Unerwünschte Direktwerbung per E-Mail

Georg Lechner

georg.lechner@bka.gv.at[1]

Schlagworte: Datenschutz, Spam, UCE, E-Mail, §§ 101, 104 Telekommunikationsgesetz, TKG, Datenschutzgesetz 2000, DSG 2000, Robinson-Liste, Electronic Commerce

Abstract: Unerwünschte Direktwerbung per E-Mail, auch als „Spam" bekannt, ist schon seit Jahren eine Plage im Internet. Der Artikel befasst sich in sehr gerafter Form mit diesem Phänomen, insbesondere im Hinblick auf die datenschutzrechtliche Unzulässigkeit der Beschaffung von E-Mail-Adressen durch Suchprogramme („Spambots"), sowie mit den rechtlichen Bestimmungen gegen Spam, u.a. auch § 101 Telekommunikationsgesetz.

Das Phänomen der Direktwerbung hat vor dem Internet nicht Halt gemacht, ganz im Gegenteil. Direkt adressierte Massensendungen mit Werbemitteilungen per E-Mail gehören zum Alltag der Internet-Benutzer. Unerwünschte Direktwerbung wird allgemein als „Spam" [2] bezeichnet. Dieser Artikel befasst sich mit Spam aus der Sicht des Datenschutzes und behandelt daher nur unerwünschte Nachrichten, zu deren Verteilung personenbezogene Daten im Sinn des Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 (DSG 2000), Verwendung finden. Andere Worte für unerwünschte Direktwerbung per E-Mail sind „Unsolicited Commercial E-Mail" (kurz „UCE"), „Unsolicited Bulk E-Mail" (kurz „UBE") und „Junk E-Mail". Bei der Suche nach Informationen im Internet sind diese Synonyme nützlich.

---

[1] Der Artikel gibt die persönliche Ansicht des Autors wieder und ist keinesfalls als Stellungnahme einer Behörde zu verstehen. Besuchen Sie bitte die Homepage der Datenschutzabteilung des Bundeskanzleramtes: http://www.austria.gv.at/regierung/VD/V3.htm

[2] Der Name geht auf ein Produkt der Lebensmittelfirma Hormel zurück (http://www.spam.com/). Zur Verwendung des Wortes für unerwünschte Nachrichten siehe http://www.cs.ubc.ca/spider/samm/sow/mpspam.html.

1.1 Der Inhalt von Spam

Im Gegensatz zu regulärer Werbepost, die auch von seriösen Firmen eingesetzt wird, ist Spam vor allem ein Medium unseriöser Unternehmen. Spam betrifft vorrangig Pyramidenspiele, Pornografie, raubkopierte Software und sonstige Angebote, die mit Vorsicht zu geniessen sind. Dienste zur Versendung von Spam werden auch gerne beworben[3].

1.2 Warum ist Spam schädlich?

Die Frage, warum Spam ein Problem darstellt, muss gestellt werden, weil zwar die Internet-Gemeinschaft allgemein gegen Spam ist, aber in der rechtswissenschaftlichen Literatur zum Teil unterschiedliche Meinungen vertreten werden[4].

1.2.1 Kosten

Spam verursacht beträchtliche Kosten, insbesondere durch Belastung der Infrastruktur des Internets mit einer großen Menge an nutzlosen Datentransfers. Spam benötigt Transportkapazität („Bandbreite") und Speicherplatz. Die Gesamtmenge der Spams lässt sich nur schätzen, weil sie von normalen E-Mails kaum zu unterscheiden sind. Viele werden am Zielort von Spam-Filtern abgefangen und werden daher nicht zur Kenntnis genommen, verbrauchen aber auf ihrem Weg Ressourcen. Die Kosten des Transports von Spam sind schwer quantifizierbar, aber sie sind vorhanden[5]. Spam ist für den Absender sehr billig, weil die Kosten von allen Usern getragen werden.

1.2.2 Rechtsunsicherheit

Ein übliches Mittel gegen Spam sind spezielle Anti-Spam-Programme („Spam-Filter"), die eingehende Post nach bestimmten Kriterien als Spam klassifizieren und löschen. Ein Spam-Filter kann auch irrtümlich eine erwünschte Nachricht ausfiltern. Die Haftungsfragen in so einem Fall sind unklar, aber die Folgen können für Unternehmer im E-Commerce be-

---

[3] Eine Liste von wegen Spamming gesperrten IP-Adressen mit Beispielen von Spams finden Sie bei EUnet unter http://service.austria.eu.net/cgi-bin/blkview

[4] „E-mail-Werbung zulässig?", RdW 1999, 386

[5] Eine recht anschauliche Darstellung, wenn auch etwas veraltet, ist der Artikel „Postage due on junk e-mail-Spam costs Internet millions every month", Internet Week, 4. Mai 1998 (http://www.techweb.com/se/directlink.cgi?INW19980504S0003).

trächtlich sein. Ohne Spam-Filter steigt wiederum der Personalaufwand, um Spams auszusortieren.

1.2.3 Schädigung der Privatsphäre

Die Kommunikation im Internet ist vielfach ungesichert und leicht einsehbar. In einer derartigen Situation ist Respekt vor der Privatsphäre der User erforderlich, um freie Kommunikation unter Gleichgesinnten zu ermöglichen. Dies ist mit Gesprächen auf einem öffentlichen Platz vergleichbar: Es kann zwar jeder Passant mithören, aber es wird erwartet, dass niemand absichtlich lauscht oder Gespräche aufzeichnet. Respekt vor der Privatsphäre anderer ist für offene Datennetze essenziell.

1.3 Spambots

Das Internet enthält große Mengen an E-Mail-Adressen, die mit geeigneter Software eingesammelt werden können. Derartige Suchprogramme heissen im Fachjargon allgemein „Robot", „Spider" oder „Webcrawler". Robots, die E-Mail-Adressen für Direktwerbung einsammeln, heißen oft „E-Mail Extractor" oder auch „Address Harvester". Die Gegner von UCE nennen sie auch „Spambots". Ein E-Mail Extractor wertet folgende Adressen aus:

- Adressen, die auf Homepages angegeben sind. Das sind hauptsächlich die Adressen der Betreiber der Seiten, aber auch der Servicetechniker. Viele moderne Extraktoren können offensichtliche Serviceadressen ausfiltern (z.B. support@business.com).
- Adressen aus dem Usenet. Es ist allgemein üblich, bei Postings im Usenet eine E-Mail-Adresse anzugeben. Extraktoren sammeln diese Adressen ein. Viele Extraktoren können eingesammelte Adressen nach Newsgroups sortieren und damit Hinweise auf mögliche Interessen des Benutzers geben. Dies schafft vor allem dann Probleme, wenn der Spambot nicht erkennt, dass ein Posting nur in einer kontroversiellen Newsgroup aufscheint, weil der Autor auf eine unerwünschtes, rassistisches oder sonst störendes Posting geantwortet hat, das in mehreren Newsgroups platziert war („Crossposting"). Die Antworten auf Crosspostings erscheinen, sofern der Autor der Antwort dies nicht ändert, in denselben Newsgroups wie die Originalnachricht. Dies bedeutet, dass ein Spambot in einer Newsgroup mit extremistischer Zielsetzung auch E-Mail-Adressen von Leuten finden kann, die sich bloss gegen ein Crossposting eines Extremisten verwahrt haben.

Spambots werden wie normale Software gehandelt (z.B. GEEWiz32, http://www. firstlinesoft.com/index.shtml [6]).

Robots werden auch von legalen Suchmaschinen benützt, um neue Webseiten zu finden. Legale Robots respektieren das „Robot Exclusion Protocol" oder bestimmte Informationen innerhalb einer Web-Seite, womit der Betreiber einer Homepage bestimmen kann, ob seine Seite erfasst werden soll [7].

Weiters ist es üblich, Adressen durch Auswertung von Mailing-Listen oder Kauf (oft viele tausend auf einer CD-ROM) zu beschaffen.

1.4 Spam und Datenschutz

§ 4 Z 1 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999, enthält folgende Definition personenbezogener Daten:

> „Daten" („personenbezogene Daten"): Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen" sind Daten für einen Auftraggeber oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Es liegt auf der Hand, dass eine E-Mail-Adresse, die den Namen des Empfängers enthält, ein personenbezogenes Datum ist (also z.B. Hans.Huckebein@provider.at). Es ist unklar, ob eine E-Mail-Adresse, deren Inhaber auch dem Betreiber unbekannt ist, ein anonymes Datum ist, solange niemand Schritte unternimmt, um den Inhaber zu identifizieren.

Das neue DSG 2000, das am 1. Jänner 2000 in Kraft getreten ist, enthält für die Zulässigkeit der Verwendung von Daten den Grundsatz der „doppelten Bedingtheit". Für die Verwendung sind erforderlich

- eine rechtliche Befugnis für die Art von Tätigkeit, der die Datenverwendung dient, und

---

[6] Das Hyperlink zu GEEWiz32 war am 9. Feber 2000 noch aktiv, aber das kann sich rasch ändern. Werbung für Spambots ist nicht gerne gesehen, und die URLs wechseln oft. Eventuell ist eine Suche nach dem Produktnamen sinnvoll.

[7] Weiterführende Informationen über legale Robots finden Sie unter http://info.webcrawler.com/mak/projects/robots/robots.html.

- die Prüfung, ob schutzwürdige Geheimhaltungsinteressen verletzt sind.

Wer mit Spambots ohne Zustimmung der Betroffenen deren E-Mail-Adressen einsammeln will, wird sich auf § 8 Abs. 2 DSG 2000 berufen, wonach bei der Verwendung von zulässigerweise veröffentlichten Daten schutzwürdige Geheimhaltungsinteressen als nicht verletzt gelten. Das Recht, gegen die Verwendung solcher Daten gemäß § 28 DSG 2000 Widerspruch zu erheben, bleibt unberührt.

Diese Bestimmung soll die Verwendung von Daten aus veröffentlichten Quellen (Telefonbuch, Firmenbuch, Prospekte, öffentliche Bekanntmachungen, etc.) entbürokratisieren. Die Frage, ob eine im Internet (WWW oder Usenet) angegebene E-Mail-Adresse wirklich in diesem Sinne „zulässigerweise veröffentlicht" ist oder die Verwendung doch einer Zweckbindung unterliegt (z.B. Kommunikation mit Gleichgesinnten zu einem bestimmten Thema, Meldung von Störungen) kann in diesem Artikel nicht beantwortet werden. Die Frage stellt sich auch z.B. bei der Auswertung von öffentlichen Ankündigungen (Bauverhandlungen) durch Unternehmer.

Allerdings erfordert der Grundsatz der doppelten Bedingtheit auch eine rechtliche Befugnis, die Daten zu verarbeiten (§ 7 Abs. 1 DSG 2000), und da in Österreich Spamming verboten ist (siehe unten) wird es generell unzulässig sein, personenbezogene Daten für diesen Zweck zu ermitteln, d.h. der Betrieb von Spambots wäre in Österreich datenschutzrechtlich unzulässig.

1.5 Abwehr von Spam

Die Möglichkeiten, Spam aus eigenen Mitteln abzuwehren, umfassen Spam-Filter, Gebrauch mehrerer E-Mail-Adressen, Beschwerden beim Provider, Einsatz von Software, die Spambots mit nutzlosen Daten füttert (was nur legal ist, wenn Spambots illegal sind!), und die Verfälschung von E-Mail-Adressen (z.B. Hans.Huckebein@nospam.provider.at).

1.6 Rechtliche Massnahmen

Um Spam im weltweiten Internet zu bekämpfen, sind vor allem flächendeckende Massnahmen erforderlich. Die rechtlichen Lösungen gegen Spam zerfallen in zwei Kategorien:

1.6.1 Opt-In

Es ist illegal, Werbenachrichten per E-Mail ohne Zustimmung des Empfängers zu versenden. § 101 TKG ist eine Opt-In-Lösung.

- \+ die für die User befriedigendste Form;
- – Politisch nicht leicht verhandelbar. Opt-In-Lösungen haben vor allem den Nachteil, dass sie eine Werbemethode vollständig verbieten, was vom Standpunkt der wirtschaftlichen Freiheiten (Recht auf freien Erwerb, etc.) nicht leicht zu argumentieren ist. Dazu kommt das Problem der Ungleichbehandlung, wenn Spam in einem Land verboten ist und im anderen nicht;
- – erfordert gesunden Menschenverstand bei der Formulierung und Anwendung, um Härtefälle zu vermeiden.

1.6.2 Opt-Out

Es ist illegal, Werbenachrichten per E-Mail an Personen zu versenden, die erklärt haben, keine erhalten zu wollen.

- \+ Politisch leicht verhandelbar. Eine Position, wonach es zulässig sein soll, Werbenachrichten per E-Mail an Personen zu versenden, die sich ausdrücklich dagegen verwahrt haben, ist kaum vertretbar. Opt-Out erscheint daher für eine weltweite Regelung als die wohl geeignetere Form;
- – Kann den Eindruck erwecken, dass Spam zulässig sei.

Opt-Out Lösungen lassen sich mit Hilfe einer Robinson-Liste realisieren, das ist eine Liste (oder Datenbank) aller E-Mail-Adressen, an die kein Spam versendet werden darf[8]. Robinson-Listen können auch eingesetzt werden, um den Handel mit Adressdaten zu unterbinden, erfordern aber eine gewisse Organisation und Infrastruktur.

Ein anderer Zugang besteht darin, für Spams ein allgemeines Kennzeichen vorzuschreiben, das eine fehlerfreie Ausfilterung ermöglicht. Dies hat den Vorteil, dass keine besonderen Vorkehrungen erforderlich sind. Die User können sich mit Hilfe einfachster Spam-Filter schützen. Der Nachteil ist, dass die Kosten für den Transport bleiben und Adressen gesammelt und gehandelt werden können [9].

---

[8] Eine Robinson-Liste für normale Werbepost existiert bereits in § 268 Abs. 8 GewO 1994.

[9] In Art. 7 der Vorschläge für einen kohärenten Rechtsrahmen für den Elektronischen Geschäftsverkehr im Binnenmarkt (KOM(1998) 586 endg. und KOM(1999) 427 endg.) wurden beide Lösungsansätze für Opt-Out vertreten (http://europa.eu.int/comm/dg15/de/media/eleccomm/eleccomm.htm).

1.7 Die Lösung in Österreich

Mit BGBl. I Nr. 188/1999 wurde das Telekommunikationsgesetz, BGBl. I Nr. 100/1997 (TKG), geändert. Die Änderung bestand in der Einfügung eines neuen Satzes in § 101 TKG sowie eines neuen verwaltungsrechtlich strafbaren Tatbestandes in § 104 Abs. 3 TKG (als Z 23). Die geltende Fassung des § 101 TKG lautet daher wie folgt:

> § 101 Abs. 1 TKG: „Anrufe - einschließlich das Senden von Fernkopien - zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers sind unzulässig. Der Einwilligung des Teilnehmers steht die Einwilligung einer Person, die vom Teilnehmer zur Benützung seines Anschlusses ermächtigt wurde, gleich. Die erteilte Einwilligung kann jederzeit widerrufen werden; der Widerruf der Einwilligung hat auf ein Vertragsverhältnis mit dem Adressaten der Einwilligung keinen Einfluß. Die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken bedarf der vorherigen - jederzeit widerruflichen - Zustimmung des Empfängers."

Die geltende Fassung des § 104 Abs. 3 Z 23 TKG lautet wie folgt:

> „Eine Verwaltungsübertretung begeht und ist mit einer Geldstrafe bis zu 500 000 S zu bestrafen, wer <...>
> 23. entgegen § 101 unerbetene Anrufe oder die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken tätigt."

Die Änderung beruht auf einem Antrag des Justizausschusses, dem keine Erläuterungen beigefügt waren [10].

Da dem Antrag des Justizausschusses keine Erläuterungen angefügt waren, bleibt unklar, ab welcher Menge von versendeten E-Mails eine „Massensendung" vorliegt. Dies ist vor allem für den Tatbestand eines strafbaren Verhaltens wichtig. Es ist klar, dass bei einer Menge von mehreren Tausend Stück der Tatbestand der „Massensendung" gegeben ist, aber wo liegt die Untergrenze? Sind 20, 50 oder 100 - nachweisbare - E-Mails bereits eine strafbare „Massensendung"? Dieses Problem betrifft jedenfalls nicht Werbezusendungen, die immer verboten sind.

---

[10] http://www.parlinkom.gv.at/pd/pm/XX/I/texte/020/I02064_.html

Es können sich auch Probleme aus der Frage der impliziten Zustimmung bei einem Ersuchen um Hilfe ergeben. Wenn z.B. ein User in einer Newsgroup ein technisches Problem schildert und um Hilfe bittet, stellt sich die Frage, ob ein Unternehmer damit das Recht hätte, ihn per E-Mail seriös über ein Produkt zu informieren, das dieses Problem lösen kann.

Die Tat des § 104 Abs. 3 Z 23 TKG ist ein Ungehorsamsdelikt. Es ist kein Erfolg (z.B. Störung, Belästigung, Verbrauch von Ressourcen bzw. Anfall von Kosten) erforderlich, obwohl derartige Erfolge üblicherweise eintreten. Dies bedeutet auch, dass keine weitere Argumentation erforderlich ist, wenn das Opfer der Tat Schutzmaßnahmen ergriffen hat, die einen Erfolg vereiteln (z.B. einen Spam-Filter installiert).

Bei Ungehorsamsdelikten wird die Tat an dem Ort begangen, wo die Tathandlung gesetzt wird, d.h. von wo aus die Spams abgeschickt werden. Die Tat würde nur unter das österreichische Verwaltungsstrafrecht fallen, wenn die Spams aus Österreich abgesendet wurden[11].

[11] Das Wort „Zusendung" in § 101 TKG scheint zwar das Eintreffen der Nachricht vorauszusetzen, aber nach einer sehr informellen Auskunft der Fernmeldebehörde besteht die Tat im Absenden von Spam.