I. Werbung im Internet

In allen Massenmedien ist Werbung eine bekannte Erscheinung. Für viele Menschen stellt sie oft eine Belästigung dar, doch bringt sie ebenso manche Vorteile mit sich und ist in einer Marktwirtschaft eine Notwendigkeit[1]. Wie normale Geschäfte nicht ohne Werbung in der einen oder anderen Form auskommen, und sei es "lediglich" Mundpropaganda, so benötigt auch E-Commerce sie; vielleicht sogar in viel stärkerem Maße, da z.B. Webseiten im WWW sehr gut versteckt sind und nicht ohne weiteres, z.B. über bekannte Domain Namen, Suchmaschineneinträge oder Links von externen Seiten, besucht werden. Da "das" Internet nicht existiert, sondern nur eine Ansammlung von Hardware-Netzwerken und Protokollen, nimmt auch die Werbung im Internet viele verschiedene Formen an.

Sie ist auch deshalb so bedeutend, da sie für viele ansonsten kostenlosen Angebote im Internet die einzige Einnahmequelle darstellt. Abgesehen von Online-Shops, welche Werbung zur Kundenakquirierung benötigen, existieren nur extrem wenige Angebote, für welche die "Kunden" bereit sind zu bezahlen. Beispiele sind: Google, StudiVZ, YouTube etc. Das ist mit ein Grund für die "Datensammelleidenschaft" dieser Sites: Personalisierte Werbung ist besser und daher teurer und erhöht die Einnahmen.

Im Allgemeinen ist Schleichwerbung, d.h. Werbung, die nicht als solche in Erscheinung tritt, verboten. Sie muss daher als solche zu erkennen sein, also entweder eindeutig sein wie z.B. Bannerwerbung, oder vom einem redaktionellen Teil klar getrennt werden[2] ("Trennungsgebot" – Verbot redaktioneller Werbung). Dies soll dazu dienen, die eindeutige gefärbte Stoßrichtung der Werbung von einem, an sich zumindest in Grundsätzen so erwarteten, unabhängigen und objektiven redaktionellen Beitrag zu unterscheiden.

I.1. Banner-Werbung

Weithin bekannt als Werbung auf Webseiten sind die bunten und oft auch animierten Banner in verschiedenen Größen, welche sich üblicherweise am oberen oder rechten Bildschirmrand befinden, mitunter aber auch mitten im Text (z.B. auf Nachrichten-Sites). In vielen Fällen handelt es sich um einfache Grafiken, welche dynamisch ausgewechselt werden, sodass bei wiederholtem Besuch der Seite jeweils andere Werbung eingeblendet wird. Heute findet jedoch auch Flash oder ähnlichen Techniken Einsatz. Vielfach wird das Bild von einem anderen Server geladen: Die Inhalts-Seite verweist auf den Server eines unabhängigen Werbeanbieters oder einer anderen Firma (Banner-Tausch; heutzutage selten). Dies ermöglicht eine Verfolgung des Benutzers über mehrere Web-Sites hinweg, was ein Datenschutzproblem darstellen kann (siehe unten).

[1] Daher auch das geflügelte Wort im Handel "Wer nicht wirbt, stirbt"!

[2] LG Berlin, 26.7.2005, 16 O 132/05 Bei Links vom redaktionellen Teil zum Werbungsteil muss der Charakter des Ziels vor dem Klicken erkennbar sein. Eine entgeltliche Anzeige präsentiert als redaktioneller Beitrag ist immer eine Verletzung des UWG: KG Berlin-Schöneberg 30.6.2006, 5 U 127/05. Für Österreich siehe § 26 MedienG: Die Kennzeichnung hat explizit als "Anzeige", "entgeltliche Einschaltung" oder "Werbung" zu erfolgen, sofern nicht Zweifel am Charakter ausgeschlossen sind, was aber streng zu beurteilen ist.

Unerwünscht sind Banner hauptsächlich deshalb, da sie sichtbaren Platz am Bildschirm belegen und den Benutzer oft durch ihre Gestaltung vom eigentlichen Inhalt ablenken bzw. es zumindest versuchen[3]. Weiters benötigen sie zum Download Bandbreite, um so mehr, je stärker animiert sie sind. Dieser Nachteil verschwindet jedoch praktisch bei Breitbandzugängen und hat daher heute nur mehr untergeordnete Bedeutung. Um den Benutzer zu einer genauen bzw. überhaupt einer Betrachtung bzw. einem Klick darauf zu verleiten, werden besondere Tricks angewendet, etwa dass die Seite erst dann weiter oder fertig geladen wird, wenn z.B. andere darauf enthaltene Bilder, die Werbung, vollständig geladen und angezeigt sind[4].

In den folgenden Abschnitten wird der Aufbau von Bannern erläutert und welche Elemente verwendet werden, die Click-through-rate[5] zu erhöhen. Nicht jeder dieser Versuche ist jedoch ohne weiteres rechtlich zulässig.

I.1.1. Typen von Bannern

Banner können, je nach ihrer Gestaltung, in mehrere Gruppen eingeteilt werden. Hier werden nur einige wichtige Grundformen dargestellt[6].

- Statische Banner: Hierbei handelt es sich um einfache statische Bilder, ähnlich einem Werbeplakat (siehe Abbildung 1). Der Vorteil dieser Banner ist die geringe Datengröße und daher geringe Bandbreite und schnelle Anzeige. Da sie keine Bewegung darstellen, wirken sie auch nicht so "aufregend" (und damit seriöser) als animierte Banner, was für den Kunden von Vorteil ist[7], doch den Nachteil besitzt, dass sie nicht unbedingt wahrgenommen werden. Die Kosten sind gering, da sie ohne größeren Aufwand hergestellt werden können. Bei diesem Typ ergeben sich aus der Art keine rechtlichen Probleme, höchstens durch einen externen Link. Wie bei jeder Werbung muss der dargestellte Inhalt allen Gesetzen entsprechen[8].

Abbildung 1: Statisches Banner

- Animierte Banner: Sie bestehen aus einer Aneinanderreihung von Einzelbildern (Abbildung 2), welche mit kurzem Abstand angezeigt werden. Interaktionen über das

[3] Dies ist mit ein Grund für den Erfolg von Google: Die dort eingeblendete Werbung wird weniger als Störung empfunden, da man ja genau nach solchen Produkten/Diensten gesucht hat. Sie stellen daher zumindest in manchen Fällen genau das gewünschte Ergebnis dar!

[4] Hierfür sind Modifikationen am Webserver nötig. Auch dies dürfte wegen dem mit der Breitbandnutzung verbundenen schnellen Aufbau eher abnehmen.

[5] Prozentueller Anteil der Benutzer, welchen das Banner gezeigt wurde und die darauf klickten. Heute erfolgt die Abrechnung meist aufgrund dieser Kennzahl, während zu Zeiten des Dot-Com Booms oft eine Abrechnung nach der Anzahl der Anzeigevorgänge erfolgte. Aufgrund schlechter Prüfbarkeit und des Interesses, Besucher auf die eigene Webseite zu bringen und nicht nur den eigenen Namen (sofern überhaupt enthalten) anzuzeigen, wird diese Abrechungsweise heute von Kunden eher gemieden. Umgekehrt ist sie jedoch für den Anbieter erwünscht, da er meist keinen Einfluss auf die Gestaltung des Banners hat und daher die Klickrate nicht selbst beeinflussen kann.

[6] Siehe http://www.online-vermarkterkreis.de/ für weitere Bannerformen, Techniken etc.

[7] Ähnlich zu HTML: Das Blink-Attribut gilt als verpönt, da es den Benutzer ablenkt, nervös macht und problemlos durch andere Hervorhebungen ersetzt werden kann (fett, kursiv, größere Schrift etc.).

[8] Etwa Besonderheiten bei vergleichender Werbung, verbotene Produkte, Verbot der Werbung für Versandhandel, ...

Anklicken hinaus sind nicht möglich. Die technische Realisierung erfolgt meist durch animierte GIFs, was auch gleich einen Nachteil mit sich bringt, da diese Bilder naturgemäß mehr Bandbreite benötigen. Der große Vorteil ist, dass dadurch die Werbefläche vervielfacht wird. Die Kosten sind naturgemäß höher als bei statischen Bannern, da mehr Bilder zu entwerfen sind. Eine Unterart davon sind narrative Banner, welche eine kurze Geschichte erzählen und eher einem Werbespot oder Kurzfilm ähneln. Dies hat zur Folge, dass auch die Herstellungskosten nochmals höher sind. Auch hier entstehen keine rechtlichen Bedenken aus der Art.

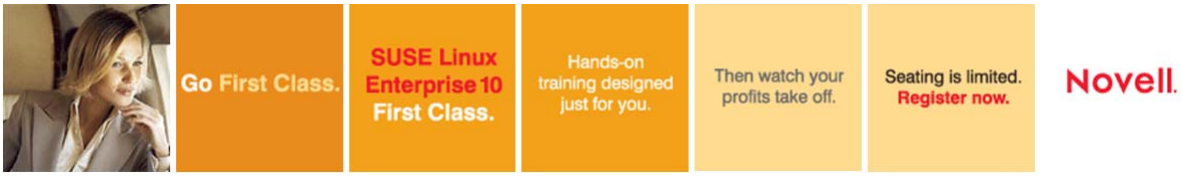

Abbildung 2: Animiertes Banner (Quadratisch; Bilder hier nebeneinander dargestellt)

- Aktive Banner: Eine Erweiterung der animierten Banner sind Flash- oder DHTML-Banner. Diese bestehen nicht mehr nur aus Animationen, sondern ermöglichen zusätzlich noch Interaktivität. Weiters besteht hier die Möglichkeit, die Banner z.B. beim Start oder beim Darüber-Bewegen des Mauszeiger zu vergrößern (Überlagerung eines Teils der Webseite), und sie später, oder auf Interaktion des Benutzers hin, wieder zu verkleinern. Rechtlich problematisch kann hier sein, dass mit der Überlagerung auch andere Inhalte, z.B. Werbung, überdeckt werden kann, was u.U. unlauterer Wettbewerb sein kann. Hier ist daher auf ein entsprechendes Layout bzw. Positionierung in der einbettenden Webseite zu achten. Weiters relevant ist, dass es sich hierbei um "Programme" handelt: Diese werden ev. auch Sicherheitsgründen blockiert, sodass die Werbung überhaupt nicht dargestellt wird.
- Applikatorische Banner: Derartige Banner können sowohl statisch als auch animiert sein, besitzen jedoch ein gemeinsames Element: Sie täuschen eine Anwendung vor. Typischerweise werden dazu Fensterrahmen, Menüs oder Dialogboxen dargestellt (siehe Abbildung 3 als Beispiel). Der "Vorteil" ist, dass vielen Benutzern nicht klar ist, dass es sich hier um Werbung handelt und sie darauf klicken, z.B. um Fehlermeldungen zu "bestätigen", und dadurch über einen Link zu einer anderen Webseite gelangen. Der Nachteil ist, dass diese unwissenden Benutzer sehr oft nicht am konkreten Angebot interessiert sind und die Zielseite möglichst schnell wieder verlassen[9]. Ein weiterer Nachteil ist, dass sie nur für einen eingeschränkten Benutzerkreis funktionieren. Wer keinen Windows-Rechner mit Standard-Farbeinstellungen verwendet, wird sich kaum täuschen lassen und die Elemente werden, da anders als gewohnt, eher kontraproduktiv wirken. Rechtlich sind derartige Banner zumindest bedenklich, da hierdurch eine Täuschung des Benutzers erfolgen kann und meist auch genau diese beabsichtigt sein wird. Die Konsequenz kann sowohl Schadenersatz bei konkreten finanziellen Einbußen sein, als auch ein Verfahren wegen unlauterem Wettbewerb auslösen[10].

[9] Daher insbesondere interessant für Web-Sites, die versuchen über Browser-Bugs Malware zu installieren!

[10] Etwa wenn durch den Klick ein Dialer installiert wird: Dies betrifft nicht nur die Person, welche den Dialer tatsächlich liefert, sondern ev. auch als Gehilfen den Betreiber der Web-Site, auf welcher dieses Banner eingeblendet war. Bei Werbung trifft den Anbieter wohl zumindest eine anfängliche einfache Prüfpflicht, sodass derartige Praktiken erkannt und verantwortet werden müssen, außer die Malware wurde erst später eingebaut; eine regelmäßige Prüfung ist sicher nicht erforderlich. Siehe dazu auch unter "Einbettungen". Verstärkt werden derartige Banne rauch verwendet, unwissenden Kunden wertlose oder gefährliche Programme zu verkaufen, z.B. Anti-Viren-Programme, welche keinerlei derartige Funktion besitzen, aber als "Ersatz" einen Trojaner installieren, sodass der Betreiber nicht nur das Geld sondern auch noch einen so genannten Bot erhält. Dies ist klar Betrug bzw. Datenbeschädigung, ….

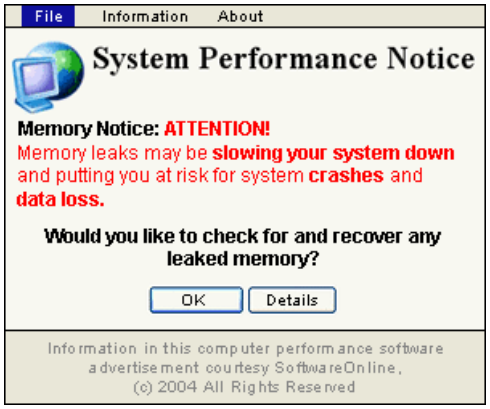

Abbildung 3: Applikatorisches Banner

- Site in the Site: Hierbei handelt es sich um eine voll funktionsfähige "Subseite" im Rahmen eines Bannerplatzes (Abbildung 4). Dies kann etwa eine Java-oder DHTML-Applikation, ein Active-X Control oder ein Flash-Element sein, sodass der Benutzer trotz Interaktion auf derselben Seite bleibt. Diese Art von Bannern ist äußerst selten. Der Nachteil ist, dass bei aktiven Komponenten erstens Sicherheitsprobleme auftreten können und zweitens für sinnvolle Anwendungen große Datenmengen (Code/Ergebnisse) übertragen werden müssen, was lange Ladezeiten bedeutet. Der große Vorteil wäre, dass der Benutzer auf der selben Seite verbleibt und dennoch die typischen Vorteile des WWW, die Interaktion, mit der Werbung ausführen kann. Fraglich ist jedoch, welche interessanten oder nützlichen Ergebnisse direkt im doch begrenzten Platz dargestellt werden können. Eine Verzweigung zu einer anderen Webseite wird daher meist das "Endziel" sein (im Beispiel von Abbildung 3 kann lokal die Kategorie gewählt und der Suchbegriff eingegeben werden, das Ergebnis erscheint jedoch in einem neuen Fenster). Rechtlich gesehen ist auf eine exakte Abgrenzung zu achten: Die Möglichkeit der Interaktion verstärkt noch den Eindruck, sich auf der "Haupt"-Seite zu befinden und nicht bei einem Dritten. Als Beispiel hierfür siehe den dunkelgrauen Text "Werbung" auf hellgrauem Grund unterhalb der roten Einrahmung in Abbildung 3.

Abbildung 4: Site-in-the-site Banner (Hervorhebung vom Autor)

I.1.2. Gestaltungselemente

Zur Erhöhung der Anklickrate werden verschiedene Elemente in Bannern verwendet:

- Produkt-/Firmenname: Hier besteht eine interessante Abweichung zu klassischer Werbung: Die Praxis hat gezeigt, dass es günstiger ist, den Firmennamen nicht anzuzeigen, da sich dadurch die Anklickrate erhöht, vermutlich durch Neugier. Andererseits bedeu-

tet die Anzeige des Firmen- oder Markennamens aber einen größeren Bekanntheitsgrad und wirkt selbst bei Personen, die nicht auf die Anzeige klicken. Es sollte nur der eigene Firmenname oder Namen tatsächlich vertriebener Produkte angeführt werden, da sonst die Gefahr von Irreführung oder Markenrechtsverletzungen besteht.

- Farben: Helle und leuchtende Farben führen zu den besten Erfolgen, da sie den Blick des Benutzer auf sich ziehen. Die Praxis zeigt, dass Blau, Grün und Gelb am geeignetsten sind, während Rot, Schwarz und Weiß geringere Wirkung besitzen. Auf einen ausreichenden Kontrast sollte geachtet werden. Ebenso sollte die Farbzusammenstellung nicht zu "stark" (besonders grelle Kontraste, sehr viele verschiedene Farben, ...) ausfallen, da sonst eher eine Abstoßungsreaktion erfolgt und der Benutzer wegschaut. In vielen Fällen ist die Auswahl jedoch von vornherein beschränkt, da auch im Internet die Corporate Identity gewahrt bleiben sollte und daher die Firmenfarben zu verwenden sind. Selbst besonders leuchtende Farben oder Blinken führen meiner Meinung nach nicht zu einer Qualifizierung als "übertriebenes Anlocken": Beispielsweise Neonschilder verwenden diese Elemente ebenso.
- Textgestaltung: Besonderen Erfolg haben folgende Elemente bei der Textgestaltung: Fragen ("Haben sie immer wieder Probleme mit Viren?"), Aufforderungen ("Besuchen Sie uns für besonders günstige Sonderangebote!") und Handlungserklärungen ("Klicken Sie hier!"). Ähnlich dem Verschweigen des Firmen- oder Produktnamens haben kryptische Aufforderungen die Wirkung, die Neugier des Benutzers zu wecken. Letzterer Punkt ist wieder mit Vorsicht einzusetzen: Man erhält zwar viele Besucher, doch ein großer Teil davon wird nicht wirklich am Produkt interessiert sein. Im Hinblick auf das UWG könnte in Extremfällen übertriebenes Anlocken vorkommen. Irreführung ist möglich wenn die Ankündigungen inkorrekt sind, also z.B. keine der angepriesenen Sonderangebote existieren.
- Mauszeiger: Auch die Integration eines, ev. sogar animierten, Mauszeigers in das Banner kann eine Steigerung der Anklickrate bewirken. Dies ist vermutlich darauf zurückzuführen, dass Benutzer konditioniert sind, zum Mauszeiger hinzuschauen, und dieser auch bei einem kurzen und oberflächlichen Blick automatisch erkannt wird. Dadurch wird die Aufmerksamkeit des Benutzers auf die Anzeige gelenkt. Hier ist, im Gegensatz zu applikatorischen Bannern, das Problem der verschiedenen Systeme weniger schlagend, da Mauszeiger überall sehr ähnlich aussehen und persönlich angepasste Zeiger eher selten sind. Verbreitet ist insbesondere die Verbindung von applikatorischen Bannern mit Mauszeigern und Aufforderungen: Neben dem Text "Click here" befindet sich ein Button und ein animierter Mauszeiger, der darauf klickt. Rechtlich gesehen ist die Irreführungsgefahr durch den Mauszeiger alleine, d.h. kein applikatorisches Banner, wohl zu gering, als dass sich daraus Probleme ergeben.

I.1.3. Sonstige Techniken

Es existieren noch weitere Möglichkeiten, die Aufmerksamkeit des Benutzers für die Werbung zu erregen. Auch wenn diese meist unbeliebt sind[11], handelt es sich nicht zwangsläufig um unzulässige Werbeformen:

- Pop-Ups: Für die Werbung wird ein eigenes Browserfenster geöffnet. Dies hat den Vorteil, dass die Werbung auch dann sichtbar bleibt, wenn der Benutzer die Seite verlässt.

[11] Am häufigsten Werden Banner eingesetzt (25% Anteil), am seltensten den Inhalt überlagernde Formen (1,6 % zusammen). Letztere besitzen jedoch die höchste Anklickrate (0,76-1,7 % vs. 0,14% für Banner). Platzer, Bernd: Werbeformate: Höchste Performance by den unbeliebten Formaten. http://www.be24.at/blog/entry/14771

Der große Nachteil ist jedoch, dass die Fenster am Arbeitsplatz des Benutzers immer mehr werden, weshalb diese Werbeart äußerst unbeliebt ist: Zusätzliche Fenster werden nach Möglichkeit sofort geschlossen, bevor sie überhaupt vollständig geladen sind. Falls diese Gestaltungsart dennoch eingesetzt wird, sollte darauf geachtet werden, dass das Fenster beim Verlassen der Site automatisch geschlossen wird (möglich über JavaScript). Die weitere Möglichkeit, beim Schließen des Fensters automatisch ein neues Fenster zu öffnen, sollte keinesfalls angewendet werden, da der Benutzer leicht in eine Endlosschleife (das Schließen der Werbung bewirkt das Öffnen des nächsten Werbefensters) gerät und insbesondere unerfahrene Benutzer manchmal keinen Ausweg mehr sehen, als den Computer abzuschalten. Allgemein sollte nur dann ein neues Fenster geöffnet werden, wenn der Benutzer dies ausdrücklich wünscht oder er beim Link darauf hingewiesen wurde, jedoch keinesfalls automatisch. Ein einzelnes Werbefenster beim Laden einer Seite zu öffnen wird noch rechtlich zulässig sein, sofern es leicht geschlossen werden kann, beim Verlassen der Seite darf jedoch keines mehr geöffnet werden. Hierbei handelt es sich um nicht angeforderte kommerzielle Kommunikation, welche unlauterer Wettbewerb ist[12]. Ob es sich um Pop-ups (Anzeige im Vordergrund) oder Pop-unders (Erscheinen im Hintergrund, daher anfangs nicht sichtbar) handelt, ist unerheblich. Rechtlich fragwürdig könnte auch hier die Überlagerung von fremder Werbung bzw. fremden Inhalten sein[13].

- Vergrößern des Fensters: Beim Öffnen einer Webseite mit Werbung das Fenster auf die maximale Größe zu vergrößern[14], ermöglicht eine gute und großflächige Darstellung der Werbung. Doch ebenso wie bei eigens geöffneten Fenstern handelt es sich hier um eine unbeliebte Verhaltensweise, da in die Bildschirmorganisation des Benutzers eingegriffen wird. Rechtlich kann es sich ebenfalls um unlauteren Wettbewerb handeln, da hierdurch dem Konsumenten die Werbung "aufgedrängt" wird und ev. auch konkurrierende Werbung Anderer, z.B. in dahinter/daneben liegenden Fenstern verdeckt wird.
- Überlagerung/Einblendung: Mittels Javascript, Flash etc. kann eine Werbung an einer bestimmten Stelle des Fensters als Überlagerung des eigentlichen Inhalts angezeigt werden. Dies kann statisch sein (→ Siehe Popups) oder dynamisch: Scrollt der Benutzer das Fenster, so wandert die Werbung auf der Seite mit, um an ihrer alten (absoluten) Position zu bleiben. Dies verlangsamt zwar das Scrollen und die Anzeige der Seite, doch bleibt die Werbung immer sichtbar und durch die Bewegung wird der Blick des Benutzers darauf gezogen. Der Nachteil ist, dass dies nur bei aktiviertem JavaScript/... funktioniert. Wiederum kann die Werbung andere Inhalte der Seite verdecken.
- Interstitial: Hierbei wird beim Klick auf einen Link nicht die gewünschte Seite angezeigt sondern eine Zwischenseite, welche meist ausschließlich ein (großes) Werbebanner enthält. Hiermit ist eine Art "Push-Werbung" möglich, da dem Benutzer jederzeit, zumindest bei jedem Site-internen Link-Klick, Werbung präsentiert werden kann. Entsprechend ist der Beliebtheitsgrad dieser Werbeform. Zum eigentlich gewünschten Inhalt kommt man über eine Zeitverzögerung, z.B. nach 10 Sekunden, oder durch Klicken auf

[12] Zumindest bei Endlosschleife: Jedes Schließen öffnet >=1 neue Fenster. LG Düsseldorf, 26.03.2003, 2 a O 186/02

[13] Siehe aber die Entscheidungen in Amerika, welche sich meist gegen eine Verletzung aussprechen. Rachman/Kibel, Online Advertising Challenges Tradition, New York Law Journal 10.10.2005. http://www.dglaw.com/images/OnlinAdvertising19D41C.pdf

[14] Aber nicht zu maximieren, sodass die Reduktion schwerer fällt. Im Extremfall wird die Fenstergröße so gewählt, dass der Fensterrand, und damit auch die Schaltflächen, außerhalb des sichtbaren Bereichs liegen (→ Tastaturkürzel nötig)!

einen weiteren Link[15]. Eine Variante davon sind Portalseiten: Homepages, welche außer Logo und Animationen/Flash etc. keinen Inhalt aufweisen. Erst durch Klick auf einen Link, die Grafik etc. gelangt man zur "eigentlichen" Homepage. Auch dies sollte nur in besonderen Ausnahmefällen eingesetzt werden. Beide Varianten sind im Allgemeinen rechtlich unproblematisch. Besonders häufige Verwendung könnten jedoch ev. als Aufdrängen von Werbung gewertet werden.

I.1.4. Datenschutz und Bannern von externen Sites

Werbebanner oder die oben erwähnten Elemente können entweder von der eigentlich besuchten Web-Site stammen oder von einem anderen Server[16]. In beiden Fällen können personenbezogene Daten über das Surf-Verhalten gesammelt werden, wobei der Personenbezug über Cookies oder URL-Codierung nach vorherigem Login erfolgt. Hierfür ist jedoch regelmäßig die Zustimmung des Benutzers erforderlich; siehe dazu den Abschnitt über den Datenschutz. Bei tatsächlich erfolgter Zustimmung stellt dies kein Problem dar.

Erfolgt jedoch die Bereitstellung der Inhalte von einem anderen Server aus, so werden zusätzlich Daten übermittelt bzw. erhoben: Cookies bzw. Browser-Informationen direkt vom Dritten beim Benutzer sowie die Tatsache des Besuchs einer bestimmten Webseite über den Referer-Header. Durch eine Codierung in den Link[17] können weitere beliebige andere Informationen über den Benutzer oder seine Handlungen vom Server der Webseite an den Server der Werbung übermittelt werden, ohne dass hierzu ein direkter Kontakt erforderlich ist (siehe Abbildung 5). Diese Art der Datenübermittlung ist datenschutzrechtlich äußerst bedenklich, da hierzu fast nie eine Zustimmung bestehen wird: Weder ausdrücklich[18] noch konkludent[19]. Eine generelle Zustimmung ("an Anbieter von Werbung") durch Teilnahme am Internet kann weder angenommen werden, noch wäre sie datenschutzrechtlich erlaubt.

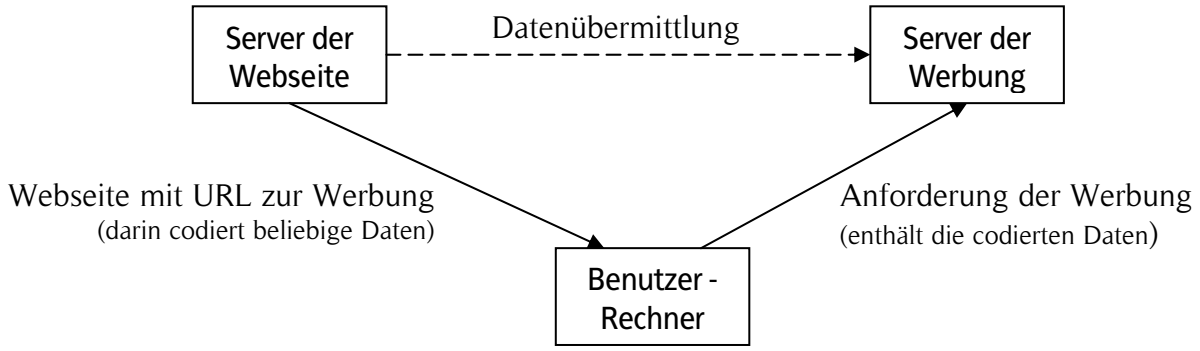

Abbildung 5: Datenweitergabe bei Bannern von Dritt-Servern

[15] Im Extremfall, z.B. bei werbefinanzierten Sites, finden auch Captchas Anwendung, um gleichzeitig automatisierten Besuch zu verhindern.

[16] Werbebanner sind dann die sichtbare Variante der unsichtbaren Web-Bugs: Sonntag, Webbugs - Wanzen im Internet. In: Schweighofer, Menzel, Kreuzbauer (Hrsg.): IT in Recht und Staat: Aktuelle Fragen der Rechtsinformatik. Wien: Verlag Österreich 2002, 355-362

[17] Beispiel: ''

[18] Die Zustimmung müsste schon in den Anmeldebedingungen für die Nutzung der Site eingebaut sein und den genauen Transfer erläutern. Bei Seiten ohne vorherige Anmeldung ist dies also unmöglich. Bedenken bestehen jedoch nur, soweit es sich um personenbezogene Daten handelt, was aber bei IP-Adressen durchaus zutreffen kann.

[19] Der bloße Besuch einer Webseite ist sicher keine Genehmigung zur Übermittlung von Daten an Dritte. Der (unbeabsichtigte, da ja vom Seitenbetreiber ausgewählt und vor dem Abruf der Webseite nicht erkennbare!) Abruf eines Werbebanners ist mangels konkreten Wissens auch keine Zustimmung. Der Besucher wird hier quasi als "Werkzeug" des Betreibers der Inhalts-Site tätig.

Datenschutzrechtlich unbedenklich ist die Einbindung lokaler Bilder und die bloße Einbettung entfernter Bilder ohne Zusatzinformationen, Cookies oder ähnlichem[20]. Die Codierung von Daten in den Link sowie die Sammlung von direkt personenbezogenen Daten auf dem Werbungs-Server, etwa über Cookies, bedarf jedoch einer zusätzlichen Zustimmung. Werden nur anonyme oder indirekt personenbezogene Daten erhoben, so ist dies zulässig.

Zu beachten ist hierbei immer, ob es sich tatsächlich um direkt personenbezogene Daten handelt (etwa weitergegebene Login-Daten, statische IP Adresse, Cookie mit Username) oder nicht (beispielsweise dynamische/nicht zuordenbare IP-Adresse, Cookie mit zufälliger Nummer). Bei der IP-Adresse ist noch zu berücksichtigen, dass oft nur ein Computer und nicht eine Person identifiziert wird.

I.2. E-Mail Werbung/Spam

Eine im Vergleich zu Bannern aktivere Werbeform ist das Versenden von Werbe–E-Mails. Dies hat den Vorteil, dass der Kunde direkt angesprochen wird und man nicht darauf warten muss, dass er eine bestimmte Web-Site besucht. Auch können so Personen erreicht werden, die von dem eigenen Web-Angebot noch nichts wissen, bzw. nur Sites besuchen, auf denen keine Werbung betrieben wird. Der Nachteil ist jedoch, dass diese Art von Werbung bei den Empfängern meist äußerst unerwünscht und großteils verboten ist.

I.2.1. Was ist Spam?

Mit "Spam" wird üblicherweise unerbetene kommerzielle Werbung per E-Mail bezeichnet, doch fällt in einem weiteren Betrachtungskreis jede unerwünschte und belästigende Nachricht, also auch in Newsgruppen, in Gästebüchern, auf Wikis etc. darunter. Spam wird meist an eine sehr große Empfängerzahl geschickt, bis zu mehreren Millionen, oder es handelt sich um eine Variante von Kettenbriefen, die jeder Empfänger an möglichst viele andere Personen weiterleiten soll.

Typische Beispiele für den, meist zusätzlich noch illegalen, z.B. verboten (Versandhandel mit Medikamenten) oder Betrug (Mitwirkung bei Geldwäsche; Waren werden nicht geliefert oder sind nichts wert; …), Inhalt sind:

- Gesundheits- / Potenzsteigerungs- und Diätangebot
- Investitionsgelegenheiten, insbesondere Penny-Stocks
- Phishing: Ausspähen von Bank-Passwörter (PIN) und TANs oder Kreditkartendaten
- Anwerben von Zwischenpersonen für illegale Geldtransfers
- Zusatzeinkommen ohne Aufwand und Kosten (Heimarbeitsangebote)
- Kredite / Kreditauskünfte / Verbesserung der Kreditwürdigkeit
- Versand von Massen-E-Mails / Anbieten von Anti-Spam-Programmen
- Kettenbriefe; meist mit Unheilsandrohung bei Nicht-Weiterleitung
- Gratisprodukte, z.B. Handys, Urlaub oder Software

[20] Die Referer-Daten geben zwar auch an, von welcher Webseite aus die Werbung aufgerufen wurde, doch fehlt jeder Bezug auf eine konkrete Person.

- Angebot gefälschter Produkte, z.B. Rolex Uhren
- Werbung für irgendwelche echten Produkte oder Dienstleistungen

Allgemein kann Spam meist daran erkannt werden, dass das Angebot "zu gut ist, um wahr zu sein". Eine Ausnahme hiervon ist die "normale" Werbung (letzter Punkt), die sowohl vom Inhalt her legal als auch korrekt ist und lediglich ohne Anforderung zugeschickt wird, und deshalb als Spam klassifiziert wird. Ansonsten werden meist Dinge angeboten oder versprochen, bei denen ein Mensch mit normalem Hausverstand kaum annehmen kann, dass es sich um ernst gemeinte bzw. legale Angebote handelt. Weiters ist ein Großteil des Spam sehr primitiv und einfach geschrieben: Einige wenige Zeilen oder eine einzige Graphik. Dies steht im Gegensatz zu ähnlichen Angeboten in konventioneller Werbung: Die dortigen "Anbieter" müssen höhere Investitionen tätigen und bereiten ihre Vorschläge daher viel besser und glaubwürdiger auf, sodass dort die Rate der Hereingefallenen viel höher ist. Bei Spam hingegen handelt es sich sehr oft um "Amateure".

Andererseits ist nicht zu übersehen, dass die organisierte Kriminalität in diesem Geschäftszweig bereits Fuß gefasst hat und auch äußerst professionelle Spams vorkommen, insbesondere im Bereich Phishing.

Will man daher E-Mail-Werbung seriös einsetzen, ist es erforderlich, echte Investitionen in die Erstellung des Inhalts zu tätigen, diesen korrekt zu formulieren, ausgiebig zu testen (Anti-Spam-Programme, verschiedenste Programme zum Lesen von E-Mail, HTML/Plaintext etc.) und sich an die gesetzlichen Einschränkungen hinsichtlich der Auswahl der Empfänger und die Sammlung der E-Mail Adressen zu halten.

Im Folgenden wird nur noch auf diese letzte Art eingegangen, da Werbung mit illegalem Inhalt, als versuchter Betrug, Vorbereitung zu solchen etc. ohnehin schon deswegen rechtswidrig und verboten ist[21].

I.2.2. Sammlung von E-Mail-Adressen

Adressen für E-Mail Werbung können u.a. folgendermaßen gesammelt werden:

- Webseiten: Auf vielen Webseiten findet sich ein Mail-Link, der zum Besitzer oder zu der Person führt, welche die Seiten wartet. Da Programme, welche ganze Web-Sites durchsuchen (automatische Link-Verfolgung) relativ einfach und weit verbreitet sind, können auf diese Weise sehr große Mengen an Webseiten rasch durchsucht werden. Für Firmen bedeutsam ist, dass ja im Impressum eine gültige und funktionsfähige E-Mail Adresse angegeben sein *muss*. Obwohl die Angabe der Adresse eine Zustimmung zur Kontaktaufnahme bedeutet, beinhaltet dies nicht Werbung, daher können nur Anfragen oder Mitteilungen legal dorthin gerichtet werden. Auch sonst ist die Angabe einer E-Mail Adresse auf einer Webseite keine Zustimmung zur Sammlung bzw. Verwendung für die Webungs-Zusendung. Dies ist daher eine illegale Sammlungsweise.
- Gästebücher/Blogs: Trägt man sich in Gästebücher ein oder postet in Blogs, so besteht oft die Möglichkeit oder sogar die Verpflichtung, die eigene E-Mail-Adresse einzugeben, wobei diese öffentlich oder geheim bleiben kann. Solche Online-Beiträge sind eine weitere Quelle ähnlich Newsgruppen, da der Inhalt regelmäßig aufgebaut ist und sie einfach identifiziert werden können, da meist bekannte Standard-Software verwen-

[21] Wenn auch nicht unbedingt strafbar, da u.U. nur eine noch straflose Vorbereitungshandlung.

det wird. Auch hier ist ein Beitrag zwar eine Erlaubnis zur Kontaktaufnahme bezüglich des Postings, z.B. für eine Diskussion, aber nicht zur Zusendung von Werbung. In der Praxis ist dies nur eine Unterart von Webseiten (vorheriger Punkt).

- Domain contact points: Die meisten Domains bzw. Mailserver besitzen allgemein übliche Adressen für festgelegte Zwecke[22]. Dies hat den Vorteil, dass man jederzeit Kontakt mit bestimmten Personen, z.B. dem Administrator, aufnehmen kann. Diese Adressen sind deshalb wertvoll, weil aus dem Namen auf bestimmte (berufliche) Interessen geschlossen werden kann und sie meist regelmäßig abgefragt werden. Hierzu gehören auch E-Mail-Adressen, die aus dem WHOIS-Register extrahiert werden[23]. Bei diesen kann von einer Zustimmung für entsprechende Kommunikation ausgegangen werden, z.B. bei "webadmin" über Probleme/Fehler auf Webseiten, nicht jedoch zu Werbung. Selbst Werbung für spezielle Tools für diese Person, z.B. E-Mail-Filterprogramme gesendet an "postmaster" ist vom Verbot umfasst und daher unzulässig.
- Guessing and Cleaning: Einfaches Raten und Ausprobieren kann zu E-Mail-Adressen führen, wobei allerdings zunächst sehr viele falsche enthalten sein werden. Grundlage dafür ist, dass E-Mail-Adressen oft nach einem bestimmten Schema aufgebaut sind, z.B. "Vorname.Nachame" oder "Nachname+erster Buchstabe des Vornamens" etc. Aus einer Mitarbeiterliste, aber auch aus allgemeinen Vor- und Nachnamenslisten, lässt sich dann eine Menge potentieller Adressen zusammenstellen, welche einfach ausprobiert werden. Da keinerlei Äußerung des Inhabers vorliegt, fehlt jede Einwilligung. Die bloße Teilnahme am E-Mail-Verkehr ist keine Zustimmung zum Werbungsempfang.
- Newsgruppen: Spammer durchsuchen regelmäßig Newsgruppen nach E-Mail Adressen. Diese werden einerseits aus dem Header (Absender) gewonnen, andererseits aus dem Mail-Inhalt selbst (Signature, sonst im Text). Das Posten in einer Newsgruppe stellt keine Zustimmung zum Empfang von Werbung dar.
- Mailinglisten: Bei mancher Software kann jeder die Liste aller registrierten Adressen einer Mailingliste abfragen. Dies sind besonders "geeignete" Adressen, da man aus der Liste auf die Interessen der Personen schließen kann und die Adressen großteils gültig sind; ungültige werden normalerweise nach "Bounces" entfernt. Für eine allgemeine Sammlung von Adressen ist dieses Vorgehen unzulässig. Der Versand von Werbung über die Liste durch den Betreiber ist jedoch erlaubt, wenn darauf schon bei der Anmeldung explizit hingewiesen wurde[24]. Diesfalls besteht eine Einwilligung analog einem Newsletter. Online-Archive von Mailinglisten entsprechen Newsgruppen bzw. Webseiten.
- Kundenverzeichnisse von ISPs: Internet-Anbieter stellten früher oft eine Seite mit den E-Mail- und Web-Adressen aller ihrer Kunden ins WWW. Da dies naturgemäß eine hervorragende Quelle war, alle Adressen waren garantiert aktiv, wurden diese von Spammern gerne verwendet. Die Anbieter gingen daher ebenso wie aus Datenschutzgründen dazu über, dies zu unterlassen oder höchstens Einzelabfragen anzubieten (eine Suche nach dem Namen ergibt die E-Mail-Adresse).

[22] Beispiele: admin@..., webadmin@..., abuse@..., postmaster@..., root@..., administrator@..., support@... etc.

[23] In deren Nutzungsbedingungen ist meist explizit geregelt, wofür diese Adressen verwendet werden dürfen, beispielsweise Meldungen über technische Probleme, aber niemals für Werbung.

[24] Jedoch nicht, wenn es sich um unbeteiligte Dritte handelt, die Werbung "einschleusen".

- Sonstige Quellen: Finger-Dämon[25], Webbrowser[26], IRC/Chat[27], lokale Benutzer[28]. Diesen ist gemeinsam, dass eine Zustimmung zum Empfang von Werbung alleine durch die Eintragung der E-Mail-Adresse nicht in Frage kommt.
- Verzeichnisse: Branchen- und Kundenverzeichnisse, aber auch die gelben Seiten des Telefonbuches, können zur Ermittlung von E-Mail Adressen verwendet werden. Im Gegensatz zu den anderen Sammlungsmethoden handelt es sich hierbei um freiwillige Werbung des Inhabers des E-Mail-Anschlusses, mit der zur Kontaktaufnahme eingeladen werden soll[29]. Listen mit verpflichtender Eintragung fallen jedoch nicht hierunter. Hier könnte ev. davon ausgegangen werden, dass für jeweils spezifisch erstellte und relevante Einzelangebote eine Zustimmung zum Empfang von Werbung besteht ("Vermutete Zustimmung"). Nach der neuen Rechtslage ist jedoch auch diese Argumentation nicht mehr möglich und jede derartige Verwendung verboten.
- Adressenkauf: Wie normale Adressen können auch E-Mail-Adressen gekauft werden. Ironischerweise werden solche Listen in Form von CD-ROMs, dem Angebot, selbst Massen-E-Mails zu versenden oder Programmen dazu, selbst oft über Spam vertrieben. Prinzipiell handelt es sich beim Kauf um eine unter bestimmten Voraussetzungen legale Möglichkeit, E-Mail Adressen für die Zusendung von Werbung zu erlangen.

Insgesamt ist daher festzustellen, dass die Sammlung von Adressen zum Versenden von E-Mail-Werbung in fast allen Fällen, ausgenommen dem letzten in bestimmten besonderen Varianten, illegal ist, da keine Zustimmung zur Verwendung dieser eindeutig personenbezogenen Daten für diesen Zweck vorliegt. Schon die Erhebung selbst ist datenschutzrechtlich verboten, sodass bereits die bloße Sammlung als Vorbereitung für eine spätere Zusendung von Werbung verboten ist. Für einen rechtlich einwandfreien Erwerb von Adressen bleiben daher übrig:

- Kauf von E-Mail Adressen, z.B. von Adressverlagen (siehe I.2.3): E-Mail Adressen sind nicht im Standard-Datensatz von Adressverlagen enthalten, daher ist immer eine ausdrückliche Zustimmung des Betroffenen zur Verwendung für Marketingzwecke und zusätzlich zur Weitergabe an Dritte erforderlich (Doppelte Zustimmung[30]!). Weiters ist

---

[25] Mittels des "finger" Befehls kann auf Unix-Rechnern festgestellt werden, welche Benutzer eingeloggt sind und ev. noch Zusatzinformationen über diese erlangt werden.

[26] Drei Möglichkeiten, an die E-Mail-Adresse eines Webseiten-Besuchers zu gelangen: Im Header der Anforderungen (Lynx, sonst eher selten), JavaScipts auf der Webseite erlauben das Auslesen (heute meist nicht mehr), Einbetten eines Bildes über eine anonyme FTP-Verbindung (der Browser versucht das Bild zu laden und gibt als Passwort die E-Mail Adresse des Benutzers an; heute meist jedoch eine neutrale und nicht die richtige Adresse).

[27] Manche IRC-Clients geben die E-Mail-Adresse des Benutzers auf Anfrage weiter. Auch aus Logs werden im Gespräch erwähnte Adressen herausgefiltert (siehe dazu Mailinglisten bzw. deren Archive).

[28] Bei Zugang zum Rechner kann oft eine Liste lokaler Benutzer abgefragt werden, etwa die Passwortliste (/etc/passwd), welche Auskunft über die existierenden Benutzernamen gibt.

[29] Typischerweise jedoch gegenüber Kunden, um diesen Waren oder Dienstleistungen zu verkaufen. Potentielle Lieferanten sind normalerweise nicht von der Intention umfasst.

[30] Die beliebte Praxis der Sammlung von Daten und Einwilligungserklärungen über Gewinnspiele ist jedoch nicht so einfach: "Bitte informieren Sie mich auch über weitere Angebote und Gewinnmöglichkeiten per Telefon (gegebenenfalls streichen)" reicht jedenfalls nicht als Zustimmung für Adresshandel und als generelle Zustimmung für Telefonwerbung. LG Düsseldorf 7.3.2007, 38 O 145/06 (Siehe weitere Urteile bezüglich Zustimmung in AGBs unter FN **Fehler! Textmarke nicht definiert.**). Dass der Satz aber nicht einmal als Willenserklärung anzusehen sei, da Verbraucher bei der Teilnahme an einem Gewinnspiel kein Erklärungsbewusstsein für Erklärungen zu einem anderen Sachverhalt besäßen, geht wohl zu weit: Inzwischen sollte dies jeder wissen und es ist klar, dass ein Gewinnspiel selten aus reiner Freigiebigkeit veranstaltet wird!

hierbei auf die Widerspruchsmöglichkeit explizit und direkt bei der Zustimmung hinzuweisen[31].

- Selbst von Kunden oder Interessenten erhoben: Diese können im Rahmen des Zwecks, der bei der Zustimmung angegeben wurde, beliebig verwendet werden. Auch ohne Zustimmung ist in einem sehr engen Bereich die Zusendung erlaubt (siehe unten).

I.2.3. Direktwerbung

Die Tätigkeit von Adressverlagen und Direktwerbeunternehmen ist nicht im DSG, obwohl in der DS-RL enthalten, sondern in § 151 GewO geregelt. In dieser Vorschrift wird keine Zulässigkeit der Zusendung von Werbung an sich geregelt, sondern nur die Voraussetzungen festgelegt, wie man an entsprechende Daten (=Adressen; E-Mail ist im Standard-Datensatz nicht enthalten) gelangen kann, sowie was mit diesen weiter erfolgen darf. Adressverlage und Direktwerbeunternehmen dürfen demnach Daten unabhängig von konkreten Aktionen aus öffentlich zugänglichen Quellen, aus eigenen Erkundungen sowie aus Kunden- und Interessentendateien anderer Adressverlage und Direktwerbeunternehmen[32] erheben und analysieren. Für die Ermittlung besteht eine Zweckbindung: Sie darf nur für die Vorbereitung und Durchführung von Marketingaktionen Dritter einschließlich der Gestaltung und des Versands für Werbemittel sowie Listbroking, dem Handel mit Adressen, erfolgen. Hierbei ist die Verhältnismäßigkeit zwischen dem wirtschaftlichen Interesse und dem Geheimhaltungsbedürfnis der Betroffenen zu beachten.

Betroffene haben das Recht, ihre Daten kostenlos auf Verlangen binnen acht Wochen löschen zu lassen[33]. Im Gegensatz zu normalen Daten besteht hier keine derartig enge Zweckbindung. Daten dürfen grundsätzlich an andere Betreiber dieses Gewerbes übermittelt werden, außer der Betroffene hat dies ausdrücklich untersagt. Werden die Daten schriftlich erhoben, so ist auf diese Möglichkeit ausdrücklich und schriftlich hinzuweisen[34]. Demgegenüber besteht allerdings eine Begrenzung der Daten über Betroffene, die zulässig übermittelt werden dürfen. Diese steht im Gegensatz zur eigenen Verwendung durch Unternehmen: Wurden Daten vom Betroffenen erhoben, so dürfen diese komplett für eigene Werbung verwendet werden. Sollen mehr Daten übermittelt werden, ist auf die Regelungen des DSG zurückzugreifen, d.h. meist eine Einwilligung erforderlich. Nach der GewO hingegen dürfen nur übermittelt werden:

- Name, Titel, Akademische Grade
- Geschlecht
- Anschrift
- Geburtsdatum
- Berufs-, Branchen- und Geschäftsbezeichnung
- Zugehörigkeit des Betroffenen zu der Kunden- oder Interessentendatei

---

[31] OGH 20.3.2007, 4 Ob 221/06p

[32] Was nach dem DSG eine Übermittlung wäre und daher meist besonderer Zustimmung bedürfte. Eine solche wäre schwer möglich, da alle Empfänger schon im Vorhinein bezeichnet werden müssten. Hier ist eine Einwilligung jedoch nicht mehr erforderlich.

[33] Solange der Betroffene nicht auf eine physische Löschung besteht, ist eine Sperre (bzw. Sperrmarkierung) ausreichend. Eine echte Löschung würde nämlich bei einer Übermittlung aus einer anderen Quelle wieder zur Zusendung von Werbung führen. Die bloße Sperre hingegen ermöglicht einen Abgleich und die Verhinderung eines Neu-Imports.

[34] Diese Untersagung hat auf ein Vertragsverhältnis mit dem Inhaber der Kunden-/Interessentendatei keinen Einfluss.

Der letzte Punkt ist bedeutsam, da er äußerst vielgestaltig sein kann: Dies könnte z.B. die "Datei der Bezieher von AIDS-Medikamenten" sein, wobei es sich folglich eindeutig um sensible Daten handeln würde.

Insbesondere *nicht* enthalten sind aber Telefonnummer und E-Mail Adresse, sodass eine Berufung auf diese Erlaubnis[35] bei Telefon-/Faxwerbung oder der Zusendung von E-Mails von vornherein ausgeschlossen ist, auch bloß als Quelle für die verwendeten Adressen.

Bei einer datenschutzrechtlichen Übermittlung ist eine schriftliche und unbedenkliche Erklärung abzugeben, dass die Betroffenen auf die Möglichkeit des Widerspruchs der Zweckänderungen bzw. Transfers an Dritte in geeigneter Weise hingewiesen wurden und kein derartiger Widerspruch vorliegt.

Für sensible Daten, siehe etwa das Beispiel oben, besteht ein weitergehender Ermittlungs- und Verarbeitungsschutz. Für diese ist eine ausdrückliche Zustimmung des Betroffenen entsprechend dem DSG notwendig, bzw. bei Übernahme aus einer anderen Datei eine unbedenkliche schriftlicher Erklärung deren Besitzer, dass eine solche ausdrückliche Einwilligung[36] eingeholt wurde. Gleiches gilt für strafrechtsbezogene Daten.

Vom Fachverband Werbung und Marktkommunikation der Bundessparte "Gewerbe, Handwerk, Dienstleistung" der Wirtschaftskammer Österreich ist eine "Robinsonliste" zu führen. An diese Personen darf keine adressierte Werbung zugestellt bzw. mit deren Daten Handel betrieben werden. Diese Liste ist mindestens monatlich zu aktualisieren und bei Aussendungen zu berücksichtigen.

Gegenüber der früheren Regelung dürfen nun auch durch Analyseverfahren gewonnene[37], d.h. nicht bei den Betroffenen erhobene, sondern berechnete, Daten verwendet und weitergegeben[38] werden. Hierbei handelt es sich z.B. um Vermutungen über das Einkommen, welches aus der Adresse (z.B. noble Wohngegend), dem Geburtsdatum, akademischen Titeln oder anderen Daten abgeleitet wird. Diese Informationen dürfen jedoch *nur* für Marketingzwecke verwendet werden, also nicht etwa für Bonitätsprüfungen.

---

[35] Das Erfordernis der Spezial-Einwilligung ist bei Werbeanrufen sehr streng: Eine allgemeine Versicherung des Verkäufers (Adressmaklers) reicht nicht, sondern es müsste für jeden einzelnen Angerufenen geprüft werden, ob tatsächlich eine Einwilligung vorliegt, da für eine Unterlassungsklage kein Verschulden erforderlich ist (für ev. Schadenersatz bzw. Bestrafung jedoch schon!). Wie dies erfolgen sollte ist schwierig zu ersehen; es müssten wohl Nachweise über die Zustimmung mitgeliefert werden. Siehe OGH 29.11.2005, 4 Ob 192/05x mit Anmerkungen von Tonninger. ecolex 2006, 216 Laut dem LG Koblenz 1.4.2008, 1 O 273/07 reicht vor Gericht das Anführen von "Zustimmungserklärung über Webseite und anschließender Kauf dieser Daten" nicht aus. Ein konkreter Geschehensablauf und der Einwilligungstext wären zumindest erforderlich, wobei die Beweislast beim Werbende liegt. Siehe auch VwGH 25.2.2004, 2003/03/0284 mit Anmerkung, MR 2004, 218, wonach die Zustimmung für SMS-Werbung zumindest eine Prüfung erfordert, ob diese Zustimmung auch von der Nummer stammt, an welche die Werbung versendet werden soll. Ähnlich LG Traunstein 20.5.2008, 7 O 318/08: Werden Daten für Telefonwerbung gekauft, hat sich der Käufer (selbst bei ausdrücklicher Zusicherung!) zu vergewissern, zu welchem Zweck die Daten erhoben wurden und wozu Betroffene zugestimmt haben (z.B. über den Umfragebogen; Zustimmung wurde im Rahmen einer Umfrage eingeholt), insb. da die Daten aus dem Ausland gekauft wurden (aber innerhalb der EU, also sollte dies wohl eher keinen besonderen Unterschied darstellen!).

[36] Diese Einwilligung ist von der Zustimmung nach dem Datenschutzgesetz zu unterscheiden: Sie kann ganz allgemein erfolgen und ist daher an geringere Informationserfordernisse gebunden. Bei Adressverlagen ist es beispielsweise schwer möglich, alle zukünftigen Kunden genau aufzuführen.

[37] "Berühmtestes" Beispiel hierzu ist die Herold Marketing CD private. Siehe dazu auch die Presseaussendung der Datenschutzkommission vom 4.12.2003. http://www.dsk.gv.at/presse_herold1.htm

[38] Dies bezieht sich nicht auf von Dritten erhobene Daten, sondern nur auf für Marketingzwecke erhobenen und mit Marketinganalyseverfahren behandelte Daten. Etwas unklar zur wörtlich wohl recht deutlichen Regelung Mayer-Schönberger, Warum Ermitteln nicht Erheben ist: Datenschutz und Direktmarketing. ecolex 2004, 417. Klar hingegen Rosenmayer-Klemenz, Neue Rechtsgrundlagen für Adressverlage und Direktmarketingunternehmen. RdW 2003/150

I.2.4. Auswirkungen von Spam

Die Auswirkungen können in drei Gruppen eingeteilt werden: Beim Sender, beim Empfänger und für die Allgemeinheit.

I.2.4.1. Beim Sender (Werber)

Durch den Einsatz von Spam kann es zu genau dem Gegenteil des Gewünschten kommen: Anstatt die eigenen Produkte zu forcieren und Bekanntheit und Ansehen zu erreichen, wird man berüchtigt und geächtet: Ein schwerer Image-Verlust kann eintreten. Es können sich auch technische Probleme ergeben: Manche Empfänger reagieren mit Beschwerden oder sehr großen Antwort-E-Mails, sodass der eigene Mailrechner abstürzen kann[39] bzw. Mitarbeiter mit der Beantwortung beschäftigt sind. Resultat können einerseits Datenverluste sein, andererseits auch entgangene Geschäfte. Die finanziellen Kosten sind meistens gering, insbesondere für das Versenden selbst, was ja der Hauptgrund für die große Verbreitung ist. In Europa kann es demgegenüber auch zu rechtlichen Gegenmaßnahmen kommen (Verwaltungsstrafe bzw. UWG-Verfahren durch Konkurrenten; Schadenersatz durch Betroffene nur höchst selten mangels Bezifferbarkeit des Schadens), was sehr teuer enden kann, sofern nicht alle Vorschriften eingehalten wurden[40]. International, d.h. der Sender verschickt ins (Außer-EU-)Ausland E-Mails, besteht jedoch keine große Gefahr von juristischen Konsequenzen. Dem gegenüber steht, dass der kommerzielle Erfolg von Spam sich dann auch in einem geringeren Bereich abspielen dürfte[41]: Nur ein winziger Bruchteil wird das beworbene Produkt kaufen. Diese minimale Erfolgsrate reicht aber bereits aufgrund der immens hohen Anzahl an versendeten E-Mails oft für einen wirtschaftlichen Erfolg aus: 0,1 Promille von 1.000.000 zugestellten E-Mails, d.h. ca. drei bis zehn Millionen verschickten, sind immer noch 100 Kunden[42], welche zu verschwindend geringen Kosten erreicht wurden!

I.2.4.2. Beim Empfänger (Beworbenen)

Hier ergeben sich zwei hauptsächliche Auswirkungen, welche beide negativ sind: Erstens wird der Benutzer oft durch den Inhalt der E-Mails belästigt (unerwünscht, unpassend, beleidigend, obszön, aggressiv, ...) und zweitens trägt er selbst nicht unerhebliche Kosten, insbesondere bei häufigerem Auftreten: bis zu 100 Spam-Mails/Tag sind durchaus üblich. Die Kosten setzen sich aus Übertragungskosten, denn Spam-Mails sind für E-Mails vielfach lang oder besitzen oft Bild-Attachments, und dem Zeitaufwand für die Identifizierung und Löschung der E-Mails zusammen. Werden automatische Filter zur Bekämpfung der Mail-Flut eingesetzt, so besteht zusätzlich noch die Gefahr, dass wichtige E-Mails gelöscht werden, da sie zufällig falsch erkannt werden. Darüber hinaus wird natürlich Bandbreite und Server-Rechenleistung belegt, welche anderweitig verwendet werden könnte.

Ein Vorteil bei E-Mails ist, dass die Störung, d.h. das Aussortieren, zu einem beliebigen Zeitpunkt erfolgen kann, ähnlich wie bei Papier-Werbung. Hierauf beruht insbesondere

---

[39] Dies ist eine selbst illegale Vergeltungsmaßnahme.

[40] In der Praxis wird dies jedoch miteinkalkuliert: Selbst dann kann sich eine Aktion noch rechnen.

[41] Daher auch die oftmalige Koppelung mit Betrug, um einen "richtigen" Gewinn zu machen!

[42] Beim Versenden von Werbung auf Papier würde dies z.B. nicht ausreichen: Billigster Tarif der Post: € 0,24/Brief (Info.Mail bis 20 g im Inland). Bei einer Million verschickter Briefe, d.h. nur an gültige Postadressen, bedeutet dies Kosten von € 240.000. Bei der gleichen Antwortrate müsste mit jedem Kunden ein Mindestgewinn von € 2.400 erzielt werden, um bloß die Portokosten zu decken!

auch die unterschiedliche Behandlung zu den generell verbotenen Werbetelefonaten. Bei letzteren bestimmt der Werbende den Zeitpunkt und der Beworbene kann nur im Vorhinein, also in Unkenntnis des Grundes des Anrufes, diesen durch Nicht-Abheben ablehnen. Ansonsten muss er sich zumindest kurz zu einem ev. unpassenden Zeitpunkt damit beschäftigen und ablenken lassen.

Rechtlich kann der Empfänger meist wenig unternehmen, da er einen konkreten Schaden nicht nachweisen wird können. Eine Anzeige an die Fernmeldebehörde ist ev. zielführend, sofern der Absender in Österreich seinen Sitz hat. In Deutschland besteht noch die Möglichkeit, wegen "Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb" (§ 823 BGB) zu klagen (Ersatz der Abmahnkosten)[43].

I.2.4.3. Im Internet

Durch den Versand von Spam wird eine hohe Bandbreite belegt[44]. Dies ist insbesondere in internationalen, z.B. Transatlantik, Leitungen ein echtes Problem, sodass auch dort an Maßnahmen zur Reduktion gearbeitet wird. Weiters werden die Mailserver sowohl des Senders, etwaige Mail-Relays, sowie auch der Empfänger stark beansprucht. Durch die Praxis, falsche Absender-Adressen anzugeben, vergrößert sich das Problem noch weiter, da dann zusätzlich die Unzustellbarkeits-Rückmeldung auf dem Rückweg weitere Bandbreite beansprucht[45].

Es sollte noch beachtet werden, dass viele ISPs den Versand von Spam bzw. allgemein jeglicher Werbe-E-Mails über bei ihnen eingerichtete Accounts bzw. Zugänge verbieten. Vor einer Werbeaktion sollte daher genau geprüft werden, ob dies der Fall ist, da es ansonsten schnell zu einer Sperrung der Internet-Anbindung kommen kann. Dies ist auch für Betroffenen Empfänger ein praktischer Weg: Kontaktieren des ISP des Absenders.

I.2.4.4. Zusammenfassung

Insgesamt können daher praktisch keine positiven, sondern nur negative Auswirkungen festgestellt werden. Das wirft naturgemäß die Frage auf, warum Spam noch immer existiert. Die Antwort darauf setzt sich aus mehreren Elementen zusammen:

- Viele Spam-Versender haben keine oder nur wenig Erfahrung mit dem Internet und sehen erst nach dem ersten Mal, welche Konsequenzen damit verbunden sind. Da weltweit noch immer viele Firmen nicht oder erst kurz im Internet präsent sind, ist bis auf weiteres der Nachschub an "Neulingen" gesichert und daher mit einer Abnahme dieser Gruppe nicht zu rechnen.
- Spam-Versender kennen zwar das Resultat, doch treten sie selbst mittels aggressiver Werbung an Firmen heran, um dann für diese Spam zu versenden. Solange es noch Kunden (siehe oben) für diese gibt, wird auch dieser Grund weiterbestehen.

---

[43] Beispiele: AG Bad Homburg 23.7.2003, 2 C 3419/02 (23), LG Berlin 23.6.2000, 16 O 115/00, OLG Bamberg 14.4.2005, 1 U 143/04, OLG Düsseldorf 24.5.2006, I-15 U 45/06

[44] Schätzungen gehen von 75 bis zu 90% Anteil an Spam vom gesamtem E-Mail-Verkehr aus. http://www.spamhaus.org/news.lasso?article=156

[45] Solche Nachrichten sollten daher im Allgemeinen gar nicht verschickt werden.

- Die Versuchung, Spam zu versenden, ist für Werber enorm: Mit minimalem Aufwand kann ein riesiges Zielpublikum erreicht werden. Und für andere, klassische, Werbeformen (Radio, Plakate, etc.) ist eine Zustimmung des Empfängers ja auch nicht nötig!
- Manche Spams wie etwa Kettenbriefe werden nur als "Scherz" oder einfach in Schädigungsabsicht (Beispiel: falsche Virenwarnungen) versandt. Ein monetärer Erfolg wird überhaupt nicht erwartet.
- In vielen professionell aufgezogenen Fällen (Webseiten-Werbung in Verbindung mit Bannern; Verkauf billiger/gefälschter Produkte zu mittleren Preisen) kann Spam durchaus finanziellen Erfolg bringen[46]. Allein die Hoffnung darauf ruft viele Werbende, seriöse wie unseriöse, auf den Plan.
- Aufgrund der Anonymität und Internationalität des Internets ist Spam eine gute Möglichkeit, illegale Aktionen zu starten. Beispiele sind Pyramidenspiele und direkter Betrug, beispielsweise der Verkauf von Produkten gegen Vorauskasse[47] oder Vorauszahlungsbetrug[48]. Nur ein verschwindend kleiner Teil der Empfänger wird darauf hereinfallen, doch wegen der minimalen bis nicht-existenten Kosten kann ein Gewinn daraus gezogen werden[49]. Hierher gehört auch Phishing, wobei dort schon einzelne Erfolge sehr hohen Gewinn bedeuten können, z.B. das "Abräumen" eines Kontos.

I.2.5. Maßnahmen gegen Spam

Gegen Spam können hauptsächlich vier Dinge unternommen werden:

1. Verhindern, dass die E-Mail Adresse in die Hand von Werbenden gelangt
2. Den Versand von Spam E-Mails verhindern (ISPs, Bot-Netze)
3. Unerwünschte Werbung automatisch herausfiltern lassen (am Server oder lokal)
4. Verbot unerbetener Werbung und andere rechtliche Maßnahmen

I.2.5.1. Maßnahmen gegen die Adressen-Sammlung

Die Verbreitung der eigenen E-Mail Adressen (Firmen- oder Mitarbeiter-Adressen) kann grundsätzlich nicht verhindert werden: Man will eben erwünschte E-Mails, z.B. von Kunden, erhalten. Doch gibt es einige Möglichkeiten, Spam-Versender zu behindern ohne den normalen Gebrauch allzu sehr einzuschränken. Beispiele hierfür sind:

- Erhält man Spam mit dem Hinweis, dass man nur eine Antwort an eine bestimmte Adresse zu senden braucht, um von der Liste entfernt zu werden, so sollte dies keinesfalls erfolgen. Falls es irgendeine Auswirkung haben sollte (Streichung), so wird die Adresse jedenfalls sehr teuer an andere Spammer verkauft weil sie garantiert aktiv ist, und die Anzahl der Spam-Mails wird eher steigen. Nur bei äußerst seriösen "Spams", z.B. bei

[46] Siehe dazu auch die Beispielrechnung in http://www.bsi.de/literat/studien/antispam/antispam.pdf Seite 17. Der finanzielle Erfolg (ca. € 5.000) ist um Größenordnungen geringer als der dadurch hervorgerufene Schaden (ca. € 153.000). Allerdings trifft dieser nicht den (einen) Versender, sondern die (vielen) Empfänger.

[47] Das Produkt ist nicht vorhanden und wird daher auch nie versandt oder es handelt sich um völlig wertlose Ware, z.B. Puderzucker als Medikamente.

[48] So genannter "Nigerian Advance-Fee Fraud", "419 Scam" (nach dem § 419 des Nigerianischen Strafgesetzbuches, der dies verbietet).

[49] Siehe Kanich et al: Spamalytics: An Empirical Analysis of Spam Marketing Conversion. ACM 2008 http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf

abonnierten Mailinglisten oder bei Nachfasswerbung (siehe unten) sollte dies in Erwägung gezogen werden.

- Analog dazu sollte man eine Empfangsbestätigung für E-Mails ("return receipt" bzw. "confirm reading") nur dann abschicken, wenn man den Sender genau kennt, ansonsten wird wiederum die eigene Adresse als gültig bekannt gegeben. Insbesondere in Verbindung mit Mailinglisten kann es vorkommen, dass in der Bestätigung alle ursprünglichen Empfänger aufgelistet sind und so ein Spammer die Adressen aller Empfänger der Mailingliste erhält, welche der Mailinglistenserver verweigert.
- Antwortet man auf Massen-Mails oder schickt man eine identische E-Mail an mehrere Personen, so darf nicht das TO sondern es muss das BCC-Feld verwendet werden[50]. Auf diese Weise erfahren die einzelnen Empfänger nicht die E-Mail Adressen aller anderen Empfänger.
- Auf Webseiten oder in Newsgruppen sollte die eigene Adresse nur angegeben werden, wenn dies unbedingt notwendig ist. Hier bestehen noch Möglichkeiten, Spammer zumindest zu behindern[51], beispielsweise durch Einfügen von "%20" zwischen "mailto:" und E-Mail Adresse, @ als Graphik, durch Tags trennen, Verwendung von JavaScript, durch das Anhängen von "_NOSPAM" oder "_@_" statt "@", ... Die Methode zur Korrektur der Adresse wird in den entsprechenden Fällen meist im Text angegeben. Dies bedeutet aber eine hohe Belastung für denjenigen, der antworten will.
- In Webseiten können (unsichtbare) Links zu so genannten Poison-Scripts eingebaut werden. Diese erzeugen eine Seite voll zufälliger ungültiger E-Mail-Adressen und abschließend einen Link auf eine neue derartige Seite. Da es sich um ein Script handelt, läuft ein automatischer Scanner (Robot, Spider) Gefahr, in eine Endlosschleife zu geraten und erhält Unmengen falscher E-Mail Adressen, was beim Versender zu Problemen führen kann. Bei gefälschter Absenderadresse erhält diese jedoch alle Fehlermeldungs-Rück-E-Mails. Ebenso wird dadurch die Netzwerkbelastung insgesamt erhöht.
- Für den Einzelnen nicht sinnvoll, jedoch für größere Organisationen möglich, ist der Einsatz von Köder-Adressen. Es werden an verschiedenen Orten spezielle E-Mail Adressen verteilt bzw. unsichtbar in Webseiten eingefügt. Wird dann an eine solche Adresse eine E-Mail geschickt, so handelt es sich fast sicher um Spam, da sie sonst nicht in praktischer Verwendung bzw. sichtbar oder erreichbar ist. Auf die erste an einer solchen Adresse empfangene E-Mail hin kann der Absender gesperrt werden, sodass alle folgenden Spam-Mails, bzw. ev. auch bereits empfangene aber von den Benutzern noch nicht abgerufene, automatisch abgeblockt, gelöscht oder markiert werden können.

Zusammenfassend kann gesagt werden, dass nur eine strenge Kontrolle der Orte, an denen die Adresse bekannt gegeben wird (Webseiten, Registrierungen, ...), die Sammlung für Spam einigermaßen kontrollieren, aber im Endergebnis nicht verhindern kann.

[50] OLG Düsseldorf 24.5.2006, I-15 U 45/06 Newsletter-Versender müssen das BCC-Feld anstatt des TO-Felds (umfasst hier im Ausdruck 9 A4-Seiten!) benützen; ansonsten liegt eine Sorgfaltswidrige Handlung vor.

[51] Ob dies noch besonders wirksam ist, darf bezweifelt werden: Adress-Suchprogramme können diese Manipulationen relativ leicht erkennen und umgehen. Wirksam ist nur, die gesamte E-Mail Adresse als Bild darzustellen. Dies bedeutet jedoch, dass Kunden diese händisch abschreiben müssen, anstatt sie zu kopieren oder darauf klicken zu können!

I.2.5.2. Maßnahmen gegen Spam-Versand

Spam wird einerseits über eigene Mailserver verschickt, oft jedoch über fremde. Hierzu dienen insbesondere offene Relays, Bot-Netze oder fehlerhaft konfigurierte Server (offene Proxies, Skripte in Diskussionsforen/Gästebüchern etc.). Die richtige Konfiguration der Systeme, sowohl bei Firmen als auch bei privaten Computern, ist daher besonders wichtig. Eine Konsequenz könnte nämlich u.U. ein Schadenersatzanspruch sein. Problematischer ist der Versand über legitime Mailserver. Hier hat der ISP nur beschränkte, aber immerhin einige, Möglichkeiten des Eingriffs.

I.2.5.3. Maßnahmen gegen Spam-E-Mails

Erhält man öfters Spam-E-Mails, so ist es mit Aktionen gegen die Adressen-Sammlung nicht mehr getan und eine aktivere Vorgehensweise ist nötig. Die üblichste Form sind Mail-Filter, welche versuchen, Spam von normalen E-Mails zu unterscheiden und anschließend vorzubehandeln, z.B. zu markieren, in einen bestimmten Ordner zu verschieben, oder gleich zu löschen. Dies kann einerseits auf dem Server erfolgen, was geringere Kosten für den Benutzer bedeutet, der diese Mails dann nicht herunterladen muss, oder auf dem Benutzer-Rechner. Aufgrund der Komplexität und der Notwendigkeit regelmäßiger Aktualisierung ist besonders der erste Ansatz empfehlenswert. Eine Pflicht zur Verwendung solcher Systeme besteht nicht[52], insbesondere im Hinblick auf die Möglichkeit von "False-Positives", d.h. als Spam eingestuften "echten" E-Mails.

Eine weitere Alternative ist die Eintragung in el. Robinsonlisten. Versender von Werbe-E-Mails sollten (in Österreich gesetzlich verpflichtend, d.h. müssen) diese konsultieren, und dort enthaltene Adressen aus ihren Datenbanken entfernen bzw. für den Versand sperren. Da sich meist nur die Versender, welche legale und reelle Angebote versenden und daher wenig Probleme verursachen, daran halten, hat dies eher geringen Erfolg. International kann überhaupt damit gerechnet werden, dass Spam-Versender nicht einmal von deren Existenz wissen und sich kaum der Mühe des Abgleichs unterziehen werden[53].

Wie bereits bei der Adressensuche erwähnt, sollte man nie auf Werbe-E-Mails antworten. Nur wenn man die Firma genauer kennt, z.B. durch eine vorherige Geschäftsbeziehung oder eine Zusendung aufgrund expliziter Anforderung, sollte dies in Frage kommen. Um sicherzugehen ist dabei noch zu empfehlen, nicht einfach auf Links in der E-Mail zu klicken, sondern diese abzuschreiben oder die Firma über eine Suchmaschine zu finden.

Die sinnvollste Art der Reaktion auf Spam ist zu versuchen, den Internet-Provider des Versenders herauszufinden und an diesen zu schreiben. Dieser hat meist kein Interesse am Versand von Spam (seine Mailserver werden sehr stark belastet) und er ist in einer guten Position, eine Wiederholung tatsächlich zu unterbinden. Da viele ISP in ihren Geschäftsbedingungen explizit den Versand von Massen-E-Mails und Spam verbieten, existieren für sie auch keine rechtlichen Schwierigkeiten. Der Nachteil ist, dass dies von manchen Spam-Versendern einkalkuliert wird: Sie kaufen einen billigen Account, versenden die Mails, und beenden ihn anschließend sofort wieder. Dies funktioniert deshalb, weil, vor allem in den

[52] OLG Düsseldorf 24.5.2006, I-15 U 45/06

[53] Derzeit nicht in der Praxis bekannt, aber durchaus möglich wäre die Anforderung der Liste, deren illegaler Export ins Ausland, und die dortige Verwendung als Ziele für den Versand von Werbung. Daher auch die technische Umstellung der Österreichischen Liste von Klartext-Adressen auf Hashwerte.

USA, keine Überprüfung der Identität des Antragstellers erfolgt und teilweise auch anonym Accounts vergeben werden[54].

Inzwischen existiert Software, mit der man Spam zwar nicht eliminieren, aber zumindest sein Ausmaß stark reduzieren kann. Hierbei handelt es sich einerseits um Klassifikationsprogramme, welche versuchen, E-Mails anhand ihres Inhalts, ihrer Formatierung etc. zu erkennen[55], andererseits um verschiedene Speziallösungen. Beispiele für letztere sind:

- Tarpits: Hierbei wird die Entgegennahme von E-Mails künstlich verzögert, indem die Mail nur sehr langsam, etwa über mehrere Stunden hinweg, empfangen wird. Dadurch werden Spam-Sender blockiert. Dies ist jedoch eine suboptimale Lösung da auch legitime Versender in großen Firmen (ein Mailserver versendet die E-Mails von 1000 Angestellten) hiermit blockiert werden sowie Spammer nicht unbedingt getroffen werden, da sie offene Relays (=fremde Rechner) bzw. Bot-Netze benützen. Auch verzögert sich der Empfang von erwünschter E-Mail stark. Dies wird in der Praxis anscheinend nicht eingesetzt.
- Spam-Mail-Listen: Eine zentrale Stelle legt Listen von Spam-E-Mails an[56]. Wird eine E-Mail empfangen, so wird eine Prüfsumme gebildet und mit der Liste der Prüfsummen dieser zentralen Stelle verglichen. Ist sie identisch, so wird die Mail als Spam angesehen. Die Befüllung der Liste erfolgt durch Benutzer, welche manuell als Spam erkannte E-Mails dorthin schicken. Problematisch ist hier, dass durch die Prüfsummenbildung manchmal auch "normale" Mails als Spam erkannt werden. Auch reicht eine geringfügige Änderung aus, um durch diesen Filter hindurchzugelangen.
- Spam-Server-Listen: Es werden Listen von IP-Adressen geführt (Blacklists[57]), von welchen bekannt ist, dass es sich um offene Relays oder Spam-Versender handelt. E-Mail von diesen Adressen wird dann nicht angenommen. Die Befüllung dieser Liste erfolgt selbsttätig oder auf besonders begründete Fälle hin. Diese Methode scheint in weit verbreitetem Einsatz zu sein.
- Absender-Server-Kennung: Über verschiedene Protokolle, wobei derzeit jedoch keine Einigung bzw. anerkannte Standards bestehen[58], wird überprüft, ob der versendende Rechner berechtigt ist, E-Mails mit der enthaltenen Absenderadresse abzuschicken. Dies verhindert Spam nur in dem Maße, als der Absender gefälscht wird, z.B. Verwendung eines gehackten Rechners zum technischen Versand.
- Kostenbasierte Verfahren: Hierbei muss der Senderechner bestimmte Ressourcen aufbringen, damit die E-Mail angenommen wird. Dies kann einerseits eine el. Briefmarke sein (=Geld), andererseits z.B. auch Rechenzeit. Letzteres ist insbesondere für legitime Versender von sehr vielen E-Mails problematisch, wie große Provider, Mailinglisten-Betreiber etc. Elektronische Briefmarken wären eine ideale Lösung, sind aber realistischerweise in der Praxis nicht umsetzbar, da die Lösung weltweit und fast ausnahmslos

[54] Daher auch der Einsatz von Captchas bei vielen Gratis E-Mail-Diensten, um ein automatisiertes Anlegen von Mail-Accounts zu verhindern.

[55] Siehe als bekanntes und sehr erfolgreiches Programm SpamAssassin (http://spamassassin.apache.org/). Dieses ist für verschiedenste Betriebssysteme verfügbar und erzielt sehr gute Quoten.

[56] Ein Beispiel ist "Vipul's Razor" http://razor.sourceforge.net/

[57] Ein Beispiel ist Mail Abuse Prevention System LLC (Realtime Blackhole List) http://www.mail-abuse.com/

[58] Beispiele: SPF: Sender Policy Framework (http://www.openspf.org/) und Sender ID (http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx), DomainKeys Identified Mail DKIM (http://www.dkim.org/)

erfolgen müsste. Auch hier wären legitime Absender vieler E-Mails wieder „Leidtragende“.

I.2.6. Rechtliche Aspekte von Spam

Die unerbetene Zusendung von Werbe-E-Mails kann rechtliche Konsequenzen nach sich ziehen. International herrscht zwar großteils Übereinstimmung, dass die Zusendung von Fax-Sendungen ohne Anforderung verboten ist, denn es entstehen dem Empfänger Kosten für Papier/Tinte/Toner/..., doch kann dies nicht unmittelbar auf E-Mails übertragen werden: E-Mails verursachen keine derartigen Kosten, da das Medium "gratis" ist[59]. Auch hier können zwar Kosten entstehen, etwa Kommunikationskosten für die Zeit der Übertragung vom Server auf den lokalen Computer oder Verlust von Arbeitszeit für die Identifizierung und Löschung der Mails, doch sind diese teilweise ohnehin immer vorhanden (auch Briefwerbung muss aussortiert werden) oder nur schwer zu erfassen bzw. äußerst gering. Der große praktische Unterschied zwischen Fax- und E-Mail-Werbung besteht jedoch darin, dass bei unerbetenen Fax- oder Briefsendungen der Sender die, bei internationalem Versand relativ hohen, Kommunikationskosten tragen muss, während der E-Mail-Versand nur marginale Kosten erzeugt[60]. Daher ist E-Mail Spam in der Praxis ein viel größeres Problem als andere Formen der Werbung ohne Aufforderung für die Zusendung. Entsprechend wurde in früheren Urteilen auf die entstehende Gefahr hingewiesen, sollte sich diese Werbeform ausbreiten, und gerade deshalb schon einzelne Mails, die an sich fast vernachlässigenswerte Kosten verursachen, verboten. In der Summe wird durch Spam die Arbeit in Firmen unzumutbar behindert und Privatpersonen unzumutbar belästigt.

Ähnlich zu konventioneller Werbung existieren zwei grundsätzliche Modelle, um dieses Problem rechtlich zu regeln, wenn kein vollständiges Verbot erfolgen soll:

1. Opt-in: Die Zusendung ist grundsätzlich verboten, außer der Benutzer erklärt explizit, dass er bereit ist, derartige Werbung (allgemein, von bestimmten Anbietern oder über einzelne Produktgruppen) zu empfangen. Das Musterbeispiel hierfür ist das österreichische Regelungsmodell bei Werbung über Telefon oder Fax.
2. Opt-out: Die Zusendung ist grundsätzlich erlaubt, es besteht jedoch jederzeit die Option, Zusendungen abzulehnen. Möglichkeiten hierfür sind die individuelle Abbestellung bei einzelnen Werbern oder auch generell über eine Sammelliste. Durch die Eintragung auf derartigen Listen ("Robinsonlisten") gibt man zu erkennen, keinerlei unerbetene Werbung zu wünschen. Dies ist das Modell für konventionelle Briefpost, hinsichtlich der z.B. Direktwerbeunternehmen verpflichtet sind, ihre Adressen regelmäßig mit solchen Listen abzugleichen.[61]

In Österreich wurde für E-Mails im Laufe der Zeit von Opt-out auf Opt-in umgestellt, doch besteht noch eine sehr eng begrenzte Ausnahme (siehe unten).

---

[59] Diese Überlegung ist allerdings nicht ganz richtig, da es immer noch Internet-Zugänge gibt, welche nach Datenvolumen bezahlt werden oder Mengenmäßig beschränkt sind.

[60] Der Versand von 100.000 Fax-Sendungen ist sehr teuer und dauert selbst bei mehreren Leitungen sehr lang, während der Versand von 100.000 E-Mails sehr billig und schnell erfolgen kann; bei Verwendung von E-Mail-Relays fast sofort. Aufgrund der höheren Kosten ist daher SMS-Spam ein verhältnismäßig unbedeutendes Problem!

[61] Analog dazu funktioniert der Robinson-Aufkleber für Postkästen: Nur persönlich adressierte Werbung darf bei Anbringung zugestellt werden. Dadurch fällt ein Großteil der Werbung weg ("An einen Haushalt"), jedoch nicht alle. Werbung von Direktwerbeunternehmen ist jeweils an Einzelpersonen adressiert und muss daher von der Post zugestellt werden. Hier hilft nur eine Eintragung in der Robinsonliste. Mit Zustimmung erhaltene Werbung oder Werbung direkt vom Erhebenden kann nur durch Kontakt mit dieser Person/Firma verhindert werden.

Bei E-Mail Werbung ist zu beachten, dass im Gegensatz zu vielen anderen Rechtsgebieten meist das Recht des Staates zur Anwendung kommt, in welchem der Empfänger seinen Sitz hat. Daher ist bei grenzüberschreitender Werbung besondere Vorsicht geboten. Erschwert wird dies noch dadurch, dass das Empfangsland aus der E-Mail Adresse selbst nicht erkennbar ist: xyz@abc.at ist nicht unbedingt ein österreichischer Empfänger und Versand an diese Adresse unterliegt daher in manchen Fällen ausländischem Recht! Eine gewisse Erleichterung besteht darin, dass inzwischen die maßgeblichen Regelungen auf einer EU-RL beruhen, sodass innerhalb der EU von einem ähnlichen Schutzniveau ausgegangen werden kann. Dies bedeutet aber auch, dass man sich auf besondere nationale Ausnahmen nicht verlassen kann, sondern nur der kleinste gemeinsame Nenner, die Richtlinie, als Grundlage dienen kann.

I.2.6.1. § 107 Telekommunikationsgesetz

Anrufe, inklusive Fax, zu Werbezwecken bedürfen nach dem Telekommunikationsgesetz (TKG) der vorherigen Zustimmung des Empfängers oder einer anderen Person, welche diesen Anschluss benützen darf[62]. Die Zustimmung kann jederzeit widerrufen werden und hat keinen Einfluss auf ein anderes Vertragsverhältnis. Eine Differenzierung nach dem Empfänger, Unternehmer oder Verbraucher findet inzwischen nicht mehr statt.

Direktwerbung umfasst neben der klassischen Werbung auch jeden Inhalt, der für eine bestimmte Idee einschließlich politischer Anliegen wirbt oder dafür Argumente liefert. Daher ist auch Wahlwerbung hiervon umfasst. Lediglich echt und ausschließlich "amtliche" Informationen, d.h. ohne Herausstellung des Initiators oder des zuständigen Politikers, wären hiervon ausgenommen[63]. Keine Werbung ist, wenn eine echte Informationssammlung geplant ist, z.B. bei Umfragen (diese also kein bloßer Vorwand für die Werbung sind)[64], oder wenn Produkte des Unternehmens angefragt werden (Kauf)[65].

---

[62] Dies hat der Werbende zu beweisen. BGH 1.3.2004, I ZR 81/01 "E-Mail-Werbung"

[63] Lehofer, Spamverbot und kommunale Informationstätigkeit, RFG 2006/14

[64] LG München I 15.11.2006, 33 O 11693/06 Eine Umfrage einer Zeitung über Branchen- und Fachspezialisierung von deutschen Steuerberatungskanzleien (die in einem 11-seitigen Bereicht resultierte) ist keine Werbung, da es nach Begleitschreiben und Fragebogen sehr sachlich um tatsächliche Informationsgewinnung geht.

[65] Nach BGH 17.7.2008, I ZR 75/06 sind auch gewerbliche Anfragen nach Waren oder Dienstleistungen "Werbung" (sie dienen mittelbar der Förderung seines eigenen Absatzes). Daher ist eine Zustimmung erforderlich. Diese ist anzunehmen (konkludente Einwilligung) für Kaufanfragen betreffend die übliche Verkaufstätigkeit (Fall: Kaufanfrage für 3 Toyotas bei der Toyota-Vertretung), nicht jedoch für anderes (Angebot von Bannerwerbung auf der Website eines Fußballvereins – Bannerwerbung auf seiner Webpräsenz zu verkaufen ist kein typischer Vereinszweck eines Fußballvereins; die E-Mail Adresse auf der Website ist nicht für solche Anfragen bestimmt). Die allgemeine Aussage ist sicherlich richtig, doch wäre im zweiten Fall durchaus daran zu denken, dass derartige Einnahmen für sehr viele Homepages höchst willkommen bzw. sogar Voraussetzung sind.

Die Zusendung von E-Mails oder SMS[66] ist verboten, wenn es sich um Werbung handelt[67] oder die Nachricht an mehr als 50 Empfänger geht[68] (=opt-in). Eine Zustimmung ist jedoch nicht erforderlich (=opt-out)[69], wenn (kumulative Voraussetzungen!):

1. Die Adresse im Zusammenhang mit einem Kauf oder einer Dienstleistung vom Kunden erfahren wurde: Wird die Adresse beim Kauf angegeben, so darf der Unternehmer an diese Adresse auch E-Mail-Werbung schicken. Bloße Anfragen von Interessenten berechtigen hierzu, abgesehen von deren Beantwortung, jedoch nicht[70].
2. Es sich um Werbung für eigene ähnliche Produkte oder Dienstleistungen handelt: Zusatzprodukte, weiterer Service etc. dürfen beworben werden, anderes oder Drittfirmen im Gegensatz dazu jedoch nicht.
3. Der Kunde bei der Datenerhebung und bei jedem Kontakt eine weitere Zusendung kostenlos ablehnen kann: Link zum Austragen aus der List, Hinweis auf Streichungsmöglichkeit etc. Falls die Abmeldung per Telefon vorgesehen ist, muss es sich um eine kostenlose Nummer handeln!
4. Keine Eintragung in die Robinsonliste besteht[71]: Diese Liste ist, im Gegensatz zu direkter Zustimmung zur Zusendung, auch hier zu beachten.

Es muss also jede Werbe-E-Mail vom Konsumenten explizit angefordert werden, er sonst[72] seine Zustimmung erklärt haben[73] oder es sich um "Nachfass-Kommunikation" zu geleisteten Lieferungen oder Diensten handeln. Eine Zustimmung muss nicht ausdrücklich oder gar schriftlich erfolgen, sondern ist auch konkludent möglich. Problematisch kann jedoch die Beweisbarkeit sein, weshalb z.B. auf einem Webformular das Anhaken eines Kästchens durch den Besucher zu empfehlen ist[74]. Die Ausnahme für Nachfass-Kommunikation bezieht sich nur auf E-Mail und SMS und gilt nicht für Telefonanrufe[75].

---

[66] Die Aufforderung per SMS zum Anruf einer Mehrwertnummer ist bereits Werbung: UVS Steiermark 29.03.2002, 30.2-153/2001 Ebenso VwGH 25.2.2004, 2003/03/0284

[67] Fast jede Mitteilung einer Firma wird als Werbung angesehen, da schon ein Hinweis auf ein neues Produkt hierzu ausreicht. Dies betrifft daher hauptsächlich Private und besitzt wohl geringe Bedeutung.

[68] Beispielsweise Kettenmails, Hoaxes, Spaß-E-Mails etc.

[69] Zusatzausnahmen für Kammern in Erfüllung ihrer Aufgaben: § 2 Abs 4 ApothekerkammerG, § 72 Abs 4 WirtschaftskammerG

[70] So wohl Weiskopf, Die neue gesetzliche Regelung gegen unerwünschte E-Mails (§ 107 TKG), JAP 2004/2005, 11 die von einem abgeschlossenen Kauf ausgeht. Wie eng der "Zusammenhang" sein muss, ist freilich umstritten. Auch die Angabe bei einer bloßen Anfrage könnte hierzu ausreichen. Nach teleologischer Auslegung sollte demgegenüber ein abgeschlossener Vertrag erforderlich sein. Ansonsten wäre jede Anfrage wegen einem bestimmten Produkt schon ausreichend für die Zusendung von Werbung für ähnliche Waren bzw. Dienstleistungen. Es muss auch ein zeitlicher Zusammenhang bestehen, d.h. nach einem Kauf darf nur für eine begrenzte Zeit geworben werden. AG Charlottenburg 10.11.2006, 220 C 170/06 (6 Monate; Verhandlungen waren endgültig gescheitert)

[71] Wurde bei der letzten Novelle explizit eingefügt. Kraft, Der neue § 107 TKG - Verbesserter Schutz vor unerbetenen Werbemails? ecolex 2006, 252

[72] Eine Zustimmung kann nicht per Telefon, Fax, SMS oder E-Mail eingeholt werden, da bereits die Anfrage nach der Zustimmung zur Werbung selbst Werbung darstellt und daher verboten ist. OGH 18.5.1999, 4 Ob 113/99t

[73] Wohl auch in AGBs möglich, allerdings nur bei besonderer Hervorhebung. OLG Hamm 15.8.2006, 4 U 78/06

[74] Zur vergleichbaren deutschen Rechtslage: BGH 16.7.2008, VIII ZR 348/06: Unter Berufung auf die Datenschutz-RL für el. Kommunikation, RL 2002/58/EG Erwägungsgrund 17, ist für die Datenschutzrechtliche Zustimmung zwar opt-out möglich (=vorangekreuztes Feld), aber für Werbung per E-Mail/SMS nur opt-in zulässig (=der Besucher muss das Feld selbst ankreuzen).

[75] Siehe OLG Wien, 24.2.2004, 8 Ra 9/04h, ARD 5549/10/2004

Immer verboten ist die Zusendung el. Post zu Werbezwecken, wenn die Identität des Absenders verschleiert oder verheimlicht wird[76] bzw. wenn die opt-out Adresse "nicht authentisch" ist. Letzteres soll wohl bedeuten, dass eine Abmeldung über diese auch tatsächlich möglich sein muss, wobei kurzfristige Störungen außer Betracht bleiben. Falsche, z.B. fremde, oder nicht-existente Absender- bzw. Reply-to-Adressen könnten daher problematisch sein, selbst wenn eine andere funktionierende Abmeldeadresse in der E-Mail angegeben ist. Weiters reicht es alleine für sich nicht aus, die E-Mail in den legalen Bereich zu bringen, wenn die Werbung zwar ohne vorherige Zustimmung erfolgt, aber in der Überschrift eindeutig als solche gekennzeichnet ist und eine funktionierende Abmeldemöglichkeit bereitgestellt wird: Dies wäre das Opt-out-Modell[77].

Nach § 109 Abs 3 TKG zieht die Verletzung dieser Vorschriften eine Verwaltungsstrafe mit einem Strafrahmen bis € 37.000 nach sich. Zusätzlich kann für Firmen noch § 1 UWG von Bedeutung sein, wonach auch Konkurrenten tätig werden können. Hinsichtlich der Internationalität von Bedeutung ist, dass der Tatort bei Telefonanrufen/Fax/SMS/E-Mails vom Ausland aus explizit (§ 107 Abs 6 TKG) als der Ort angesehen wird, an dem die Nachricht den Teilnehmeranschluss erreicht (=und daher dann in Österreich liegt).

Nach einer Entscheidung des OLG Nürnberg[78] sind Produktempfehlungen an sich erlaubt, da sie von Dritten und nicht dem "Werbenden" kommen. Dies ist jedoch problematisch, da zumindest in Österreich die Qualität des Senders nicht (mehr) berücksichtigt wird: Jegliche Werbung, auch von Privaten an Private ist verboten. Hier könnte jedoch u.U. mit vermuteter Einwilligung des Empfängers gearbeitet werden bzw. mit der Nicht-Anwendbarkeit des UWG (Private; daher höchstens Verwaltungsstrafe). Wie im angesprochenen Urteil entschieden, ist das heimliche Anfügen von zusätzlicher Werbung auf jeden Fall verboten.

I.2.6.2. Art. 10 Fernabsatz-Richtlinie

In der Fernabsatz-Richtlinie aus 1997 wird lediglich ein Mindeststandard festgelegt. Danach ist nur für die Kommunikation mit Automaten (Voice-Mail-Systeme) und für Telefax eine vorherige Zustimmung des Verbrauchers nötig. Alle anderen Fernkommunikationstechniken dürfen immer dann und unabhängig vom Inhalt verwendet werden, wenn der Verbraucher ihre Verwendung nicht offenkundig abgelehnt hat. Hier ist daher die opt-out Variante verwirklicht, da eine Eintragung in eine Robinson-Liste eine solche Ablehnung darstellt. Aufgrund späterer Richtlinien besitzt dies für E-Mails keine Bedeutung mehr.

---

[76] Verwendung eines fremden Markennamens als Absender-E-Mail kann eine Markenverletzung darstellen: OLG Karlsruhe 25.10.2006, 6 U 35/96 (hier: Marke eines Internet-Dienstleisters, die auch für Werbung und Marketing eingetragen ist; Die "hotmail"-Absenderadressen waren gefälscht - Spam wurden tatsächlich nicht über Hotmail-Accounts verschickt)

[77] LG Dortmund 30.8.2005, 19 O 20/05 (Deutschland: § 7 Abs 2 Z 3 iVm § 7 Abs 3 UWG). Auch der Hinweis auf existierende und zuverlässige Filterprogramme reicht nicht aus.

[78] OLG Nürnberg, 25 10.2005, 3 U 1084/05 http://www.affiliateundrecht.de/olg-nuernberg-produktempfehlung-mails-wettbewerbwidrig-3-U-1084-05.html Vom BGH aus formellen Gründen inzwischen aufgehoben, BGH 29.5.2008, I ZR 189/05, daher keine inhaltliche Entscheidung. Ergebnis: Das Erstinstanzliche Urteil wurde wiederhergestellt, nach dem Produktempfehlungen uneingeschränkt zulässig sind. Siehe http://forum.computerbetrug.de/showthread.php?t=38041 für weitere Überlegungen zu werbefinanzierten E-Mails. Entscheidend ist wohl: Erfolgt die Zusendung zur privaten Information oder will auch der Dritte hier werben (für jemand anderen), z.B. zum späteren Erhalt von Prämien, ist der Dritte also nur "Werkzeug" des Website-Betreibers oder Eigenständig? Allgemein zu dem Thema mit einem Überblick über die Deutsche Rechtsprechung: Keller, Ist Produktmarketing via "Mailingpoint-Funktion" rechtlich zulässig? http://www.commercemanager.de/magazin/artikel_1746_produkt_marketing.html

I.2.6.3. Art. 6 und 7 E-Commerce-Richtlinie

Auch hier wurde im Jahre 2000 die Opt-out Lösung vorgeschrieben, wobei eine Erlaubnis zur Zusendung unerbetener Werbe-E-Mails von den Einzelstaaten festgelegt werden kann oder auch nicht. Die EU-Mitgliedsstaaten konnten sich daher auch freiwillig für opt-in entscheiden. Ist die Zusendung von Werbung möglich, dann muss ein gewisser inhaltlicher Mindeststandard für jede, d.h. auch explizit angeforderte, kommerzielle Kommunikation erfüllt sein[79]; siehe oben.

I.2.6.4. Art. 13 Telekom-Datenschutz-Richtlinie

In dieser derzeit letzten einschlägigen Richtlinie aus dem Jahr 2002 wurden die Bestimmungen gegen Spam weiter verschärft. So ist für automatische Anrufsysteme, Fax und E-Mail das Direktmarketing verboten, außer der Empfänger hat vorher seine Zustimmung gegeben (=opt-in). Allerdings gibt es von diesem Grundsatz eine sinnvolle Ausnahme. Wenn beim Verkauf eines Produktes oder einer Dienstleistung eine E-Mail-Adresse bekannt wird, kann diese Person (d.h. *keinerlei* Weitergabe dieser Daten an andere Firmen oder Personen erlaubt!) die Adresse zur Direktwerbung verwenden. Dies darf jedoch nur für eigene ähnliche Produkte oder Dienstleistungen erfolgen, beispielsweise darf nach einem Software-Verkauf später Werbung für ein Update per E-Mail zugesandt werden. Weiters muss klar, deutlich, einfach und kostenfrei die Möglichkeit für opt-out eröffnet werden, sowohl bei der Erhebung der Adresse als auch bei jeder einzelnen Kommunikation. Für alle anderen Fälle der kostenfreien Direktwerbung (z.B. Flugblätter, Post, …) können die Mitgliedsstaaten entscheiden, ob opt-in oder opt-out gewünscht ist. Hier wird vermutlich überall das Modell opt-out beibehalten werden, da bisher keine Probleme damit aufgetreten sind (Aufkleber am Postfach/Eingangstüre). Diese Regelungen wurden im TKG in § 107 umgesetzt (siehe oben).

Zu beachten ist, dass diese Ausführungen ausschließlich für natürliche Personen gelten. Für juristische Personen bleibt die vorherige Rechtslage (siehe oben) weiterhin gültig. Sie sollen jedoch von den Einzelstaaten "adäquat" geschützt werden. In Österreich war daher (nicht ganz der EU-RL entsprechend[80]) bis März 2006 Werbung an Nicht-Konsumenten erlaubt. Wegen richtlinienwidrigen Umsetzung wurde dies jedoch geändert und auf alle, natürliche und juristische, Personen erweitert. Daher ist inzwischen auch die unverlangte Zusendung von Werbung per E-Mail an Unternehmen verboten.

I.2.6.5. Rechtslage in den USA

In den USA existieren diverse Regelungen in einzelnen Bundesstaaten bzw. für separate Sachgebiete. Seit 2003 besteht jedoch auch eine bundesweit einheitliche Regelung[81], welche den opt-out Ansatz verfolgt. Enthalten ist insbesondere:

- Verbot irreführender Header, Titelzeilen oder Rückantwort-Adressen: Die Fälschung von E-Mail Daten oder der Versuch, den Empfänger mittels falschem Titel zum Öffnen und Lesen zu bringen ist nicht erlaubt.

---

[79] Zusätzliche Erfordernisse bestehen für Preisnachlässe, Zugaben, Gewinnspiele etc. Siehe dazu das ECG.

[80] Einzelunternehmen sind keine Konsumenten und waren daher nach Österreichischem Gesetz nicht geschützt. Nach der Richtlinie ist jedoch E-Mail-Werbung an alle *natürlichen* Personen verboten.

[81] CAN-SPAM Act of 2003: http://www.spamlaws.com/federal/can-spam.shtml Für Vorschriften in Einzelstaaten siehe http://www.spamlaws.com/state/index.shtml

- Verbot der Sammlung von E-Mail Adressen von Webseiten oder durch zufällige Generierung, wobei ein Nachweis hier bezüglich einer konkreten E-Mail schwer sein dürfte. Interessant ist dies ev. in Hinsicht auf den eigentlichen Suchvorgang.
- Sexuell orientierte E-Mails müssen eine klare Kennzeichnung enthalten: Hier handelt es sich wohl um eine Schutzvorschrift für Minderjährige, sodass derartige Mails automatisch gefiltert werden können. Ob dies jedoch technisch realisierbar ist, muss bezweifelt werden, da keine bestimmte (z.B. "[Sexually explicit content]"), sondern nur eine "klare" Kennzeichnung (in welcher Form und mit welchem Text auch immer) vorgeschrieben wird.
- Funktionierende Abmelde-Möglichkeit: Opt-out muss tatsächlich möglich sein, und zwar für mindestens 30 Tage nach der letzten Werbeaktion.
- Verpflichtende Angabe der (konventionellen) Postadresse: Dies soll eine Durchsetzung der Rechte ermöglichen.
- Die Federal Trade Commission (FTC) hat Vorschläge und einen Zeitplan für die Implementation einer Robinsonliste zu erstellen[82].

Dies betrifft nicht nur den Versender der E-Mail sondern auch denjenigen, dessen Produkte beworben werden. Damit wird verhindert, die Haftung auf einen etwa im Ausland befindlichen und daher nicht erreichbaren Dritten abzuschieben.

Die Strafen sind mit US$ 2.000.000 (Verdreifachung bei Absicht; kein Limit bei Betrug) und bis zu fünf Jahren Gefängnis relativ hoch angesetzt[83].

I.2.7. Informationspflichten

Nach dem § 6 ECG muss kommerzielle Kommunikation klar und eindeutig die unten angeführten Regeln befolgen. Zu beachten ist, dass jede Art der erlaubten Werbung davon betroffen ist, also auch explizit angeforderte Zusendungen.

- Kommerzielle Kommunikation muss als solche erkennbar[84] sein. Dies soll es den Benutzern ermöglichen, eine einfache Filterung vorzunehmen, wenn sie dies wünschen. Eine bestimmte Bezeichnung ist aber *nicht* erforderlich (z.B. "Werbung", "ADV:", ...), weshalb die technische Filterung daher wohl kaum erleichtert wird. "Unabhängige Berichte" oder eine Vermischung mit redaktionellen Artikeln[85] ist damit nicht erlaubt.
- Die natürliche oder juristische Person, in deren Auftrag die Kommunikation erfolgt, muss erkennbar sein. Eine direkte Angabe ist nicht erforderlich, aber wohl meist sinnvoll; siehe jedoch gegebenenfalls die Impressumspflichten.
- Angaben zur Absatzförderung (=Werbeversprechen, Zugaben, Geschenke etc.) müssen als solche erkennbar sein. Weiters muss ein einfacher Zugang zu den Bedingungen für

[82] http://www.ftc.gov/spam/

[83] Diese werden nun auch zumindest in Einzelfällen verhängt, siehe etwa http://www.theregister.co.uk/2001/01/03/evil_spammers_jailed_for_two/ oder die Fälle rund um Sanford "Spamford" Wallace, den "Spam-König" aus den USA http://en.wikipedia.org/wiki/Sanford_Wallace

[84] Der Maßstab hierfür wird wohl ungefähr einem normalen Mitglied des Empfängerkreises entsprechen, d.h. unterschiedlich, ob Konsumenten oder Unternehmen beworben werden.

[85] D.h. Werbung kann sich sehr wohl mitten in einem Artikel befinden, muss jedoch abgegrenzt und als solche gekennzeichnet sein. "Product Placement" im *redaktionellen* Teil ist daher verboten!

ihre Inanspruchnahme enthalten sein. Eine direkte Einbettung der Bedingungen ist daher nicht erforderlich; ein Link zu einer Webseite reicht aus.

- Preisausschreiben und Gewinnspiele müssen als solche erkennbar sein.

Hierbei handelt es sich explizit nur um besondere Informations- und Klarheitspflichten, die keine Aussage über die Zulässigkeit bestimmter Elemente enthalten. Die Verletzung der Informationsvorschriften ist eine Verwaltungsübertretung mit Strafe bis zu € 3.000.

Für Angehörige von Berufen mit besonderen berufsrechtlichen Vorschriften (Anwälte, Ärzte, ...) bestehen noch strengere Regeln. Diese dürfen ebenfalls Werbung verschicken, wenn es sich um einen von ihnen bereitgestellten Dienst handelt. Bestehende allgemeine Einschränkungen der Werbung bleiben jedoch unberührt und gelten auch im Internet.

Bei regelmäßiger E-Mail Werbung, also Newslettern, handelt es sich um ein wiederkehrendes el. Medium, weshalb das Impressum nach § 24 MedienG erforderlich ist. Dieses erfordert Name bzw. Firma und Adresse des Medieninhabers und des Herausgebers. Zusätzlich sind auch die Offenlegungspflichten nach § 25 MedienG[86] entweder direkt im Newsletter oder auf einer verlinkten Webseite zu erfüllen.

I.2.8. Richtlinien für verträgliche E-Mail Werbung

E-Mail Werbung kann durchaus nützlich und erfolgreich sein, doch sollten einige Grundsätze befolgt werden:

1. Werbung sollte nur dann an eine Person geschickt werden, wenn von dieser ernsthaft angenommen werden kann, dass sie sich dafür interessiert. Dies bedeutet, dass hauptsächlich auf Anforderung hin[87] eine Zusendung erfolgt oder zumindest schon eine längere Geschäftsbeziehung bestehen muss. Zustimmung in AGBs sollte eher nicht verwendet werden, sondern nach Möglichkeit eine explizite Aktion, z.B. Anmeldung über Werbformulare. Um sicherzustellen dass nur der tatsächliche Empfänger die Erklärung abgibt, ist das "double-opt-in" Verfahren[88] zu verwenden.
2. Dem Empfänger muss eine einfache, kostenlose und unkomplizierte Möglichkeit gegeben werden, den Versand für die Zukunft zu unterbinden – und dies muss dann auch tatsächlich erfolgen. Die einfachsten Möglichkeiten sind ein Rückmail (entsprechende Reply-to Adresse) oder der Besuch einer Webseite (Link in der E-Mail; Anklicken alleine sollte reichen), wobei die Identifikation und der Abmeldungswunsch bereits eincodiert sind.

---

[86] Name/Firma und Wohnort/Sitz des Medieninhabers, vertretungsbefugte Organe (Geschäftsführer, Vorstand) und Aufsichtsrat, Beteiligungen, Unternehmensgegenstand und Blattlinie.

[87] Bezüglich SMS: Gratis-Telefonnummer zur Angabe einer, ev. anderen, Telefonnummer zum Empfang von Werbe-SMS reicht nicht aus. VwGH 25.2.2004, 2003/03/0284 Zusätzliche Nachprüfungen, z.B. nur an die Telefonnumer des Anrufers, wären zumindest erforderlich.

[88] Auch "confirmed opt-in" genannt. Hier erfolgt die Anmeldung durch die Eingabe einer E-Mail Adresse. An diese wird eine E-Mail mit zusätzlichen Informationen geschickt. Erst wenn diese befolgt werden, z.B. Antwort oder typischerweise Klicken auf einen Link, wird die Anmeldung wirksam. Ignorieren dieser E-Mail führt *nicht* zur Anmeldung. Damit wird die Eingabe fremder E-Mail Adressen bei der Anmeldung für Newsletter verhindert. Eine ev. falsche E-Mail (z.B. weil jemand eine fremde E-Mail Adresse angemeldet hat) ist noch kein Spam, sofern sie selbst keine Werbung enthält. AG München 16.11.2006, 161 C 29330/06. Zu hohe Anforderungen (Überprüfung außerhalb der virtuellen Welt, …) AG Hamburg 11.10.2006, 6 C 404/06 (Es könnte jedoch sein, dass das double-opt-in Verfahren an eine andere E-Mail gerichtet war, als an die schließlich Werbung zugesandt wurde; aufgrund der Anonymisierung des Urteils nicht exakt feststellbar!). Die Beweislast für die Verwendung des double-opt-in Systems liegt beim Werbe-Versender.

3. In den Zusendungen müssen echte Informationen für den Kunden enthalten sein, wie Sonderangebote, neue Produkte, Hinweise etc. Diese Information sollte zumindest in den Grundzügen schon in der Mail selbst stehen und nicht erst auf der Webseite, welche der Kunde besuchen soll. Schon aufgrund der Mail muss eine echte Entscheidung möglich sein, ob das Angebot für den Empfänger relevant ist oder nicht.
4. Die Mails sollten einigermaßen kurz und optisch gut gestaltet sein, keine besonderen Attachments enthalten sowie mit allen E-Mail-Programmen gelesen werden können.
5. Bereits aus der Subject-Zeile sollte hervorgehen, dass es sich um Werbung handelt bzw. welchen Inhalt die Mail hat. Schon danach sollte eine Vorauswahl möglich sein.

I.3. Messenger-Popups

Eine weitere Art der Werbung ist die "Zusendung" von Popup-Mitteilungen. Hierbei wird ungefragt ein Fenster (Betriebssystem, nicht Browser, daher unabhängig vom Web-Surfen!) auf dem Bildschirm des Empfängers mit einem beliebigen, hier wohl Werbung enthaltenden, Text geöffnet. Nur durch die Ausnutzung spezieller Protokolle, wie etwa dem MS Windows Befehl "net send", wird dies möglich. Solche Befehle dienen typischerweise administrativen Mitteilungen, wie dass der Server abgeschaltet wird, Benachrichtigungen von Drucker-Warteschlangen etc. Glücklicherweise ist eine technische Verhinderung relativ einfach möglich: Derartige NetBios-Pakete sollten durch eine Firewall in keinem Fall weitergeleitet werden, da sie nur in einem lokalen Netzwerk Sinn machen, sodass alles von außen kommende unterbunden wird. Damit wird es auch Dritten unmöglich, Mitteilungen an einen Computer zu senden, ohne nützliche Verwendungen innerhalb eines Unternehmens zu behindern. Quellen innerhalb des Firmennetzes[89] sind davon klarerweise nicht betroffen, doch ist dort die Zurückverfolgung technisch sehr einfach und eine Unterbindung auch rechtlich problemlos (Weisung an Arbeitnehmer).

Popups sind noch störender als E-Mails und sogar Telefonanrufe, da nicht einmal die Zeit frei bestimmbar ist und keine Ablehnungsmöglichkeit (=Nicht-Abheben) besteht: Popups können z.B. auch ungefragt und mitten während einer Präsentation auftauchen. Da kein Opt-out möglich bzw. vorgesehen ist[90] und auch keine Robinson-Listen existieren, wäre auch keine der sonstigen Rechtshandhaben dagegen möglich. Rechtlich gesehen handelt es sich wohl um eine Sonderform der "el. Post"[91], sodass die Regeln für E-Mails anzuwenden sind, wobei jedoch der Störfaktor noch stärker ist und sogar über den von Telefonanrufen hinausgeht. Als Werbung könnte sie daher nur nach explizitem Einverständnis verwendet werden.

I.4. Meta-Tags

Bei Meta-Tags handelt es sich um für den Surfer unsichtbare Informationen auf Webseiten für Suchmaschinen. Sie dienen dazu, Schlüsselwörter und eine Beschreibung der Webseite sowie sonstige Metadaten zu speichern. Aufgrund vielfachen Missbrauchs werden diese Daten von Suchmaschinen inzwischen nur mehr in geringem Umfang berücksichtigt.

---

[89] Problematisch können hier offene WLANs sein. Sie sind jedoch ganz allgemein aus Sicherheitsgründen zu vermeiden.

[90] Eine direkte Rückantwort ist unmöglich, E-Mails oder Webadressen müssten händisch abgeschrieben/kopiert werden.

[91] "Post" darf nicht zu eng gesehen werden. Laut dem Gesetz umfasst diese auch SMS, welche Popups stark ähneln.

Als Konzept an sich sind derartige Techniken rechtlich kein Problem[92]. Schwierigkeiten treten erst im Zusammenhang mit dem konkreten Inhalt auf. Relevant werden Meta-Tags hauptsächlich in zwei Fällen: Wörter ohne Bezug zum Inhalt sowie geschützte Wörter, typischerweise Markennamen. Die Grundprinzipien gelten weiters für ähnliche Werbeformen, von denen nur Word-Stuffing kurz erläutert wird.

I.4.1. Verwendung von Wörtern ohne/mit geringem Bezug zum Inhalt

Derartige Wörter sollen dazu dienen, auch auf (teilweise) "sachfremde" Anfragen bei Suchmaschinen hin in der Trefferliste zu erscheinen.

Da es sich bei Wörtern ohne Bezug zum Inhalt eben um nicht-verwandte Begriffe handelt, kann auch nicht mit unlauterem Anlocken bzw. Abfangen von Kunden argumentiert werden, weil der Konkurrenz nichts weggenommen wird, da eben noch kein auch nur einigermaßen konkreter Kaufentschluss getroffen ist[93]. Ebenso kann normalerweise keine Subsumption unter den Begriff der irreführenden Werbung[94] erfolgen, da ebenfalls keine potentiellen Kunden betroffen sind[95]. Erst wenn trotz fehlenden Bezugs ein solcher suggeriert wird, könnte dies relevant werden[96]. Ev. könnte eine solche Praxis als übertriebenes Anlocken qualifiziert werden. Praktisch besitzt diese Art der Werbung wohl geringe Bedeutung, insbesondere auch durch die Anstrengungen der Suchmaschinen ausschließlich passende Websites als Ergebnis aufzulisten.

Anders ist die Sachlage zu beurteilen, sollte zumindest ein gewisser Zusammenhang zu den angebotenen Produkten bzw. Dienstleistungen bestehen[97], also wenn potentiell an derartigen Produkten interessierte Verkehrskreise angesprochen werden. Entgegen der Ansicht des OLG im angeführten Fall ist meiner Meinung nach sehr wohl ein übertriebenes Anlocken darin zu sehen, mit Schlüsselwörtern mit geringem, aber doch vorhandenem Bezug zu werben. Es werden insbesondere diejenigen Verkehrskreise angesprochen (Angehörige von Rechtsberufen), welche potentielle Kunden darstellen, wobei diese jedoch bei der Suche (noch) keinerlei Interesse für die angebotenen Produkte zeigen, sondern im Augenblick eben für andere Gebiete. Auch die Argumentation, dass bei Suchmaschinen keine "Sortenreinheit" besteht, d.h. sich unter Suchergebnissen auch unpassende befinden, geht meiner Meinung nach fehl. So existiert zwar keine Reinheit, doch wird diese sehr stark angestrebt und ist vielfach auch in gewissem Ausmaß gegeben[98]. Selbst wenn durch die Beschreibung auf den ersten Blick erkennbar sein sollte, um welche Produkte es sich han-

---

[92] Siehe Thiele, Meta-Tags und das österreichische Wettbewerbsrecht. ÖJZ 2001, 168 sowie Jaeschke, Die höchstrichterliche Rechtsprechung zum gewerblichen Rechtsschutz und geistigen Eigentum unter informationsrechtlichen Gesichtspunkten

[93] Jahn/Häussle, Aktuelle Entscheidungspraxis zum Internet im Bereich des gewerblichen Rechtsschutzes (Teil II), GesRZ 2003, 144, Unter V A 1

[94] Das Beispiel von Zankl, OGH erlaubt meta-tags im Internet, AnwBl 2001, 316 dass der Sucher nach Pornographie in den Suchergebnissen auf einen Buchladen trifft und daher dort Bücher kauft, ist jedoch eher als theoretisch anzusehen.

[95] Ein konventionelles Analogon wäre die Verteilung von Werbezetteln für Pelzmäntel bei Fußballspielen: Unpassend und nicht sehr zielführend, und daher wohl kaum wettbewerbswidrig.

[96] So ohne nähere Begründung Pierson: Online-Werbung nach der UWG-Reform – Zusammenfassende Übersicht. JurPC Web-Dok. 139/2006

[97] Siehe "Keywords in Meta-Tags. OLG Düsseldorf 1.10.2002, 20 U 93/02 http://www.jurpc.de/rechtspr/20030072.htm sowie die vorherige entgegengesetzt lautende Entscheidung des LG. Konkret wurde die Verwendung von "Urteil, Entscheidungen, StVO, ..." durch ein Geschäft, das Roben für Rechtsanwälte, Richter etc. anbietet, nicht beanstandet.

[98] Genau dies ist ein wichtiger Punkt bei der Auswahl der verwendeten Suchmaschine: Ob viele unpassende Ergebnisse angezeigt werden oder nicht.

delt, so ist allein schon die Darstellung auf der Suchergebnis-Seite eine Werbung: Die Bekanntmachung des Namens und die Anregung, dass ein Bedürfnis nach solchen Produkten bestehen könnte.

I.4.2. Verwendung von Namen, Marken etc. der Konkurrenz

Viel problematischer ist die Verwendung fremder Marken oder Firmennamen, insbesondere wenn es sich hierbei um Konkurrenzunternehmen handelt. Hier können u.A. Markenrecht, z.B. unberechtigte Verwendung fremder Marken, und Wettbewerbsrecht, etwa Ausbeutung fremder Leistung oder Abfangen von Kunden, schlagend werden[99].

Bei der Beurteilung ist hier wichtig, dass beim Markenrecht ausschließlich Handeln im geschäftlichen Verkehr von Bedeutung ist, sodass sich für Private solche Probleme nicht stellen. Voraussetzung ist in vielen Fällen weiters, dass die Marke auch kennzeichenmäßig gebraucht wird. Ob dies beim Einfügen als Meta-Tag der Fall ist, ist strittig[100], aber wohl zu bejahen[101]. Zwar ist sie auf diese Art nicht unmittelbar sichtbar, doch bei einer Suche nach dieser Marke erscheint die "falsche" Webseite in der Ergebnisliste und erzeugt damit den Anschein einer besonderen Beziehung zu dem weiter oben angeführten Suchbegriff. Auch hier muss die Marke nicht unmittelbar sichtbar werden, doch entspricht dies einer Eintragung in einem Branchentelefonbuch unter der Rubrik des Namens genau dieser Marke (ohne sie allerdings nochmals zu erwähnen). Anstatt dort nur autorisierte Vertriebspartner oder Filialen zu finden, ist die Konkurrenz eingetragen, was wohl eindeutig für eine Verwendung der Marke als Kennzeichen spricht. Dies ist deshalb meiner Meinung nach unzulässig[102].

Das OLG Düsseldorf vertritt hingegen die Meinung, dass die Verwendung einer Marke in Meta-Tags keine kennzeichenmäßige Benützung darstellt[103], da die Marke nicht direkt wahrgenommen werden kann. Es handle sich um eine bloße Kennzeichen-Nennung, aber nicht um eine Benützung. Daher wäre eine Verwendung praktisch frei möglich. Dies war jedoch eine Mindermeinung und wurde inzwischen vom BGH zurückgewiesen[104]: Maßgeblich ist, dass mit Hilfe des Suchwortes (=der fremden Marke) das Ergebnis des Auswahlverfahrens beeinflusst wird und der Nutzer zur entsprechenden Ziel-Site (=der Konkurrenz) geführt wird.

---

[99] Details dazu in Thiele, Meta-Tags und das österreichische Wettbewerbsrecht. ÖJZ 2001, 168

[100] Kein kennzeichenmäßiger Gebrauch liegt bei Verwendung der catch-all Funktion eines Domainnamens vor, da die Marke dort überhaupt nirgends eingetragen und damit tatsächlich unsichtbar ist. Erst die Eingabe durch den Benutzer "erzeugt" die Darstellung der Marke. OGH 12.7.2005, 4 Ob 131/05a Der Leitsatz 1 in MR 2005, 446 ist verfehlt formuliert, da das Urteil genau darüber nicht abspricht, sondern nur die Literatur wiedergibt. Die catch-all Funktion stellt im Gegensatz zu Meta-Tags auf gar keine bestimmte einzelne, oder anders gesagt gleichzeitig sowohl auf alle derzeit wie auch zukünftig existierenden, Marken ab.

[101] So auch Stomper, Markenrechtliche Aspekte bei Meta-Tags. MR 2002, 340

[102] Siehe "Numtec Interstahl" OGH 19.12.2000, 4 Ob 308/00y, wo dies offen gelassen wird, aber wohl eher von einer Benutzung ausgegangen wird (Entscheidung: jedenfalls gerechtfertigt). Dies eindeutig bejahend: LG München I 24.6.2004, 17HK 0 10389/04 http://www.aufrecht.de/3355.html

[103] OLG Düsseldorf: 1.10.2002, 20 U 93/02 http://www.aufrecht.de/2605.html; 15.7.2003, 20 U 21/03 http://www.aufrecht.de/2024.html, anders jedoch zu diesem Fall der BGH, siehe FN 104; 17.2.2004, I 20 U 104/03 http://www.aufrecht.de/3235.html. Ebenso 14.2.2006, I-20 U 195/05 . Eine Übersicht über die Deutsche Rechtsprechung bringt Terhaag, Lichtblick im Tunnel neuerer Meta-Entscheidungen - München hält den aktuellen Entwicklungen aus Düsseldorf stand http://www.aufrecht.de/3317.html

[104] BGH 18.5.2006, I ZR 183/03 "Metatags"/"Impuls"

Dies bedeutet jedoch nicht, dass keinerlei Verwendung fremder Marken in Meta-Tags erlaubt ist[105]: Besteht ein berechtigtes Interesse an der Verwendung und entsteht dadurch kein falscher Eindruck, kann auch das Einfügen als Meta-Tag nicht untersagt werden. Berechtigte Interessen sind etwa Verkauf von Produkten dieser Marke[106], Bereitstellung von Informationen darüber, oder bei gesetzeskonformer vergleichender Werbung. Wird also die Marke zusätzlich im Inhaltstext der Seite verwendet und erfolgt dies dort rechtmäßig, so kann sie auch als Meta-Tag verwendet werden[107]. Eine Ausnahme gilt nur dann, wenn die Verhältnismäßigkeit fehlt: Eine flüchtige und unbedeutende Erwähnung am Rande im Seiteninhalt reicht wohl nicht aus, eine Marke in den Meta-Tags anzuführen[108, 109].

I.4.3. Word-Stuffing

Word-Stuffing beruht darauf, Wörter, welche die Webseite besonders gut beschreiben, wenn möglich am Beginn der Seite (oder auch am Ende) und möglichst oft im Text anzuführen. Diese häufige Wiederholung soll zu einem besseren Platz in den Ergebnislisten von Suchmaschinen führen. Um menschliche Benutzer nicht zu irritieren werden die Texte jedoch unsichtbar dargestellt, z.B. weiß auf weißem Hintergrund, extrem kleine Schrift, oder überlagert von anderen Elementen. Mittlerweile sind die meisten Suchmaschinen jedoch in der Lage, solche Versuche zu erkennen und zu ignorieren. Vielfach werden sie sogar explizit "bestraft", indem derartige Seiten schlechtere Platzierungen erhalten.

Es ergeben sich keine rechtlichen Unterschiede zu Meta-Tags aufgrund der Technik[110]: Es handelt sich nur um eine andere "Unterbringung" der Wörter. Sie sind wiederum für den normalen Benutzer unsichtbar und nur für Suchmaschinen gedacht. Die obigen Ausführungen sind daher identisch auch auf weitere ähnliche Techniken, z.B. externe Metadaten entsprechend der Dublin Core Spezifikation, anzuwenden: Bei allen "versteckten" Daten zur Beeinflussung der Ergebnislisten von Suchmaschinen kommen die gleichen Grundprinzipien zur Anwendung.

I.5. Keyword Advertising

Bei Keyword Advertising werden von Suchmaschinen zu den jeweils eingegebenen Suchbegriffen "passende" bezahlte Anzeigen dargestellt. In der Praxis erfolgt dies so, dass der Werbende bestimmte Suchwörter bestimmt, bei welchen seine Mitteilung dann erscheinen soll. Die Auswahl erfolgt daher im Allgemeinen nicht durch die Suchmaschine bzw. nur zwischen mehreren Werbenden für dasselbe Suchwort, wobei verschiedene Mechanismen Verwendung finden können, z.B. Versteigerungen.

---

[105] OGH 19.12.2000, 4 Ob 308/00y mit Anmerkung von Thiele, http://www.eurolawyer.at/pdf/OGH_4_Ob_308-00y.pdf

[106] "Aidol" BGH 8.2.2007, I ZR 77/04: Metatags bzw. weiß-auf-weiß Schrift sind keine Markenverletzung insofern sie sich auf Webseiten befinden, auf der konkrete Originalprodukte angeboten werden (=Erschöpfung des Markenrechts).

[107] So auch Schanda in der Anmerkung zu OGH 19.12.2000, 4 Ob 308/00y, ecolex 2001, 158

[108] Siehe Stomper, Markenrechtliche Aspekte bei Meta-Tags. MR 2002, 340.

[109] Kommt die Marke im Text überhaupt nicht vor, kann wohl auch nicht von einer berechtigten Nutzung in Meta-Tags ausgegangen werden: Die bloße Möglichkeit einer Verwendung im Inhalt führt nicht dazu, dass ein berechtigtes Interesse an der Verwendung als Meta-Tag besteht, da dann ja nicht der Inhalt der Seite beschrieben wird.

[110] Siehe FN 106!

Solange es sich bei den ausgewählten Suchwörtern um allgemeine Gattungs- und Sachbegriffe handelt, stellen sich keine Probleme[111]: Jeder darf damit werben, "Bücher" zu verkaufen. Wird jedoch hierzu ein fremder Markenname[112] verwendet, können sich marken- und wettbewerbsrechtliche Probleme stellen. Es kann sich etwa um unlauteres Abfangen von Kunden handeln, wenn bei der Suche nach einer bestimmten Marke die Werbung der Konkurrenz besonders aufdringlich erscheint[113]. Separat zu beurteilen ist jedoch immer die Verwendung fremder Markennamen in der Anzeige selbst: Hier besteht kein Unterschied zur Offline-Rechtsprechung der Verwendung z.B. in Zeitungsanzeigen.

Außer in besonderen Fällen ist die Verwendung fremder Marken als bloßer Auslöser jedoch kein markenrechtliches Problem[114]: Der Unterschied zu Meta-Tags liegt darin, dass die beworbene Webseite nicht unter den normalen Suchergebnissen aufscheint, sondern separat, und dort auch explizit als Werbung gekennzeichnet ist[115]. Dadurch liegt zwar eine markenmäßige Verwendung vor (strittig), diese ist jedoch jedenfalls mangels Verwechslungsgefahr nicht zu beanstanden[116] (ebenfalls strittig): Nutzer bringen getrennt angezeigte Werbung nicht direkt mit dem eingegebenen Markennamen in Verbindung, sodass allein wegen dem Anzeigen der Werbung kein besonderes Naheverhältnis erwartet wird[117]. Auch eine Behinderung des Markeninhabers liegt nicht vor, da dieser wie bisher an normaler Stelle im Suchergebnis aufscheint. Dies gilt wohl selbst dann, wenn die Anzeige direkt über der Trefferliste angeordnet ist (besonders strittig; ev. vom OGH als unzulässig beurteilt): Auch dort ist die Trennung klar und die Annahme, dass Suchende diese als Treffer ansehen oder irrtümlich darauf klicken, wohl fehlerhaft. Es handelt sich lediglich um eine "prominentere" Platzierung, analog einem Werbeplakat auf der Hauptstraße im Vergleich zu einem in einer Nebenstraße.

---

[111] Jahn/Häussle: Aktuelle Entscheidungspraxis zum Internet im Bereich des gewerblichen Rechtsschutzes (Teil II). GesRZ 2003, 144. Anders ev., wenn keinerlei Zusammenhang zum eigenen Angebot besteht. Siehe hierzu I.4.1! Die "stellen-online.de AG" kann nicht verhindern, dass ein Konkurrent "Stellen online" als Werbung bucht (bzw. über "weitgehend passende Keywords" besetzt), da beschreibende Begriffe für alle frei sind: OLG Karlsruhe 26.9.2007, 6 U 69/07

[112] Oder Unternehmensbezeichnung oder sonstige Begriffe, auf die eine Person ein Ausschließlichkeitsrecht besitzt.

[113] Siehe den besprochenen Fall in Thiele: Keyword-Advertising – lauterkeitsrechtliche Grenzen der Online-Werbung, RdW 2001, 492. Hier war zusätzlich die Anzeige der tatsächlichen Suchergebnisse verzögert, sodass anfangs ausschließlich das (bezahlte) Werbebanner sichtbar war. Ebenso Seidelberger: Wettbewerbsrecht und Internet, RdW 2000, 500

[114] Sehr strittig: Gerichtsentscheidungen divergieren stark! Für einen Überblick (die eigenen Stellungnahmen können nicht ganz überzeugen) siehe Kump/Dippelhofer: Google-Adwords zu den Marken der Konkurrenz – legitime Werbung oder Rechtsverletzung? Ebenso für eine differenziierende Betrachtung, aber mit der Grundvermutung einer Verletzung Jaeschke, Die höchstrichterliche Rechtsprechung zum gewerblichen Rechtsschutz und geistigen Eigentum unter informationsrechtlichen Gesichtspunkten

[115] Siehe etwa OLG Frankfurt 26.2.2008, 6 W 17/08. Wird daher nicht "externe" Werbung verkauft, sondern unmittelbar und ohne besondere Kennzeichnung ein (bestimmter) Platz in der Ergebnisliste, gelten diese Überlegungen nicht. In diesem Fall ist auf die Erörterungen zu Meta-Tags zu verweisen, wonach solches Verhalten verboten ist.

[116] So OLG Wien 14.7.2005, 1 R 134/05s "Glucochondrin", das die Verwechslungsgefahr verneint. Zum selben Fall der OGH 19.12.2005, 4 Ob 194/05s: Die Anzeigen sind nicht so aufdringlich gestaltet, dass sie vom eigentlichen Suchergebnis ablenken oder dieses überhaupt verdrängen; aber keine konkrete Entscheidung über Marken- oder Wettbewerbsrecht. Das LG Hamburg 21.9.2004, 312 O 324/04 hingegen geht, wohl fälschlicherweise, von gar keiner markenmäßigen Verwendung aus (stellt aber fest, dass eben kein Bezug Marke ⇔ Anzeige besteht). Siehe auch LG Leipzig 08.02.05, 5 O 146/05, das anscheinend nur im konkreten Fall die markenmäßige Benutzung verneint, da die Marke nicht unterscheidungskräftig war. Äußerst unklar OGH 20.3.2007, 17 Ob 1/07g, wonach eine Anzeige über der Suchergebnisliste wohl verboten wäre, eine daneben hingegen eher nicht. Siehe dazu auch die Anmerkungen von Noha, http://www.internet4jurists.at/literatur/noha_adwords2007.pdf

[117] Genau dies nimmt etwa OLG Braunschweig 12.7.2007, 2 U 24/07 an: Der Verkehr gehe davon aus, dass sowohl in Trefferliste als auch Anzeigen (nur?) Produkte einer Marke zu finden sind, für die die Suchanfrage durchgeführt wurde. ME nach ist dies eher zweifelhaft. Explizit entgegengesetzt OLG Köln, 31.8.2007, 6 U 48/07: Nutzer haben bei Anzeigen gerade keine herkunftsbezogenen Vorstellungen und differenzieren zwischen Ergebnisliste und Anzeigen. Noch genau entgegengesetzt die Vorinstanz in LG Köln, 9.2.2007, 81 O 174/06.

Problematisch ist hingegen der wettbewerbsrechtliche Aspekt: Ein sittenwidriges Abfangen von Kunden oder Rufausbeutung können vorliegen. Die bloße und getrennte Anzeige von Werbung ist zwar wohl noch erlaubt, ebenso wie in einer Zeitung neben einem Artikel über eine Marke Werbung für die Konkurrenz erscheinen darf[118]. Die meisten Entscheidungen und Literaturstellen gehen jedoch von einem Verbot aus, zumindest was Marken bzw. Bezeichnungen der Konkurrenz betrifft[119]. Dies kann jedoch nicht ganz überzeugen. Es kommt mM nach darauf an, ob z.B. Kunden schon einen konkreten Kaufentschluss gefasst haben und nur mehr nach einem Verkäufer suchen, oder ob sie sich allgemein informieren möchten. Hier ist eine Beurteilung des vorherrschenden Verhaltens bzw. der Verkehrsansicht schwierig, wobei in der Praxis wohl eher die allgemeine Suche verwendet wird, sodass auch kein Kundenabfangen vorliegen würde[120]. Handelt es sich um Bezeichnungen von tatsächlich verkauften Produkten, so kann dies keinesfalls beanstandet werden[121].

Besondere Vorsicht ist erforderlich, wenn die Suchworte zu denen die Werbung erscheinen soll, nicht explizit vorgegeben werden. Google ermöglicht es etwa, eine Option namens "weitgehend passende Keywords“ einzuschalten. Hierbei wird die Werbung auch bei Suchwörtern angezeigt, die von Google als ähnlich zu den explizit für die Anzeige eingegebenen Wörtern angesehen werden. Die Ähnlichkeit beruht hier nicht auf einer Wortähnlichkeit sondern der Auswertung von Suchanfragen/-ergebnissen. Hier kann Ausbeutung eines fremden Rufs bzw. Kundenumleitung vorliegen[122].

Wichtig in dem Zusammenhang ist weiters die Haftung des Betreibers der Suchmaschine für etwaige Rechtsverletzungen durch die Anzeigen. Hierzu ist festzuhalten, dass sie nicht selbst als Störer tätig wird, sondern allenfalls als Gehilfe[123]. Auch hier trifft den Betreiber keine Verpflichtung zur aktiven Suche nach Rechtsverletzungen. Eine Haftung besteht daher nur dann, wenn bewusste Förderung, d.h. Kenntnis von den tatsächlichen Umständen, vorliegt und die Rechtsverletzung auch für juristische Laien offensichtlich ist[124].

---

[118] LG Hamburg 21.12.2004, 312 O 950/04. Eine solche Platzierung darf auch explizit verlangt werden.

[119] Siehe Anderl, RdW 2006/129, 143, der in der Verwendung fremder Marken als AdWords generell ein sittenwidriges Abfangen von Kunden sieht. Hierbei wird nicht berücksichtigt, dass Meta-Tags und AdWords sich in einem ganz wichtigen Punkt unterscheiden: Meta-Tags beeinflussen die normale Ergebnisliste, während AdWords eine separate und als Werbung gekennzeichnete Anzeige erzeugen. Die "Distanz" zum "Besitzer" des betroffenen Wortes ist daher bei Meta-Tags weitaus geringer als bei AdWords. Ähnlich LG Braunschweig 28.12.05, 9 O 2852/05

[120] Ähnlich, allerdings zu einem Gattungsbegriff OLG Karlsruhe 26.9.2007, 6 U 69/07

[121] Beispiel: Coca-Cola darf "Pepsi-Cola" nicht als AdWord buchen (→ Sittenwidrig). Ein Getränkehändler der beide Getränke verkauft jedoch sehr wohl, sofern nicht zusätzliche Umstände hinzukommen, die an Rufausbeutung denken lassen. Als Meta-Tag wäre dies jedoch eher nicht mehr erlaubt: Mit der Marke darf zwar Werbung betrieben werden (=AdWords), jedoch besteht keine so enge Beziehung, als dass man in der Ergebnisliste auftauchen könnte. Anders wiederum ev. wenn es sich um ein Spezialgeschäft für Cola-Getränke handeln würde.

[122] OLG Köln, 8.6.2004, 6 W 59/04 Gebuchtes Suchwort war "Flüssiggas". Durch die Option wurde die Werbung auch dann angezeigt, wenn als Suchwort der Name einer Konkurrenzfirma eingegeben wurde. Hierbei bestehen Ähnlichkeiten zur Verwendung der catch-all Funktion bei Domain Namen.

[123] Anders und verfehlt Thiele, Keyword-Advertising – lauterkeitsrechtliche Grenzen der Online-Werbung, RdW 2001, 492: Der Verkauf von Suchbegriffen (was gerade nicht erfolgt: Nicht die Suchmaschine stellt bestimmte Begriffe zur Verfügung, sondern der Werbende bzw. der Suchende gibt diese ein!) führe zu einer direkten Haftung wegen Anmaßung der Nutzungsrechte an der Marke. Durch das Anzeigen von Werbung beim „Auftauchen“ bestimmter Wörter wird jedoch sicherlich kein Recht an diesen Wörtern behauptet, sondern bestenfalls dass deren Nutzung nicht verboten ist.

[124] "Glucochondrin": OGH 19.12.2005, 4 Ob 195/05p mit Anmerkung von Noha, ecolex 2006, 93

Zusammenfassend kann daher festgestellt werden, dass zu Keyword Advertising weder eine gefestigte Rechtsprechung noch eine einheitliche Lehrmeinung besteht. Daher ist bei fremden Marken Vorsicht empfehlenswert.

I.6. Literatur

I.6.1. Allgemein

Anderl, Axel: Aktuelles zum Keyword-Advertising, RdW 2006/129, 143 http://www.dbj.at/publ343.pdf

Baldwin, Lawrence: MyNetWatchman Alert – Windows Popup Spam: http://www.mynetwatchman.com/kb/security/articles/popupspam/

Coalition Against Unsolicited Commercial Email: http://www.cauce.org/

Fellner, Georg: Spam-SMS und Werbung zur Inanspruchnahme von Mehrwertdiensten. Master Thesis 2003. http://www.it-law.at/papers/Fellner_Spam_SMS.pdf

IRTF Anti-Spam Research Group (ASRG): http://asrg.sp.am/

Jaeschke, Lars: Die höchstrichterliche Rechtsprechung zum gewerblichen Rechtsschutz und geistigen Eigentum unter informationsrechtlichen Gesichtspunkten, Jur-PC Web-Dok. 10/2008, http://www.jurpc.de/aufsatz/20080010.htm

Jahn, Harald, Häussle, Klaus: Aktuelle Entscheidungspraxis zum Internet im Bereich des gewerblichen Rechtsschutzes (Teil II), GesRZ 2003, 144

Jahnel, Dietmar: Datenschutz im Internet. ecolex 2001, 84-89

Kanich, Chris, Kreibich, Christian, Levchenk, Kirill, Enright, Brandon, Voelker, Geoffrey M., Paxson, Vern, Savage, Stefan: Spamalytics: An Empirical Analysis of Spam Marketing Conversion. http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf

Kraft, Thomas: Der neue § 107 TKG - Verbesserter Schutz vor unerbetenen Werbemails? ecolex 2006, 252

Kresbach, Georg: E-Commerce. Nationale und internationale Rechtsvorschriften zum Geschäftsverlehr über el. Medien. Wien: Linde 2000

Kronegger, Dieter, Riccabona, Elisabeth: Informationen betreffend unerwünschte Werbung mittels el. Post (Spamming): http://www.rtr.at/web.nsf/deutsch/Telekommunikation_Konsumentenservice_E-Commerce-Gesetz/$file/Spam_Infoblatt.pdf

Kump, Patrizia, Dippelhofer, Mischa: Google-Adwords zu den Marken der Konkurrenz – legitime Werbung oder Rechtsverletzung? JurPC Web-Dok. 109/2008. http://www.jurpc.de/aufsatz/20080109.htm

Laga, Gerhard: E-Mail-Werbung 2004: http://rechtsprobleme.at/doks/laga-e-mail-werbung-endg.pdf

Lehofer, Hans Peter: Spamverbot und kommunale Informationstätigkeit. RFG 2006/14

Liston, Tom: Schädlingen auf der Spur. http://www.heise.de/security/artikel/49687

Mayer-Schönberger, Viktor: Warum Ermitteln nicht Erheben ist: Datenschutz und Direktmarketing. ecolex 2004, 417

Noha, Birgit: Anmerkungen zu OGH 19.12.2005, 4 Ob 195/05p "Glucochondrin", ecolex 2006, 93

Osborne, Brian: New "Messenger Spam" invades desktops. http://www.geek.com/news/geeknews/2002Oct/gee20021017016848.htm

Pierson, Matthias: Online-Werbung nach der UWG-Reform – Zusammenfassende Übersicht. JurPC Web-Dok. 139/2006

Rachman, Marc, Kibel, Gary: Online Advertising Challenges Tradition, New York Law Journal 10.10.2005. http://www.dglaw.com/images/OnlinAdvertising19D41C.pdf

Rivard, J.: The Campaign to Stop Junk Email. http://www.jcrdesign.com/junkemail.html

Rosenmayer-Klemenz, Claudia: Neue Rechtsgrundlagen für Adressverlage und Direktmarketingunternehmen. RdW 2003/150

Schanda, Reinhard: Anmerkung zu OGH 19.12.2000, 4 Ob 308/00y, ecolex 2001, 158

Schauer, Bernd: Werbung im Internet. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther, Liebwald, Doris (Hg.): Zwischen Rechtstheorie und e-Government. Wien: Verlag Österreich 2003

Schoberberger, Bernhard: Identifikation und Klassifizierung unerwünschter Nachrichten sowie Spezifikation von Abwehrmaßnahmen. Diplomarbeit. Johannes Kepler Universität Linz, 2000

Seidelberger, Hannes: Wettbewerbsrecht und Internet, RdW 2000, 500

Sonntag, Michael: Webbugs - Wanzen im Internet. In: Schweighofer, Menzel, Kreuzbauer (Hrsg.): IT in Recht und Staat: Aktuelle Fragen der Rechtsinformatik. Wien: Verlag Österreich 2002, 355-362

Stomper, Bettina: Markenrechtliche Aspekte bei Meta-Tags. MR 2002, 340

Terhaag, Michael: Lichtblick im Tunnel neuerer Meta-Entscheidungen - München hält den aktuellen Entwicklungen aus Düsseldorf stand http://www.aufrecht.de/3317.html

Thiele, Clemens: Meta-Tags und das österreichische Wettbewerbsrecht. ÖJZ 2001, 168

Thiele, Clemens: Keyword-Advertising – lauterkeitsrechtliche Grenzen der Online-Werbung, RdW 2001, 492

Thiele, Clemens: Anmerkungen zu OGH 19.12.2000, 4 Ob 308/00y http://www.eurolawyer.at/pdf/OGH_4_Ob_308-00y.pdf

Windows Messenger Delivery options: SMB vs. MS RPC: http://www.mynetwatchman.com/kb/security/articles/popupspam/netsend.htm

Zankl, Wolfgang: OGH erlaubt meta-tags im Internet, AnwBl 2001, 316

I.6.2. Rechtsvorschriften

TKG: Bundesgesetz mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003) BGBl. I Nr. 70/2003, idF BGBl I Nr. 133/2005

Bundesgesetz, mit dem bestimmte rechtliche Aspekte des el. Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG) BGBl. I Nr. 152/2001

Bundesgesetz vom 12. Juni 1981 über die Presse und andere Publizistische Medien (Mediengesetz - MedienG) BGBl. Nr. 314/1981 idF BGBl. I Nr. 151/2005

Gewerbeordnung 1994 (GewO 1994). BGBl. Nr. 194/1994 idF BGBl. I Nr. 15/2006

Fernabsatz-Richtlinie: Richtlinie 97/7/EG des Europäischen Parlamentes und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz. Abl. L 144; 4.6.1997; S 19ff http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:DE:HTML

E-Commerce Richtlinie: Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des el. Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den el. Geschäftsverkehr") ABl. L 178/1; 17.7.2000 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:DE:HTML

Telekom-Datenschutz-RL der EU: Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der el. Kommunikation (Datenschutzrichtlinie für el. Kommunikation) ABl. L 201/37 vom 31.7.2002 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:DE:HTML

CAN-SPAM Act of 2003: http://www.spamlaws.com/federal/can-spam.shtml

I.6.3. Elektronische Robinson-Listen

Robinsonliste des Fachverband Werbung & Marktkommunikation: http://www.fachverbandwerbung.at/de-service-robinsonliste.shtml

Robinsonliste der RTR (offizielle Österreichische E-Mail Robinsonliste): http://www.rtr.at/web.nsf/deutsch/Telekommunikation_Konsumentenservice_E-Commerce-Gesetz

E-ROBINSON: http://www.robinsonliste.de/

Direct Marketing Associtaion (USA): http://www.dmaconsumers.org/optoutform_emps.shtm