage in Deutschland immer möglich sein, Spam-Mails aus Staaten mit liberalerer Gesetzeslage zu verschicken. Aus diesem Grund wird auch nicht „auf internationaler Ebene ein Signal gesetzt werden“ können. Eine weltweite Kontrolle dürfte auf absehbare Zeit wohl kaum erwartet werden dürfen.

Es erscheint jedenfalls nicht nachvollziehbar, wie das deutsche Gesetz „daher nicht nur in Deutschland, sondern auch weltweit zur Abschreckung von Spammern und zum Schutz von Verbrauchern beitragen“ können soll, wie dies unter dem Stichwort „B. Lösung“ des Entwurfs prognostiziert wird. Die auch in der Begründung vorgebrachte „Abschreckungswirkung“ ist nicht erkennbar, da ausländische und außereuropäische Versender die deutschen Normen wohl kaum wahrnehmen oder gar beachten werden. Der hier gewünschte staatliche Kontrollanspruch ist über das deutsche Hoheitsgebiet hinaus nicht zu realisieren.

2. Problem der Identitätsermittlung führt zu faktischer Unmöglichkeit der Verfolgung

Schwierig dürfte sich auch die Frage gestalten, ob und ggf. wie ein Absender, der über seine tatsächliche Identität täuscht, ermittelt werden kann. Diejenigen, die über ihre Identität bewusst täuschen wollen oder sie verschleiern, werden nach wie vor keine Sanktion befürchten müssen, da gegen sie mangels Kenntnis des Namens und der Herkunft nicht vorgegangen und vollstreckt werden kann. Die Ermittlung des Absenders hat bereits technisch gesehen wenig Erfolgsaussichten: Spam-Mails werden meist von so genannten Bot-Netzen (gekaperte PCs), von offenen Mail-Relays, über kostenlose Mailaccounts oder aus Ländern, in denen keinerlei gesetzliche Mittel gegen den Spam-Versand bestehen, versendet. Die Feststellung des Nutznießers der Spam-Mail (Anbieter der beworbenen Sache) könnte einen Anhaltspunkt liefern, der konkrete Beweis für seine Urheberschaft an der Mailversendung wird sich aber schwerlich erbringen lassen.

Die hier geschilderten faktischen und rechtlichen Probleme der Identitätsermittlung und Identitätsverfolgung finden in der Entwurfsbegründung keinen Niederschlag.

Betroffen sind somit vor allem in Deutschland tätige Unternehmen, die sich auch bislang weitestgehend gesetzeskonform verhalten haben bzw. bei den jetzt schon möglichen Verfolgungsmaßnahmen in der Regel schnell und unproblematisch weitere Verstöße unterlassen (sanktioniert durch Vertragsstrafeversprechen). Zudem bemühen sich gerade Internet-Service-Provider um einen wirksamen Anti-Spam-Schutz in ihren E-Mail-Programmen. Diese Schutzmechanismen werden zunehmend verbessert und den geänder-

ten Bedingungen (aufgrund von Virenprogrammen usw.) angepasst. Die Selbstkontrolle der Unternehmen, die insbesondere im Interesse der Nutzer ist, sollte auch weiterhin im Vordergrund stehen. Sie ist einer staatlichen Regulierung mit derzeit absehbar geringem Verbesserungspotential auf jeden Fall vorzuziehen.

Da also gegen etwaige kriminelle Verwender das Gesetz bzw. das Bußgeld faktisch nicht durchsetz- und vollstreckbar sein wird, sollte man von solch einer nutzlosen Gesetzesregelung absehen, solange die technische und rechtliche Ermittlung der Identität sowie die weitere (internationale) Verfolgbarkeit nicht sichergestellt werden kann.

3. Bestehende Regelungen besser nutzen

Verbraucher sind durch die gegenwärtige Rechtslage schon recht gut geschützt. In § 7 Gesetz gegen Unlauteren Wettbewerb (UWG) ist geregelt, dass insbesondere auch in E-Mails die Herkunft bzw. der Autor nicht verschleiert sein dürfen. Aufgrund der gegenwärtigen Praxis in der Wirtschaft, gegen Verstöße im Wettbewerbsrecht vorzugehen, hält sich bereits die überwiegende Anzahl der in Deutschland tätigen Unternehmen faktisch an die für das TDG vorgeschlagene Regelung, so dass die geforderte Transparenz im elektronischen Verkehr bereits hinreichend besteht. Die Erfahrung zeigt, dass wettbewerbsrechtliche Abmahnungen deutscher Spammer, soweit man ihre Identität ermitteln kann, in der Regel zur unmittelbaren Abgabe der strafbewehrten Unterlassungserklärung führen. Das neue Gesetz führt daher auch an dieser Stelle nicht zu einer wirklichen Verbesserung des Schutzes der Verbraucher und der Wirtschaft.

Das UWG geht sogar noch weiter und umfasst neben E-Mails auch SMS und Fax. Es ist an dieser Stelle darauf zu verweisen, dass eine Sonderbehandlung von E-Mails im neuen § 7 TDG gerade mit Blick auf das UWG nicht gerechtfertigt ist.

Neben dem UWG enthält auch das bisherige TDG im § 6 Satz 1 Nr. 1 bereits eine Regelung, die zu einer verbesserten Transparenz beiträgt. Dort ist geregelt, dass eine E-Mail mit Werbecharakter leicht erkennbare und ständig verfügbare Informationen zu Identität und Kontaktdaten des Absenders enthalten muss. Auch diese Vorschrift ist bußgeldbewehrt.

Die bestehenden Strafvorschriften, wie sie auch in der Begründung des Entwurfs aufgezählt werden, werden unseres Wissens viel zu selten in der Praxis angewandt, was aber sicherlich auch wieder an der fehlenden Ermittelbarkeit der Identität liegen mag. Schon hieran wird der nur sehr geringe – wenn nicht gar fehlende – Nutzen weiterer Vorschriften deutlich.

Einen weiteren ordnungsrechtlichen Schutz sehen wir daher als nicht systemkonform und wegen der drohenden negativen Auswirkungen des Anti-Spam-Gesetzes als sachlich nicht gerechtfertigt an. Das Gesetz würde keine Verbesserung der Praxis bewirken.

4. Abgrenzungsschwierigkeiten verstärken die Rechtsunsicherheit

Die vorgeschlagene Regelung enthält eine Vielzahl unbestimmter Rechtsbegriffe. Dies führt zu Abgrenzungsschwierigkeiten bei den Unternehmen und verstärkt die Rechtsunsicherheit. Insbesondere das Verhältnis zu § 7 UWG bleibt unklar. Letzten Endes wird diese Rechtsunsicherheit die Untenehmen in ihrem legitimen Interesse an einer Bewerbung ihrer Produkte stark behindern, wobei gerade die Werbung über das Internet in der Zwischenzeit zu den bedeutendsten Medien in der Werbung zählt und weiter wachsen wird.

Besonders betroffen sind Unternehmen durch die gesetzgeberische Forderung, dass die Werbenachricht über ihren kommerziellen Charakter bereits in der Kopf/Betreffzeile Auskunft geben muss. Hier werden Unternehmen vor eine schwer lösbare Aufgabe gestellt, da zwischen reinen Informationsmails und Werbemails unterschieden werden muss. Z. B. dürfte eine sog. Auto-Reply-Mail zur Bestätigung des E-Mail-Eingangs keine zusätzlichen Produktinformationen enthalten, ohne dass in der Betreffzeile darauf hingewiesen wird. Wird aber in der Betreffzeile einer Informationsmail auf eine zusätzliche Information mit möglicherweise werbendem Charakter hingewiesen, erreicht diese Mail den Empfänger erst gar nicht, weil er sie als Werbemail eingeordnet und daraufhin gelöscht hat. An diesem Beispiel erkennt man bereits, dass das Gesetz an der wirklichen Sache vorbeizielt.

Zu berücksichtigen ist ferner, dass die Betreff-/Kopfzeile im Einzelfall nicht ausreichend sein wird, die im § 7 TDG-E geforderten Informationen vorzuhalten.

5. Kosten

Dem beschriebenen, zweifelhaften Nutzen des Gesetzes stehen erhebliche Zusatzkosten gegenüber. Ausdrücklichen Widerspruch verdient daher die Begründung des Gesetzesentwurfs hinsichtlich der vermuteten Kostenfolgen. Denn selbst wenn diese nur unzureichend quantifizierbar sind, so dürften sie doch recht erheblich sein. Bei den Kosten ist zu differenzieren zwischen den Kosten der öffentlichen Haushalte und den sonstigen Kosten.

Da ein Ordnungswidrigkeitstatbestand geschaffen wird, also auch (Straf-)Anzeigen betroffener Dritter möglich sind, besteht die Verpflichtung der Strafverfolgungsbehörden, die nötigen Vor- und Einrichtungen für erforderliche Ermittlungen jedenfalls vorzuhalten. Der Aufwand, z. B. verschleierte Absender von Spam-Mail zu ermitteln, dürfte beachtlich sein. Dass der Gesetzesentwurf hier ausdrücklich „keine“ zusätzlichen Kosten ausweist, später aber auch einräumt, sie lediglich nicht quantifizieren zu können, ist insgesamt eine sehr merkwürdige Vorgehensweise.

Zudem dürfen auch die zusätzlichen Kosten für die Wirtschaft nicht unterschätzt werden. Die Aussage unter „E: Sonstige Kosten“, dass hier „keine“ entstünden, sondern „vielmehr mit einer deutlichen Kostensenkung bei der Wirtschaft und den Verbrauchern zu rechnen“ sei, ist eine Fehleinschätzung. Denn wie bereits bei den Regelungen zu Pflichtangaben im Internetimpressum werden die vielen unbestimmten Rechtsbegriffe wieder zu einer Flut von neuen Abmahnungen führen, die weit überwiegend nur jene deutschen Unternehmen treffen werden, welchen aus fehlender Beratung oder Unkenntnis heraus geringfügige Unterlassungen anzulasten sind. Das heißt, die Unternehmen werden erhebliche Geldmittel aufwen-

den müssen, um vorab die nötige Beratung zu erhalten. So dürfte allein die Frage, ob z. B. bereits eine Verschleierung des Absenders einer Nachricht vorliegt, wenn nicht die komplette Firma mit vollständiger Anschrift bereits in der Betreffzeile angeben wird, höchst kontrovers zu diskutieren sein und damit Beratung erfordern. Außerdem sind erhebliche Rechtsverteidigungskosten zu erwarten, da - insbesondere ungerechtfertigte Abmahnungen – abgewehrt werden müssen. Es ist nach unseren Erfahrungen u. a. mit § 6 TDG recht wahrscheinlich, dass Betrüger und bewusste Schadensverursacher das Gesetz als Grundlage heranziehen, um bei den Unternehmen Schaden zu verursachen oder sich selbst zu bereichern.

III. Zusammenfassung

Im Ergebnis ist festzuhalten, dass die Intention des vorliegenden Entwurfes, Spam zu bekämpfen, zwar begrüßenswert ist. Jedoch bestehen an der praktischen Wirksamkeit angesichts der (bislang) ausschließlich nationalen Vorgehensweise so erhebliche Zweifel, dass das Gesetz insgesamt abzulehnen ist. Was man weder kontrollieren noch durchsetzen kann, bedarf weder einer Regelung, noch einer (kostenintensiven) Bürokratie. Letzteres belastet allenfalls die sich rechtstreu verhaltende Wirtschaft.

Eine wirksame rechtliche Bekämpfung des Spam-Mail-Problems erscheint nur auf internationaler Ebene möglich. Bis zur Erreichung einer internationalen Einigung muss weiter an technischen Lösungen gearbeitet werden. Es ist zu überlegen, inwieweit das Herausfiltern von Spam rechtlich erleichtert werden kann. Und zusätzlich muss weiterhin die Selbstkontrolle der Wirtschaft sowie Aufklärung der Nutzer im Vordergrund stehen.

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1854**

12. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Dr. Irini E. Vassilaki, Deutsche Gesellschaft für Recht und Informatik e.V. DGRI

"Spam": Das Phänomen und seine strafrechtliche Bewertung

- Sind neue Strafvorschriften für die Bekämpfung dieser Plage notwendig? -

I. Einführung - Das Phänomen "Spam"

Die Zahlen sprechen für sich! Studien belegen, dass es sich bei mindestens 50% des E-Mail-Verkehrs um Spam handelt. Eine Firma, die anti-spam Software entwickelt und anwendet, schätzt, dass im Jahre 2003 4,9 Trilliarden Spammails gesendet wurden. Nach Angaben von AOL wurden im April 2003 2,37 Billionen Spammails pro Tag abgeblockt.[6] Tendenz steigend! Die Kosten für die Internetnutzer entwickeln sich entsprechend. Eine EU-Studie hat berechnet, dass im Jahr 2001 einem durchschnittlichen Internetnutzer Kosten bis zu 30 € für das Herunterladen von etwa 15 Werbe-E-Mails pro Tag mit einer Speicherbelegung von insgesamt 500 bis 800 KB entstanden sind. Bei weltweit etwa 400 Millionen Internetnutzern ergäbe das Herunterladen der Werbe-E-Mails unter Zugrundelegung des derzeitigen technologischen Entwicklungstandes allein auf Seiten der User pro Jahr Gesamtausgaben in Höhe von etwa 10 Milliarden €.[7] Die Kosten der Firmen, die mit Werbe-E-Mails bombardiert werden, haben in Europa im Jahr 2002 $ 2,5 Milliarden und in der USA im Jahr 2003 $ 10 Milliarden überschritten. Als Kostenfaktoren wurden dabei berechnet:

- die Zeit, die von den Arbeitnehmern verwendet wird, um die Werbe-E-Mails zu checken und auszusortieren,
- die Kosten, die durch die zusätzlichen Computer- und Netzwerkressourcen entstehen, die für die Bewerkstelligung von Werbe-E-Mails erforderlich sind, entstehen und
- die finanzielle Investition in technische Maßnahmen wie Filter und "man power" bzw. Arbeitskraft, die sich nur mit der Abwehr von Angriffen durch Werbe-E-Mails beschäftigen.[8]

Auch die Internet Service Provider (ISP) zahlen für die Flut von Werbe-E-Mails. In den Kosten sind - unter anderem - enthalten: die erweiterte Datenspeicherung, das zusätzliche Personal, die elektronische Erreichbarkeit und die erforderlichen Investitionen für die Entwicklung geeigneter E-Mail-Filter. Nach einer Studie der Firma "Ferris Research" kostet die unerbetene E-Mail-Werbung die ISPs ca. $ 500 Millionen pro Jahr.[9] Es liegt auf der Hand, dass diese Kosten letztendlich dem Internetnutzer aufgebürdet werden.

Diese Zahlen alarmieren. Strategien zur Bekämpfung vom Spam werden entworfen, neue Normen, die die unerbetene Werbung als rechtswidrig ausweisen, werden hastig verfasst, Tagungen und Workshops zu diesem Thema werden organisiert und - last but not least - die Stimmen, die die Einführung einer Norm proklamieren, die Spam ahnden soll, vermehren sich.[10] Machen solche Vorschläge Sinn? Um dies festzustellen, muss eine mehrstufige Untersuchung vorgenommen werden:

Erstens: Die Phänomenologie von Spam muss dargestellt werden. Denn nur die umfassende Darstellung der Erscheinungsformen von Spam ergibt ein hinreichendes Bild dieses Problems und liefert Ansätze für seine Bekämpfung.

Zweitens: Nachdem das Problem erkannt und eingegrenzt wurde, soll geprüft werden, ob und wie weit die bestehenden Strafvorschriften die Erscheinungsformen von Spam ahnden können. Denn nur wenn Gesetzeslükken festgestellt werden, kann über die Schaffung neuer Strafvorschriften nachgedacht werden.

II. Definition und Umfang von Spam

Es ist bekannt, dass das Wort "Spam" sich aus den Begriffen "spiced" und "ham" zusammensetzt und zum ersten Mal von den "Monthy Pythons" in einem Sketch verwendet wurde. Im Internet versteht man unter Spam die unerbetene Zusendung von E-Mails mit kommerziellem Inhalt.

Gleichwohl deckt diese Umschreibung nur einen Teil des Phänomens "Spam". Denn eine Untersuchung der Massenversendung von E-Mails führte zu dem Ergebnis, dass diese nicht nur kommerziellwerbenden Charakter haben. Das ergibt sich aus einer Untersuchung der Firma Bightmail, die Softwarefilter gegen Spam entwickelt und im Juli 2004 über 106 Milliarden Spam aus der Internetkommunikation inhaltlich überprüft hat. Nach dieser Untersuchung lässt sich Spam in folgende Kategorien einteilen:[11]

1. Erscheinungsformen von Spam

a) Spam mit Produktwerbung

28% der gesendeten Spammails bieten Produkte oder Dienstleistungen an oder werben dafür, wie etwa Kleidung, Kosmetik, Autozubehör, detektivische Leistungen oder Autovermietungen.

b) Spam für Erwachsene

17% der Spam bieten an oder verweisen auf Dienstleistungen für Erwachsene. Hier findet man Angebote für Partnervermittlung, Familienberatung, Psychoanalyse aber auch Verweise auf Webseiten mit Erotikangeboten. Solche Spammails haben oft den Charakter offensiver Werbung.

c) "Finanzspam"

15% der Spam enthalten Informationen über Finanzangebote, etwa über Anlageberatung, Fonds, Aktiengesellschaften. In vielen Fällen werden Kredite mit besonders günstigen Konditionen angeboten, die jedoch hohe "versteckte" Gebühren enthalten, so dass der Endbetrag, die von Banken angebotenen Kredite häufig beträchtlich übersteigt.

d) Scams oder "Nigeria"-E-Mails

9% der Spam sind E-Mails, die dem Empfänger eine große Summe Geldes versprechen, wenn er etwa afrikanischen Geschäftsleuten, einer Diktatorenwitwe oder einem verschollenen Prinzen helfen würde, riesige Beträge - regelmäßig Millionen Dollar - außer Landes zu schaffen. Der E-Mail-Empfänger soll - nach dem Inhalt der E-Mail - sein Konto kurzfristig zur Verfügung stellen, um die Millionen für kurze Zeit zu "parken". Geht der Internetnutzer auf diese E-Mail ein, dann wird eine "geringe

6 Entsprechende Zahlen s. in: OECD, Background Paper for the OECD Workshop on Spam, S. 4.

7 S. Gauthroner/Etienne Drouard, Unsolicited Commercial Communications and Data Protection, S. 67.

8 S. dazu J. Krim, "Spam Cost to Business Escalates, Washington Post, 13. März 2003.

9 S. dazu *Ferris Research*, The Costs of Spam False Positives, S. 29 ff.

10 Dazu s. nur http://www.heise.de/newsticker/meldung/45873; Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz).

11 S. die detallierten Ausführungen in: Brightmail´s Prove Network, The State of Spam - Impact and Solutions".

Gebühr" für das gewinnbringende Geschäft verlangt, z. B. für Überweisungen, Anwaltskosten oder Steuern, die oft einige tausend Dollar hoch sein kann. Dass die versprochenen Millionen nie ausgezahlt werden, ist systemimmanent.[12]

e) "Pharmaspam"

Obwohl der Begriff "Spam" oft mit dem Verkauf von Viagra verbunden wird, enthalten nur 7% der unerbetenen E-Mails Angebote über Arzneimittel, unkonventionelle Heilmethoden oder alternative Medikamente.

f) "Phishing"

Eine in letzter Zeit massiv angewandte Methode, die 6% der gesendeten Spam ausmacht, stellt die Zusendung von sogenannten Phishing-E-Mails dar: Die Internetnutzer werden auf gefälschte Bankseiten im Internet gelockt. Dort sollen sie etwa eine neue Homebanking-Anwendung ihrer Bank nutzen. Beantwortet der Kunde die E-Mail, wird er auf eine gefälschten Kopie der Originalseite der Bank geführt, auf der er seine Kontodaten eingeben soll. Gibt der Kunde seine Konto- und PIN-Nummer ein, ist es dann für die Betrüger ein Kinderspiel, sein Konto zu plündern. Laut einer USA-Studie des Forschungsunternehmers Garnter, die im Mai 2004 veröffentlicht wurde, sind im Jahre 2003 den Finanzdienstleistern und Kreditkarteninhabern durch Phishing Schäden in Höhe von $ 1,2 Milliarden entstanden.[13]

g) "Freizeitspam"

5% der versendeten Spam bieten Werbung zum Thema "Freizeit" an. Hierunter fallen Angebote für Online-Casinos, Spiele aber auch Urlaubsangebote, Fitness-Studios oder verschiedene Sportangebote.

h) "Internetspam"

Gesondert sollen die Spammails erwähnt werden, die Produkte anbieten, die den IT-Bereich betreffen. 4% der unerbetenen Werbung bietet Software, Rechner oder IT-Dienstleistungen an, etwa Web Hosting oder Web Design. Weil die Preise der Softwareprodukte sehr niedrig sind, besteht der begründete Verdacht, dass die angebotenen Softwareprodukte illegal erworben worden sind.[14]

i) Politischer Spam

4% von Spammails haben politischen Inhalt. Werbung für politische Parteien, für Politiker oder Aufforderungen für Spenden seien als Beispiel für politischen Spam genannt. Aber auch Spam mit ausländerfeindlichem oder rassistischem Inhalt stellen keine Seltenheit dar. Am 10. Juni 2004 etwa wurde das Internet mit E-Mails überflutet, die unter dem Betreff "Geschrieben von Margrit" und "Polizei traute sich nicht, kriminellen Ausländer festzunehmen" über angebliche Verbrechen von Ausländern berichteten und auf rechtsradikale Webseiten verwiesen. Dabei wurden gefälschte Absender benutzt und der Virus "Sober.G" eingesetzt, um diese E-Mails an Millionen von Internetuser zu versenden.[15]

k) Spiritueller Spam

Werbung per E-Mail betreiben auch Religionen oder Religionsgemeinschaften, Beratungsstellen oder Webseiten zum Thema Astrologie. Sie betragen etwa 1% der Spammails.

l) Diverse Spam

Es bleiben 4% des gesamten Spam-Aufkommens, die keiner der genannten Spam-Kategorie zugeordnet werden können.

An dieser Stelle sei freilich erwähnt, dass es sich bei den Prozentangaben nur um Schätzungen handelt. Andere Untersuchungen kommen zu anderen Ergebnissen. Nach der britischen Firma "Clearswirft" etwa, die sich auf den Bereich der Web-, E-Mail und Internetsicherheit spezialisiert hat, beträgt der Anteil der Gesundheitsspams 30,6% der gesamten Spammails, während 24,6% der Spammails Finanzangebote enthalten und nur 4,60% der Spammails Angebote mit pornographischen Inhalten.

Gleichwohl sind die Unterschiede bei den Zahlen in diesem Zusammenhang irrelevant.[16] Wichtig ist vielmehr die Erkenntnis, dass durch Spam

- unterschiedliche Produkte und Dienstleistungen angeboten
- politische Botschaften oder Weltanschauungen verbreitet
- auf betrügerische Weise personenbezogene Daten abgefragt werden.

2. Spammethoden

a) Spam-Zombies

Um unerkannt zu bleiben und Spam-Filter zu umgehen, verwenden die Spammer sog. "Zombie-Viren". Sie versenden E-Mails mit Trojanern, die ungesicherte Privatrechner erkennen und diese in einen Spam-Zombie bzw. Verteiler verwandeln. Der Internetnutzer bemerkt meist nicht, dass fünf oder sechs Spammer seinen Computer für die Weiterverbreitung ihrer Mails nutzen. Oft registriert er das Problem nur dann, wenn sein Provider seinen Account aufgrund der riesigen Übertragungsvolumen, die sein Rechner sendet, sperrt.[17]

b) Spim

Spim ist die unerwünschte Werbung innerhalb von Instant-Messaging-Sitzungen. Sie sind noch aufdringlicher als Spam, denn sie erscheinen automatisch, sobald ein Benutzer auf seiner IM-Plattform eingeloggt hat. Dadurch sind sie schwer zu ignorieren. Bis Ende des Jahres 2004 sollen in den Chat-Rooms schätzungsweise 1,2 Millionen Spim-Beiträge abgesetzt werden. Um IM-Benutzer zu entdecken, verwenden die "Spimmer" spezielle Software, die Chat-Rooms und Websites nach IM-Usernamen ausforscht.[18]

3. Prämissen von "Spam"

Schon die ausgewählten Beispiele unerbetener E-Mails weisen darauf hin, dass Spam ein Phänomen darstellt, das über den bloßen Versand von Werbe-Mails hinaus geht. Der Versand von Spam stellt nicht nur eine Werbemethode dar, deren Erfolg von zwei Voraussetzungen abhängig ist, nämlich

- dem Bestehen von E-Mail-Adressen und

12 s. dazu etwa www.nigeria-connection.de
13 Garnter, Phishing Victims Likely Will Suffer Identity Theft Fraud, 5.
14 S. dazu www.zdnet.de/news v.29.6.2004.
15 S. dazu http://www.heise.de/newsticker/meldung/48121.
16 S. den Index des Monats Juni 2004 unter: www.clearswift.com.
17 s. dazu etwa www.stern.de/computer-technik/internet/?id=520713&nv=pr&pr=1.
18 S. dazu etwa "Spam, Spim, Spum" in: NZZ v. 28.5.2004

- dem Verwischen der Spuren der Spamversender, so dass diese nicht entdeckt werden können.

Auf der Grundlage dieser beiden Voraussetzungen existiert eine spezielle, oft in der Grauzone operierende, Computerbranche. Als Beispiel seien die Entwickler der sog. "Spamware" erwähnt, die als "Pull"-Tool zur Gewinnung von Adressen eingesetzt wird und als "Push"-Tool die massenhafte Versendung von E-Mails unterstützt. Ertragreich ist auch die Vermittlung und der Verkauf von E-Mail-Adresslisten. Die Durchführung einer Spam-Kampagne kostet $ 20 pro 1000 E-Mails bei Mitlieferung der Adressen von Adressenbrokern. Die Adressenbroker bieten in diesem Zusammenhang einen Dienst an, der die Filter von ISP überlisten kann. Der Kunde bzw. Spammer kann etwa 300.000 Adressen pro Woche für 19,95 $ pro Monat oder 500.000 Adressen pro Woche für 29,95 $ pro Monat oder 1.000.000 Adressen für 39,95 $ pro Monat erwerben.[19] Dass dabei nicht alle E-Mail-Adressen mit dem Einverständnis der E-Mail-Adressaten weitergegeben werden, kann wohl vorausgesetzt werden.

Um die Spam-Filter zu umgehen und die Spam-Verfolger zu verwirren, geben die Spammer falsche Absender oder gefälschte E-Mail-Adressen an, oder - wie schon zuvor bei Spam-Zombies erwähnt - verwenden Trojaner, die Computer von Privatpersonen als Versender vorspiegeln. Viren-Programmierer werden für teueres Geld eingestellt, um Software zu entwickeln, die PCs in Spam-Zombies verwandeln.[20]

4. Gewinne von Spam

Es liegt auf der Hand, dass Spammer diesen Aufwand betreiben, weil Spam lukrativ ist. Nach Angaben des Forschungsinstituts "Forrester Research" liegt die Erfolgsquote beim E-Mail-Marketing zwischen 5% und 15%, verglichen mit nur 0,5% bis 2% bei konventionellen Mailings. Über die Höhe der Gewinne der Spammer legt eine Studie des "Wall Street Journal" dar, dass Spam noch Gewinne erzielt, wenn die Erfolgsquote niedriger als 0,001% ist. Die Studie erläutert den Fall einer Spam-Kampagne für den Verkauf eines konkreten Produkts. Es wurden 3,5 Millionen Spammails versendet. Daraus ergaben sich 81 Bestellungen in der ersten Woche, was einer Quote von 0,0023% entspricht. Das Produkt kostete $ 10, was einen Umsatz von $ 1500 in der ersten Woche bedeutete. Die Kosten für die konkrete Versendung der Spammails waren niedriger als $ 100. Hochgerechnet hat die Spam-Firma, die mehr als 100 Millionen E-Mail-Adressen besitzt, Provisionen von mehr als $ 25.000 durch diese Versendungsaktion verdient.[21]

5. Definition von Spam

Die Ausführungen des vorangegangenen Abschnitts machen deutlich, daß das Phänomen "Spam" eine Form unerbetener Kommunikation darstellt, die drei Bestandteile hat:

- Das Erwerben, nämlich Sammeln, Kaufen oder Ausspähen, von E-Mail-Adressen
- Technische Maßnahmen, die diese Kommunikationsform unterstützen.
- Die Zusendung unerbetener E-Mails, die - unter anderem - Werbecharakter haben.

Die drei Bestandteile sind eng miteinander verbunden und von einander abhängig, so dass sie gleichwertig sind.

Die strafrechtliche Bewertung des Spam-Phänomens muss demzufolge alle drei Teile erfassen. Ferner müssen bestimmte Elemente, die diese Kommunikationsform auszeichnen, berücksichtigt werden: Diese Kommunikationsform ist nämlich

- unerbeten,
- grenzüberschreitend als Folge der Globalität des Internet,
- nicht an Netze gebunden
- billig für den Versender,
- attraktiv bzw. lukrativ für den Versender, denn der Inhalt von Spam erreicht eine riesige Zahl von Adressaten und
- sie hat Massencharakter, denn die gesendeten E-Mails haben denselben Inhalt.

III. Strafrechtliche Bewertung von Spam

Wie schon erläutert, verlangt die sachgerechte strafrechtliche Beurteilung von Spam eine rechtliche Bewertung der einzelnen Bestandteile dieser Kommunikationsform.

1. Erhebung und Übermittlung von E-Mail-Adressen als Ordnungswidrigkeit gem. § 43 Abs. 1 Nr. 8 BDSG

Da, wie schon dargelegt, Prämisse für eine erfolgreiche Spam-Kampagne der Besitz von E-Mail-Adressen ist, stellt dieser ein wertvolles Kapital der Spammer dar. Fraglich ist aber, ob das Sammeln von E-Mail-Adressen rechtmäßig bzw. ob und unter welchen Voraussetzungen das Sammeln von E-Mail-Adressen strafbar ist.

E-Mail-Adressen stellen personenbezogene Daten dar, soweit ihre Inhaber durch einen entsprechenden Suchdienst oder auf andere Weise als natürliche Person identifizierbar sind.[22] Sie fallen damit unter dem Anwendungsbereich des BDSG. Das Erheben von personenbezogenen Daten zu Geschäftszwecken von nicht-öffentlichen Stellen ist gem. § 28 Abs. 1 Nr. 3 1. Alt. BDSG grundsätzlich zulässig, wenn die Daten allgemein zugänglich sind. Allgemein zugänglich sind Daten, die sich sowohl ihrer Zielsetzung als auch ihrer Publikationsform nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[23] Wenn E-Mail-Adressen auf Internetseiten zu finden sind und von einer unbestimmten Zahl von Internetnutzern wahrgenommen werden können, stellen diese - vergleichbar mit Adressen, die in Adress- und Telefonverzeichnissen veröffentlicht sind - allgemein zugängliche Daten dar.

Die Erhebung von allgemein zugänglichen Daten ist gem. § 26 Abs. 1 Nr. 3 BDSG aber unzulässig, wenn schutzwürdige Interessen des Betroffenen, die der Erhebung entgegen stehen, den Interessen der verantwortlichen Stelle "offensichtlich" überwiegen. Es ist mehrmals erwähnt worden, dass die Sammlung von E-Mail-Adressen der Versendung unerbetener Werbung dient.

19 S. Gauthroner/Étienne Drouard, Unsolicited Commercial Communications and Data Protection, S. 35.
20 S. http://www.stern.de/computer-technik/internet/index.html?id=520713.
21 S. Wall Street Journal, vom 13.11.2002.
22 Schmitz in: Schuster (Hrsg.), Vertragshandbuch Telemedia, Kap. 3 Rdnr. 146.
23 BVerfGE 27, 71, 83; 27, 104, 108; 33, 52, 65.

Diese stellt nach § 7 Abs. 2 Nr. 3 UWG eine unzumutbare Belästigung dar, wenn sie ohne die vorherige Einwilligung des Verbrauchers geschieht und ist als unlautere Wettbewerbshandlung gem. § 3 UWG unzulässig. In § 1 UWG wird zum ersten Mal ausdrücklich der Schutz des Verbrauchers vor unlauterem Wettbewerb erwähnt,[24] und damit dem Interesse des Verbrauchers Vorrang vor den Interessen der Werbebranche gegeben. Weil der Verbraucher Betroffener und der Werbende die verantwortliche Stelle i.S.d. § 28 BDSG darstellt, überwiegt folglich das Interesse des Verbrauchers das des Werbenden "offensichtlich", wie § 28 Abs. 1 Nr. 3 BDSG verlangt, weil die Gestaltung der Werbung unmittelbar der wettbewerbsrechtlichen Gesetzgebung zu entnehmen ist.

Ähnlich ist die geschäftsmäßige Erhebung von personenbezogenen Daten zu Übermittlungszwecken bzw. der Handel mit E-Mail-Adressen zu bewerten. Gem. § 29 Abs. 1 Nr. 2 1. Alt. BDSG ist die Erhebung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können. Die Zulässigkeit entfällt aber, wenn schutzwürdige Interessen des Betroffenen das Interesse der Erhebung und Speicherung offensichtlich überwiegen. Um die Frage zu beantworten, wann dies der Fall ist, sind wiederum die Grundsätze des neuen UWG heranzuziehen. Würde die Anwendung der einschlägigen UWG-Vorschriften zum Ergebnis führen, dass der Handel mit E-Mail-Adressen zum Zweck unerbetener Werbung nicht erlaubt ist, stellte gleichwohl diese datenschutzrechtlich rechtswidrige Handlung keine Straftat dar. Streitigkeiten in Zusammenhang mit der (Un)Zulässigkeit der Erhebung und Übermittlung von E-Mail-Adressen fallen vielmehr in den Zuständigkeitsbereich der Zivilgerichte.

Werden nun personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, muss dieser gem. § 33 Abs. 1 S. 1 BDSG von der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle benachrichtigt werden. Werden darüber hinaus die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist dieser schon von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen gem. § 33 Abs. 1 S. 2 BDSG. Die Benachrichtigungspflicht besteht nicht, wenn gem. § 33 Abs. 2 Nr. 7a, Nr. 8 a BDSG die Daten allgemein zugänglichen Quellen entnommen wurden und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

Geht man davon aus, dass das Erlangen von E-Mail-Adressen durch automatische Ausforschung im Internet erfolgt, ist die erste Prämisse, nämlich die Entnahme der Daten aus allgemein zugänglichen Quellen, erfüllt. Hinsichtlich der "Unverhältnismäßigkeit" des Benachrichtigungsaufwandes seitens der verantwortlichen Stelle ist die Rechtslage jedoch anders zu beurteilen. Bei der Prüfung der Frage, ob die Benachrichtigung unverhältnismäßig ist, soll der durch die konkrete Benachrichtigung entstehende Verwaltungsaufwand berücksichtigt werden.[25] Hierzu ist zu bemerken, dass dieser gering wäre, wenn die Spamware zugleich mit dem "Sammeln" von E-Mail-Adressen automatisch eine Benachrichtigung an den Inhaber senden würde. Dass diese automatische Meldung - ähnlich wie der Bestätigungsbefehl bei der Zusendung von gewünschten E-Mails zwar möglich aber seitens der Spammer nicht vorgesehen, weil nicht gewollt ist, bedeutet nicht, dass die Einrichtung dieser technischen Maßnahme einen hohen Verwaltungsaufwand erfordern würde.

Auch das Argument, dass die verantwortliche Stelle hundert Tausende von E-Mail-Adressen besitzt, so dass die Benachrichtigung der Inhaber der E-Mail-Adressen einen unverhältnismäßigen Aufwand erfordern würde, kann nicht anerkannt werden. Denn ähnlich wie kein Strafmilderungsgrund für einen Fahrer bestehen kann, der durch selbstverschuldete Trunkenheit einen Unfall verursacht,[26] darf der rechtswidrige Zustand, den die verantwortliche Stelle vorsätzlich veranlasst hatte, nicht zur ihren Gunsten wirken. Daher ist die Voraussetzung der Unverhältnismäßigkeit bei der Benachrichtigung von E-Mail-Adressaten nicht erfüllt und die Befreiung von der Benachrichtigungspflicht gem. § 33 Abs. 2 BDSG entfällt. Die Benachrichtigungspflicht trifft sowohl diejenigen, die E-Mail-Adressen für eigene bzw. Werbezwecke erheben, als auch diejeninge, die sie geschäftsmäßig speichern.

Unterlassen die Verpflichteten die Benachrichtigung, dann handeln sie gem. § 43 Abs. 1 Nr. 8 BDSG ordnungswidrig und können mit einer Geldbuße bis zu € 25.000 geahndet werden.

2. Anwendung von technischen Maßnahmen für die Unterstützung von Spam-Versendung

a) Datenveränderung nach § 303a StGB

Von strafrechtlicher Bedeutung sind die technischen Manipulationen, die den Zweck haben, die Herkunft von Spam zu verwischen. Ein Beispiel dafür ist etwa die Anwendung von "Spyware", die einen Computer in einen Spam-Zombie verwandelt. Vorab ist festzustellen, dass diese Handlung kein "Ausspähen von Daten" nach § 202a StGB darstellt, denn der Gesetzeswortlaut setzt die Überwindung besonderer Sicherungen voraus. Die Aufgabe von Spyware ist allerdings, auf "ungesicherte" Rechner zuzugreifen, so dass der objektive Tatbestand des § 202a StGB nicht erfüllt wird.

Der Einsatz von Spyware kann gleichwohl als Datenveränderung nach § 303a StGB bestraft werden. Die Umwandlung eines Privatcomputers zum Spamverteiler bedeutet zugleich die Veränderung von Daten des "Zombierechners", die die Netzverbindung aufbauen. Damit erfüllt diese Handlung den objektiven Tatbestand des § 303a Abs. 1 4. Alt. StGB. Weil die Umwandlung auch vorsätzlich seitens der Versender von Spyware geschieht, kann sie mit einer Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden.[27]

b) Urkundenstraftaten

Es ist weiterhin zu prüfen, ob die Versendung von Spam mit gefälschten E-Mail-Adressen oder IP-Adressen eine Urkundenstraftat darstellt, indem als Absender eine andere Person als der geistige Urheber der elektronischen Nachricht erscheint oder eine falsche Kennung des Computers, der die E-Mail sendet, vorgespielt wird.

---

24 Dazu vgl. nur Köhler, NJW 2004, 2121.

25 Simitis (Hrsg.), BDSG/Mallman § 33 Rdnr. 64a.

26 Dazu vgl. nur BGHSt 77 f.; BGH StV 1991, 254; BGH NStZ-RR 1997, 165.

27 S. dazu auch Vassilaki/Martens, Computer- und Internetstrafrecht, 47 f.

Zunächst stellt sich die Frage, ob eine E-Mail eine Urkunde darstellt, nämlich eine verkörperte, allgemein oder für Eingeweihte verständliche, menschliche Gedankenerklärung, die geeignet und bestimmt ist, im Rechtsverkehr Beweis zu erbringen und ihren Aussteller erkennen lässt.[28] Diese Definition macht deutlich, dass man für die Beantwortung dieser Frage unterscheiden muß zwischen

- E-Mails, die geöffnet und ausgedruckt werden
- E-Mails, die geöffnet und lediglich am Bildschirm gelesen werden und solche die nicht geöffnet, sondern deren Absender und "Betreff"-Thema nur im Inbox-Ordner wahrgenommen bzw. gelesen werden.

aa) Ausdrucke von E-Mails

Ausdrucke von E-Mails können wie Computerausdrucke bewertet werden, die als Urkunden anerkannt und gegen Fälschung strafrechtlich geschützt werden, wenn sich ihr Inhalt von einer Person oder Behörde zu eigen gemacht wird.[29] Ähnlich wie auf dem Papier kann der Absender der E-Mail als Urheber erkannt werden. Dabei wird freilich vorausgesetzt, dass ein Absender angegeben wird oder als Absender kein Deckname verwendet wird, die der Feststellung des Ausstellers vereiteln soll. Bei Fällen sog. "offener" oder "verdeckter" Anonymität fehlt die Urheberangabe, so dass die Urkundeneigenschaft der ausgedruckten E-Mail verneint wird.[30] Der Inhalt der E-Mail ist meistens geeignet, für ein Rechtsverhältnis Beweis zu erbringen, ob etwa Medikamente zum Kauf angeboten oder ob rassistische Mitteilungen verbreitet werden. Für die Bejahung der Beweiseignung reicht es aus, dass der Inhalt der E-Mail auf die Meinungsbildung des E-Mail-Empfängers mitbestimmend einwirken kann. Die Tatsache, dass E-Mails leicht manipulierbar sind, liefert kein Argument, das grundsätzlich die Beweiseignung von elektronischen Nachrichten in Frage stellen würde.[31] Es ist nicht erforderlich, dass sie allein den vollen Beweis erbringt.[32] Die Beweisbestimmung kann dem Ausdruck einer E-Mail auch nachträglich gegeben werden, wenn etwa um die Qualität bzw. Garantie eines per E-Mail bestellten Produktes oder über den beleidigenden Inhalt der E-Mail gestritten wird.[33] Die Tatsache, dass die E-Mail-Vorlage im Rechner des Absenders gespeichert ist, beeinträchtigt nicht die Urkundeneigenschaft des Ausdrucks von E-Mails. Denn im Wege des Ausdrucks wird zum ersten Mal die menschliche Erklärung hergestellt, die in der Form der E-Mail verfasst wurde. In diesem Sinne kann - um Puppe zu zitieren - "eine Urkunde jederzeit in eine Datenurkunde verwandelt werden und umgekehrt".[34]

Stellen nun Ausdrucke von E-Mails Urkunden im strafrechtlichen Sinne dar, können sie auch gefälscht werden. Der Absender, der eine E-Mail verfasst und diese mit dem Namen einer anderen Person unterzeichnet, stellt eine neue Urkunde her, die über die Person des Ausstellers täuscht, wie es bei den "Nigeria-E-Mails" der Fall ist. Diese "Identitätstäuschung" wird gem. § 267 Abs. 1 1. Alt. StGB als Herstellung einer unechten Urkunde bestraft.[35] Dabei ist unerheblich, ob der angebliche Urheber der E-Mail existiert oder ob seine Ermittlung nicht möglich ist,[36] was oft bei der Verfolgung von E-Mails mit gefälschten E-Mail-Absenderadressen der Fall ist.

bb) Gespeicherte E-Mails

Werden die E-Mails nicht ausgedruckt, sondern wird ihr Inhalt oder lediglich ihre E-Mail-Adresse im Bildschirm gelesen, scheidet die Anwendung von § 267 StGB aus, denn es fehlt die vom Gesetz geforderte Körperlichkeit des Tatobjekts. In Betracht kommt vielmehr § 269 StGB, der die Fälschung beweiserheblicher Daten unter Strafe stellt. Schutzgegenstand stellen die Daten dar bzw. die codierten und auf einem Datenträger fixierten Informationen über eine außerhalb des verwendeten Zeichensystems befindliche Wirklichkeit.[37] Da der Datenbegriff auch Ausgabedaten impliziert,[38] wird die IP-Adresse, die auf den Rechner hinweist, von dem aus die E-Mail gesendet wurde, vom Anwendungsbereich der Norm erfasst.

Um nach § 269 StGB geschützt zu werden, muß die IP-Adresse beweiserheblich sein, nämlich dazu "bestimmt, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Tatsachen benutzt zu werden".[39] Da die IP-Adresse die Feststellung der Identität des E-Mail-Absenders unterstützt, was im Rechtsverkehr, etwa im E-Commerce, von erheblicher Bedeutung ist, bestehen für die Beweiserheblichkeit der IP-Adresse keine Bedenken.[40]

Strafbar ist die Speicherung oder Veränderung der beweiserheblichen Daten, was bei der Versendung von Spam mit manipulierten IP-Adressen der Fall ist. Für die Strafbarkeit der Handlung wird ferner vorausgesetzt, dass die manipulierten Daten wahrnehmbar sind, um eine unechte oder verfälschte Urkunde darzustellen. Diese sog. hypothetische Subsumption ist in diesem Fall gegeben. Denn die IP-Adresse, die etwa durch Computerausdruck sichtbar und damit wahrnehmbar gemacht werden kann, wird eine Zahl anzeigen, die zur Identifizierung des Computerabsenders führt. Ist nun die IP-Adresse manipuliert, wird ein anderer Computer als der tatsächlich agierende erschienen. Ist darüber hinaus Vorsatz, Rechtswidrigkeit und Schuld bei derartigen Manipulationen zu bejahen, dann macht sich derjenige, der technische Unterstützung für die Versendung von Spam leistet, gem. § 269 StGB strafbar.

3. Zusendung von unerbetenen E-Mails

a) Vorbemerkungen

Im Kap. II ist dargestellt worden, dass Spammails verschiedene Inhalte haben. Aus diesem Grund werden in die strafrechtliche Bewertung der Zusendung unerbetener E-Mails die angebotenen Produkte und Dienstleistungen einbezogen und es soll geprüft werden, nach welchen Strafvorschriften dieses Angebot strafbar ist. Unter die-

28 BGHSt, 16, 96; 18, 66; Sch/Schr/Cramer § 267 Rdnr. 2; Tröndler/Fischer, § 267 Rdnr. 2.
29 S. dazu nur Sieber, Computerkriminalität und Strafrecht, (2. Aufl.), 276 ff.; Winkelbauer, CR 1985, 42; Sch/Schr/Cramer, § 267 Rdnr. 4.
30 Dazu s. Sch/Schr/Cramer, § 267 Rdnr. 18.
31 So allerdings Frank, CR 2004, 125, der auf zivilrechtliche Literatur hinweist und anscheinend übersieht, dass im Zivilprozess andere Regel als im materiellen Strafrecht bezüglich des Urkundenbegriffs gelten.
32 So Sch/Schr/Cramer, § 267 Rdnr. 11.
33 Über die sog. Zufallsurkunden s. etwa BGHSt 13, 385 f.; 17, 299 und die Kritik von Schilling, Reform der Urkundenverbrechen, 53 ff.
34 S. Puppe, NStZ 2001, 483.
35 Über die Strafbarkeit der Identitätstäuschung vgl. BGHSt 1, 121; 33, 160.
36 So auch RGSt 46, 298, BGHSt 5, 187.
37 So die Datendefinition nach Haft, NStZ 1987, 8.
38 So Tröndle/Fischer § 268 Rdnr. 4.
39 So BT-Drucks. 10/5058, 8.
40 So auch Rinker, MMR 2002. 664.

sem Gesichtspunkt wird im folgenden die Strafbarkeit der Zusendung von Spammails i.V.m. ihrem Inhalt geprüft. Vorab sind die Leitlinien der Prüfung festzulegen:

aa) Anwendbarkeit des deutschen Strafrechts

Weil, wie schon erwähnt, es sich beim Phänomen "Spam" um eine grenzüberschreitende Form der Internetkriminalität handelt, liegt es nahe, die Frage über die Anwendbarkeit des deutschen Strafrechts zu stellen. Macht sich ein Spammer, der aus den USA heraus unerbetene Werbung per E-Mail versendet, etwa für den Verkauf von pornographischen Schriften, nach § 184 StGB strafbar?

An dieser Stelle sollen nicht die Diskussion und die unterschiedlichen Ansichten über die Anwendbarkeit des deutschen Strafrechts auf die grenzüberschreitende Kriminalität wiederholt werden.[41] Im folgenden werden nur die Grundsätze erläutert, die für die hier zu behandelnde Frage von Bedeutung sind.

Nach dem **Territorialitätsprinzip,** das seine Verankerung in § 3 StGB hat, werden der Strafgewalt eines Staates alle Handlungen unterworfen, die auf dessen eigenem Staatsgebiet begangen werden, auch wenn der Täter Ausländer ist. § 9 StGB betrachtet als Begehungsort sowohl den Ort der Handlung als auch den Ort des tatbestandsmäßigen Erfolges (Ubiquitätstheorie). Fallen Handlungs- und Erfolgsort auseinander, ist als tatbestandsmäßiger Erfolg der Erfolg zu bewerten, durch den der strafrechtliche Tatbestand erfüllt wird, etwa die Überlassung von pornographischen Schriften an einer Person unter achtzehn Jahren nach § 184 Abs. 1 Nr. 1 StGB.

Um eine konturlose Auslegung der § 9 StGB zu vermeiden,[42] ist die Feststellung des Erfolgseintritts in enger Beziehung zum Straftatbestand zu sehen. Demzufolge wird bei jeder Fallgestaltung der Zusendung von Spammails der in Frage kommende Tatbestand herangezogen und - unabhängig davon, ob dieser ein Erfolgs- oder Gefährdungsdelikt darstellt – untersucht, ob der zum konkreten Straftatbestand gehörende Erfolg eingetreten ist. Es wird auf die Auslegung des konkreten Tatbestandes abgestellt und überprüft, ob durch die Tathandlung der im einschlägigen Tatbestand enthaltene Taterfolg eingetreten ist. Auf diese Weise wird die Frage nach der Feststellung des Erfolgsortes von der Unterscheidung zwischen Erfolgs- und Gefährdungsdelikten losgelöst, so dass der Erfolgsbegriff i.S.v. § 9 StGB eigenständig definiert wird. Zugleich wird sie mit der Untersuchung über die tatsächliche Wirkung der Zusendung von unerbetener Werbung verbunden, so dass die Ermittlung des Erfolgsortes eingegrenzt wird.

Dies bedeutet, dass es ermittelt werden soll, ob das durch den einschlägigen Tatbestand geschützte Rechtsgut beeinträchtigt, d. h. durch die Tathandlung entweder verletzt oder gefährdet worden ist. Bei den Erfolgsdelikten wird somit die Rechtsgutbeeinträchtigung „festgestellt", während bei den Gefährdungsdelikten eine solche „prognostiziert" wird. Für die „Prognose" einer Rechtsgutbeeinträchtigung ist freilich eine „Prognoseentscheidung" erforderlich, die die Frage behandelt, ob der konkrete Geschehensablauf im ungestörten Fortgang zu einer Rechtsgutbeeinträchtigung führen wird.

bb) Strafbarkeit von "Spammern und werbenden Unternehmern"

Um ihre Aktivitäten auszuüben, kooperieren die Spammer mit den Unternehmern, deren Produkte und Leistungen sie im Internet bewerben. Demnach liegt es auf der Hand zu fragen, ob auch die werbenden Unternehmer zur strafrechtlichen Verantwortung herangezogen werden können. Für Spammer und werbende Unternehmer könnte Mittäterschaft gem. § 25 Abs. 2 StGB in Betracht kommen.

Mittäterschaft setzt gemeinschaftliche Tätigkeit voraus. Für die Zusendung unerbetener Werbung ist die Zusammenarbeit von Spammer und werbendem Unternehmer erforderlich. Der zweite liefert die Nachricht bzw. den Inhalt, den der erste mittels technischer Unterstützung verbreitet. Der Tatbeitrag des werbenden Unternehmers stellt damit die Grundlage für die Zusendung unerbetener Werbung dar. Die Zusendung der E-Mail als solche ist der Anteil des Spammers bei der Verwirklichung dieser Tätigkeit. Beide Handlungen sind gleichberechtigte Tatbeiträge, die sich gegenseitig ergänzen, um eine Aktivität zu erzeugen.[43] Dadurch wird ein gemeinschaftliches Mitwirken gebildet, das die Ausführung der Versendung von Spammail und die gemeinsame Begehung der etwaigen Straftaten, die durch die Zusendung von Spam erfüllt werden, ermöglicht. In objektiver Hinsicht ist demnach ein arbeitsteiliges Handeln und eine Rollenverteilung zu bejahen. Die Mittäterschaft setzt auch einen gemeinsamen Tatentschluss voraus. Die Arbeitsteilung zwischen Spammer und werbendem Unternehmer beruht auf der Absprache, aus unerbetener Werbung bzw. Verkauf der Produkte oder Dienstleistungen Profit zu erzielen. Daraus lässt sich der Schluß ziehen, dass ein gemeinsamer Wille von Spammer und werbendem Unternehmer vorhanden ist.

Die vorangegangenen Ausführungen führen zum Ergebnis, dass zwischen den beiden Akteuren ein bewusstes und gewolltes Zusammenwirken entsteht, die das Ziel haben, unerbetene Werbung per E-Mail zu versenden. Verletzt nunmehr diese Handlung strafrechtliche Vorschriften, können Spammer und werbender Unternehmer als Mittäter der entsprechenden Straftat zur Verantwortung gezogen werden.

cc) Verlinkte Inhalte

In den meisten Spammails sind Links eingebaut, die an Webseiten weiterleiten, die die angebotenen Produkte oder Dienstleistungen verkaufen. Aus diesem Grund ist zu fragen, ob der Spammer für die rechtswidrigen Angebote, die durch die Aktivierung seines Link offeriert werden, strafrechtlich verantwortlich gemacht werden kann.

Rechtswidrige Angebote, die zugleich Straftatbestände erfüllen, lassen sich in Verbreitungs- und in Äußerungsdelikte einteilen. Bei den Verbreitungsdelikten, etwa §§ 86, 86a, 130 Abs. II Nr. 1, 130a Abs. 2 Nr. 1, 184, 287 StGB, § 106 UrhG liegt der Schwerpunkt des strafrechtlichen Verhaltens und damit der Grund der Bestrafung an der strafbaren Handlung. Maßgebend ist, dass durch die strafbare Handlung, im vorliegenden Fall das Anbieten der verlinkten Produkte oder Leistungen, rechtswidrige Inhalte verbreitet werden. Für die Erfüllung des Tatbe-

41 Eine Darstellung der Problematik vgl. etwa in Vassilaki/Martens, Computer- und Internetstrafrecht, 3 ff.

42 Ausführlich über die unterschiedlichen Auslegungsansätze: Vassilaki/Martens, Computer-und Internet-Strafrecht, S. 9 ff.

43 Über die "Wesentlichkeit" der Tatbeiträge bei der Mittäterschaft vgl. etwa BGH NStZ 1982, 243; BGH NStZ 1990, 130; BGH NStZ 1997, 336.

stands eines Äußerungsdelikts gemäß §§ 90a, 103, 111, 185 StGB ist dagegen erforderlich, dass der Täter bzw. Spammer sich in irgendeiner Weise zum missbilligten Inhalt, den er durch das Linksetzen verbreitet, bekennt. Der Schwerpunkt der strafrechtlichen Handlung liegt in diesem Fall an der positiven Einstellung bzw. Billigung des Täters gegenüber den verbreiteten Inhalten.[44]

Nach Rechtsprechung und Literatur werden Verbreitungsdelikte durch die Zusendung von E-Mails begangen. Die ältere Ansicht, die für die Tatbestandserfüllung die Weitergabe eines körperlichen Gegenstandes voraussetzte, ist aufgegeben worden.[45] Unter strafbare Verbreitung fällt unter anderem das "Zugänglichmachen" von rechtswidrigen Inhalten. Unter Zugänglichmachen wird jede Tätigkeit erfasst, die die konkrete Möglichkeit unmittelbarer Kenntnisnahme von den rechtswidrigen Inhalten für kurze oder längere Zeit eröffnet, wobei es gleichgültig ist, ob jemand von der Möglichkeit Gebrauch macht.[46]

Durch die Zusendung unerbetener Werbung mit verlinkten Inhalten wird von einem Spammer diese Möglichkeit, z. B. die Weiterleitung an Webseiten mit pornographischen Angeboten, eröffnet. Damit stellt sie eine strafbare Verbreitungshandlung dar, die unter dem einschlägigen Tatbestand subsumiert wird.

Die Äußerungsdelikte bestehen aus Gedankenäußerungen, die etwa das Auffordern zu oder das Billigen von Straftaten,[47] die Missachtung Dritter[48] oder die Androhung von Straftaten[49] enthalten. Sie stellen einen Willen, eine Absicht oder eine Bewertung dar, deren Verbreitung unter Strafe steht. Unwichtig ist, ob der Urheber selbst den Gedanken verbreitet oder ob der Gedanke von einem Dritten, dem mutmaßlichen Täter, übernommen und verbreitet worden ist. Es ist nämlich unwesentlich, ob die Bekanntmachung der Gedankenäußerung vom Urheber oder lediglich von einem Dritter in der Öffentlichkeit zugänglich gemacht worden ist.

Für die Strafbarkeit des Spammers, der mit einem Link auf eine Seite verweist, die Äußerungsdelikte enthält, ist demzufolge die Einstellung des Täters entscheidend, die fremde Gedankenäußerung ihm zuzurechnen. Um ein Urteil über die subjektive Zurechnung der Gedankenäußerung zu dem Spammer fällen zu können, sind zwei Elemente erforderlich:

- das Wissen des Inhalts der Gedankenäußerung seitens des Spammers und
- das Wollen des Spammers, den dort enthaltenen Gehalt zu seinem eigenen zu machen.

Dieses „Wissen und Wollen“ darf nicht mit dem subjektiven Tatbestand des jeweiligen Äußerungsdelikts verwechselt werden. Die Untersuchung der Feststellung der positiven Einstellung des Täters gegenüber der Äußerung betrifft nicht die Frage der subjektiven Zurechnung des Erfolges bzw. Gefährdung eines Straftatbestandes, §§ 111, 130 StGB, die auch den Willen, die Gedankenäußerung zu veröffentlichen bzw. zugänglich zu machen, umfaßt. Es handelt sich vielmehr um die Klärung einer Vorfrage, deren Bejahung die Prüfung der Erfüllung des Äußerungsdelikts erlaubt.

Ob ein Äußerungsdelikt einem Spammer zugerechnet wird, etwa Zusendung von E-Mails, die auf Webseiten verweisen, die strafbare rechtsradikale Inhalte enthalten, muß freilich durch eine Einzelfallprüfung beurteilt werden. Dabei ist der Inhalt der Spammail von Bedeutung, aus dem hervorgehen kann, ob der Spammer sich von der von ihm verwiesenen Äußerung distanziert oder ob er sich den fremden Gedankeninhalt aneignet. Wird im konkreten Fall festgestellt, dass der Spammer sich die verlinkten rechtswidrigen Aussagen von Dritten zu eigen macht, dann macht er sich des einschlägigen Äußerungsdelikts strafbar.

b) Straftaten durch die Zusendung von Spammail

Unter II.1 sind die verschiedenen Inhalte von Spammails beschrieben worden. Im folgenden werden Straftaten geschildert, die durch die Zusendung von Spam begangen werden. Dabei wird die Zusendung von Spammails als "modus operandi" bewertet, nämlich als Tathandlung, einer Straftat, die sich auf den Inhalt der Mail bezieht. Die Ausführungen erheben keinen Anspruch auf Vollständigkeit, denn die Inhalte von Spammails verändern sich kontinuierlich. Es sollen lediglich die häufigsten Straftaten dargestellt werden, die durch die Zusendung von unerbetenen E-Mails begangen werden.

aa) Urheberrechtsbezogene Straftaten

Die Produkte, die im Wege der unerbetenen Werbung angeboten werden, unabhängig davon, ob es sich dabei um Kleidung, Software oder Autozubehör handelt, stellen in den meisten Fällen Fälschungen i.w.S. dar. Plagiate werden verkauft, nämlich Werke, die durch die Verletzung urheberrechtlicher Vorschriften hergestellt werden.[50] Die Dumpingpreise etwa der angebotenen Software weisen darauf hin, daß illegale Software veräußert wird. Nach Angaben der Internetsicherheitsfirma Clearswift hat sich der Anteil der "Software-Spam" innerhalb zwei Monate mehr als verdoppelt.[51] Viele angebotene Produkte stammen darüber hinaus aus dem sog. "grauen Markt." Dabei handelt es sich um echte Produkte, die etwa aus Diebstähle stammen oder nach Verletzung von Lizenzverträgen im Markt offeriert werden.

Die Angebote solcher Produkte per Spammail stellen gem. § 17 Abs. 1 1. Alt. UrhG ein Angebot an die Öffentlichkeit dar und zwar unabhängig davon, ob es angenommen wurde oder erfolglos geblieben ist. Diese Handlung bildet einen Unterfall der Verbreitung von urheberrechtlich geschützten Werken und ist strafbar gem. § 106 Abs. 1 2. Alt. UrhG, wenn sie ohne Einwilligung des Urhebers stattfindet,[52] was beim Anbieten von gefälschten Produkten der Fall ist.

---

44 Grundlegend zur Unterscheidung zwischen Verbreitungs- und Äußerungsdelikten s. *E. Kern,* Die Äußerungsdelikte, 1919.

45 Über die verwirklichung eines Verbreitungsdelikts durch die Zusendung von E-Mail vgl. etwa BGHSt 46, 212; 47, 55; Vassilaki, in: Ernst/Vassilaki/Wiebe, Hyperlinks, 170; Gercke, MMR 2001, 678; Hörnle, NStZ 2002, 118; Kudlich, JZ 2002, 310.

46 S. dazu RGSt 14, 398; BGH, NJW 1976, 1984; Sch/Schr/*Lenckner,* § 184 Rz. 9; SK-*Horn,* § 184 Rdnr. 19; *Tröndle/Fischer,* § 184 Rdnr. 13; *Römer,* Verbreitungs- und Äußerungsdelikte im Internet, 93.

47 So etwa §§ 130 Abs. 1 Nr. 1, 140 Abs. 1 Nr. 2 StGB.

48 So etwa §§ 185, 186 1. Alt. StGB.

49 So etwa § 126 StGB.

50 Zum Begriff des Plagiats vgl- etwa Loewenhein in: Schricker UrhG, § 23 Rdnr. 22 ff.

51 Vgl. "Spammer handeln mit illegaler Software, in: www.zdnet.de/news v.29.6.2004.

52 S. dazu Schricker/Hass-Vassilaki, § 106 Rdnr. 15; Tröndler/Fischer, § 9 Rdnr. 5 ff.

Verschafft das Angebot von Fälschungen dem Spammer eine fortlaufende Einnahmequelle, dann handelt er gewerbsmäßig und wird nach § 108a UrhG mit einer Freiheitsstrafe bis zu fünf Jahren oder mit einer Geldbuße belegt.[53]

bb) Pornographiebezogene Straftaten

Schon die oberflächliche Betrachtung von Erotikangeboten, die durch unerbetene E-Mails die Mailbox überfluten, zeigt auf, dass sie den Tatbestand der §§ 184 ff. StGB erfüllen. Die Spammails enthalten Darstellungen sexuellen Verhaltens, die, da sie den Menschen zum bloßen bzw. auswechselbaren Objekt geschlechtlicher Begierde oder Betätigung machen, als pornographisch i.S.d. §§ 184 ff. StGB zu betrachten sind.[54]

Die Zusendung solcher Erotikspammails stellt eine "Verbreitungshandlung" gem. § 184 Abs. 1 StGB dar. Nach dem BGH kommt es für das Merkmal des "Verbreitens" auf eine körperliche Übertragung ebenso wenig wie auf eine Speicherung auf einem permanenten Speichermedium an. Verbreiten i.S.v. § 184 StGB liegt vielmehr vor, wenn eine Datei auf dem Rechner des Nutzers angekommen ist, unabhängig davon, ob sie vom Nutzer abgerufen wurde.[55]

Der gerichtlichen Argumentation ist zuzustimmen. Weder der Gesetzeswortlaut noch die theleologische Auslegung stehen der Entmaterialisierung des Verbreitungsbegriffs entgegen. Die Erweiterung des Schriftenbegriffs auf Datenspeicher in § 11 Abs. 3 StGB bringt vielmehr die Erweiterung bzw. Entkopplung des Verbeitungsbegriffs von der physischen Sendung zwangsläufig mit sich. Indem nun die Zusendung von Spammails mit pornographischem Inhalt eine strafbare Verbreitung darstellt, macht sich der Spammer der Straftaten, die diese Handlung ahnden, strafbar. Er kann etwa wegen Verbreitung von Pornographie an Minderjährige gem. § 184 Abs.1 Nr. 1 StGB bestraft werden. Denn Spam unterscheidet nicht zwischen minderjährigen und erwachsenen Adressaten. Darüber hinaus kommt auch eine Bestrafung wegen Verbreitung "harter" Pornographie gem. § 184a Nr.1, wie diese in § 184a Halbsatz 1 StGB definiert wird oder wegen Verbreitung von Kinderpornographie gem. § 184b Abs. 1 Nr. 1 StGB in Betracht. Für die Strafbarkeit wird freilich vorausgesetzt, dass die per Spam verbreiteten Erotikangebote Tatgegenstände enthalten, die vom Anwendungsbereich der entsprechenden Strafvorschriften erfasst werden, was durch Einzelfallprüfung festgestellt wird.

cc) Vermögensbezogene Straftatbestände

Dass "Finanzspam" ein Produkt von Betrügern darstellt, ist weitgehend bekannt. Unabhängig davon, ob Anlageberatung oder Kredite mit niedrigen Zinsen angeboten werden oder ob es sich um die sog. "Nigeria-E-Mails" handelt, haben die Absender bzw. Spammer ein Ziel: Vor der Auszahlung der versprochenen Gelder, Anteile, Raten etc. sollen "Gebühren" eingezahlt werden, die die Kapitalabzahlung angeblich beschleunigen bzw. ermöglichen sollen. Es liegt auf der Hand, dass die "Finanzexperten" nach der Geldereinzahlung nicht mehr ausfindig gemacht werden können.

Die Absendung von Finanzspam kann als Betrug gem. § 263 StGB bestraft werden. Das Angebot etwa von billigen Krediten stellt ein Vorspiegeln "falscher Tatsachen" dar, nämlich die unwahre Behauptung von Tatsachen, die in Wahrheit nicht gegeben sind. Diese Behauptung bzw. Erklärung erfolgt in einer technischen Übermittlung bzw. durch E-Mail[56] und erregt den Irrtum des E-Mail-Adressaten, indem ein Widerspruch zwischen einer subjektiven Vorstellung und der Wirklichkeit verursacht wird. Für das Vorliegen des Irrtums reicht es aus, dass der Getäuschte Zweifel an der Wahrheit des Vorgespiegelten hat, die Möglichkeit der Unwahrheit aber jedenfalls für geringer hält.[57]

Die freiwillige Einzahlung von "Gebühren" vom E-Mail-Adressaten etwa für die "Genehmigung" des Kredits, stellt eine Verfügung des Opfers dar, nämlich eine Handlung des E-Mail-Adressaten, die unmittelbar, nämlich ohne weitere Handlung des Spammer, vermögensmindernd auswirkt.[58] Denn die Einzahlung führt zu einer nicht durch Zuwachs ausgeglichene Minderung des wirtschaftlichen Gesamtwertes des Vermögens des E-Mail-Adressaten.[59] Da die Spammer sich durch die Zusendung von "Finanzspam" Vermögensvorteilen schaffen wollen, wird ihnen Betrugsabsicht gem. § 263 StGB unterstellt, so dass jede Täuschung der Spammail Adressaten, die zu ihrem Vermögensschaden führt, als vollendeter Betrug gem. § 263 Abs. 1 StGB bestraft wird.

Für die Bestrafung der Spammer ist die Vollendung der Betrugshandlung nicht zwingend. Da gem. § 263 Abs. 2 StGB auch der Versuch des Betruges strafbar ist, kann schon die Zusendung von Finanzspam strafbar sein. Als versuchter Betrug wird die Vornahme einer auf Täuschung und der Verwirklichung aller Tatbestandsmerkmale abzielenden, aber nicht zum Erfolg gelangenden Handlung gesehen.[60] Die Zusendung vom Finanzspam erfüllt diese Voraussetzungen. Die Spammail enthält falsche Tatsachen und soll vom Spam-Adressat als ernstgemeintes Vertragsangebot angesehen und angenommen werden. Weil darüber hinaus für die Strafbarkeit des versuchten Betrugs nicht erforderlich ist, dass der zu Täuschende von der Täuschung Kenntnis erlangt oder sich täuschen lässt,[61] reicht für die Strafbarkeit des Spammers gem. § 263 Abs. 2 StGB die bloße Zusendung von Finanzspam aus.

Dabei darf nicht übersehen werden, dass die massenhafte Zusendung von Finanzspam darauf hinweist, dass die Spammer bzw. Täter gewerbsmäßig handeln. Dadurch wird auch der besonders schwere Fall des gewerbsmäßigen Betruges erfüllt, der gem. § 263 Abs. 1 Nr. 1 StGB mit einer Strafe von sechs Monaten bis zu sechs Jahren geahndet wird.

Auch das "Phishing" kann als Betrug gem. § 263 StGB bestraft werden. Die Zusendung von gefälschten Webseiten stellt eine "falsche Tatsache" dar, die Herbeiführung eines Irrtums erzielt, dass nämlich die Bank, auf die sich das Konto des E-Mail-Adressaten befindet, die konkrete

53 S. dazu Schricker/Hass-Vassilaki, § 108a Rdnr. 2.
54 Vgl. dazu OLG Düsseldorf, NJW 1974, 1474; Sch/Schr/Lenckner-Peron, § 184 Rdnr. 5; LK-Laufhütte § 184 Rdnr. 1017.
55 BGHSt 47, 55.
56 So Tröndler/Fischer, § 263 Rdnr. 11.
57 Vgl. etwa BGHSt 24, 260; OLG Düsseldorf, NJW 1989, 2003; LK-Tiedemann, § 263 Rdnr. 84 f.; Sch/Schr/Cramer § 263 Rdnr. 38 ff.
58 Vgl. BGHSt 14, 170 f.; BGHSt 31, 178 f.; Lackner/Kühl, § 263 Rdnr. 22; SK-Samson/Günther, § 263 Rdnr. 77.
59 Sog. Prinzip der Gesamtsaldierung vgl. dazu etwa BGHSt 16, 321; 34, 201; Sch/Schr/Cramer, § 263 Rdnr. 91, 119; Tröndle/Fischer, § 263 Rdnr. 71; Bottke, JR 1987, 428.
60 So etwa BGHSt 2, 380; 4, 272; BGH, NJW 1989 1436.
61 So BGH Wistra 1984, 225 f.; BGH NStZ 1994, 236.

Anfrage gesendet hat. Man könnte freilich argumentieren, dass der Betrugstatbestand nicht anwendbar ist, weil eine Vermögensverfügung seitens des E-Mail-Adressaten nicht vorliegt. Denn das Erlangen von Konto- und PIN-Nummer des E-Mail-Adressaten von einem Buchungs- oder Girokonto, das die Folge des Irrtums sein soll, führe "per se" zu keinem unmittelbaren Eintritt der Verschiebung von Vermögenswerten. Die Täter-Phisher müssen vielmehr weitere Handlungen vornehmen, um auf das Vermögen des Phishingmail-Adressaten zuzugreifen. Gegen diese Beanstandung ist folgendes einzuwenden: Die Abgabe von Konto- und PIN-Nummer des E-Mail-Adressaten kann vermögensmindernd wirken und unmittelbar vermögensrelevante Folgen haben. Ähnlich wie bei der Übergabe der Zahlenkombination eines Tresors, zu dem der Täter ungehinderten Zugang hat, oder bei der Überreichung eines blanko unterschriebenen Schecks[62] hängt die Vermögensminderung beim "erfolgreichen" Phishing lediglich vom Willen des Täters bzw. Täuschenden ab. Ein eigener Zugriff des Phishers auf den Vermögenswert des E-Mail-Adressaten, der eine Verfügung i.S.d. § 263 StGB ausschließen würde, ist nicht erforderlich. Denn durch die auf die Täuschung beruhende Handlung, nämlich die Abgabe von Konto- und PIN-Nummer des E-Mail-Adressaten, ist die wesentliche Zugriffsschwelle bereits überschritten worden. Damit ist die Abgabe von Konto- und PIN-Nummer des E-Mail-Adressaten als Vermögensverfügung zu bewerten, die zum Vermögensschaden und schließlich zum Erfüllung des objektiven Tatbestands des § 263 ABs. 1 StGB führt.

Für die Zusendung von Phishingmails kommt die Strafbarkeit wegen versuchten Betrugs gem. § 263 Abs. 2 StGB in Betracht. Diese Handlung setzt unmittelbar zur Tat an, denn nach dem Plan der Phisher ist die Zusendung der E-Mail der Verwirklichung eines Tatbestandsmerkmals, nämlich die Herbeiführung des Irrtums bei den E-Mail-Adressaten, unmittelbar vorgelagert und wird im Falle ungestörten Fortgangs ohne Zwischenakte in die Tatbestandshandlung, nämlich die durch die Angabe von Konto- und PIN-Nummer des E-Mail-Adressaten ermöglichte Vermögensverfügung, unmittelbar einmünden.[63] Weil darüber hinaus für die Strafbarkeit wegen versuchten Betruges nicht erforderlich ist, dass der zu Täuschende von der Täuschung Kenntnis erlangt oder sich täuschen lässt, ist die Strafbarkeit der Zusendung von Phishingmails wegen strafbaren versuchten Betrugs gem. § 263 Abs. 2 StGB zu bejahen.

dd) Arzneimittelrechtsbezogene Straftaten

In den ersten Phasen der Zusendung von unerbetenen E-Mails wurden Spammails durch Angebote für Medikamente wie Viagra bekannt. Beachtlich sind auch heute die niedrigen Preise, die der Internetkunde für Medikamente, die mittels Spammails angeboten werden, zahlen muss. Ein Grund für diese Dumpingpreise liegt in der Tatsache, dass die angebotenen Medikamente Plagiate darstellen.

Gleichwohl ist es nicht nur das Angebot von Plagiaten, das die Zusendung von Spammails mit pharmazeutischem Inhalt strafrechtlich bedenklich macht. Im Hinblick auf die Straf- und Bußeldvorschriften des Arzneimittelgesetzes (AMG), lassen sich die Aktivitäten der Spammer, die bestraft werden können, in drei Gruppen gliedern:

(1) Anbieten von Plagiaten.

In vielen Fällen bieten die Spammer Produkte an, die

- nur temporär funktionell dem Original gleichwertig sind,
- bestimmten Medikamenten ähnlich sind, wobei sie das Image der Originalmedikamente nutzen oder
- positive Assoziationen beim Käufer hervorrufen, indem sie ähnliche Medikamente mit Bildern und Zeichen des Originalmedikaments versehen.[64]

Durch solche Angebote machen sich die Spammer wegen Verletzung des AMG strafbar. Ist die Qualität der angebotenen Arzneimittel erheblich gemindert, ist es gem. § 8 Abs. 1 Nr. 1 AMG verboten, solche Arzneimittel im Verkehr zu bringen bzw. nach § 4 Abs. 17 AMG zum Verkauf anzubieten. Die Verletzung dieses Verbots stellt eine strafbare Handlung dar, die nach § 95 Abs. 1 3a AMG mit Freiheitsstrafe bis zu drei Jahren oder mit Geldbuße belegt wird. Werden dagegen für den Verkauf des Medikaments Bezeichnungen oder Angaben verwendet, die für die Bewertung des Medikaments von Bedeutung sind, sind solche Angaben irreführend und gem. § 8 Abs. 1 Nr. 2 AMG verboten. Diese irreführende Handlungen werden gem. § 96 Abs. 3 AMG mit einer Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.

Es trifft zwar zu, dass der Spammer, der solche Medikamente zum Verkauf anbietet, behaupten kann, dass ihm nicht bekannt war, dass die Produkte, die er per Internet im Verkehr bringt, gefälschte Medikamente sind. Ob ein solcher Irrtum vorliegt, der den Vorsatz gem. § 16 StGB ausschließt, hängt aber davon ab, ob der Spammer die ihm zumutbaren Erkundigungen eingeholt hatte. So hat der Spammer, der ein Arzneimittel von einer international angesehenen Firma anbietet, die ordnungsgemäße Beschaffenheit der Ware weniger intensiv zu überprüfen als derjenige, der Arzneimittel von einem unbekannten Hersteller durch die Zusendung von Spam wirbt.[65]

(2) Anbieten von verschreibungspflichtigen Medikamenten an Endverbraucher

In vielen Fällen sind die durch die Zusendung von Spammails angebotenen Medikamente verschreibungspflichtig. Viele Spammails aber werben gerade damit, dass kein ärztliches Rezept für den Verkauf der verschreibungspflichtigen Produkte erforderlich ist. Die freie Abgabe bzw. Zusendung von verschreibungspflichtigen Medikamente wird gem. § 95 Abs. 1 Nr. 8 AMG mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Weil darüber hinaus auch der Versuch dieser Tat unter Strafe gem. § 95 Abs. 2 AMG gestellt wird, ist schon die Zusendung von Spammails mit dem Angebot, verschreibungspflichtige Medikamente ohne Rezept zu liefern, strafbar.

(3) Anbieten von verschreibungspflichtigen Medikamenten an nicht pharmazeutischen Unternehmen

Gem. § 47 AMG dürfen pharmazeutische Unternehmer und Großhändler Arzneimittel, deren Abgabe den Apotheken vorbehalten ist, nur an bestimmte pharmazeuti-

62 Vgl. dazu nur Sch/Schr/Cramer, § 263 Rdnr. 61; Tröndler/Fischer, § 263 Rdnr. 46.

63 Dazu etwa BGHSt 26, 203.

64 Über die unterschiedlichen Formen von Produktpiraterie im Pharma-Bereich vgl. etwa Maul/Maul, GRUR 1999, 1059 ff.

65 Über die Irrtumsfrage im AMG vgl. Sander/Epp, AMG, Einl. § 95 Nr. 2.

sche Unternehmer, Großhändler und Einrichtungen abgeben. Diese Kontrolle der Vertriebswege soll eine Garantie dafür bieten, dass diejenigen, die solche Arzneimittel besitzen, sorgsam damit umgehen, so dass keine Gefahr für die Gesundheit der Öffentlichkeit daraus entsteht. Spammer sind im ausschließlichen Katalog der Norm nicht enthalten und können nicht in eine Kategorie der in der Vorschrift erwähnten Gruppen eingeordnet werden. Weil darüber hinaus die Abgabe an andere als die in § 47 AMG bezeichneten Personen oder Stellen gem. § 95 Abs. 1 Nr. 5 AMG unter Strafe steht, machen sich die Lieferanten der Medikamente, die durch die Zusendung von Spammails angeboten werden, strafbar und können mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden.

ee) Politikbezogener Spam

Obwohl Spammail mit politischem Inhalt nur einen kleinen Anteil des Spamverkehrs ausmacht, werden solche E-Mails von der Öffentlichkeit mit Beunruhigung registriert. Der Verfassungsschutzbericht hebt hervor, dass in den Jahren 2002-2003 der Einsatz von E-Mail-Kommunikation unter den Rechtsextremisten an Bedeutung gewann. So wurde etwa im Januar 2003 eine große Anzahl Spammails mit verschiedenen gefälschten Absenderkennungen versendet, die eine von Rechtsextremisten geplante Demonstration bewarb. Mitte September 2003 rief ein Rechtsextremist mit einer Spammailaktion Kameraden dazu auf, durch Gewalttaten gegen Ausländer einen Bürgerkrieg zu provozieren und dadurch einen Systemumsturz herbeizuführen.[66] Die Zusendung solcher Spammails kann nach §§ 111, 130 StGB bestraft werden.

§ 111 StGB bestraft die Aufforderung zu rechtswidrigen Taten, sofern sie öffentlich in einer Versammlung oder durch Verbreiten von Schriften erfolgt. Unter Aufforderung ist eine bestimmte Erklärung zu verstehen, dass jemand etwas tun oder unterlassen soll. Diese Erklärung muss sich aus der Schrift ergeben und über eine bloße Befürwortung hinausgehen.[67] Unter III.3.b.bb ist erläutert worden, dass nach BGH-Rechtsprechung Schriften auch durch das Versenden von E-Mails verbreiten werden können, so dass die in § 111 StGB ausgeführte Begehungshandlung durch die Zusendung von Spammails gegeben ist. Enthält die Spammail eine an die Motivation Dritter gerichtete Erklärung, die erkennbar ein bestimmtes rechtswidriges Tun - etwa die Ausführung von Gewalttaten gegen Ausländer - verlangt, was eine Tatfrage ist, dann ist der objektive Tatbestand der öffentlichen Aufforderung zu Straftaten erfüllt. Nimmt der Spammer darüber hinaus billigend in Kauf, dass seine Aufforderung ernst genommen wird, dann ist auch Vorsatz und damit die Strafbarkeit nach § 111 StGB gegeben.

Enthält die Spammail volksverhetzende Äußerungen, dann kommt für den Spammer eine Strafbarkeit nach § 130 Abs. 2 Nr. 1 a StGB in Betracht. Für die Erfüllung des objektiven Tatbestandes ist entscheidend, dass die Äußerungen geeignet sind, den öffentlichen Frieden zu stören, was wiederum eine "öffentlichkeitsfähige" Äußerung voraussetzt.[68] Diese liegt vor, wenn "nach den konkreten Umständen damit zu rechnen ist, dass der Angriff einer breiteren Öffentlichkeit bekannt wird".[69] Weil die Größe des Empfängerkreises ein wesentliches Kriterium für die Annahme der öffentlichkeitsfähigen Äußerung darstellt und das wesentliche Element von Spam ist, dass er einen breiten Adressatenkreis erreichen will, ist auch dieses Tatbestandsmerkmal zu bejahen.[70] Der subjektive Tatbestand verlangt Vorsatz, der auch die Störungseignung umfassen soll. Weil den Spammern die Wirkung der Zusendung von Spammails bewusst ist, ist auch der subjektive Tatbestand erfüllt.

c) Strafbare Werbung nach dem § 16 Abs. 1 UWG

In den meisten Fällen bringt die Zusendung von Spammails eine Strafbarkeit wegen strafbarer Werbung gem. § 16 UWG Abs. 1 mit sich und zwar unabhängig davon, was für Inhalte sie haben. Die Norm bestraft mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe denjenigen, der in der Absicht, den Anschein eines besonders günstigen Angebots hervorzurufen, in öffentlichen Bekanntmachungen oder in Mitteilungen, die für einen größeren Kreis von Personen bestimmt sind, durch unwahre Angabe irreführend wirbt.

Für die Erfüllung des Tatbestandmerkmals "Mitteilungen, die für einen größeren Kreis von Personen bestimmt sind" ist nach der Rechtsprechung von RG und BGH die Wiederholung entscheidend der "in ihrer sachlichen Gehalt gleichbleibenden Behauptung".[71] Weil das Hauptelement von Spam die Versendung von E-Mails mit demselben Inhalt ist, liegt dieses Merkmal nach § 16 Abs. 1 UWG vor.

Die Angaben, die in den Mitteilungen gemacht werden, müssen "unwahr" sein. „Unwahr“ sind die Angaben, wenn sie mit der objektiven Wahrheit nicht übereinstimmen und zwar unabhängig davon, wie der Empfänger sie erfasst.[72] Dies ist etwa der Fall, wenn die per Spammails angebotenen Waren Fälschungen darstellen.

Die Werbung muss darüber hinaus "irreführend" sein. Nach dem neuen UWG ist Maßstab für de Bejahung der Irreführung der durchschnittlich informierte aufmerksame und verständige Verbraucher.[73] Erweckt nun die Spammail beim durchschnittlichen Spam-Adressat Vorstellungen, die aufgrund der falschen Grundlage nicht realisiert werden können, begeht der Spammer eine irreführende Werbung. Die Feststellung, wann eine Irreführung vorliegt, ist eine richterliche Aufgabe. Der Tatrichter kann sich ohne großen Aufwand eine Meinung bilden, wenn er selbst zu dem Verkehrskreis gehört, auf den es für die Ermittlung des Sinnes einer Angabe ankommt. So ist es etwa, wenn es um die Irreführung von Verbrauchern geht, zu denen auch der Richter gehört oder wenn die Angaben einer Werbung beurteilt werden müssen, die sich an das allgemeine Publikum wendet.[74]

Der Spammer wird wegen strafbarer Werbung gem. § 16 Abs. 1 UWG bestraft, wenn er mittels des Inhalts der

---

66 Ausführlich dazu Verfassungsschutzbericht 2003, S. 107 ff.; dazu vgl. auch Verfasschungsschutzbericht 2002, 103 ff.

67 BGHST 28, 314; 32, 310; ausführlich dazu Vassilaki/Martens, Computer- und Internetstrafrecht, 14 ff.

68 So etwa BGHSt 29, 27; 34, 332; 46, 42; Sch/Schr/Lekcner, § 130 Rdnr. 11; LK-von Bubnoff § 130, Rdnr. 13; Tröndler/Fischer § 130, Rdnr. 14.

69 So BGHSt 29, 27; 34, 332.

70 So auch Hörnle, NStZ 2002, 117.

71 S. etwa RGSt 64, 248; BGHSt 24, 274.

72 *BGH* BB 1954, 299; *Erbs/Kohlhaas/Führmann,* § 4 UWG Rdnr. 12; *Müller-Gugenberger/Niemeyer,* § 49 Rdnr. 12; *Hernández,* Strafrechtlicher Vermögensschutz vor irreführender Werbung, 181 f.; *Gribkowsky,* Strafbare Werbung, 47 f.; *Meyer/Möhrenschlager,* WiVerw 1982, 21, 24; *Pfeiffer,* in: FS für Lieberknecht 1997, S. 210.

73 S. dazu RegE UWG BT-Drucks. 15/1487, 19.

74 S. dazu etwa *BGH,* NJW 1962, 2151; *BGH,* NJW 1980, 468; *BGH,* GRUR 1984, 468; *Otto,* UWG-Großkommentar, § 4 UWG Rdnr. 43.

Spammail den Anschein eines besonders günstigen Angebots hervorruft. Ein solcher Anschein liegt vor, wenn der Werbende sein Angebot durch das Hervorheben besonderer Vorteile als besonders günstig erscheinen lässt. Damit ist nicht unbedingt ein materieller Vorteil verbunden, d.h. sein Angebot muss nicht grundsätzlich preisgünstig sein.[75] Nicht maßgebend ist auch, ob der angepriesene Vorteil in Wirklichkeit fehlt. Es genügt vielmehr, dass ein möglicherweise vorhandener Bonus durch die irreführende Werbung besonders akzentuiert wird.[76] Dieses subjektive Merkmal wird in den meisten Fällen zu bejahen sein. Denn die Spammer versuchen Käufer zu gewinnen, indem sie etwa außerordentlich billige Software oder eindrucksvolle Bedingungen für die Gewährung eines Kredits anbieten. In den meisten Fällen reicht es den Titel der Spammail zu lesen, um den subjektiven Tatbestand bzw. die Absicht des Spammers zu bejahen.

d) Zusenden von Spammails als Störung von Telekommunikationsanlagen gem. § 317 StGB

Mehrmals ist die Forderung aufgestellt worden, das Zusenden von E-Mails "per se" unter Strafe zu stellen. Zweifelhaft ist allerdings, ob eine solche neue Strafvorschrift notwendig ist oder ob das "Spamming" schon strafbar ist. Denn in vielen Fällen wird durch die Zusendung von Spammails das ordnungsgemäße Funktionieren des E-Mail-Verkehrs beeinträchtigt. Unter diesem Gesichtspunkt ist zu prüfen, ob die Prämissen des § 317 StGB erfüllt werden, der die "Störung von Telekommunikationsanlagen" bestraft.

Schutzobjekte des § 317 Abs. 1 StGB sind Telekommunikationsanlagen. Für die Konkretisierung dieses Begriffs verweist die strafrechtliche Kommentierung auf das TKG, das in § 3 Nr. 23 unter Telekommunikationsanlagen technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können, definiert. Hierzu zählt jede Datenübermittlung[77] und - daher - Server, die die Internetkommunikation steuern und auch Nachrichten- bzw. E-Mail-Übertragung zwischen Provider und Internetnutzer vermitteln.[78] Die strafrechtlich geschützten Telekommunikationsanlagen müssen öffentlichen Zwecken dienen. Dies ist der Fall, wenn der Betrieb der Anlagen ausschließlich oder überwiegend im Interesse der Allgemeinheit liegt. Werden demzufolge Server eingesetzt, und den Datentransfer zwischen Internetteilnehmer aus unterschiedlichen Netzen zu ermöglichen, ist die öffentliche Zweckdienlichkeit zu bejahen. Server dagegen, die nur die interne Telekommunikation (Intranet) etwa einer Firma unterstützen, dienen - ähnlich wie die rein hausinternen Sprechanlagen - keinen öffentlichen Zwecken.

Damit ist festzuhalten, dass Server, die Online-Kommunikation außerhalb von LAN-Netzwerken ermöglichen, Schutzobjekte des § 317 StGB darstellen.

Gem. § 317 Abs. 1 StGB wird derjenige bestraft, der den Betrieb der Telekommunikationsanlage bzw. des Servers verhindert oder gefährdet. Eine Gefährdung ist bereits dann gegeben, wenn das genaue Funktionieren des Betriebes beeinträchtigt ist, so dass ein potentieller Benutzungswunsch nicht erfüllbar wäre.[79] Die Gefährdung soll - unter anderem - dadurch erfolgen, indem eine dem Betrieb dienende Sache vom Täter beschädigt wird. Beschädigung liegt auch dann vor, wenn die Einwirkung auf die Sache die bestimmungsgemäße Brauchbarkeit der Telekommunikationsanlage mindert.[80]

Werden nunmehr von Spammern hunderttausend von E-Mails an einem Server versendet, werden die Kapazitäten der einzelnen E-Mail-Boxen rasch belegt bzw. ausgeschöpft. Dies hat zur Folge, dass der Teil des Servers, der die Aufgabe hat, die E-Mails zu verwalten, nämlich der spezielle Mail-Server, überfordert und damit das Empfangen von weiteren Nachrichten verhindert wird. Damit haben die E-Mail-Adressaten keine Möglichkeit, ihre Mailboxen bestimmungsgemäß zu benutzen und der Server lässt sich nicht funktionsentsprechend voll einsetzen. Weil darüber hinaus für das Vorliegen einer Beschädigung gem. § 317 Abs. 1 StGB nicht von Bedeutung ist, ob die Beeinträchtigung längere Zeit oder nur kurzfristig dauert,[81] ist es unerheblich, ob der Mail-Server nur ein paar Stunden oder Tage außer Betrieb ist. Um die Beschädigung des Mail-Servers zu bejahen, die zur Gefährdung des Betriebs des gesamten Servers führt, reicht es aus, dass der Inhaber einer E-Mail-Adresse keinen Zugang auf seine E-Mails hat bzw. keinen neuen E-Mails empfangen kann.

Ist nunmehr der objektive Tatbestand des § 317 Abs. 1 StGB erfüllt, muss der Täter mit Vorsatz oder Fahrlässigkeit handeln. Der Vorsatz muss sowohl die Beschädigung der konkreten Sache als auch die Gefährdung des Betriebes erfassen, wobei bedingter Vorsatz genügt. Es liegt auf der Hand, dass die Spammer damit rechnen und davon ausgehen bzw. es für möglich halten, dass die tägliche Zusendung von Millionen E-Mails Mail-Server überfüllt und die reibungslose Funktion der Internetkommunikation, die durch diese Server ermöglicht wird, gefährdet wird. Davon auszugehen ist auch, dass die Spammer um ihr Ziel, nämlich die erfolgreiche Zusendung von unerwünschten E-Mails, zu erreichen, es dem Zufall überlassen, ob die Beeinträchtigung der Mail-Server realisiert wird und damit den Erfolg bzw. die Störung der Telekommunikationsanlage billigen. Demnach machen sich Spammer durch die massive Zusendung von Spammails gem. § 317 StGB strafbar.

IV. Das geplante "Anti-Spam-Gesetz"

Die vorangegangene Darstellung belegt, dass es eine Reihe von Strafvorschriften gibt, nach denen die Zusendung von Spammail sowohl wegen ihren Inhalten als auch wegen der Zusendung "per se" strafbar ist. Die materiellen Strafnormen sind somit vorhanden, so dass die Diskussion über die Einführung neuer Strafvorschriften nicht fortgeführt werden muß.

In bezug auf das konkrete gesetzgeberische Vorhaben sind insbesondere folgende Einwände vorzubringen:

- Die Einführung einer Ordnungswidrigkeit, die lediglich die Zusendung von Spam ahndet, übersieht die Komple-

---

75 S. etwa *RGSt* 40, 122 ff.; 47, 280 ff.; *BGHSt* 4, 44 ff.; 27, 293 ff.; *KG,* JR 1973, 428 ff.; *BayObIG,* GRUR 1959, 427.

76 S. dazu etwa *RGSt* 40, 281.

77 So Sch/Schr/Cramer/Sternberg-Lieben, § 317 Rdnr. 3; Tröndler/Fischer § 317, Rdnr. 2, Haß, in: Manssen TKMMR, § 85 Rdnr. 11.

78 So ausdrücklich, BeckTKG-Komm/Büchner § 85 Rdnr. 2, auch Würmeling/Felixberger, CR 1997, 231.

79 Sch/Schr/Cramer/Sternberg-Lieben, § 317 Rdnr. 5.

80 RGSt 66, 205; BGHSt 44, 38;Tröndle/Fischer, § 303 Rdnr. 5; Sch/Schr/Stree, § 303 Rnd. 8b.

81 Stree, JuS 1988, 188.

xität des Phänomens "Spam", das - wie oben (II. 5) ausgeführt - drei gleichwertige Bestandteile hat, nämlich das Erwerben von E-Mail-Adressen, das Einsetzen von technischen Maßnahmen, die diese Kommunikationsform unterstützen, und die Versendung von Spammails. Das vorgeschlagene Anti-Spam-Gesetz läßt die Tatsache außer Acht, dass nur der Angriff gegen alle Bestandteile des Phänomens "Spam" eine erfolgversprechende Strategie für seine Bekämpfung darstellen kann.

- Aus demselben Grund ist die Platzierung der vorgeschlagenen Normen im Teledienstegesetz verfehlt. Denn dadurch wird Spam als ein Teledienst eingestuft, der unter bestimmten Voraussetzungen zulässig ist. Diese Schlussfolgerung bringt zwei Konsequenzen mit sich:

Erstens: Es droht die Verwischung der Grenzen zwischen zulässigem rechtskonformen E-Mail-Marketing und Spammailing. Dies kann zur Rechtsunsicherheit bzw. -unklarheit in bezug auf das elektronische Direktmarketing führen.

Zweitens: Es wird nicht genügend der Tatsache Rechnung getragen, dass der Versand und Empfang von Spammails in den meisten Fällen auf rechtswidrige Handlungen, nämlich Ausspähen von personenbezogenen Daten und Mißbrauch von Sicherheitslücken in Computersystemen, beruht.

- Der Gesetzentwurf nimmt keine Stellung zu der Frage, ob und gegebenenfalls unter welchen Voraussetzungen Provider Spammails filtern und löschen dürfen. Insbesondere nach dem Beschluß des OLG Karlsruhe vom 10.1.2005 (Az: 1 Ws 152/04), nach dem das gezielte Ausfiltern von E-Mails von Providern wegen Verletzung des Post- und Fernmeldegeheimnisses strafbar sein kann, sind entsprechende Klarstellungen in einem Gesetzesvorhaben notwendig.
- Indem der Gesetzentwurf nur die Zusendung von "kommerziellen Spammails" regeln und gegebenenfalls ahnden will, erfasst dieser nicht alle Erscheinungsformen von Spam. So wird z. B. aus dem Anwendungsbereich der vorgeschlagenen Norm die Zusendung von politischem Spam ausgenommen, der ausländerfeindlichen oder rassistischen Inhalt hat. Ferner werden Spammer verschont, die, etwa durch die Zusendung von Spam in Chatgroups von Kindern, Opfer für perverse Praktiken suchen.
- Die Einführung des Verbotes, in der Kopfzeile einer kommerziellen E-Mail die wahre Identität des Absenders zu verschleiern oder zu verheimlichen, und die Ahndung der Verletzung dieses Verbots ist unentbehrlich. Wie schon oben (s. III. 2b) dargestellt wurde, können diese Handlungen als Urkundenstraftaten gem. §§ 267, 269 StGB bestraft werden.
- Die vorgeschlagenen §§ 7 Nr. 3 und 12 Abs. 1 Nr. 2 TDG sind unglücklich formuliert. Als Verschleiern oder Verheimlichen definiert § 7 Nr. 3 TDG/Entw. insbesondere die "absichtliche" Gestaltung der Kopf- oder Betreffzeile auf eine Weise, dass die wahre Identität des Absenders oder der kommerzielle Charakter der E-Mail nicht ersichtlich ist. Demgegenüber belegt § 12 Abs. 1 Nr. 2 TDG/Entw. jeden mit Geldbuße, der "vorsätzlich oder fahrlässig" die Identität des Absenders oder den kommerziellen Charakter der E-Mail verschleiert oder verheimlicht. Dies würde aber bedeuten, dass derjenige mit einer Geldbuße belegt werden kann, der fahrlässig eine identitätsverschleiernde oder identitätsverheimlichende Gestaltung der Kopf- oder Betreffzeile vornimmt. Dass dies keine sinnvolle Subsumption wäre, liegt auf der Hand.

Diese Bemerkungen sollen verdeutlichen, dass es in dem vorliegenden Gesetzentwurf nicht gelungen ist, das Problem umfassend zu regeln und Spam erfolgreich zu bekämpfen. Es trifft zwar zu, dass die Schwierigkeiten, die mit der Frage verbunden sind, ob und in welchen Fällen das deutsche Strafrecht anwendbar ist oder wie man aus strafprozessualer Sicht Beweise gewinnen kann, die für die Aburteilung von Spammern notwendig sind, nicht unterschätzt werden dürfen. Diese Rechtsprobleme sind allerdings immer präsent und zwar unabhängig davon, ob neue oder schon vorhandene Strafvorschriften anzuwenden sind. Aus diesem Grund gelten für die Bekämpfung von Spam dieselben Regeln, die für andere Formen der Internetkriminalität anerkannt sind: Ein Bündel von Maßnahmen ist erforderlich, die organisatorischer, technischer und last but not least rechtlicher Natur sind.

- Die **organisatorischen** Maßnahmen betreffen - im wesentlichen - die Regeln nach denen die "Markt-Players" etwa die Firmen, die Online-Marketing betreiben, agieren. Selbstregulierung kann unter diesem Gesichtspunkt hilfreich sein, um die seriösen Marktteilnehmer von den unlauteren zu unterscheiden. Darüber hinaus ist der Einsatz von Kampagnen notwendig, die den Verbraucher informieren, was Spam ist, wie man es vermeidet und sich dagegen wehrt.
- Die Entwicklung von **technischen Lösungen,** die Spammail erkennen und herausfiltern können, stellt eine unentbehrliche Bedingung bei der Bekämpfung von Spam dar.
- Aus **rechtlicher Sicht** kann die Anwendung von bestehenden Strafnormen hilfreich sein. Dafür sind allerdings in größerem Umfang Schulungen beispielsweise in Form von speziellen Ausbildungsseminaren der Strafverfolgungsbehörden (Staatsanwaltschaft und Polizei) im Bereich IT-Recht erforderlich. Denn es ist verständlich, dass ein Staatsanwalt, der keine speziellen Kenntnisse in diesem Bereich hat, keine Ermittlungen einleiten kann und will. Nicht zuletzt ist die internationale Zusammenarbeit von Ermittlungsbehörden erforderlich, denn Spam stellt kein nationales, sondern ein internationales Problem dar.

Wird ein Bündel solcher Maßnahmen in der Praxis umgesetzt, dann gibt es ausreichende Chancen, diese Plage zu besiegen. Der Ruf nach neuen Strafnormen bzw. Ordnungswidrigkeiten kann dagegen nur populistische Erfolge haben und den symbolischen Charakter des Strafrechts wieder einmal betonen. Der Bekämpfung des Übels hilft er nicht!

Für den Fachausschuß Strafrecht
PD Dr. Irini E. Vassilaki

Für den Vorstand
Prof. Dr. Alfred Büllesbach

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1847**

8. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

Rechtsanwaltskanzlei Härting

Thesen zu einem „Anti-Spam-Gesetz"

1. **Kriminalisieren statt Bagatellisieren:**

   In der Begründung des Gesetzentwurfes heißt es, man wolle „Spammer" nicht „kriminalisieren" (Gesetzentwurf S. 14). In dieser Formulierung kommt eine bedenkliche Bagatellisierung des Spamming zum Ausdruck, die der Problematik nicht gerecht wird. Die Bagatellisierung ist weitverbreitet und kommt u.a. darin zum Ausdruck, dass Verbraucherschutz- und Wettbewerbsverbände von ihrem gesetzlichen Klagerecht nach dem UWG so gut wie keinen Gebrauch machen. Fragt man nach den Gründen, hört man immer wieder, dass sich „wegen einer einzigen Spam-Mail" der Aufwand eines Streitverfahrens nicht lohne. Diese Sichtweise hat dazu geführt, dass die (zahlreichen) Unterlassungsurteile, die es gegen Spammer gibt, zum ganz überwiegenden Teil von Rechtsanwälten in eigener Sache erstritten wurden.

2. **Global Denken**: Der Trend geht zum Strafrecht.

   In zahlreichen Staaten sind in den letzten Jahren Gesetze geschaffen worden, die Geldbußen, Geldstrafen und sogar Freiheitsstrafen für Spammer vorsehen. Entsprechende Bestimmungen gibt es bereits nicht nur ~~bereits~~ in vielen Ländern der Europäischen Union, sondern beispielsweise auch in Australien, den USA und Norwegen (vgl. die Übersichten anbei). Wer daher vor einer „Kriminalisierung" des Spamming zurückschreckt, scheut sich vor dem notwendigen gesetzlichen Standard, der in anderen Ländern bereits erreicht ist.

3. **National ~~ist~~ ist International**: Internationale Maßnahmen setzen nationales Handeln voraus.

   Häufig hört man den achselzuckenden Satz, der nationale Gesetzgeber könne gegen das Spamming wenig ausrichten, da es sich um ein globales Phänomen handle und ausländische Spammer dem Zugriff des nationalen Gesetzgebers zumeist entzogen sind. So richtig es indes ist, Internationale Maßnahmen zu fordern, ist doch ein einheitlicher nationaler Gesetzesstandard die Grundvoraussetzung für den Erfolg des internationalen Kampfes gegen das Spamming. Dies spricht eindeutig für die Notwendigkeit strafrechtlicher Bestimmungen in Deutschland.

4. **Schutzgut Telekommunikation**: Es geht um den Missbrach von Telekommunikations-Infrastruktur.

   Das Spamming bedroht die Funktionstüchtigkeit der E-Mail als Kommunikationsmittel. Es geht somit beim Kampf um Spamming nicht nur um unlautere Werbung, sondern um den Schutz von Telekommunikations-Infrastruktur gegen Missbrauch.

5. **Alle Spammer sind gleich**: Es gibt keinen Unterschied zwischen „harmlosen" und „kriminellen" Spammern.

   Der Kampf gegen das Spamming erfordert konsequentes Handeln. Jede einzelne Spammail trägt zur Gefährdung einer effizienten E-Mail-Kommunikation bei. Jedwede Unterscheidung zwischen „Einzelmails", „Massen-Spammern", „irreführenden Spam-Mails" u.a. Unterformen des Spamming läuft letztlich auf eine Bagatellisierung hinaus.

6. **Die RegTP ist eine Behörde, die für die Verfolgung des Spamming als Ordnungswidrigkeit geeignet wäre.**

   Die geplante Einfügung des Bußgeldtatbestandes in § 12 TDG ist verfehlt. Zuständig für die Verfolgung von Ordnungswidrigkeiten nach dem TDG sind die Ordnungsbehörden der Städte~~n~~ und Gemeinden. Dass dies nicht effizient ist, zeigt sich daran, dass – ob-

wohl § 12 TDG in seiner jetzigen Form bereits seit mehreren Jahren in Kraft ist – kein einziges Verfahren bekannt ist, dass nach der jetzigen Fassung des § 12 UWG (Verletzung der Impressumspflicht) geführt wurde. Im übrigen ist es nicht einsichtig, weshalb die geplante Regelung sachlich dem Teledienste- und nicht dem Telekommunikationsrecht zugeordnet wird, da es doch (auch) um den Schutz von Telekommunikations-Infrastruktur geht.

Die RegTP hingegen hat ihre Handlungsfähigkeit und Effizienz bereits bei der Bekämpfung des Dialer-Missbrauchs erfolgreich unter Beweis gestellt.

7. Der Gesetzesentwurf geht zu weit.

Der Gesetzesentwurf unterscheidet nicht zwischen erwünschter und unerwünschter bzw. zwischen wettbewerbsrechtlich zulässiger und unlauterer Werbung. Nach dem jetzigen Gesetzentwurf würde die Bußgeldbestimmung auch für Werbemails gelten, die – wegen Zustimmung des Empfängers – wettbewerbsrechtlich erlaubt sind. Eine irreführende Betreffzeile könnte bereits genügen, um den Tatbestand zu erfüllen.

8. Der Gesetzentwurf geht nicht weit genug.

Verfehlt und bagatellisierend ist es, dass der Gesetzesentwurf sich nicht generell gegen Spammails richtet, sondern nur gegen Mails mit gefälschten bzw. irreführenden Angaben zum Absender bzw. zum Werbecharakter der Mail. Wegen des in soweit höchst eingeschränkten Anwendungsbereichs des Gesetzentwurfs ist die Bezeichnung als „Anti-Spam-Gesetz“ selbst irreführend.

9. Wettbewerbsrecht: Kein Gesetzes-, sondern ein Vollzugsdefizit.

Die geltenden wettbewerbsrechtlichen Bestimmungen gegen das Spamming sind scharf gefasst. Dass diese Bestimmungen bislang im Kampf gegen das Spamming wenig bewirken, liegt nicht an den Normen, sondern an der fehlenden Bereitschaft der Verbraucherschutz- und Wettbewerbsvereine, von ihren Klagerechten Gebrauch zu machen.

10. Klagerecht der Provider: Kein Gesetzes- sondern ein Mutdefizit

Die gelegentlich geforderte Einführung eines wettbewerbsrechtlichen Klagerechts der Provider ist nicht nur aus rechtssystematischen Gründen abzulehnen. Vielmehr müssen sich die Provider fragen lassen, weshalb sie bislang keine Streitverfahren gegen Spammer führen. Unterlassungsansprüche lassen sich aus dem Deliktsrecht (insbesondere § 1004 i.V.m. § 826 BGB) ableiten. Leider fehlt den Providern bis dato offenbar der Mut, einen entsprechenden Rechtsstandpunkt gerichtlich durchzusetzen (vgl. zu dieser Problematik Härting/Eckart, CR 2004, S. 119 - 122 Kopie anbei).

11. Das Telekommunikationsgeheimnis bei Spamfiltern stellt ein Scheinproblem dar

Das Telekommunikationsgeheimnis steht zur Disposition der Betroffenen. Willigt der Empfänger von Mails in eine – wie auch immer geartete – Filterung ein, stellt sich die Frage einer Verletzung des Telekommunikationsgeheimnisses nicht.

Anlage 1

Anti-Spam-Gesetze in der EU

	Gesetz	Vorschrift	Höchststrafe	Beschränkung
Belgien	Loi sur certains aspects juridiques des services de là société de l'information	Chapitre IV, Art. 14, 21, 26	Bußgeld von 250 – 50.000.- EUR	Opt-in-Prinzip
Dänemark	Markedsfoeringsloven (Marketing Practices Act)	Section 6 a	10.000 Kronen (etwa 1300 EUR) für eine einzige Spam-Mail; für jede weitere 100 Kronen (Quelle: heise.de)	Soft-opt-in-Prinzip = haben Nutzer ihre E-Mail-Adresse bereits bei einem Unternehmen hinterlassen, darf der Unternehmer diese für die Bewerbung ähnlicher Angebote nutzen
Frankreich	Keine extra Bußgeldvorschriften für Spam, allgemeines Strafrecht (Betrug, Computersabotage...)			
Großbritannien	Privacy and Electronic Communication Regulations	Reg. 2, 22, 23, 30ff.	Zuständig: Information Commissioner – Jeder Verstoß gegen einen Bescheid (enforcement notice) durch den Information Commissioner stellt eine Straftat dar, die mit einer Geldstrafe von bis zu 5.000 Pfund vor einem Magistrates Court bestraft werden kann	Opt-in-Prinzip
Irland	European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003	Reg. 13ff.	Geldbuße bis zu 3.000 EUR	Opt-in-Prinzip

	Gesetz	Vorschrift	Höchststrafe	Beschränkung
Italien	DL 196/2003	Sec. 130, 161, 167	Straftatbestand mit Haftstrafe bis zu zwei Jahren, wenn Gewinnerzielungs- oder Schädigungs-absicht vorliegt; wenn zudem Verstöße gegen allg. Datenschutzregeln vorliegen, kann eine Geldbuße von max. 90.000 EUR verhängt werden	
Luxemburg	Gesetzgebungsverfahren ist im Gange; Voraussichtlich Erweiterung des Loi au commerce électronique	Art. 46, 47, 48	Voraussichtlich Haftstrafen von 8 Tagen bis zu einem Jahr und Geldstrafen von 250 – 125.000 EUR	Opt-in-Prinzip
Niederland	Telecommunicatiewet (Telecommunication Act) wohl im Mai 2004 in Kraft getreten	11.7, 23	Freiheitsstrafen bis zu zwei Jahren und Geldstrafen bis 11.250 EUR nach anderer Auskunft bis 450.000 EUR (Quelle: Gesetzentwurf Nr. 28851)	Soft-opt-in-Prinzip
Österreich	TKG (Telekommunikationsgesetz)	§§ 107, 109 TKG	Geldstrafe bis zu 37.000 EUR bei - Direktwerbung, oder - Zusendung an mehr als 50 Personen, oder - Absenderidentität nicht korrekt Zudem Bereicherungsabschöpfung	Opt-in-Prinzip
	ECG (E-Commerce Gesetz)	§ 7 ECG		Opt-out-Prinzip
Portugal	Gesetzgebungsverfahren zur Umsetzung der RL 2002/58/EG ist im Gange (PROJECTO DE LEI N.º 208/IX)	Artigo 13, 18, 19	Vorgesehen ist wohl eine Geldstrafe von 600 – 6.000 EUR	Opt-in-Prinzip
Spanien	Ley de Servicios de la Sociedad de la Información (LSSI) (Gesetz zur Regelung der Informationsdienste)	Articulo 19ff., 38ff.	Geldstrafen bis zu 150.000 EUR	Opt-in-Prinzip

Anti-Spam-Gesetze weltweit

	Gesetz	Vorschrift	Höchststrafe	Beschränkung
Australien	Spam Act 2003		Geldstrafen bis zu 1,1 Millionen Dollar; zudem gibt es einen Gewinnabschöpfungsanspruch der Regierung	Verbotene Nachrichten sind lediglich solche mit einer speziellen Verbindung zu Australien
Neuseeland	Unsolicited Electronic Messages Bill		Bußgeld bis zu 500.000 NZD für Unternehmen; Bis zu 200.000 NZD für Privatpersonen	Opt-In-Prinzip
Norwegen	The Marketing Control Act	Sec. 2b, 2c, 17f	Bußgeld und Freiheitsstrafe bis 6 Monate	Opt-in-Prinzip
USA	CAN-Spam Act 2003	Sec. 5	Geldstrafen oder Freiheitsstrafe bis zu 5 Jahre	Opt-out-Prinzip i.V.m. einer Robinsonliste (Do-not-call-Registry) - Werbe-E-Mails müssen Anweisungen enthalten, wie die Opt-out-Erklärung abgegeben werden kann, sowie die reale Geschäfts- oder Privatadresse des Absenders; - die Header-Informationen müssen korrekt sein; - E-Mails müssen deutlich als Werbung erkennbar sein - CAN-Spam Act setzt weitergehende Regelungen (etwa opt-in-Prinzip) in den Bundesstaaten ausser Kraft

Anlage 2

Von Spammern und Providern

Können sich Provider gegen die Mailflut wehren?

Nationale und internationale Organisationen, Verbände, Parteien und Regierungen haben sich den Kampf gegen unerwünschte E-Mail-Werbung auf die Fahnen geschrieben. Für die Empfänger der Werbung für Diätpillen, Viagra und „Penis Enlargements“ sind Spam-Mails ein ständiges Ärgernis. Die millionenfache Versendung unerwünschter Werbung gefährdet die Attraktivität und Zuverlässigkeit der E-Mail als Kommunikationsmittel.

Bei der Diskussion um den weltweiten Kampf gegen Spammer geht es zum einen um Spam-Filter und andere technische Schutzvorkehrungen. Zum anderen werden zivil- und strafrechtliche Sanktionen diskutiert. Während das Spamming in Deutschland grundsätzlich keinen Straftatbestand erfüllt[82], besteht zivilrechtlich weitgehende Einigkeit über die Rechtswidrigkeit unerwünschter elektronischer Werbepost.

Unaufgeforderte Werbung per E-Mail wird immer beliebter und bereitet nicht nur den Empfängern, sondern auch den Providern von E-Mail-Accounts erhebliche Probleme und Kosten. So blockieren Spam-Mails Speicherplatz und andere Kapazitäten der Provider und die Bearbeitung von Kundenbeschwerden fordert wachsenden Personaleinsatz. Alle größeren Provider haben mittlerweile Anti-Spam-Abteilungen eingerichtet.

Im Mittelpunkt der Maßnahmen, die Provider gegen das Spamming ergreifen, stehen derzeit technische Schutzvorkehrungen (Spam-Filter). Je massiver und trickreicher Spammer vorgehen, desto größer wird der Aufwand, der mit den technischen Schutzvorkehrungen verbunden ist. Der Kampf gegen das Spamming ist letztlich aus Sicht der Provider (auch) ein Kampf um die Zukunftsfähigkeit der E-Mail als Kommunikationsmittel.

Aus Deutschland sind bislang keine Fälle bekannt, in denen Provider gegen Spammer gerichtlich vorgegangen sind. Dies erstaunt insoweit, als vieles dafür spricht, dass eigene Unterlassungsansprüche der Provider gegen Spammer bestehen.

I.

Rechtswidrigkeit des Spamming

Die Versendung elektronischer Werbepost ohne vorherige Zustimmung des Empfängers ist in Deutschland rechtswidrig. Zahlreiche gerichtliche Entscheidungen haben dies mittlerweile geklärt[83], obwohl eine ausdrückliche gesetzliche Regelung fehlt.

Vereinzelte Stimmen, die hierzulande für ein Opt-Out-System plädierten[84], konnten sich nicht durchsetzen. E-Mail-Werbung ist daher nicht nur dann rechtswidrig, wenn dem Empfänger keine Gelegenheit gegeben wird, der künftigen Zusendung derartiger Werbung zu widersprechen. Vielmehr gilt das Opt-In-Prinzip, wonach bereits die erstmalige Versendung von Werbung ohne vorherige Zustimmung des Empfängers untersagt ist.[85]

Wird Werbung an eine private E-Mail-Adresse versandt, ohne dass der Empfänger mit der E-Mail-Werbung (tatsächlich oder mutmaßlich) einverstanden ist, erfüllt dies den Tatbestand eines rechtswidrigen Eingriffs in das allgemeine Persönlichkeitsrecht gemäß § 823 Abs. 1 BGB.[86] Der Empfänger hat somit gegen den Spammer einen Unterlassungsanspruch gemäß § 1004 BGB. Handelt es sich um einen geschäftlich genutzten E-Mail-Anschluss, geht die Rechtsprechung ganz überwiegend von einem rechtswidrigen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb aus[87], so dass gleichfalls wegen der Verletzung eines sonstigen Rechts gemäß § 823 Abs. 1 BGB nach § 1004 BGB ein Unterlassungsanspruch besteht, sofern kein (tatsächliches oder mutmaßliches) Einverständnis des Empfängers vorliegt.

II.

Wettbewerbswidrigkeit des Spamming

Spamming ist nicht nur rechtswidrig, sondern auch wettbewerbswidrig. Auch hierüber besteht bereits nach jetzigem Recht weitgehende Einigkeit.[88] In Umsetzung der EU-Datenschutzrichtlinie[89] wird die anstehende UWG-Novelle[90] durch eine ausdrückliche Regelung endgültige Klarheit bringen.

Dass der Missbrauch fremder Telefaxgeräte für unerwünschte Werbung gegen die guten Sitten im Wettbewerb verstößt (§ 1 UWG), ist seit langem geklärt.[91] Für die unerwünschte E-Mail-Werbung kann nichts anderes gelten.[92] Ebenso wie bei der Telefax-Werbung liegt eine unzumutbare Belästigung vor, da der Werbende Kosten für den Versand von Werbung spart, indem er den Empfänger der Werbung gegen dessen Willen dazu nötigt, seinerseits Zeit und Kosten für das mühsame Aussortieren der Werbung aufzuwenden.

Bei der geplanten Neufassung des UWG soll die unerwünschte E-Mail-Werbung ausdrücklich als unlauter untersagt werden. In Umsetzung der EU-Datenschutzrichtlinie ist die Einführung eines § 7 Abs. 1 Nr. 3 UWG geplant, der die Werbung unter Verwendung von automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post ohne Einwilligung der Adressaten als unzumutbare Belästigung und somit als unlauter im Sinne von § 3 UWG-E bezeichnet. Nach § 7 Abs. 3 UWG-E soll dem

---

82 ~~vgl~~Vgl. zur Strafbarkeit des Spamming Frank, CR 200~~3~~4, ???.

83 KG v. 20.06.2002, KG-Report 2002, 353; OLG Koblenz v. 10.06.2003, MMR 2003, 590; LG München v. 15.04.2003, JurPC Web-Dok. 152/2003; LG Berlin v. 16.05.2002, MMR 2002, 631; AG Bonn v. 13.05.2003, BRAK-Mitt. 2003, 244 (LS); AG Hamburg v. 04.03.2003, JurPC Web-Dok. 265/2003; AG Leipzig v. 27.02.2003, MMR 2003, 610; AG Rostock v. 28.01.2003, NJW-RR 2003, 1282.

84 Ziem, MMR 2000, 129.

85 Tettenborn in Moritz/Dreier, Rechts-Handbuch zum E-Commerce, ~~Rdnr~~Teil- C Rdnr. 468; OLG Koblenz v. 10.06.2003, MMR 2003, 590; LG Berlin v. 16.05.2002, MMR 2002, 631.

86 KG v. 20.06.2002, KG-Report 2002, 353; LG Berlin v. 19.09.2002, CR 2003, 219; AG Rostock v. 28.01.2003, NJW-RR 2003, 1282.

87 KG v. 08.01.2002, MMR 2002, 685; LG München v. 15.04.2003, JurPC Web-Dok. 152/2003; LG Berlin v. 16.05.2002, MMR 2002, 631; AG Bonn v. 13.05.2003, BRAK-Mitt. 2003, 244 (LS); AG Hamburg v. 04.03.2003, JurPC Web-Dok. 265/2003; AG Leipzig v. 27.02.2003, MMR 2003, 610.

88 Vgl. Baumbach/Hefermehl, Wettbewerbsrecht, 22. Aufl., 2001, § 1 UWG, Rdnr. 70a; Schneider, Handbuch des EDV-Rechts, 3. Aufl., 2003, Teil B Rdnr. 869.

89 Richtlinie 2002/58/EG des EP und des Rates v. 12.07.2002, Bl. EG~~,~~ Nr. L 201, S. ~~/~~37.

90 Vgl. den Gesetzentwurf der Bundesregierung v. 09.05.2003, BT-Drucks. 301/03.

91 Vgl. Baumbach/Hefermehl, Wettbewerbsrecht, 22. Aufl., 2001, § 1 UWG, Rdnr. 69b.

92 LG Ellwangen v. 27.08.1999, CR 2000, 188; LG Traunstein v. 18.12.1997, K&R 1998, 117.

Unternehmer ohne vorherige Zustimmung des Adressaten die E-Mail-Werbung nur dann erlaubt sein, wenn er die E-Mail-Adresse des Empfängers im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten hat und die E-Mail-Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen genutzt wird (§ 7 Abs. 3 Satz 1 UWG-E). Bei der Erhebung der Daten und jeder Nutzung muss der Kunde zudem klar und deutlich auf die Möglichkeit hingewiesen werden, die Nutzung jederzeit unterbinden zu können, ohne dass ihm hierfür andere als die gewöhnlichen Übermittlungskosten entstehen (§ 7 Abs. 3 Satz 2 UWG-E).

III.

Ansprüche der Provider

Fest steht damit, dass Empfänger von Spam-Mails aus § 1004 in Verbindung mit § 823 Abs. 1 BGB Unterlassungsansprüche geltend machen können. Verbraucherschutzvereine, Wettbewerbsverbände und Konkurrenten können zudem aus § 1 UWG gegen Spammer vorgehen (§ 13 Abs. 2 UWG). Ungeklärt ist bislang, ob und unter welchen Voraussetzungen auch die Provider zivil- oder wettbewerbsrechtliche Unterlassungsansprüche gegen Spammer besitzen.

1.

Wettbewerbsrecht

Das Wettbewerbsrecht liefert den Providern in aller Regel keine Handhabe, gegen Spammer vorzugehen. Auch wenn an der Wettbewerbswidrigkeit des Spamming kein Zweifel besteht, wird die Geltendmachung von Abwehransprüchen durch einen Provider regelmäßig an der fehlenden Klageberechtigung gemäß § 13 Abs. 2 UWG scheitern. Nur wenn der Spammer ausnahmsweise ein Konkurrent des Providers ist, lässt sich eine Anspruchsberechtigung aus § 13 Abs. 2 Nr. 1 UWG herleiten. An dieser Rechtslage wird sich auch durch die anstehende UWG-Novelle nichts ändern. Die Regelungen des § 13 Abs. 2 UWG werden durch § 8 Abs. 3 UWG-E im Kern übernommen.

2.

Eingriff in den Gewerbebetrieb

Versendet jemand eine E-Mail, so läuft die Mail vom Provider des Versenders — meist über weitere Provider als Zwischenstationen - zum Provider des Empfängers (z.B. web.de, gmx oder msn), wo diese gespeichert wird. Die gespeicherte Mail wird vom Provider bereitgehalten, um vom Benutzer abgerufen oder eingesehen zu werden. Hierzu verwendet der Provider eine Software, die regelmäßig gewartet, also vom Personal überprüft wird. Je größer die Anzahl der gespeicherten Mails, desto größer ist die Fehleranfälligkeit.

Der erhöhte Anfall von Spam-Mails führt dazu, dass Provider größere Speicherkapazitäten bereithalten müssen. Unerwünschte Werbung blockiert Speicherplatz, der eigentlich für „normale“ E-Mails benötigt wird.

Ohne die durch den Provider bereitgehaltene Infrastruktur wäre dem Spammer die - oft millionenfache - Versendung von E-Mail-Werbung nicht möglich. Der Spammer nutzt somit gezielt die Leitungen, den Speicherplatz, und andere Ressourcen des Providers, um auf besonders kostengünstige Art Massenwerbung zu betreiben. Es liegt daher nicht fern, das Spamming nicht nur als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb der Empfänger anzusehen, sondern auch als Eingriff in den Gewerbebetrieb der Provider.

a. Betriebsbezogene Beeinträchtigung

Bei den (gewerblichen) Empfängern bejaht die Rechtsprechung einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb gemäß § 823 Abs. 1 BGB mit drei Argumenten[93]:

- Dem Empfänger entstehen Kosten, indem er Arbeitszeit zum Aussortieren und Löschen unerwünschter E-Mails aufwenden muss.
- Durch das Herunterladen unerwünschter E-Mail-Werbung fallen bei dem Empfänger gegen dessen Willen Online-Gebühren an.
- Bei massenweisem Spamming besteht die Gefahr, dass die E-Mail-Box des Empfängers „überläuft“ mit der Folge, dass er wichtige E-Mails nicht erhält.

Trotz der vergleichsweise geringfügigen Belästigung, die von einer einzelnen E-Mail ausgeht, bejaht die Rechtsprechung bereits bei dem Versand einer einzigen E-Mail einen Eingriff in den Gewerbebetrieb. Begründet wird dies mit der Ausuferungsgefahr, die dem Kommunikationsmittel E-Mail innewohnt und die vor allem darin liegt, dass sich mit geringen Kosten massenhaft E-Mails versenden lassen[94].

Die geringen Anforderungen, die die Rechtsprechung an die Bejahung eines Eingriffs in den Gewerbebetrieb durch E-Mail-Werbung stellt, stehen in einem gewissen Spannungsverhältnis zu den herkömmlichen Anforderungen an einen betriebsbezogenen Eingriff, der zur Erfüllung des Tatbestandes des § 823 Abs. 1 BGB in anderen Fällen erforderlich ist. Nach herkömmlicher Auffassung muss ein Angriff auf die Grundlagen unternehmerischer Betätigung vorliegen, damit ein rechtswidriger Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb als sonstiges Recht gemäß § 823 Abs. 1 BGB bejaht werden kann.[95] Eine bloße Belästigung reicht hierfür ebenso wenig aus wie eine lediglich mittelbare Beeinträchtigung des betroffenen Betriebes.[96]

Auch wenn einiges dafür spricht, dass die Kriterien, die der Rechtsprechung zum Eingriff in den Gewerbebetrieb durch E-Mail-Werbung zugrunde liegen, nicht mit den allgemeinen Anforderungen an einen betriebsbezogenen Eingriff übereinstimmen, können für die Ansprüche der Provider gegen Spammer keine anderen Maßstäbe gelten als die Kriterien, die für das Verhältnis zwischen Spammern und den betroffenen Empfängern maßgeblich sind. Dann aber spricht alles dafür, dass Unterlassungsansprüche der Provider gegen Spammer gem. § 1004 in Verbindung mit § 823 Abs. 1 BGB bestehen.

- So wie der Empfänger unerwünschter E-Mail-Werbung Arbeitszeit zum Aussortieren von Spam-Mails aufwenden muss, ist der Provider gezwungen, zur Vermeidung von Kundenbeschwerden und ungewoll-

---

93 Vgl. KG v. 08.01.2002, MMR 2002, 685; LG München v. 15.04.2003, JurPC Web-Dok. 152/2003; LG Berlin v. 16.05.2002, MMR 2002, 631; AG Leipzig v. 27.02.2003, MMR 2003, 610.

94 Vgl. KG v. 08.01.2002, MMR 2002, 685; LG Berlin v. 16.05.2002, MMR 2002, 631; AG Leipzig v. 27.02.2003, MMR 2003, 610.

95 Vgl. Sprau in Palandt, BGB, 63. Aufl., 2004, § 823 Rdnr. 126 f.

96 Vgl. Sprau in Palandt, BGB, 63. Aufl., 2004, § 823 Rdnr. 128.

ter Nutzung seines Speicherplatzes Personal einzusetzen, das versucht, die Speicherung und Weiterleitung derartiger E-Mails zu unterbinden.

- Während der Empfänger von Spam-Mails durch das Herunterladen der E-Mails Online-Gebühren aufwenden muss, fallen bei dem Provider Kosten für die Bereithaltung von Speicherplatz, Strom und sonstiger Infrastruktur an.
- Eine ähnliche Gefahr wie das Risiko des Überlaufens der E-Mail-Box besteht auch für den Provider. Nutzlose Spam-Mails blockieren Speicherplatz mit dem Risiko, dass der Provider seinen vertraglichen Verpflichtungen gegenüber seinen Kunden nicht mehr nachkommen kann.

Ein Eingriff in den Gewerbebetrieb des Providers lässt sich demnach ohne weiteres begründen. Dies jedenfalls soweit der Provider mit dem Empfang der Spam-Mails nicht einverstanden ist.

b. Fehlendes Einverständnis der Provider

Da Spammer für gewöhnlich die Provider nicht vorab fragen, ob sie Einwände gegen die Werbepost haben, fehlt es an einem tatsächlichen Einverständnis. In Betracht kommt allenfalls ein mutmaßliches Einverständnis der Provider.

Für ein mutmaßliches Einverständnis könnte sprechen, dass der Provider die E-Mails lediglich weiterleitet und seinen Kunden gegenüber auch zur Weiterleitung von Mails verpflichtet ist. Würde der Spammer indes den Provider tatsächlich fragen, ob er die bei dem Provider eingerichteten Accounts zur Versendung von Werbung benutzen kann, so wäre die Antwort des Providers klar: An dem Versand der Werbung kann ihm nur dann gelegen sein, wenn die Inhaber der jeweiligen Accounts mit dem E-Mail-Empfang einverstanden sind. Nur dann kann vermutet werden, dass der Provider als Dienstleistungsunternehmen bereit ist, ihm entstehende Kosten zu tragen, um die gegenüber seinen Kunden bestehenden vertraglichen Pflichten zu erfüllen.

Am Erhalt von Spam-Mails hat der Kunde des Providers jedoch keinerlei Interesse. Daher kann der Versender auch nicht davon ausgehen, dass der Provider mit der für ihn kostenintensiven Speicherung der Mails einverstanden ist.

Ein mutmaßliches Einverständnis des Empfängers lässt sich auch nicht daraus ableiten, dass der Provider nicht ohne weiteres erkennen kann, dass es sich um eine Spam-Mail handelt. Maßgeblich ist, ob der Versender der Mail von einem mutmaßlichen Einverständnis des Empfängers hinsichtlich der abgesandten Mail ausgehen kann. Entscheidend ist somit die Sicht des Spammers, der genau weiß, dass es sich bei den von ihm versandten Nachrichten um unerwünschte Werbung handelt, an denen der Provider kein Interesse hat. Mit der Versendung von Spam an seine Kunden und den eigenen Server ist daher der Provider weder tatsächlich noch mutmaßlich einverstanden.

c. Zwischenergebnis

Nach den Maßstäben der Rechtsprechung zum Eingriff in den Gewerbebetrieb durch den Versand von E-Mail-Werbung spricht somit alles dafür, dass auch Provider Inhaber von Abwehransprüchen gegen Spammer aus § 1004 in Verbindung mit § 823 Abs. 1 BGB sind. Ein Grund, weshalb sich die Versendung einer einzelnen E-Mail als Eingriff in den Gewerbebetrieb des Empfängers darstellt, der millionenhafte Versand von Spam-Mails an E-Mail-Adressen eines Providers dessen Gewerbebetrieb jedoch nicht beeinträchtigen soll, ist nicht ersichtlich.

3.

Vorsätzlich-sittenwidrige Schädigung

Auch aus einer drohenden vorsätzlich-sittenwidrigen Schädigung gemäß § 826 BGB kann sich ein Unterlassungsanspruch nach § 1004 BGB ergeben.[97] Für den Provider kommt daher gegen den Spammer auch ein Unterlassungsanspruch aus § 826 in Verbindung mit § 1004 BGB in Betracht.

Ob und unter welchen Voraussetzungen die unerwünschte E-Mail-Werbung den Tatbestand des § 826 BGB erfüllt, ist bislang weder in der Rechtsprechung noch in der Literatur eingehend diskutiert worden. Es spricht indes vieles dafür, dass § 826 BGB alles andere als ein stumpfes Schwert im Kampf gegen das Spamming ist.

Durch Werbung per E-Mail spart der Absender im Vergleich zur Werbung per Post erhebliche Kosten ein, während für den Empfänger und auch den Provider Kosten entstehen. Eine Möglichkeit, dieser Belästigung aus dem Weg zu gehen, besteht dabei für die Betroffenen nicht. Da dem Spammer all dies auch bestens bekannt ist und er die aufgedrängten Mehrkosten gezielt in Kauf nimmt, verwirklicht er durch die in Gang gesetzte Werbeflut den Tatbestand des § 826 BGB.

a. Schadenszufügung

Spam-Mails fügen sowohl den Empfängern als auch den beteiligten Providern Schaden zu. Die Arbeitszeit der Mitarbeiter, die in einem Unternehmen „Werbemüll" aussortieren und löschen, kostet das Unternehmen teures Geld. Darüber hinaus sind die Online-Kosten, die für den Abruf der Werbepost anfallen, ein wirtschaftlich messbarer Schaden.

Der Schaden bei dem Provider liegt in den Kosten, welche für den Speicherplatz und die sonstige Infrastruktur aufgewendet werden müssen, die durch die Spam-Mails nutzlos in Anspruch genommen werden. Darüber hinaus fallen erhebliche Personalkosten für technische Schutzvorkehrungen und für die Bearbeitung von Kundenbeschwerden an.

Um seine Dienstleistung am Markt erbringen zu können, muss der Provider dafür sorgen, jederzeit genug Speicherplatz zur Verfügung zu haben, um die E-Mails seiner Kunden speichern zu können. Die hierzu notwendigen Kapazitäten berechnet der Provider anhand des durchschnittlichen E-Mail-Aufkommens. Da es sich derzeit bei mindestens der Hälfte aller Mails um Spam-Mails handelt, ist der Provider gezwungen, erhebliche Kapazitäten für unerwünschte Werbepost vorzuhalten.

Der erhebliche Mehraufwand an Kapazitäten und Personal ist nicht auf die einzelne Spam-Mail zurückzuführen, sondern auf alle „schwarzen Schafe", die per unerwünschter E-Mail Werbung versenden. Die Mitverantwortung zahlreicher anderer Spammer erschwert daher eine genaue Bezifferung des Schadens, der durch die Aktivitäten eines einzelnen Spammers entsteht. An der (Mit-)Ursächlichkeit der Handlungen des einzelnen Spammers

[97] Bassenge in Palandt, BGB, 63. Aufl., 2004, § 1004 Rdnr. 4.

ändert dies indes nichts. Hier muss gleiches gelten wie im Rahmen des § 823 BGB, wo im Hinblick auf die Ausuferungsgefahr, die dem Spamming innewohnt, jeder einzelne Spammer als Mitverursacher für die Gesamtwirkung verantwortlich gemacht wird. [98]

b. Sittenwidrigkeit

Das Spamming ist nach allgemeiner Anschauung verwerflich und verstößt gegen die guten Sitten. Der Spammer versendet die Werbung allein aus eigenem Gewinnstreben und in dem Wissen, dass der Empfänger den Erhalt der E-Mail gerade nicht billigt, da ihm hierdurch ein Schaden entsteht. Wer aus Gewinnstreben andere belästigt, indem er auf deren Kosten wirbt, um zugleich eigene Kosten zu sparen, handelt verwerflich.

Spamming verstößt nach einhelliger Meinung gegen die guten Sitten im Wettbewerb (§ 1 UWG).[99] Der Maßstab, der für die guten Sitten im Wettbewerb gilt, ist zwar nicht notwendig identisch mit den Wertungen, die für die §§ 138 und 826 BGB maßgeblich sind.[100] Es gibt indes keinen einleuchtenden Grund, weshalb das Spamming nur im Wettbewerb, nicht jedoch auch nach den §§ 138 und 826 BGB sittenwidrig sein sollte.

c.Vorsatz

Der Spammer handelt auch vorsätzlich. Zwar geht es ihm bei der E-Mail-Werbung darum, seine Waren und Dienstleistungen möglichst erfolgreich zu verkaufen und nicht darum, den betroffenen Empfängern und Providern Schaden zuzufügen. Eine absichtliche Schädigung fehlt daher. Die beträchtlichen Kosten, die den Providern durch die Bekämpfung des Spamming entstehen, sind jedoch gemeinhin bekannt. Dasselbe gilt für die aufgedrängten Kosten, die den Empfängern der Mails entstehen. Der Versand der Werbe-E-Mails erfolgt daher seitens des Spammers im sicheren Wissen um die hierdurch verursachten Kosten. Er handelt daher mit direktem Schädigungsvorsatz. Dies reicht für eine Haftung aus –§ 826 BGB aus, da § 826 BGB keine Schädigungsabsicht verlangt.[101]

IV.

Fazit

Die Provider von E-Mail-Accounts gehören zu den Hauptleidtragenden der Mailflut, die derzeit den E-Mail-Verkehr beeinträchtigt. Um diese Flut zumindest einzudämmen, können sie Unterlassungsansprüche gegen Spammer geltend machen und durchsetzen. Unterlassungsansprüche lassen sich sowohl aus § 823 Abs. 1 BGB als auch aus § 826 BGB jeweils in Verbindung mit § 1004 BGB ableiten. Zum einen spricht vieles dafür, dass die Rechtsprechung zum Eingriff in den Gewerbebetrieb des Empfängers von E-Mail-Werbung auf Provider übertragbar ist. Zum anderen erfüllt das Spamming den Tatbestand einer vorsätzlich-sittenwidrigen Schädigung. Eine vorsätzlich-sittenwidrige Schädigung tritt nicht nur bei den betroffenen Providern, sondern auch bei den Empfängern der E-Mail-Werbung ein. Dieser Gesichtspunkt, der neben die Tatbestände des § 823 Abs. 1 BGB und des § 1 UWG tritt und auch den Empfängern von Spam-Mails einen Anspruch aus §826 BGB einräumt, wurde in der Diskussion um das Spamming bislang noch nicht präzise erkannt.

Härting/Eckart, CR 2004, 119ff

98 Vgl. KG v. 08.01.2002, MMR 2002, 685; LG München v. 15.04.2003, JurPC Web-Dok. 152/2003; LG Berlin v. 16.05.2002, MMR 2002, 631; AG Leipzig v. 27.02.2003, MMR 2003, 610.

99 Baumbach/Hefermehl, Wettbewerbsrecht, 22. Aufl., 2001, § 1 UWG, Rdnr. 70a; Schneider, Handbuch des EDV-Rechts, 3. Aufl., 2003, Rdnr. B 869.

100 Baumbach/Hefermehl, Wettbewerbsrecht, 22. Aufl., 2001, Einl. UWG, Rdnr. 69.

101 Vgl. Sprau in Palandt, BGB, 63. Aufl., 2004, § 826 Rdnr. 10.

DEUTSCHER BUNDESTAG
Ausschuss für
Wirtschaft und Arbeit
15. Wahlperiode

Ausschussdrucksache 15(9)**1846**

8. April 2005

Schriftliche Stellungnahme

zur öffentlichen Anhörung am 18. April 2005 in Berlin zu

a) Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz) - Drucksache 15/4835 -

b) Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Klöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU

Spam effektiv bekämpfen - Drucksache 15/2655 -

HK2 Rechtsanwälte

A Zum Gesetzentwurf der Fraktionen SPD und Bündnis90/Die Grünen: Entwurf eines zweiten Gesetzes zur Änderung des Teledienstegesetzes, Anti-Spam-Gesetz, BT-Ds. 15/4835

1. Problem und Lösungsansatz

Einig sind sich alle Beteiligten und Interessengruppen darüber, dass das massenhafte Zusenden unverlangter Nachrichten in eigennütziger Weise auf Kosten Dritter die Ressourcen der elektronischen Kommunikation inzwischen **erheblich beeinträchtigt** und nicht gebilligt wird (siehe sowohl BT-Ds. 15/2655 als auch BT-Ds. 15/4835).

1.1. Aktuelle Rechtslage

Ein solches Verhalten ist bereits nach ständiger Rechtsprechung **unzulässig**. Das Zusenden unverlangter Werbung ist wettbewerbswidrig und eine vom Betroffenen nicht hinzunehmende Störung.[102] Die wettbewerbsrechtliche Unzulässigkeit des Spammings wurde dabei nicht erst durch die Novelle des UWG von 2004 begründet, sondern vom Bundesgerichtshof bereits aus § 1 UWG a.F. abgeleitet.[103] Schon das Zusenden einer Bestätigung der Eintragung in einen E-Mail-Verteiler soll der Betroffene untersagen können, wenn eine entsprechende Einwilligung nicht vorgelegen habe.[104] Verboten wurde auch die unverlangte E-Mail-Werbung von politischen Parteien durch Dritte („E-Card“).[105]

Die Anforderungen an E-Mail-Werbung sind daher **strenger** als beispielsweise an die Briefwerbung. Dies wird üblicherweise mit den unterschiedlichen wirtschaftlichen Rahmenbedingungen begründet. Dabei schränken die Regelungen die sinnvollen Möglichkeiten kommerzieller Kommunikation bereits jetzt übermäßig ein. Als Beispiel kann der vom Bundesgerichtshof entschieden Fall dienen.[106] Während dieses Urteil allgemein als erste „Anti-Spam-Entscheidung“ begrüßt wurde, betraf sie weder Werbung noch unverlangtes Zusenden im engeren Sinne. Versendet wurde ein redaktioneller Newsletter, der allerdings vom journalistischen Teil getrennte Werbung enthielt und außerdem vom Gericht insgesamt als Werbung für den Versender verstanden wurde. Der Zusendung lag eine Bestellung zugrunde, jedoch hatte sich der Abonnent bei der Eingabe seiner E-Mail-Adresse vertippt.[107] Die bestehenden Bestimmungen verbieten also wesentlich mehr als das, was unter Spamming allgemein verstanden wird. Unsere Kanzlei berät Internet- und Werbeagenturen, Anbieter von Kundenkommunikationslösungen oder auch andere Unternehmen in rechtlichen Fragen der elektronischen Kundenansprache. Dabei machen wir die Erfahrung, dass

102 Abwehransprüche bestehen aus Wettbewerbsrecht (siehe dazu Baumbach/Hefermehl UWG 23. Aufl. § 7 Rz. 79 ff. m.w.N.) und dem allgemeinen Zivilrecht (Palandt BGB 64. Aufl. § 1004 Rz. 10 m.w.N.)

103 BGH v. 11.03.2004, I ZR 81/01 – E-Mail-Werbung

104 LG Berlin v. 10.01.2002, 16 O 626/02, bestätigt durch KG v. 20.06.2002, 10 U 54/02

105 OLG München v. 12.02.2004, 8 U 4223/03, AG Rostock v. 28.01.2003, 43 C 68/02, (LG München I, 21 O 9959/02) zur Unternehmenswerbung: LG Nürnberg 04.03.2004, 4 HK O 2056/04, JurPC Web-Dok 20040185

106 Der Verfasser war an dem Verfahren als Anwalt beteiligt.

107 Der Vorfall spielte 1998 und zu diesem Zeitpunkt war in der Bestellung noch kein Double-Opt-In vorgesehen.

schon die existierenden Informationspflichten und Unklarheiten der Anforderungen ein Hemmnis für die elektronische Kommunikation mit den Kunden und entsprechende innovative Dienste darstellen.

1.2. Problem der Versendung aus dem Ausland

Massenhafte Versendung von unverlangter Werbung per E-Mail spielt keine Rolle soweit der Arm des Rechtssystems reicht. Dies zeigen die veröffentlichten Zahlen.[108] Allerdings zieht der Entwurf nicht die sich daraus ergebenden Konsequenzen: Kommerzielles Spamming stammt nicht aus dem räumlichen Geltungsbereich des TDG und bewirbt auch ganz überwiegend **keine Angebote inländischer Unternehmen**.

In der in Fußnote 7 der Begründung aufgeführten Commtouch-Studie ist Deutschland weder als Land unter den wichtigsten Heimatländern für die beworbenen Internetangebote zu finden noch unter den 10 wichtigsten Ursprungsländern für Spam. Dabei ist zu berücksichtigen, dass Platz 10 der durch Spam beworbenen Webseiten von Japan mit einem Prozentsatz von 0,01 % eingenommen wird. Beim Ursprungsland hätte eine Beteiligung von mehr als 1,2 % am Gesamtspamaufkommen bereits für Platz 10 gereicht. Weiter möchte Commtouch beobachtet haben, dass 9,8 % des Spamaufkommens den Anforderungen des CAN-SPAM-Act genügt. Diese seit dem 01.01.2004 in Kraft getretene US-amerikanische Vorschrift verbietet die Verschleierung von Absenderinformationen sowie die Verwendung irreführender Betreffzeilen[109].

Aus den zitierten Quellen ergibt sich somit, dass nur ein **verschwindender Bruchteil** des Spam aus dem Anwendungsbereich des TDG stammt. Welche Quote dieser geringen Teilmenge zugleich den nun vorgeschlagenen Tatbestand verwirklicht, bleibt unbekannt.[110]

Dem steht gegenüber eine absurd hohe Zahl von Verstößen durch vom Ausland aus operierende Spammer. Täglich dürften Millionen von Spamnachrichten an Adressen im Anwendungsbereich des TDG geschickt werden. Daraus ergeben sich jeden Tag hunderttausende von Verdachtsfällen einer Verschleierung des Absenders.

Wenn laut Begründung mit quantifizierbaren finanziellen Auswirkungen für die öffentliche Hand nicht gerechnet werden kann (Seite 6), dann gründet sich diese Einschätzung vermutlich aus der Annahme, dass das Gesetz in der Praxis **kaum durchzusetzen** sein wird. Anderenfalls wäre die Zuweisung erheblicher Ressourcen erforderlich, um der Flut von Verdachtsfällen nachzugehen. Diese Akten wären sogleich nach Ermittlung des nicht inländischen Ursprungs wieder zu schließen. Die Verfolgung von Ordnungswidrigkeiten gegen Täter im Ausland erscheint kaum praktikabel.[111]

Die Begründung erkennt sodann folgerichtig, dass es um eine Signalwirkung auf internationaler Ebene geht (Seite 5).

1.3. Werbeklarheit

Mehr Anwendungsmöglichkeit bietet das Gesetz bezüglich des Verheimlichen und Verschleierns des kommerziellen Charakters einer Werbemail. Hier dürfte der Entwurf als **Verschärfung** der Vorschriften anzusehen sein, ohne dass dies notwendig oder auch nur vorrangig Fälle von Spamming betrifft.

Für eine **Neuregelung der Werbeklarheit** wäre eine eindeutige, möglichst international - zumindest aber innerhalb der EU - abzustimmende Kennzeichnung erwägenswert gewesen. Die jetzt vorliegende Fassung verschleiert, was verboten sein soll und bevorteilt auf diese Weise unseriöse Anbieter, die die unklaren Grenzen der Vorschrift eher ausnützen dürften.

1.4. Lücken und Mängel

Drängende Probleme durch Regelungslücken werden nicht angegangen (Bsp. Phishing, unverlangte Werbung auf Kommunikationsplattformen).

Die Entwurfsformulierung weist eine Reihe gesetzgeberischer Mängel auf, die die **Praxis komplizierter** machen. Der erfolgreiche und wachsende Markt des elektronischen Handels wird hier erneut mit unklaren Vorschriften konfrontiert, deren Nutzen sich in dem politischen Signal erschöpft.

2. Zu den einzelnen Tatbestandsmerkmalen des § 7 Nr. 3 TDG–E

2.1. „Teledienst“

§ 7 TDG-E wird nur auf Teledienste anwendbar sein, § 2 Abs. 1 TDG. Damit wirken sich die ohnehin hemmenden **Abgrenzungsschwierigkeiten der IT/TK-Regulierung** auch auf diese Bestimmung aus. Alternativ wäre die Schaffung eines eigenen Tatbestandes im OWiG denkbar.

2.1.1. Abgrenzung zu Mediendiensten

Im Rahmen von **Mediendiensten** zumindest in Form von Verteildiensten versandte Spam-Mails werden durch die Neuregelung **nicht erfasst**, § 2 Abs. 4 Nr. 3 TDG.[112] Dies betrifft beispielsweise politische Werbung und Agitation. So dürfte etwa der Vorfall aus Juni 2004[113], bei dem massenhaft rechtsradikale Propaganda unter Verschleierung des Absenders versandt wurde, nicht im Anwendungsbereich des TDG liegen. Aber auch Newsletter und andere redaktionelle E-Mails, die gleichzeitig an eine Vielzahl von Empfängern verschickt werden, unterfallen regelmäßig nicht den Regelungen des TDG, § 2 Abs. 4 Nr. 3.[114] Dies eröffnet Umgehungsmöglichkeiten.

---

108 Die Zahlen stammen allerdings, soweit ersichtlich, nicht aus neutralen Quellen.

109 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Sec. 5.

110 Dann wären noch die Fälle abzuziehen, die bereits jetzt geahndet werden können, § 6 i.V.m. § 12 TDG

111 Sofern überhaupt eine Tatbestandsverwirklichung im räumlichen Geltungsbereich des TDG angenommen werden kann.

112 Es erscheint in jedem Falle zweckmäßig bei einer Ergänzung des TDG zugleich das Datum des Mediendienstestaatsvertrages in § 2 Abs. 4 Nr. 3 TDG zu aktualisieren.

113 http://www.netzeitung.de/internet/290463.html

114 Die als erstes „Anti-Spam“ Urteil des BGH bekannt gewordene Entscheidung vom 11.3.2004 (I ZR 81/01 – E-Mail-Werbung) betraf einen redaktionell gestalteten Newsletter (siehe http://juris. bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=d115c89ecbaee791a71dfb96006 b9c7a&client=12&nr=28908&pos=6&anz=30).

2.1.2. Abgrenzung zu Telekommunikationsdiensten

Das TDG gilt nicht für Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten, § 2 Abs. 4 Nr. 1 TDG und § 3 Nr. 18 und Nr. 5 TKG-1996.

§ 2 Abs. 4 Nr. 1 TDG ist an das TKG-2004 anzupassen. „Geschäftsmäßiges Erbringen von Telekommunikationsdiensten" ist dann das „nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht", § 3 Nr. 10 TKG-2004. Telekommunikation ist der „technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen", § 3 Nr. 22 TKG-2004. „Telekommunikationsdienste" sind „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen", § 3 Nr. 24 TKG-2004.

Die Abgrenzung zu den Telediensten ist bislang noch nicht gelungen.[115] Problematisch ist, dass die in § 12 TDG-E bußgeldbewehrten Formen des Header-Spoofing vor allem die technischen Informationen der E-Mail-Übermittlung betreffen und somit den vorrangig vom TKG geregelten Bereich der technischen Übertragung der Nachricht. Spam über den Short Message Service (SMS) der Mobilfunkanbieter könnte grundsätzlich als elektronischer Nachrichtenaustausch von § 7 TDG-E erfasst sein[116]. Auch SMS enthalten einen Header. Allerdings wird deren Übermittlung unter den Regelungsbereich des TKG fallen. Dasselbe Problem besteht in der Abgrenzung etwa bei an Voice over Internet Protocol (VoIP) gekoppelten Nachrichtensystemen.[117]

2.1.3. Anwendbarkeit auf Spam fraglich

Die **Anwendbarkeit** der Regelungen des TDG **auf Spam ist fraglich**. Damit ist der Zweck des Entwurfes insgesamt gefährdet. Sachlich gilt das TDG nur für Teledienste, § 2 Abs. 1 TDG.

Ein Teledienst ist ein Informations- und Kommunikationsdienst, der für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt ist und dem eine Übermittlung mittels Telekommunikation zugrunde liegt (§ 2 Abs. 1 TDG). Als Regelbeispiel des § 2 Abs. 2 Nr. 2 TDG werden zwar Angebote zur Information oder Kommunikation genannt und hier insbesondere die Verbreitung von Waren und Dienstleistungsangeboten. Der Gesetzeswortlaut legt jedoch nahe, dass es hierbei um das **Angebot von E-Mail-Diensten und nicht um die einzelne E-Mail** geht. Dies ergibt zumindest die wörtliche Auslegung des § 2 Abs. 2 Nr. 2 TDG, der eben von Angeboten spricht. Das Zusenden einer einzelnen E-Mail als solches ist jedoch kein Angebot zur Information oder Kommunikation, sondern die Durchführung. Die systematische Einordnung der „Anti-Spam-Vorschriften" in das TDG übergeht dieses Problem. Dies wird nicht zur Rechtssicherheit beitragen.

Nachdem der Gesetzgeber aber mit dem Entwurf davon ausgeht, dass bereits die einzelne Werbemail ein Teledienst ist, steht zu befürchten, dass die vollständigen Impressumspflichten des bestehenden § 6 TDG nun für jedes geschäftsmäßige E-Mail gelten.[118] Dies wäre ein neuer sinnfreier **Formalismus** im ohnehin überregulierten Bereich des E-Commerce.

Wenn einzelne E-Mails bereits Angebote im Sinne des TDG darstellen, so bestünde gar **kein Regelungsbedarf**. Nach § 6 TDG haben Diensteanbieter bei geschäftsmäßigen Telediensten über ihre Identität aufzuklären. Neben Name und Anschrift des Anbieters sind auch Angaben über die schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation einschließlich der Adresse der elektronischen Post zu integrieren (§ 6 Satz 1 Nr. 2 TDG). Korrekte Angaben zur Identität und E-Mail wären dann ohnehin bereits Pflichtbestandteil einer E-Mail und unterlägen der Bußgeldbewehrung des bereits bestehenden § 12 Abs. 1 TDG. Eine besondere Regelung für solche Fälle, in denen der Anbieter seine gesamten Pflichtinformationen gemäß § 6 TDG vollständig erfüllt, aber Header-Informationen über seine Identität verheimlicht oder verschleiert, erscheint kaum notwendig. Die Pflichtangaben umfassen Namen, ladungsfähige Anschrift, E-Mail-Adresse, etwaige Vertretungsberechtigte, Handelsregister- und sonstige Registernummern, bestimmte Aufsichtsbehörden bis hin zur Umsatzsteueridentifikationsnummer nach § 27a UStG. Welcher Spammer wird den Header verfälschen, aber alle Pflichtangaben des § 6 TDG mitteilen?

Die Begründung geht dagegen davon aus, dass eine Verletzung der Anbieterkennzeichnungspflicht nach §§ 6, 12 Abs. 1 TDG durch den neuen Bußgeldtatbestand als lex specialis verdrängt würde (Fn 13 auf Seite 9).

Bezüglich der klaren Angaben über den Charakter der kommerziellen Kommunikation und den Auftraggeber enthält **§ 7 TDG bereits ausreichende Vorschriften**, die allerdings bislang nicht bußgeldbewehrt sind.

Eine praxistaugliche Abgrenzung der Anbieterpflichten aus §§ 6 und 7 Satz 1 Nr. 1 und Nr. 2 TDG zu den neuen Pflichten in § 7 Satz 1 Nr. 3 TDG-E ist nicht erkennbar.

2.2. „Kommerzielle Kommunikation"

§ 7 Nr. 3 TDG-E beschränkt sich auf kommerzielle Kommunikationen. Der Begriff wird in § 3 Nr. 5 TDG definiert in Umsetzung von Artikel 2 f der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (ECRL). Laut Begründung zu § 3 Satz 1 Nr. 5

115 Siehe zur Diskussion etwa Spindler/Schmitz/Geis TDG § 2 Rz. 22 ff.
116 Zum fraglichen Kriterium der „elektronischen Post" siehe unten Ziffer 2.3, zur Unzulässigkeit: LG Berlin v. 14.01.2003, 15 O 420/02.
117 z.B. Chat Messages bei Skype.
118 siehe etwa Fußnote 13 auf Seite 9 des Entwurfs.

TDG ist der Begriff „in einem umfassenden Sinn zu verstehen und schließt daher sämtliche Formen der Werbung, des Direktmarketing, des Sponsoring, der Verkaufsförderung und der Öffentlichkeitsarbeit ein (BT-Drs 14/6098, Seite 16). Unter kommerzielle Kommunikation dürfte daher **jede Art** der unternehmens- oder produktbezogenen **Werbung** fallen. Bei extensiver Auslegung des Begriffes dient jede Kundenkommunikation der Absatzförderung, die nicht ausschließlich der Leistungserbringung selbst dient.

Damit sind dennoch **nicht alle Formen** der belästigenden und die Internetressourcen beeinträchtigenden Versendung **elektronischer Kommunikationen** erfasst. Die Begründung nimmt an (S. 5), auch Viren-Mails oder Phishing-Attacken stellten Werbemails dar. Dies erscheint kaum vertretbar. Solche Kommunikationen, ebenso wie Kettenbriefe, der sog. Nigeria-Spam[119], Virus-Hoaxes und vergleichbare Sendungen dienen weder werblichen noch gewerblichen Interessen.

2.3. „Per elektronischer Post (E-Mail)“

Der Anwendungsbereich des § 7 Nr. 3 TDG-E wird beschränkt auf solche kommerziellen Kommunikationen, die per elektronischer Post versandt werden. Unter elektronischer Post oder E-Mail dürften alle Nachrichten verstanden werden, die mittels einem auf elektronischer Übertragung basierenden Kommunikationssystem ausgetauscht werden.

Das weltweit bekannteste und verbreitetste E-Mail-System wird durch das Simple Mail Transfer Protocol (SMTP) beschrieben und ermöglicht den Nachrichtenaustausch zwischen Teilnehmern des Internets. Begründung und Gesetz beziehen sich wohl **nur auf solche SMTP-Mails**. Dies ergibt sich etwa aus der Annahme einer Kopf- und Betreffzeile. Auch eine Mobilfunk-Nachricht im Short Message Service (SMS) enthält zwar einen Header, aber keine Betreffzeile.[120] Wohl nicht erfasst sind außerdem andere Formen des Messaging-Spam, ungenehmigte Einträge in Gästebüchern, auf offenen Plattformen oder auch in anderen offenen Netzressourcen (Beispiele: Newsgroup Spam, Wiki-Spam, Spamdexing, Blog Spam).[121] Allerdings ist der Entwurf hier ungenau. Nach dem Wortlaut des § 7 TDG-E wäre eine Anwendung auf solche anderen elektronischen Nachrichtensysteme denkbar, allerdings scheint die Begründung nicht davon auszugehen. Der Anwendungsbereich sollte klargestellt werden.

Außerhalb des Anwendungsbereiches liegen jedenfalls Methoden des sogenannten Guerilla-Marketings, die darin bestehen, in allgemein verfügbaren Netzressourcen von den Betreibern nicht gewünschte Werbebotschaften unterzubringen. Das ist umso bedauerlicher, da das allgemein als erstes kommerzielles Spamming bekannt gewordene Verhalten Postings in Usenet-Foren betraf und keine E-Mails.[122] Diese Formen des Spammings sind auch in gleicher Weise schädlich. Auch hier liegen zumeist automatisierte, massenhafte Eintragungen zu Lasten individueller oder zu Gunsten der Allgemeinheit vorgehaltener Ressourcen vor.

2.4. „In der Kopf- und Betreffzeile“

Sprachlich sollte dieses Merkmal **präzisiert** werden:

2.4.1. Gemeint sind Manipulationen in „den Kopfzeilen“, also Plural. Eine einzelne oder eine besondere „Kopfzeile“ gibt es innerhalb einer E-Mail nicht. Betroffen sind die sogenannten Header-Informationen einer E-Mail also der Kopfteil im Gegensatz zum Haupt- oder Inhaltsteil (siehe hierzu: Request for Comments (RFC) 2822 Seite 6[123], früher: RFC 821[124]). Im Kopfteil sind verschiedene Metainformationen zur Nachricht, einschließlich der Routinginformationen enthalten. Absenderinformationen können dabei in verschiedenen E-Mail-Kopfzeilen enthalten sein.[125] Die Beschränkung auf den Singular dürfte daher ein Redaktionsversehen sein.

2.4.2. Das verwendete „und“ ist nicht kumulativ gemeint. Daher könnte eine Ersetzung durch „oder“ erfolgen. Andererseits ist die Betreffzeile eine der „Kopfzeilen“.[126] Technisch ist die Angabe eines Betreffs nicht erforderlich. Informationen in der Betreffzeile können sowohl den Absender als auch den kommerziellen Charakter verschleiern. Klarer dürfte daher die Formulierung sein „(...) in den Kopfzeilen, insbesondere der Betreffangabe (...)“.[127]

2.5. „Absender oder kommerzieller Charakter“

2.5.1. „Absender“

Der Gesetzentwurf führt den neuen Begriff des „Absenders“ ein. Dieser ist zu unterscheiden vom „Diensteanbieter“[128] gemäß § 3 Satz 1 Nr. 1 TDG und dem Auftraggeber, § 7 Nr. 2 TDG.

Der Begründung kann entnommen werden, dass der **Begriff des Absenders weit zu verstehen** sei und sich von dem des Diensteanbieters unterscheide (Seite 13). So soll ein Hinweis auf die Organisationseinheit, für die der Versender tätig ist oder auf den Auftraggeber gemäß § 7 Nr. 2 TDG genügen. Zugleich soll ein Hinweis auf den **tatsächlichen Versender** der E-Mail nicht erforderlich sein. Damit entfernt sich die Verwendung des Wortes „Absender“ jedoch erheblich vom üblichen Sprachgebrauch. Unsicherheiten bei der Umsetzung sind daher zu befürchten.

---

119 Siehe hierzu: http://en.wikipedia.org/wiki/Advance_fee_fraud.
120 http://de.wikipedia.org/wiki/SMS#Aufbau_der_SMS.
121 bei den meisten dieser Spam-Formen dürfte bereits das TDG nicht anwendbar sein (s.o.).
122 der Canter & Siegel Green Card Spam von 1994.
123 http://www.ietf.org/rfc/rfc2822.txt.
124 ftp://ftp.rfc-editor.org/in-notes/rfc821.txt.
125 Siehe dazu 3.6.2 auf Seite 20 der RFC 2822.
126 Siehe dazu 3.6.5 auf Seite 25 der RFC 2822.
127 bestehen bleibt dann allerdings die unter Ziffer 2.6.2 dargestellte Unklarheit.
128 Schon bei diesem im Gesetz selbst definierten Begriff ist es nicht gelungen, eine einheitliche Verwendung innerhalb des Gesetzes zu gewährleisten, wie sich daraus ergibt, dass nicht alle Diensteanbieter im Sinne der Haftungsprivilegien der §§ 8 ff. TDG zugleich informationsverpflichtet gemäß § 6 TDG sein können.

Gemeint scheint zu sein, dass eine funktionierende E-Mail-Adresse anzugeben ist, die der Sphäre des Spam-Versenders oder des Auftraggebers zuzurechnen ist. Diese hat mit der Identität des Absenders allerdings nicht notwendig zu tun. Erhebliche Umgehungsmöglichkeiten eröffnet der Entwurf dadurch, dass der „Absender" nur im Zeitpunkt der Versendung unverschleiert sein muss. Spammer wechseln ihre Organisationseinheit jedoch tätigkeitsbedingt sehr oft. Nicht erfasst scheinen solche Fälle zu sein, in denen eine zum Zeitpunkt der Versendung gültige E-Mail-Adresse angegeben wird, die anschließend vom Versender aufgegeben wird.[129]

Ob **Verschleierungen des Routings** (etwa durch falsche IP-Adressen) eine Absendertäuschung darstellen, bleibt unklar.

Die Verschleierung oder Verheimlichung des Absenders festzustellen wird sich als außerordentlich schwierig erweisen, wenn sich aus dem Gesetz nicht bestimmen lässt, wer als Absender anzugeben sein soll.

Gewünscht ist stattdessen, dass der Veranlasser kommerzieller Kommunikationen im Header gültige E-Mail-Adressen, über die eine Kontaktaufnahme mit ihm erfolgen kann, anzugeben hat und die Routinginformationen nicht manipulieren darf.

2.5.2. „Kommerzieller Charakter"

Der kommerzielle Charakter einer Nachricht dürfte sich aus der Tatsache ergeben, dass die E-Mail nicht für den privaten Informationsaustausch bestimmt ist, sondern der gewerblichen Tätigkeit des Versenders zuzurechnen ist.

Problematisch werden Fälle sein, in denen eine kommerzielle Mail privat (weiter-) gesendet wird.[130] Sofern nicht angenommen wird, dass durch das private Dazwischentreten der kommerzielle Charakter der Kommunikation beseitigt wird[131], dürfte der private Nutzer regelmäßig den kommerziellen Charakter der Mail nicht deutlich machen. Diese Fälle können dann erst durch den subjektiven Tatbestand erledigt werden.

2.6. Verschleiern oder Verheimlichen

2.6.1. Regelbeispiele des Verschleierns oder Verheimlichen

2.6.1.1. Absicht

Durch das Erfordernis eines besonderen subjektiven Tatbestandes („absichtlich") **im Rahmen eines Regelbeispieles** wird der Grundtatbestand nicht modifiziert. Gesetzestechnisch fehlerhaft erscheint es daher, das nur das Regelbeispiel eine besondere Anforderung an den subjektiven Tatbestand fordert. Die Absicht, Bagatellfälle auszuklammern wird nicht durch Einschränkungen lediglich auf Ebene der Regelbeispiele für die Verwirklichung erreicht.

Der Gesetzesentwurf enthält als Beispiel für das Verschleiern oder Verheimlichen eine absichtliche Gestaltung der Kopf- oder Betreffzeile durch die der Empfänger vor Einsichtnahme in die Inhalte der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält. Nach der Begründung soll die Verschleierungs- oder Verheimlichungsabsicht im Regelbeispiel die Anforderung an die subjektive Seite erhöhen, um unabsichtliche Unklarheiten kleinerer oder mittlerer Unternehmen zu entkriminalisieren. Das dabei eingrenzend gedachte Kriterium der absichtlichen Gestaltung wird diese Funktion jedoch nicht leisten.

Die Absicht bezieht sich außerdem **auf die tatsächliche Frage**, ob der Empfänger im Kopfteil keine oder irreführende Informationen über den kommerziellen Charakter der Nachricht erhält. Unerheblich ist nach dem Wortlaut dagegen die Intention des Absenders, den Empfänger der E-Mail hierüber zu täuschen. Entscheidend ist lediglich, ob der Absender absichtlich die erforderlichen Informationen eingefügt hat oder nicht. Der Begründung kann zwar entnommen werden, dass eigentlich eine Verschleierungs- oder Verheimlichungsabsicht Voraussetzung sein sollte (S. 8). Nachdem diese Motivation sich im Wortlaut der Vorschrift nicht wiederspiegelt, wird sie wohl auch keine Berücksichtigung bei der Auslegung finden.[132]

Das subjektive Erfordernis einer absichtlichen Verschleierung oder Verheimlichung oder einer beabsichtigten Täuschung sollte, da die Privilegierung fahrlässiger Spammer zweckmäßig erscheint, in den Tatbestand in § 7 Satz 1 der Nr. 3 TDG-E aufgenommen werden.

2.6.1.2. Informationspflicht in Betreffzeile

Im Ergebnis führt die vorgeschlagene Norm zur **Einführung** einer Kennzeichnungspflicht kommerzieller Kommunikation **im Kopfteil einer E-Mail**. Aufgrund der Verwendung der unklaren Tatbestandsalternativen des Verschleierns und Verheimlichens wird für seriöse Unternehmen kaum eine Alternative zur ausdrücklichen Bezeichnung als kommerzielle Kommunikation bleiben.

2.6.1.3. „Tatsächliche Identität des Absenders"

Weitere Unsicherheit wird dadurch verursacht, dass im Regelbeispiel des Verschleierns oder Verheimlichens auch fehlende oder irreführende Informationen über „die tatsächliche Identität des Absenders" genannt sind. Die **tatsächliche Identität** des Absenders ist nach dem Grundtatbestand der Norm gar nicht anzugeben sondern nur „der Absender". Unter der tatsächlichen Identität des Absenders dürf-

---

129 Spammer fälschen auch häufig ihre Whois-Daten: http://www.heise.de/newsticker/meldung/58172

130 beispielsweise die beliebten „Send to a Friend" Angebote wie E-Cards.

131 Wettbewerbswidrigkeit der Aufforderung zur Versendung von Werbeemails durch private Nutzer nimmt offenbar an: LG Nürnberg 04.03.2004, 4 HK O 2056/04, JurPC Web-Dok 20040185.

132 siehe bereits zum TDG in der Fassung des IuKDG: Einstellungsverfügung des Generalbundesanwalts beim BGH vom 26.11.1997, 2 BJs 104/96-4, JurPC Web-Dok. 17/1998.

te nach der bisherigen Gesetzesterminologie **der wirkliche Name des Absenders** zu verstehen sein (vgl. § 6 Nr. 1 TDG, § 312 c Abs. 1 BGB i.V.m. § 1 Abs. 1 Nr. 1 BGB-InfoV). Das Regelbeispiel enthält somit strengere Anforderungen als der Grundtatbestand und widerspricht so dem weiten Verständnis des Begriffs des Absenders (s.o.) und führt zu Unklarheiten.

2.6.2. „Verschleiern oder Verheimlichen"

Verschleiern und Verheimlichen sind unscharfe Begriffe. Während unter Verheimlichen analog zu § 283 Abs. 1 Nr. 1, 6 und 8 StGB wohl ein Verhalten verstanden wird, das darauf abzielt, eine offenbarungspflichtige Tatsache der Kenntnis anderer zu entziehen[133], ist der Tatbestand des Verschleierns auch im Strafrecht noch nicht konkretisiert worden. Allgemein wird unter Verschleiern wohl die aktive Veränderung von Informationen zum Zwecke der schlechteren Erkennbarkeit einer Tatsache verstanden werden können. Sowohl Verschleiern als auch Verheimlichen setzen wohl eine wahre Tatsache sowie eine berechtigte Erwartung des Kommunikationspartners auf wahrheitsgemäße Information voraus.

Angesichts des eingeschränkten Umfanges, der in einer Betreffzeile vom durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Verbraucher wahrgenommen werden wird, erschiene jede Formulierung einer Betreffzeile riskant, die **nicht ausdrücklich** auf den kommerziellen Charakter hinweist.

Bei impliziten Angaben in der Betreffzeile wird es dagegen auf die konkrete Formulierung ankommen.

Unklar lässt der Entwurf, ob **weitere Headerangaben** bei der Beurteilung einer Verschleierung Berücksichtigung finden. Während der Tatbestand des § 7 Nr. 3 TDG-E von Verschleierung in Kopf- **und** Betreffzeile spricht, soll nach dem Beispiel des § 7 Nr. 3 TDG-E eine Verschleierung in Kopf- **oder** Betreffzeile ausreichen. Folge ist weitere Unklarheit und Auslegungsspielraum. Beispielsweise dürfte die Angabe eines bekannten Unternehmens oder einer beschreibenden E-Mail-Adresse als Absender eine Verschleierung über den kommerziellen Charakter ausschließen. Bereits die Verwendung einer E-Mail-Adresse unterhalb einer Top-Level-Domain „.com" weist auf den kommerziellen Charakter der Kommunikation hin.

Andererseits erscheint eine Verschleierung des werblichen Charakters im Kopfteil **außerhalb** der Betreffzeile möglich, wenn man eine Täuschung durch Verwendung einer irreführenden Toplevel Domain als Bestandteil der E-Mail-Adresse annimmt (bspw. .org). Dieser Interpretationsspielraum wird eher von unseriösen Anbietern genutzt werden können.

Es ist nicht erkennbar, welches Problem durch die Einführung des Tatbestandes der Verschleierung des kommerziellen Charakters einer E-Mail gelöst wird. § 7 Nr. 1 TDG enthält bereits die Verpflichtung zur Klarheit kommerzieller Kommunikationen. Sinnvoll erschiene die Durchsetzung einer **international einheitlichen Kennzeichnung Werbung**, die dem Nutzer ermöglichen würde, solche Nachrichten automatisiert bearbeiten zu lassen (und beispielsweise auszufiltern oder nur bestimmte Versender zuzulassen). Der Entwurf kann dieses nicht leisten, da implizite Hinweise auf den kommerziellen Charakter ausreichen und eine automatisierte Erkennung solcher Angaben derzeit technisch noch nicht möglich sein wird.

Der Entwurf dürfte dagegen zur Folge haben, dass beim legalen E-Mail-Marketing **weitere unklare Informationspflichten** zu beachten sind. Wohl unbeabsichtigt gilt dies nicht nur für E-Mail-Marketing sondern für alles, was unter den wenig trennscharfen Begriff der kommerziellen Kommunikation fällt.[134] Gerade in den Fällen, in denen der Absender gar nicht daran denkt, dass seine (individuelle) E-Mail auch den Absatz von Waren oder Dienstleistungen fördern könnte, wird leicht eine Verschleierung in der Betreffzeile verwirklicht. Dies erst auf der subjektiven Ebene zu lösen erscheint inadäquat, da es sich um ein harmloses Alltagsgeschehen handelt.

3. § 12 TDG

Die Formulierung des § 12 TDG ist missglückt. Zum einen wird auf die Verwirklichung des Tatbestandes des § 7 Satz 1 Nr. 3 TDG verwiesen, zum anderen werden wesentliche Teile dieser Vorschrift in § 12 TDG wiederholt. Dies schafft Spielraum für Interpretationen darüber, ob den **wiederholten** Tatbestandsmerkmalen eine besondere Bedeutung zukommt. Gleichzeitig enthält § 12 TDG zusätzlich Modifikationen, die in der Praxis für Rechtsunsicherheit sorgen werden. Die bereits angeführten Unklarheiten und Widersprüche des § 7 TDG-E lassen bezweifeln, dass der Tatbestand des § 12 TDG-E überhaupt ausreichend bestimmt ist.

3.1. Fahrlässige Begehung

Während § 7 Nr. 3 Satz 2 TDG-E die absichtliche Verschleierung oder Verheimlichung als Regelbeispiel des Verschleierns und Verheimlichens postuliert und der Begründung entnommen werden kann, dass dieses besondere subjektive Merkmal allgemein für einen Verstoß gegen § 7 Nr. 3 Satz 1 TDG-E gelten solle, reicht nach § 12 Abs. 1 Satz 1 TDG-E eine vorsätzliche oder fahrlässige Begehung. Damit soll eine fahrlässige Verwirklichung des Tatbestandes des § 7 TDG-E ausreichen, der wiederum bezüglich des Verschleierns und Verheimlichens Absicht voraussetzen soll. Die fahrlässige Begehung einer absichtlichen Handlung ist indes nicht denkbar.

3.2. „Bei der Versendung"

Während § 7 Nr. 3 TDG-E des Entwurfes verbietet, beim Versand bestimmte Informationen zu verschleiern oder zu verheimlichen, deutet die Formulierung in § 12 TDG-E darauf hin, dass das Buß-

133 vgl. Tröndle/Fischer, StGB § 283, Rz. 5.

134 s.o. 2.2.

geld nur durch Verheimlichung oder Verschleierung „bei der Versendung“ verwirkt werden könne. Probleme wird dies bezüglich des Handlungsortes verursachen, der für die Anwendbarkeit der Bußgeldvorschrift von entscheidender Bedeutung ist. Tätig wird der Spammer regelmäßig **nur im Ausland**.[135] Somit setzt die Verfolgbarkeit einen Erfolgsort im Inland voraus, § 7 OWiG. § 12 TDG-E setzt aber einen tatbestandlichen Erfolg i.S.d. Zugangs der E-Mail nicht voraus. Die Betonung der Begehung „bei der Versendung“ durch die Formulierung des § 12 Abs. 1 Nr. 2 TDG-E begrenzt die Anwendbarkeit auf im Inland versandte E-Mails.

Außerdem erscheint fraglich, ob durch die Beschränkung auf Begehungen „bei der Versendung“ verbreitete Spammethoden ausgeklammert werden. Insbesondere gilt dies für Falle des als besonders verwerflich erscheinenden Okkupierens eines fremden Servers zur Versendung von Spam.

Dem liegt folgender technischer Vorgang zugrunde: Spam-Versender nutzen oft aus, dass manche Inhaber von Netzinfrastrukturen ihre zum Mailversand zugelassenen Server (SMTP-Server) nicht ausreichend absichern. Sie können so von Spam-Versendern für die Versendung missbraucht werden und zugleich dem tatsächlichen Versender Anonymität bieten. Die Nichtangabe der Absenderinformationen erfolgt dabei aufgrund der vom okkupierten Server zugelassenen Einstellungen erst im Zeitpunkt der Versendung. Der Initiator des Spam dagegen verschleiert in seiner Kommunikation mit dem okkupierten Server unter Umständen weder seine Identität noch den kommerziellen Charakter etwaiger Handlungen.

Durch die abweichende Formulierung des § 12 TDG-E vom Tatbestand des § 7 Nr. 3 TDG-E ließe sich argumentieren, dass es ausdrücklich nur auf den Vorgang des Versendens ankäme und somit etwaige technische Einstellungen des okkupierten aber insoweit offenen Servers nicht dem ursprünglichen Erzeuger der Mail zugerechnet werden können. Der Serverbetreiber selbst dürfte nicht tatbestandlich unterlassen.

3.3. Durchführung

Unklar bleibt, wo die erforderlichen personellen und sachlichen Ressourcen zur Aufklärung und Bearbeitung der zahllosen potentiellen Sachverhalte zu finden sein werden. Auf welche Weise die Ermittlung von Absendern ohne Angaben zur wahren Identität durch die örtlichen Behörden erfolgen soll bleibt rätselhaft. Besondere Befugnisse enthält der Entwurf nicht. Die Informationen, die zu ermitteln sind, dürften dem Fernmeldegeheimnis unterfallen, § 88 Abs. 1 TKG 2004.

Eine wirksame Bekämpfung von Spam ist durch § 12 Abs. 1 Nr. 2 TDG-E nicht zu erwarten.

B Zum Antrag der Abgeordneten Dr. Martina Krogmann, Ursula Heinen, Julia Glöckner, weiterer Abgeordneter und der Fraktion der CDU/CSU, Spam effektiv bekämpfen, BT-Ds. 15/2655

[135] s.o. 1.2

1. Es erscheint geboten zur Etablierung internationaler Standards auch in Deutschland das Spammen oder typischerweise damit einhergehende Manipulationen und Täuschungen durch straf- oder bußgeldrechtliche Verbote zu ächten. Entsprechende Tatbestände sollten jedoch klar und eindeutig nur das Verhalten bestrafen, welches missbilligt wird. Jede unilaterale nationale Ausweitung von Informationspflichten ist zu vermeiden. Die Anzahl der Informationspflichten im elektronischen Geschäftsverkehr sprengt bereits jede Aufnahmekapazität.

2. Die Ausdehnung einer etwaigen ordnungsrechtlichen Verantwortung und Bußgeldpflicht für Spam auf die Beworbenen erscheint nicht zweckmäßig. Die Zurechnung nach den allgemeinen Normen ist ausreichend, insbesondere unter Berücksichtigung der sonst erheblich gesteigerten Missbrauchsgefahr falscher Bewerbung in Schädigungsabsicht[136].

3. Das Ausmaß und die negativen Auswirkungen des Spam sind unmittelbare Folge der Globalisierung der Kommunikationseinrichtungen. Spammer weichen auf diejenigen Länder aus, die das niedrigste Niveau an Schutzvorschriften haben. Gelöst wird das Problem daher nur durch Selbstregulierung des Internets, insbesondere der beteiligten Provider, oder internationale Regelungen und Standards.

4. Die Einrichtung einer Melde-/Beschwerdestelle für Spambetroffene erscheint nur insoweit sinnvoll, als die Koordinierung sowie die Entwicklung von Regelungen und Standards auf internationaler Ebene auf diese Weise gefördert werden könnte.

5. Effektiver und sicherer Umgang mit Informationstechnologie und Kommunikationsmitteln dürfte eine Schlüsselkompetenz für Unternehmer und Verbraucher gleichermaßen darstellen, um an der Informationsgesellschaft teilhaben zu können. Eine Über-Förderung ist kaum denkbar.

C Zusammenfassung der Empfehlungen

1. Das Verbot des Manipulierens von E-Mail-Headerinformationen zur Verschleierung des Absenders bei der Versendung massenhafter unverlangter Nachrichten erscheint sinnvoll, um entsprechende internationale Standards zu bilden. Ein enger Straftatbestand erscheint für die Signalwirkung geeigneter als eine weit formulierte Ordnungswidrigkeit. Ein solches Verbot sollte klar formuliert sein und keine weiteren Unsicherheiten bei der Verwendung moderner Kommunikationsmöglichkeiten für die Unternehmen mit sich bringen. Der Gesetzesentwurf ist insoweit ungeeignet.

2. Die Einführung eines international einheitlichen Kennzeichens für Werbung im E-Mail-Header erscheint sinnvoll, um automatisierte Verarbeitungen zu ermöglichen. Dies wird nur durch allgemeine Anerkennung neuer Standards gelingen. Das vorliegende Verbot einer Verschleierung des

[136] Verschiedentlich finden sich Berichte über Spammer, die bekannte Bekämpfer unverlangter Werbenachrichten als Absender in ihren Werbeschreiben angeben. Auch gab es bereits Presseberichte über das automatisierte Anklicken von Werbebannern des Mitbewerbers, um diesen durch die dabei entstehende Vergütung an den Werbepartner zu schädigen.

kommerziellen Charakters in der Betreffzeile ist dagegen abzulehnen. Die Anforderungen an die elektronische Kommunikation mit Kunden sind bereits überspannt. Das vorgeschlagene Verbot wird gegen Spam nicht nützen und der Kundenkommunikation schaden.

3. **Es sollte sichergestellt werden, dass die Provider die erforderlichen Maßnahmen zur Spamabwehr treffen dürfen, ohne dass entsprechende Befugnisse zugleich die Vertraulichkeit der Kommunikation preisgeben.**
4. **Unsicherheit besteht bezüglich der Anforderungen an rechtskonforme E-Mail-Kommunikation. (Zusendung der Opt-In Bestätigung, Anbieterinformation nach § 6 TDG, E-Mail-Werbung von Kunden an Bekannte). Eine Erleichterung und Klärung der Anforderungen an dieses zeitgemäße Kommunikationsmittel erscheint sinnvoller als neue Vorschriften.**
5. **Bedrohungen der elektronischen Kommunikation sollten frühzeitiger identifiziert und die Erforderlichkeit von Maßnahmen geprüft werden. (Beispiele: Phishing, nichtkommerzieller Spam, geringe Nutzung von Verschlüsselungstechnologie, große Datensammlungen im EU-Ausland). Die meisten dieser Bedrohungen sind Folgen der Globalisierung der Kommunikationseinrichtungen. Erforderlich sind internationale Standards und Vereinbarungen. Die Reaktionszeit ist hierfür zu lang. Als Beginn des kommerziellen Spammens gilt der 05.03.1994.**

Matthias Hartmann