Ausspioniert und zugemüllt

Eingriffe in die Rechte von InternetnutzerInnen von Privaten

Tanja Nitschke / Andre Lammel

Schon fast selbstverständlich nutzen viele Menschen täglich verschiedene Services im World Wide Web zum Informationsaustausch und setzen dabei meist unbewußt voraus, dass die von ihnen verschickten Daten unterwegs vertraulich behandelt werden. Ebenso selbstverständlich scheint es zu sein, das sie nur erwünschte, unverfälschte Informationen erhalten bzw. ihnen keine Informationen vorenthalten werden. Angesichts der technischen Gegebenheiten und Möglichkeiten wird allerdings schnell klar, das es sich dabei um eine mehr als naive Vorstellung handelt. Vielfältige Eingriffe in die Rechte von NutzerInnen, von diesen häufig völlig unbemerkt, sind technisch problemlos möglich und gängige Praxis. Die Mitverfolgung und Aufzeichnung personenbezogener Daten ist im Internet - leider - üblich. Entsprechend der sprunghaft gestiegenen kommerziellen Nutzung des Internet bezieht sich Datenspionage überwiegend auf solche Daten, die zu Werbe- und Marktforschungszwecken verwertbar sind. Im harmlosesten Fall werden dabei lediglich Emailadressen zur Zusendung von Werbung gesammelt.Neben dem im Internet ebenso wie offline praktizierten Adressenhandel werden Emailadressen häufig über Mailinglisten gesammelt: Einfach an eine gut frequentierte Mailingliste schreiben und die Adressen aller Antwortenden speichern. Ebenso einfach und billig: Obligatorische oder häufige (z. B. info@..., kontakt@..., hostmaster@...) Emailadressen mit zufällig ausgewählten Domainnamen kombinieren, die in der öffentlich einsehbaren Whois-Datenbank der jeweiligen Domainregistratur, für .de-Domains also Denic, auf ihre Existenz überprüft werden können. Nach den so genannten rfc (request for comment, technische Regeln des Datentransfers im Internet, vergleichbar mit DIN-Normen[1]) sind für jede Domain die Emailadressen postmaster@... und abuse@... obligatorisch. Oft sind es Freemail-AnbieterInnen oder Internetportale, die NutzerInnendaten an andere weitergeben oder in Adressenverzeichnissen veröffentlichen. Wer sich z. B. beim Freemail-Anbieter Hotmail anmelden möchte, findet im Anmeldeformular standardmäßig die Zustimmung zur automatischen Veröffentlichung in einem Adressenverzeichnis vorausgewählt. Diese Daten werden auch an die Suchmaschine Infospace.com weitergegeben, mit deren Hilfe sich problemlos Tausende von Adressen sammeln lassen.[2]

Wirksamer Schutz gegen solche Praktiken ist nur durch Nichtinanspruchnahme der jeweiligen Angebote möglich. Verbunden ist damit in jedem Fall eine Einschränkung der eigenen Auswahl- und Bewegungsmöglichkeiten im Netz.

Gläserne NutzerInnen?!

Über die Sammlung von Adressen hinaus werden, mit oder ohne Zustimmung bzw. Wissen der NutzerInnen, in großem Umfang weitere Daten erhoben, gespeichert, ausgewertet und weitergegeben. Ziel ist es, umfassende und präzise Profile über Interessen, Kaufverhalten, Vorlieben der NutzerInnen zu erstellen, um mit maßgeschneiderten Werbemaßnahmen noch größeren Rücklauf erzielen zu können. Die technischen Möglichkeiten, personenbezogene Daten über NutzerInnen während des Besuchs verschiedener Services zu sammeln, sind unüberschaubar: Cookies, Webformulare, Hidden Fields in Webformularen, JavaScript, Java, Flash, Logging von IP-Adressen in Verbindung mit Cookies und Webformularen, Datenbanken, etc. Insbesondere die Folgen des Zusammenwirkens von Webformularen, in denen personenbezogene Daten angegeben wurden, Cookies, Logging von IP-Adressen und zentralen Datenbanken sind gravierend: Die Aktivitäten der NutzerInnen lassen sich so fast lückenlos verfolgen. Den Anfang stellt meist ein Webformular dar, in dem z. B. für die Anmeldung zu einem kostenlosen Service die Eingabe personenbezogener Daten erforderlich ist. Dies allein wäre aus datenschutzrechtlicher Sicht unproblematisch, solange die Angaben freiwillig erfolgen - d.h. insbesondere nicht der Eindruck erweckt wird, ohne die Angaben sei der Dienst nicht erhältlich - und nicht über deren Zweck getäuscht wird.

Spionierende Kekse

Nach erfolgreichem Versand dieser Daten bekommen die NutzerInnen meist so genannte Cookies an ihren Browser geschickt. Das sind kleine Datenpakete, die beliebige Daten enthalten können, z. B. persönliche Daten, Datenbankreferenzen, Daten über Browser, Betriebssystem, IP-Adresse, etc. Sie werden an den Server zurückgeschickt, der sie versandt hat, sobald Daten von ihm abgerufen werden. NutzerInnen wissen oft nicht, dass so über den Wert der Cookies die auf der Website vorher eingegebenen persönlichen Daten referenziert und dadurch gezielt Informationen über das Verhalten der NutzerInnen gesammelt werden können. Da sie die Datenerhebung regelmäßig nicht mitbekommen, verstößt diese Praxis gegen Datenschutzrecht.[3] Einige Werbefirmen wie z. B. Doubleclick, Akamai, Adtech, erheben auf diese Weise zentral NutzerInnendaten. Der Trick: Alle Webseiten der KundInnen solcher

Firmen liefern Cookies nicht mehr selbst an die Browser der NutzerInnen aus, sondern lassen dies von der jeweiligen Werbefirma erledigen. Daher bekommt diese die Cookies später wieder zurückgesandt, egal, für welche Webseite ein Cookie stellvertretend zugestellt wurde, da technisch gesehen ja der Server der Werbefirma Absender war. Die so erhobenen Daten werden durch die Werbefirmen ausgewertet und in Form von NutzerInnenprofilen allen KundInnen zur Verfügung gestellt.[4] Der einzig wirkungsvolle Schutz gegen solche Ausspähversuche ist das kategorische Ablehnen von Cookies durch entsprechende Konfiguration des Browsers bzw. das regelmäßige Löschen der Cookies. Allerdings lassen sich einige Webseiten gar nicht ansehen, ohne dass vorher Cookies akzeptiert wurden. Nach einem ähnlichen Muster arbeitet das Rabattsystem Payback. Die dahinter stehende Werbefirma Loyalty Partner erhebt unter dem Vorwand der Rabattgewährung umfassende Daten über das Konsumverhalten der an Payback teilnehmenden VerbraucherInnen (was wurde wann und bei wem gekauft und womit bezahlt?) und wertet diese zentral für ihre KundInnen aus - dabei handelt es sich um Firmen aus allen Bereichen des täglichen Lebens, sowohl im Internet als auch real. So können personalisierte KundInnenprofile zu Werbe- und Marktforschungszwecken erstellt werden.[5] Das Landgericht München erachtete in seinem Urteil vom 1. Februar 2001 entsprechende Klauseln in den Allgemeinen Geschäftsbedingungen von Payback, die die Einwilligung der KundInnen in die Verarbeitung und Nutzung ihrer personenbezogenen Daten enthielten, für unwirksam.[6] Begründet wurde dies mit Verstößen der Klauseln gegen § 4 Abs. 2 Bundesdatenschutzgesetz (BDSG), wonach KundInnen eindeutig über Umfang und Zweck der Speicherung sowie die Übermittlung ihrer persönlichen Daten informiert werden müssen, sowie gegen die Zweckbindung der Datenübermittlung gemäß § 28 BDSG.

Während sich mit großer Wahrscheinlichkeit voraussagen läßt, dass sich Werbepraktiken wie die beschriebenen auch weiterhin großer Beliebtheit erfreuen werden, läßt sich eine künftige Linie der Rechtsprechung, auch angesichts der aktuellen Reformüberlegungen zum BDSG, kaum prognostizieren. Es ist allerdings zu bezweifeln, dass allzu bald eine nennenswerte Anzahl von Urteilen zur Erstellung von NutzerInnenprofilen ergehen wird - schließlich findet die Erschleichung von Daten in aller Regeln von den Betroffenen völlig unbemerkt statt und die datensammelnden Firmen, wie die Beispiele von Payback, Doubleclick usw. zeigen, sind nicht immer einfach zu ermitteln. Dennoch stellt das Urteil ein wichtiges Signal zugunsten der informationellen Selbstbestimmung von InternetnutzerInnen dar.

Wollen Sie ganz schnell Geld verdienen?

Eine Möglichkeit der Verwendung von so erhobenen Daten ist Spam. Der Begriff Spam meint den unaufgeforderten Versand möglichst vieler Kopien der gleichen Email an möglichst viele EmpfängerInnen zugleich, um diese faktisch zur Kenntnisnahme des Inhalts zu zwingen. In aller Regel handelt es sich dabei um Werbeemails, am häufigsten mit den folgenden Inhalten: Software und Daten, die es ermöglichen sollen, noch mehr Spam zu produzieren; (Kinder-)Pornographie; dubiose Geldanlagen; Pharmaka, Kosmetika und Büroartikel zu zweifelhaften Konditionen; als Drohung formulierte Werbung für Software zum Ausspionieren anderer NetzbenutzerInnen; auch die allseits bekannten Kettenemails fallen unter Spam. Dass allein solche Inhalte eine Belästigung der EmpfängerInnen darstellen, ist offensichtlich - besonders massiv ist dies auf Mailinglisten oder im geschäftlichen Bereich, wo häufig hunderte solcher Emails täglich eingehen. Das infolgedessen oft erheblich gesteigerte Datenvolumen verursacht den so beglückten EmpfängerInnen höhere Kosten beim Abruf ihrer Emails, ganz zu schweigen vom Zeit- und Nervenaufwand für das Aussortieren des Spams. Was den EndnutzerInnen meist nicht bekannt ist, sind die negativen Folgen für die BetreiberInnen der zum Spammen mißbrauchten Mail Transfer Agents (MTAs). Auch diesen entstehen, meist ohne ihr Wissen, zusätzliche Kosten durch das erhöhte Datenvolumen. SpammerInnen nutzen dies gezielt aus, um so die Kosten für ihre Werbemaßnahmen auf andere abzuwälzen. Besonders schmerzlich für die BetreiberInnen ist die resultierende Listung in so genannten Blacklists, in denen öffentlich solche MTAs angeprangert werden. Abgesehen von dem Aufwand, der nötig ist, um wieder von einer solchen Liste gestrichen zu werden kann die Listung für die BetreiberInnen häufig auch Imageschädigung und Rechtsstreitigkeiten nach sich ziehen. Zum Schutz ihrer KundInnen vor Spam verweigern viele Provider die Annahme von Emails dort gelisteter MTAs. Das bedeutet, dass NutzerInnen selbst erwünschte Emails von Menschen, die einen Emailprovider mit gelistetem MTA benutzen, nicht empfangen können, und dass KundInnen eines solchen Providers keine Emails verschicken können. Durch Spam kann also auch der Emailverkehr unbeteiligter NutzerInnen erheblich behindert werden.Technisch gesehen lassen sich die Quellen für Spam in zwei Klassen unterteilen: Von den BetreiberInnen der jeweils genutzten MTAs gebilligter Mißbrauch und Mißbrauch ohne Wissen der BetreiberInnen. Bei der ersten Form billigen die jeweiligen BetreiberInnen den Versand von Spam über ihre MTAs - Mißbrauch meint insofern,

Glossar

Internet: weltweiter, dezentral organisierter Zusammenschluß einer nicht bekannten Anzahl von Rechnern und Netzen verschiedener Größenordnungen

www: Sammelbegriff für alle Internetdienste, z. B. HTTP (hypertext transfer protocol: angucken von Webseiten); POP3 (post office protocol version 3: Emailabruf); SMTP (simple mail transfer protocol: Emailversand); FTP (file transfer protocol: Dateitransfer)

IP-Adresse: technisch-numerische Adresse, unter der ein Rechner im Netzwerk erreichbar ist

Domain: literarisches Alias für eine IP-Adresse (z. B. 213.198.63.221 = www.amnesty.de);

Whois-Datenbank: Datenbank, die InhaberInnen, AnsprechpartnerInnen und Nameserver von Domains enthält

Mail Transfer Agent (MTA): Rechner, der zum Transfer von Emails dient; gemeinhin: Mailserver

Anmerkungen:

1 Vgl. www.rfc.net.

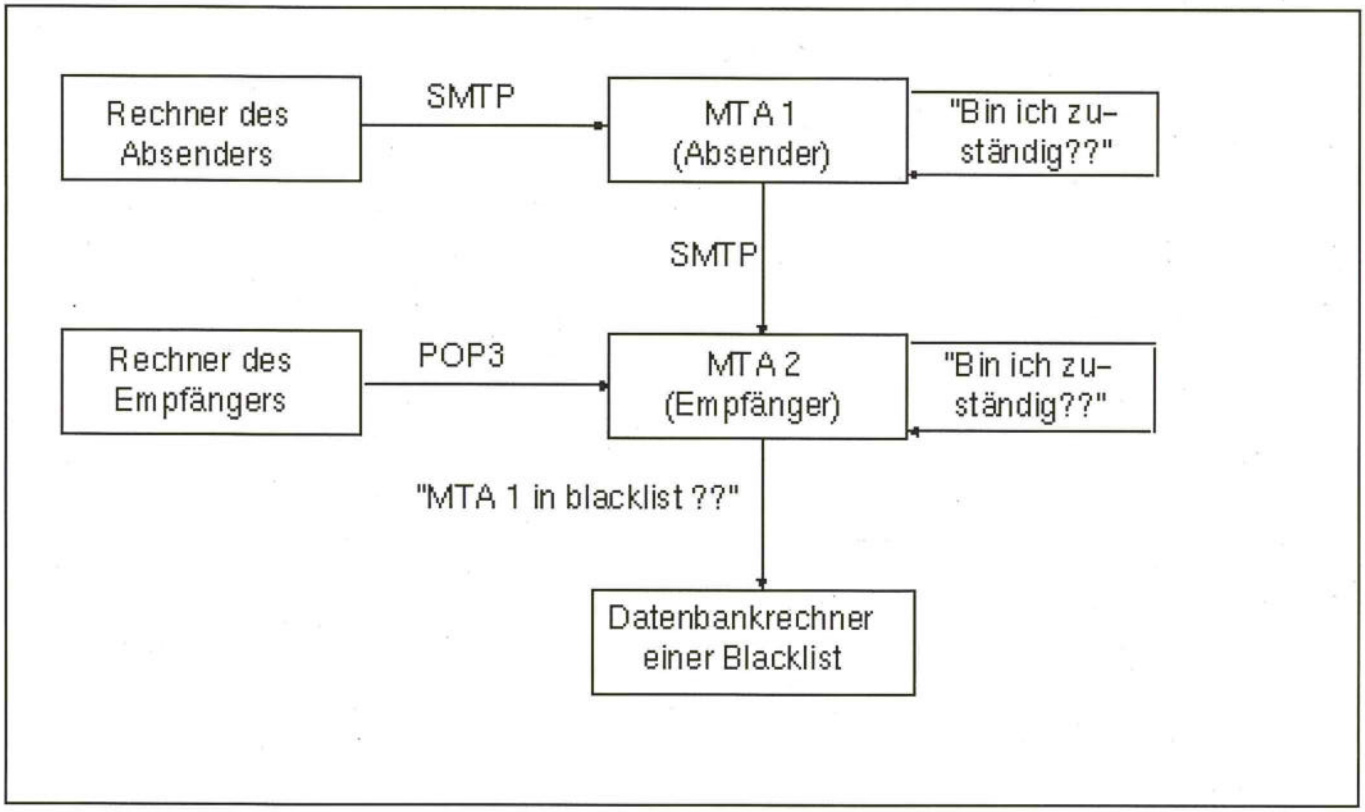
2 Vgl. http://www.heise.de/newsticker/data/fro-07.03.01-000/.

3 Näher Steckler, Grundz,ge des EDV-Rechts, S. 256 f, 281 ff.

4 Vgl. Eitel Dignatz, Linux-Magazin 1/2001, S.67.

5 Vgl. http://www.bigbrotherawards.de/2000/.com/index.html.

6 Aktenzeichen 12 O 13009/00; soweit bekannt noch nicht rechtskräftig.



dass Spamming nicht der eigentliche Verwendungszweck von MTAs ist. Bei in Unwissenheit der BetreiberInnen mißbrauchten MTAs kommen Konfigurationsfehler und Sicherheitslücken zum Tragen, die zur Folge haben, dass der mißbrauchte MTA nicht nur Emails für seinen definierten Zuständigkeitsbereich annimmt und weiterleitet, sondern auch Emails, die von nicht authorisierten AbsenderInnen für x-beliebige EmpfängerInnen bestimmt sind, für Spam-Opfer eben (vgl. Diagramm). Im einfachsten - und leider häufigsten - Fall brauchen SpammerInnen einen solchen "offenen" MTA lediglich als Mailserver für abgehende Emails in ihrer Emailsoftware eintragen. Oft kommen diese Konfigurationsfehler oder Sicherheitslücken, durch mangelhaftes Fachwissen der BetreiberInnen erzeugt, erst nach einem solchen Mißbrauch zu Tage. Eine Listung in den oben schon erwähnten Blacklists erfolgt prompt und zieht viele Unannehmlichkeiten nach sich. - Für SpammerInnen eine rücksichtslose Marketingstrategie auf Kosten der Unwissenheit anderer.

Schwarze Listen

In den vorherigen Abschnitten mag der Eindruck entstanden sein, dass sogenannte Blacklists die Freiheit der NutzerInnen einschränken; es handelt sich jedoch um einen freiwilligen und zuverlässig funktionierenden Mechanismus zur Selbstkontrolle auf technischer Ebene: Für alle NetzbenutzerInnen existieren frei zugänglich mehrere Anlaufstellen,[7] denen mutmaßlich zum Spammen mißbrauchte MTAs (genauer: deren IP-Adressen) gemeldet werden können. Nach der "Anmeldung" eines solchen MTAs wird dieser für den Zeitraum von ca. einer Woche intensiv auf Sicherheitslücken überprüft. Fällt der Test negativ aus, so wird der MTA nicht in die Liste aufgenommen, anderenfalls wird er je nach Klassifizierung der Sicherheitsmängel in die jeweilige Liste eingetragen. Die BetreuerInnen dieser Listen bieten allen BetreiberInnen von MTAs kostenlos die Möglichkeit, über eine automatisierte Abfrage vor der Annahme von Emails durch Ihren MTA den ausliefernden MTA auf Listung zu überprüfen und gegebenenfalls die Annahme der jeweiligen Mail zum Schutz potentieller EmpfängerInnen zu verweigern. Ebenso existiert eine sehr gut gepflegte Dokumentation zu Spam und wie ihm entgegnet werden kann und darüber hinaus verschiedene technische Hilfeangebote und Dokumentationen, die den BetreiberInnen mißbrauchter MTAs bei der Sicherung Ihrer Rechner und der Behebung von Konfigurationsfehlern Leitfaden sein sollen. Nach erfolgreicher Schließung aller Sicherheitslücken und erneuter Überprüfung erfolgt bei negativem Ergebnis eine Streichung von der Liste. Für Unverbesserliche, die auch auf massive und wiederholte Beschwerden von hunderten von NetzbenutzerInnen die Schließung ihrer Sicherheitslücken verweigern, existiert ein besondere Liste, die Realtime Blackhole List (RBL). MTAs, die auf dieser Liste stehen, werden von einigen Netzwerkadministratoren für Emailverkehr und die übrigen Dienste komplett gesperrt.[8] Genau betrachtet stellen Blacklists eine nicht zu unterschätzende Bereicherung für alle, die schon einmal Opfer von Spam wurden, dar - ein effektiver und gut funktionierender Selbstkontrollmechanismus der Internet-Community.

Spam verbieten?

Aus rechtlicher Sicht ist eine Bekämpfung von Spam prinzipiell auf zwei Ebenen denkbar: Durch gesetzliche Sanktionierung einerseits und durch die individuelle Geltendmachung von Abwehrrechten andererseits. Auf letzterer werden seit Ende der 90er Jahre durch die Rechtsprechung Unterlassungs- und Schadensersatzansprüche bei unaufgeforderten Werbeemails anerkannt. Im Falle von Spamming an private Emailadressen wird dies mit der Verletzung des allgemeinen Persönlichkeitsrechts der EmpfängerInnen begründet: Werbeemails griffen tiefer in den Tagesablauf ein, als dies etwa bei Werbung per Post der Fall sei - insbesondere, weil ohne Lektüre der Email nicht feststellbar ist, ob es sich um Werbung handelt und damit den EmpfängerInnen Zeit- und Kostenaufwand aufgezwungen wird. Verletzt wird damit auch das Grundrecht der negativen Informationsfreiheit (also der Freiheit, sich nicht zu informieren). Spamming an geschäftliche Emailadressen wird dagegen als Eingriff in das Recht der Betrieb-

sinhaberInnen am eingerichteten und ausgeübten Gewerbebetrieb angesehen. Unaufgeforderte Werbeemails stellen deshalb als unlauterer, belästigender KundInnenfang auch Wettbewerbsverstöße gemäß § 1 des Gesetzes gegen unlauteren Wettbewerb dar.[9] Voraussetzung für die Abwehransprüche ist nach wohl einhelliger Rechtsprechung, dass die Empfängerin nicht mit der Zusendung von Werbung einverstanden bzw. ihr Einverständnis nicht aufgrund einer bereits bestehenden Geschäftsverbindung zu vermuten war; das soll sogar dann gelten, wenn die Emailadresse der Empfängerin in einem allgemein zugänglichen Verzeichnis veröffentlicht wurde.[10] Die Anti-Spam-Rechtsprechung (wenngleich von den Gerichten nicht so bezeichnet) steht damit in der Tradition bisheriger höchstrichterlicher Rechtsprechung, die Werbemaßnahmen unter Inanspruchnahme fremder Telekommunikationseinrichtungen (z. B. BTX, Telefon, Fax) regelmäßig unter den Aspekten des Persönlichkeits- und Wettbewerbsschutzes als unzulässig angesehen hat.[11] Dass Spamming von der weit überwiegenden bislang ergangenen untergerichtlichen Rechtsprechung als unzulässig erachtet wird[12], klingt aus der Sicht potentieller und tatsächlicher Spam-Opfer zunächst durchaus erfreulich. Es drängt sich allerdings die Frage nach der Effektivität solcher gerichtlichen Abwehrmöglichkeiten auf: Der bezifferbare Vermögensschaden, der durch Spam eines Absenders entsteht, dürfte sich regelmäßig in Pfennigbeträgen bemessen lassen - dafür wird sich kaum ein Mensch die Kosten und Mühe machen, Klage zu erheben. Gegen SpammerInnen mittels Unterlassungsklage vorzugehen ist faktisch in vielen Fällen unmöglich, da sich die AbsenderInnenadressen von Emails kinderleicht ändern lassen und es sich dabei technisch gesehen nicht einmal um tatsächlich existente Adressen handeln muss. Gerade professionelle SpammerInnen bedienen sich in aller Regel solcher Verschleierungsmethoden - ein verklagbarer Absender mit ladungsfähiger Anschrift ist deshalb nur in den seltensten Fällen ermittelbar. Darüber hinaus dürfte sich die übliche Verfahrensdauer, selbst im einstweiligen Rechtsschutzverfahren, vor dem Hintergrund als abschreckend erweisen, dass in der Zwischenzeit ungehindert weiter Spam eingehen kann. Positive Wirkung kann der Anti-Spam-Rechtsprechung daher allenfalls auf symbolischer Ebene zugesprochen werden. Dies verdeutlicht um so mehr, wie wichtig die Existenz von Blacklists als Selbstkontrolle auf technischer Ebene ist. Den Weg der gesetzlichen Sanktionierung hat Österreich mit der im August 1999 in Kraft getretenen Neufassung des § 101 Telekommunikationsgesetz beschritten. Jeglicher Versand von Emails zu Werbezwecken - gleich, ob einzeln oder massenweise - ist danach ohne vorherige Zustimmung der Empfängerin mit einer Geldstrafe von bis zu 500.000 österreichischen Schilling (rund 70.000 DM) bedroht. In Verbindung mit einer großzügigen Auslegung der "Werbezwecke" durch österreichische Gerichte wurde so eine bislang weltweit einzigartige Verbotsnorm geschaffen, die Meinungsfreiheit und informationelle Selbstbestimmung von NutzerInnen erheblich einschränkt - nicht nur für VerbraucherInnen, die sich informieren möchten, sondern auch für Geschäftsleute, die KundInnenbeziehungen online so pflegen möchten, wie sie es offline unproblematisch tun dürfen. Kritisiert wird am Spamverbot auch dessen mangelnde Durchschlagskraft: Ein Großteil des Spam wird von AbsenderInnen außerhalb Österreichs verschickt, auf die folglich österreichisches Recht unanwendbar ist. Probleme bei der Durchsetzung des Spamverbots ergeben sich - ebenso wie bei der gerichtlichen Durchsetzung von Unterlassungsansprüchen - aus der leichten Fälschbarkeit von AbsenderInnenadressen. An seinem Ziel, die Privatsphäre von InternetnutzerInnen zu schützen, schießt das Spamverbot deshalb vorbei.[13]

Fazit

Abschließend bleibt festzustellen, dass Spam auf juristischem Wege - sei es gesetzlich oder gerichtlich - nur ungenügend bekämpft werden kann, insbesondere bei den häufigen grenzüberschreitenden Fällen. Ebensowenig können die von vielen ServiceanbieterInnen zur Verfügung gestellten Filtermechanismen auf der Basis von Absenderadressen oder Betreffzeilen Spam dauerhaft wirkungsvoll ausfiltern, da diese sich frei manipulieren lassen und teilweise stündlich geändert werden. Es zeigt sich dabei eine ähnliche Hilflosigkeit des Rechts wie sie im Bereich des Datenschutzes beklagt wird. In der juristischen Literatur wird demgegenüber unter Hinweis auf strafrechtlich relevanten Mißbrauch und die Möglichkeit der gezielten Ausnutzung der dezentralen Struktur des Internet eine Verrechtlichung gefordert.[14] Die Erfahrung zeigt jedoch, dass freiwillige Selbstkontrolle auf der Basis von Blacklists, die auf rein technischer Ebene operieren, den einzig wirkungsvollen Schutz vor Spam bieten kann.

Tanja Nitschke ist Rechtsreferendarin und
Andre Lammel studiert Informatik
beide leben in Nürnberg

Literatur

Steckler, Brunhilde, Grundzüge des EDV-Rechts, 1999.

Querica, Valerie, Internet in a Nutshell (Deutsche Ausgabe), 1998.

Schwartz, Alan/Garfinkel, Simson, Stopping Spam, 1998 (engl.).

Zarzer, Brigitte, Datensammler und Kundenjäger, http://www.heise.de/tp/deutsch/inhalte/te/8263/1.html.

Rützer, Florian, Nach den Cookies die WebBugs, http://www.heise.de/deutsch/inhalte/te/5482/1.html.

Anmerkungen:

8 Ausführlich dazu http://www.mailabuse.org/rbl/usage.html.

9 Vgl. Steckler, Grundzüge des EDV-Rechts, S. 249 ff.

10 Vgl. etwa LG Ellwangen, Urteil vom 27.08.1999 (2 KfH O5/99); LG Traunstein, Beschluß vom 18.12.1997 (2 HKO 3755/97); AG Brakel, Urteil vom 11.02.1998 (7 C 748/97); LG Berlin, Urteil vom 13.10.1998 (16 O 320/96).

11 Vgl. Entscheidungen des Bundesgerichtshofs in Zivilsachen, Band 103, S. 203 ff (BTX-Werbung).

12 Anders LG Kiel, Urteil vom 20.06.2000 (8 S 263/99) - jedoch wurde hier eine Einwilligung des Empfängers in die Zusendung angenommen.

13 Ausführlich Gerhard Laga, Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht 2000, S. 243 ff (http://www.rechtsprobleme.at/doks/00-obl-243-249.pdf).

14 Vgl. Haft/Eisele, JuS 2001, S. 112 ff (115) mit weiteren Nachweisen; LG Berlin, Urteil vom 13.10.1998 (16 O 320/96).

Links

http://www.euro.cauce.org (European Coalition against unsolicited commercial emails).

http://www.antispam.de.

http://www.politik-digital.de/spam/de.

http://www.bigbrotherawards.de.

http://www.fitug.de (Förderverein Informationstechnik und Gesellschaft).

http://www.heise.de/tp (Online-Magazin Telepolis).