TRAUNER VERLAG
UNIVERSITÄT

Schriftenreihe E-Learning

Herausgegeben von
Jörg R. Mühlbacher
Günter Pilz
Bernad Batinic

Michael Sonntag

E-Business Recht

Eine Einführung für Informatiker

Impressum

Schriftenreihe E-Learning

Michael Sonntag
E-Business Recht
Eine Einführung für Informatiker

Herstellung:
Kern: Johannes-Kepler-Universität Linz, A 4045 Linz-Auhof
Umschlag: TRAUNER Druck GmbH & Co KG, A 4020 Linz, Köglstraße 14

ISBN 3-85499-120-7
ISBN 978-3-85499-120-5
www.trauner.at

Michael Sonntag

E-Business Recht

Eine Einführung für Informatiker

Universitätsverlag Rudolf Trauner

Motivation

In diesem Buch mit interdisziplinärer Zielsetzung sollen bestimmte Aspekte der österreichischen (und aufgrund des EU-Beitritts teilweise auch der europäischen) Rechtsordnung dargestellt werden: Gesetze, Vorschriften, Richtlinien, Delikte etc., welche in einem besonderen Zusammenhang mit E-Business bzw. dem Internet oder Netzwerken stehen. Die Zielgruppe dieses Buches sind auf dem Gebiete der Informatik tätige Nicht-Juristen, welche mit den technischen Grundlagen vertraut sind und mehr über die rechtlichen Aspekte wissen möchten, sowie alle an dem Themenkreis Interessierten.

Bei dem Thema „E-Business“ handelt es sich um eine Querschnittsmaterie, welche verschiedenste Gebiete des Zivilrechts wie auch des Strafrechts berührt. Öffentliches Recht (z.B. Telekommunikationsrecht, Vorratsdatenspeicherung) bleibt in dieser Abhandlung jedoch fast vollständig ausgeklammert, da dieses stärker im Zusammenhang mit E-Government, worauf hier nicht eingegangen wird, zu sehen ist.

Die Ausführungen in diesem Buch erheben keinen Anspruch auf Vollständigkeit, sondern stellen nur bestimmte subjektiv ausgewählte Zonen dar, die näher erläutert werden. Die Auswahl erfolgte sowohl nach Gesichtspunkten der Wichtigkeit wie auch der Praxisrelevanz und Didaktik.

Es sollen Grundlagen dargestellt sowie der Blick für die verschiedenen weiterführenden Probleme geschärft werden, sodass der Leser anschließend in der Lage ist, heikle Punkte zu erkennen und fachlichen Rat bei Spezialisten, wie Rechtsanwälten oder Notaren, für dieses besondere Thema einzuholen. Als weiterer Punkt soll dieses Buch auch dazu dienen, das Wissen über rechtliche Verbote und Gebote zu erweitern, da derzeit bei Informatikern oft manches noch als "Kavaliersdelikt" (z.B. Kopien im Zusammenhang mit Webseiten, Framing, E-Mail Werbung) oder weniger wichtig (etwa Datenschutz oder elektronische Signaturen) angesehen wird. Für solch scheinbare Nebensächlichkeiten Aufmerksamkeit und Verständnis zu erwecken ist ein weiteres Anliegen des vorliegenden Werkes.

Linz, 2006

Michael Sonntag

Aktualisierungen und Errata zu Buch und Begleit-CD sind online unter folgender URL einsehbar:
http://elearning.fim.uni-linz.ac.at/

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABGB	Allgemeines bürgerliches Gesetzbuch (ABGB)
AGB	Allgemeine Geschäftsbedingungen
B2B	Business-to-Business
B2C	Business-to-Consumer
BG	Bezirksgericht (Österreich)
BGH	Bundesgerichtshof (Deutschland)
B-VG	Bundes-Verfassungsgesetz (B-VG)
ccTLD	Country-Code Top-Level Domain
CS	Computersystem
d.h.	das heißt
DN	Domain Name
DNS	Domain Name System
DRM	Digital Rights Management
DSG	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)
DSK	Datenschutzkommission
DSRL	Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
ECG	Bundesgesetz, mit dem bestimmte rechtliche Aspekte des el. Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG)
el.	elektronisch
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Gemeinschaften
EuGVVO	Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (EuGVVO)
ev.	eventuell
EVÜ	EG-Römer Übereinkommen vom 19. Juni 1980 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (EVÜ)
EWR	Europäischer Wirtschaftsraum
GewO	Gewerbeordnung 1994 - GewO 1994
gTLD	Generic Top-Level Domain
HGB	Handelsgesetzbuch
ICANN	Internet Corporation For Assigned Names and Numbers
inkl.	inklusive
ISP	Internet Service Provider
IT	Informationstechnologie
KSchG	Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG)
LG	Landesgericht (Österreich)
LG	Landgericht (Deutschland)

MedienG	Bundesgesetz vom 12. Juni 1981 über die Presse und andere Publizistische Medien (Mediengesetz - MedienG)
MSchG	Markenschutzgesetz 1970
NS	Name Server
OGH	Oberster Gerichtshof (Österreich)
OLG	Oberlandesgericht (Deutschland, Österreich)
PIN	Persönliche Identifikationsnummer
RDNHJ	Reverse Domain Name Hijacking
RIS	Rechtsinformationssystem des Bundes
RL	Richtlinie
SigG	Bundesgesetz über el. Signaturen (Signaturgesetz - SigG)
SigRL	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für el. Signaturen
SigVO	Verordnung des Bundeskanzlers über el. Signaturen (Signaturverordnung - SigV)
StGB	Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB)
StPO	Strafprozeßordnung 1975 (StPO)
TAN	Transaktionsnummer
TKG	Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003)
TKK	Telekom-Control-Kommission
TLD	Top-Level Domain
u.a.	unter anderem
u.U.	unter Umständen
UDRP	Uniform Domain Name Dispute Resolution Policy
UrhG	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz)
UWG	Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG
VfGH	Verfassungsgerichtshof (Österreich)
VO	Verordnung
VwGH	Verwaltungsgerichtshof (Österreich)
z.B.	zum Beispiel
ZDA	Zertifizierungsdiensteanbieter

I. Informatik und Recht

Durch das Internet resultiert eine drastische Ausweitung der mit der Informatik verbundenen Rechtsprobleme. Während früher die hauptsächlichen Fragen im Bereich der Softwareentwicklung lagen, etwa im Bereich der Erfüllung der Anforderungen im Pflichtenheft sowie bei Software-Verträgen, verlagert sich der Fokus nunmehr hin zur Online-Abwicklung von Geschäftsprozessen. Zusätzlich ist in vielen Fällen nicht mehr nur nationales Recht bedeutsam, sondern es sind aufgrund der Internationalität des Internets auch weitere, ausländische oder internationale, Vorschriften zu berücksichtigen. Hinzu kommt, dass sowohl in absoluten Transaktionszahlen als auch vom betroffenen Gegenwert her immer mehr Geschäfte über Computer bzw. das Internet abgewickelt werden. Wie die Erfahrung zeigt, werden Rechtsvorschriften besonders dann relevant, wenn es um Geld geht. Diese Phase hat das Internet inzwischen erreicht.

I.1. Rechtliche Regeln und ihre Auswirkungen auf die Informatik

In den Anfangszeiten des Internet verbreitete sich der Mythos des Internets als "rechtsfreier Raum". Inzwischen ist den meisten Personen klar, dass dies so nicht zutrifft, sondern die "normalen" Gesetze auch für das Internet gelten. Zusätzlich ergaben sich neue Herausforderungen, auf welche mit speziellen Rechtsvorschriften reagiert wurde. So können heute drei Schichten, wenn auch ohne scharfe Trennlinien, unterschieden werden:

1. Allgemeines Recht: Hierbei handelt es sich um Rechtsvorschriften, die praktisch unverändert anzuwenden sind. Dazu gehört z.B. die Ehrenbeleidigung: Ob jemand vor zehn physisch anwesenden Menschen oder in einer E-Mail an zehn Personen beleidigt wird, macht keinen Unterschied bezüglich des anzuwendenden Rechts[1]. Im Bereich des E-Business ist für diese Schicht etwa der Vertragsabschluss beispielhaft: Auch bei SMS sind Angebot und Annahme erforderlich. Ein weiteres Beispiel ist der unlautere Wettbewerb, welcher auch im Internet, selbst in den gleichen Fallgruppen wie "klassisch" offline, stattfindet, wenn auch in geringfügig anderer Umsetzung[2].
2. Recht mit gesteigerter Bedeutung oder besonderen Anwendungsfällen: Manche Rechtsvorschriften besitzen ohne Internet nur marginale Bedeutung, so etwa das Namensrecht. In Verbindung mit Domain Namen kommt ihm jedoch eine ganz erhebliche Wichtigkeit zu. Ähnliches gilt für das Urheberrecht: Während früher der Großteil der Bevölkerung kaum damit in Kontakt bzw. Widerspruch kam[3], betrifft dies nun breite Bevölkerungsschichten: Tauschbörsen z.B. für Musik oder Filme, Softwarekopien, Übernahme von Teilen von Webseiten, ...

[1] Es sollte jedoch dabei nicht übersehen werden, dass manches Verhalten durch das Internet leichter wird, öfter vorkommt oder schwerer nachzuweisen ist!

[2] Beispielsweise Werbebanner statt Plakaten oder E-Mails statt Postwurfsendungen.

[3] Raubdrucke von Büchern wurden kaum daheim hergestellt und Tonbandaufnahmen bzw. Fotokopien waren bald durch die Leerkassetten- bzw. Reprographieabgabe legalisiert, sofern nicht ohnehin die Ausnahme der Privatkopie zutraf.

3. IT-Recht: Diese Rechtsvorschriften wurden speziell für Informations- und Kommunikationstechnologie eingeführt und besitzen ohne diese keine Bedeutung. Beispiele hierfür sind der Straftatbestand des Computerbetrugs, welcher ausschließlich bei automationsunterstützter Datenverarbeitung begangen werden kann. Weiters gehören hierzu u.a. die Regelungen über elektronische Signaturen.

Wie aus den Beispielen zu entnehmen ist, betreffen rechtliche Regelungen nicht mehr nur besondere Gruppen, etwa Unternehmer in bestimmten engen Geschäftsbereichen (z.B. Urheberrecht → Verleger), sondern auch breite Teile der Bevölkerung und insbesondere auch alle Informatiker. Wer Software programmiert, muss sich mit dem Urheberrecht vertraut machen[4], wer Waren im Internet verkauft, benötigt Kenntnisse über Domainrecht und Konsumentenschutz[5], und Planer von IT-Systemen, beispielsweise im Fernunterricht[6], haben den Datenschutz zu berücksichtigen[7] etc. All dies sollte nach Möglichkeit schon beim Entwurf[8] berücksichtigt werden, wobei aber einzelne Teile auch erst bei der konkreten Implementierung relevant werden können[9]. Auch können nicht beliebige Sicherheitsmaßnahmen eingeführt werden[10].

Obwohl inzwischen einige Literatur über Rechtsfragen der IT existiert, beschränkt sich deren Zielgruppe meist auf professionelle Rechtsanwender, d.h. Rechtsanwälte, Wirtschaftsjuristen, Notare oder Richter. Dementsprechend sind derartige Werke für Nicht-Juristen und ganz besonders für Techniker schwer verständlich und oft auch mit für diese Zielgruppe wenig bedeutsamen rechtswissenschaftlichen Details gefüllt. Das vorliegende Werk versucht demgegenüber, die Rechtsvorschriften auf eine Art darzustellen, die für Techniker leicht(er) verständlich ist und die thematischen Gebiete nach praktischen anstatt rechtlichen Gesichtspunkten zu ordnen und zu erläutern. Zusätzlich finden sich Verweise auf Literatur oder Rechtsprechung um eine vertiefte Untersuchung zu ermöglichen bzw. auf mögliche Detailprobleme hinzuweisen.

I.2. Kurzeinführung in wesentliche Rechtsaspekte

Um das Verständnis der besprochenen Themen zu erleichtern, werden einige wesentliche Punkte allgemein die Rechtswissenschaft betreffend kurz angesprochen. Hierzu zählen insbesondere die spezifische Fachsprache der Juristerei sowie das Schichtenmodell der Rechtsordnungen.

---

[4] Sonntag, Michael, Chroust, Gerhard: Legal protection of component metadata and APIs. In: Trappl, Robert (Ed.): Cybernetics and Systems 2004. Proc. of the 17th European Meeting on Cybernetics and Systems Research. Wien: Austrian Society for Cybernetic Studies 2004, 445-450

[5] Sonntag, Michael: Das Rücktrittsrecht nach dem Fernabsatzgesetz beim Online-Musikkauf. In: Schweighofer, Erich, Liebwald, Doris, Augeneder, Silvia, Menzel, Thomas (Hrsg.): Effizienz von e-Lösungen in Staat und Gesellschaft. Aktuelle Fragen der Rechtsinformatik. Stuttgart: Boorberg 2005, 419-426

[6] Sonntag, Michael: Datenschutz im Fernunterricht. In: Plöckinger, Oliver, Duursma, Dieter, Mayrhofer, Michael (Hrsg.): Internet-Recht. Wien: Neuer Wissenschaftlicher Verlag 2004, 455-474

[7] Sonntag, Michael: Engineering for Privacy. Reducing personal information and complying to privacy laws. In: Hofer, Christian, Chroust, Gerhard (Ed.): IDIMT-2002. 10th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2002, 205-215

[8] Sonntag, Michael: Legal Engineering. In: Chroust, Gerhard, Hofer, Christian (Eds.): IDIMT-2003. 11th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2003, 91-101

[9] Beispiel: Darf man das Kästchen auf Webseiten neben "Ich habe die AGBs gelesen und akzeptiere sie" automatisch anhaken oder muss der Kunde dies selbst machen?

[10] Sonntag, Michael: Voluntariness of permissions required for security measures. In: Steinmetz, Ralf, Mauthe, Andreas (Eds.): Euromicro 2004. Proc. of the 30th Euromicro Conference. Los Alamitos, IEEE Computer Society 2004, 551-557

I.2.1. Rechtssprache und Abkürzungen

Genau wie die Informatik besitzt auch die Rechtswissenschaft eine eigene "Sprache". Dies beruht auf verschiedenen Gründen, z.B. dem oft hohen Alter von Gesetzen[11], aber insbesondere auch der Notwendigkeit einer exakten Darstellung. "Borgt" sich jemand beispielsweise etwas aus[12], so ist dies rechtlich gesehen höchst unklar: Handelt es sich um "Leihe" (=kostenlos[13]!) oder "Miete"? Und kann man sich auch Software "ausborgen"[14]? Hier wird versucht, besondere Bedeutungen nach Möglichkeit zu vermeiden bzw. diese explizit zu erläutern, sowie Formulierungen zu verwenden, die juristisch ev. etwas unscharf sind, aber dafür den Vorzug der Verständlichkeit für rechtliche Laien besitzen.

In der Rechtssprache werden viele Abkürzungen verwendet, weshalb juristische Bücher oft ein seitenlanges Abkürzungsverzeichnis beinhalten. Auf Abkürzungen wird daher nach Möglichkeit im vorliegenden Werk verzichtet, um bessere Lesbarkeit zu erreichen und auch das unabhängige Studium einzelner Teile zu ermöglichen. Insbesondere bei Bezeichnungen von Gesetzen werden dennoch Abkürzungen verwendet. Deren Titel sind oft sehr lang und komplex[15], sodass der Text unnötig verlängert würde. Solche "Kurzfassungen" werden daher auch hier verwendet und bei der ersten Verwendung erklärt; alternativ erfolgt ein Verweis über Fußnoten.

I.2.2. Rechtsordnungen

Insbesondere im Bereich des E-Business Rechts sind in vielen Fällen mehrere Rechtsordnungen von Bedeutung. Ein vereinfachtes Schichtenmodell ist in Abbildung 1 dargestellt. Im Hinblick auf E-Business sind jedoch die beiden untersten Schichten (Lokal und Regional) in Österreich nicht von Bedeutung, da dort praktisch keine Rechtsnormen erzeugt werden, welche diesen Bereich beeinflussen[16]. Ebenso besitzt die oberste Schicht nur geringe Bedeutung in der Praxis, da dort normalerweise keine unmittelbar verbindlichen Regelungen aufgestellt werden. So beschreibt beispielsweise das TRIPS Abkommen[17] Aspekte des Urheberrechts, muss jedoch erst durch nationale Gesetze umgesetzt werden. Orthogonal dazu stehen die verschiedenen nationalen Rechtsordnungen.

---

[11] Beispiel: Das ABGB stammt aus dem Jahr 1811 und wurde in vielen Teilen niemals novelliert, in anderen hingegen wieder recht häufig, z.B. dem Ehe- und Familienrecht. Siehe etwa § 19 ABGB für eine "originale" Bestimmung: "Jedem, der sich in seinem Rechte gekränkt zu seyn erachtet, steht es frey, seine Beschwerde vor der durch die Gesetze bestimmten Behörde anzubringen. Wer sich aber mit Hintansetzung derselben der eigenmächtigen Hülfe bedienet, oder, wer die Gränzen der Nothwehre überschreitet, ist dafür verantwortlich." Abgesehen von der Rechtschreibung wäre auch die Wortwahl heute wohl deutlich anders!

[12] So ist etwa rechtlich gesehen das "Ausborgen" von Zucker nicht möglich, da er durch die Nutzung verbraucht wird. Hier kann es sich beispielsweise um eine Schenkung handeln. Anders hingegen z.B. bei der metallenen Zuckerdose.

[13] Juristisch: „unentgeltlich“

[14] Miete ist etwa bei Software durchaus möglich. Es sind jedoch die Lizenzbestimmungen zu beachten, welche eine Weitervermietung gekaufter Software meist verbieten. Ebenso darf es durch die Vermietung naturgemäß nicht zu einer mehrfachen Nutzung kommen.

[15] Siehe etwa die Titel von Rechtsakten der EU: Dort ist im Titel meist eine Erklärung enthalten, wer genau etwas festsetzte und wann dies geschah. Beispiel: ´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")´. Diese wird oft als "E-Commerce Richtlinie", "E-Commerce RL", oder "EC-RL" bezeichnet.

[16] Unter die Landeszuständigkeit fällt etwa der Datenschutz für Dateien, welche *nicht* automationsunterstützt verarbeitet werden, d.h. Zettel-Karteien.

[17] Agreement on Trade-Related Aspects of Intellectual Property Rights, http://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm. Dieses ist als internationals Abkommen auf der globalen Ebene anzusiedeln.

Abbildung 1: Schichtenmodell der Rechtsordnung

Von unmittelbarer Bedeutung ist daher das nationale Recht, wobei hier lediglich das österreichische behandelt wird. Gleich wichtig aufgrund der Internationalität des E-Business ist das supranationale Recht, d.h. für Österreich das Recht der Europäischen Union. EU-Recht wird im Wesentlichen in zwei hier interessanten Formen erzeugt: Richtlinien und Verordnungen[18]. Während Verordnungen unmittelbar gelten und direkt wie nationales Recht anzuwenden sind, müssen Richtlinien erst in nationales Recht "umgegossen" werden. Eine direkt Berufung auf letztere ist nur in wenigen besonderen Ausnahmefällen möglich.

Analog zu den Rechtsordnungen besteht auch eine Hierarchie der Gerichte[19]. Zuerst zuständig sind die nationalen Gerichte, wobei der Rechtszug normalerweise beim Obersten Gerichtshof (OGH) endet[20]. In einzelnen Fällen, insbesondere wenn es um die Auslegung von EU-Recht geht, wird ev. noch der Europäische Gerichtshof (EuGH) eingeschaltet, indem das oberste nationale Gericht eine Rechtsauskunft bei diesem einholt (Vorabentscheidungsverfahren), um sicherzustellen, dass das Recht der Europäischen Union in der gesamten Union einheitlich interpretiert wird.

I.2.3. Die Bedeutung von Entscheidungen

Rechtsordnungen können grob in zwei Kategorien eingeteilt werden: Kontinentales Recht (auch "civil law" genannt) und Fallrecht ("common law"). In ersterem Fall wird Recht durch die Erlassung von Gesetzen erzeugt (siehe oben), im zweiten Fall durch die Entscheidungen von Richtern. Diese Einteilung ist inzwischen nicht mehr sehr scharf, da etwa das Straf- und Prozessrecht auch in England und den USA (→ common law) stark durch Gesetze geregelt ist, während in Kontinentaleuropa Gerichtsentscheidungen ebenso gewisse rechtsbildende Bedeutung besitzen. Als Beispiel kann unlauterer Wettbewerb dienen. § 1 UWG[21] legt fest, dass Verstöße gegen die guten Sitten für Wettbewerbszwecke im geschäftlichen Verkehr verboten sind. Was nun jedoch im Wettbewerb als "unsittlich" anzusehen ist, wurde und wird durch die Gerichte genauer festgelegt. So besteht zwar keine Bindung von Gerichten an frühere Entscheidungen, aber ein Urteil, das anders lautet als die ständige Rechtsprechung des Obersten Gerichtshofs (OGH), wird wahrscheinlich von höheren Instanzen aufgehoben werden, woraus sich eine praktische, wenn auch nicht rechtliche Bindung ergibt.

---

[18] Achtung: Österreichische Verordnungen sind im Gegensatz zu Verordnungen der EU *keine* Gesetze sondern allgemeine Anordnungen von Verwaltungsbehörden!

[19] Stark verkürzte Darstellung: Sollte es bei den hier behandelten Themen zu einem Gerichtsverfahren kommen, ist ohnehin ein Anwalt mit detaillierten Kenntnisse unentbehrlich.

[20] In Zivilrechtssachen, z.B. Vertragsstreitigkeiten. Handelt es sich um Rechte aus Verfassungsgesetzen (sowie in einigen anderen Sonderfällen) kann auch noch der Verfassungsgerichtshof (VfGH) angerufen werden.

[21] BG gegen den unlauteren Wettbewerb, BGBl. Nr. 448/1984

Insbesondere dann werden Entscheidungen wichtig, wenn kein entsprechend detailliertes Gesetz existiert bzw. neue Probleme auftreten. Beides traf auf das Recht im Internet zu, sodass dort Entscheidungen auch im Bereich des kodifizierten (kontinentalen) Rechts große Bedeutung besitzen. Es muss daher zusätzlich jedes Mal geprüft werden, ob nicht inzwischen neuere Urteile ergingen oder Gesetzte zu diesem Problemgebiet erlassen wurden. Deshalb finden sich in diesem Buch immer wieder Verweise auf Urteile, welche gesetzliche Regelungen näher präzisieren oder auf konkrete Sachverhalte anwenden.

Um das Zitieren von Nummern zu vermeiden, werden wichtige Entscheidungen meist von der Praxis mit einem Kurztitel versehen, unter welchem sie dann veröffentlicht und bekannt werden; dies ist jedoch keine offizielle Bezeichnung. Als gutes Beispiel kann etwa das weithin bekannte Urteil "Meteodata" (OGH 17.12.2002, 4 Ob 248/02) dienen, bei welchem über das Verhältnis von Wettbewerbsrecht und Links/Framing entschieden wurde. Es klagte die Firma "METEO-data Wetteranalysen GmbH", nach der das Urteil dann benannt wurde. Die "offizielle" Bezeichnung ist hingegen "4 Ob 248/02b"[22], die Geschäftszahl der Entscheidung, unter welcher sie am schnellsten gefunden werden kann.

Im vorliegenden Werk werden keine Entscheidungen besprochen, obwohl diese in manchen Fällen als Grundlage für die Darstellung dienen. Entsprechende Verweise dienen dazu, eine vertiefende Beschäftigung mit einem konkreten Thema zu ermöglichen.

I.2.4. Quellen für Rechtstexte

Der Zugang zu Rechtstexten und Entscheidungen ist in Österreich, einem Vorreiter auf diesem Gebiet, besonders einfach: Das Rechtsinformationssystem des Bundes (RIS[23]) ist über das Internet öffentlich und ohne Registrierung einsehbar. Enthalten sind u.a. nationale Gesetze, Verordnungen und Entscheidungen[24]. Es ist sowohl eine Abfrage des aktuellen Rechts wie auch nach früheren Regelungen möglich. Die Suche nach Gesetzestexten erfolgt am zweckmäßigsten direkt mit der Abkürzung (z.B. "StGB"), alternativ mit dem vollen Titel (beispielsweise "Strafgesetzbuch") und dem gewünschten Paragraphen.

Regelungen der EU sind über das EUR-Lex Portal[25] zugänglich. Es enthält sowohl das Amtsblatt in elektronischer Form, in welchem z.B. Richtlinien und Verordnungen veröffentlicht werden, ebenso wie Entscheidungen der EU-Gerichte. Die Suche ist am einfachsten, wenn die genaue Nummer bekannt ist, welche sich meist aus dem Titel ergibt[26].

Gerichtsentscheidungen können außerhalb des Rechtsinformationssystem zusätzlich oft im Internet gefunden werden, sofern es sich um höherrangige Gerichte handelt. Hierbei ist entweder der Titel oder die Geschäftszahl hilfreich. Bei letzterer ist aber zu beachten, dass oft die Schreibweise, z.B. mit/ohne Leerzeichen, divergiert.

---

[22] Syntax: Nummer des Senates ("4"), Gattungszeichen (=Art des Verfahrens; "Ob" = Rechtsmittel in bürgerlichen Rechtssachen, ...), laufende Nummer ("248"), Jahr des Anfalls ("02" = 2002) und einem Prüfzeichen ("b"). Siehe auch die Geschäftsordnung des OGH http://www.ogh.gv.at/ogh/index.php?nav=7#18

[23] http://www.ris.bka.gv.at/

[24] Die OGH Entscheidungen sind seit 1991 komplett und in gewissem Ausmaß fand eine Rückerfassung statt. Von unteren Gerichten sind auch weiterhin nur ausgewählte Entscheidungen enthalten.

[25] http://eur-lex.europa.eu/

[26] So ist die "Richtlinie 2000/31/EG des Europäischen Parlaments ..." (E-Commerce RL) am schnellsten über "Einfache Suche" – "Suche nach Nummer" Jahr 2000, Nummer 0031 zu finden.

I.3. Übersicht der behandelten Gebiete

E-Business ist weder technisch noch rechtlich ein einheitliches Thema; viele verschiedene Aspekte aus beiden Gebieten sind von Bedeutung. Dementsprechend und im Hinblick auf die Zielgruppe "Techniker" ist dieses Buch auch weniger nach Rechts- als vielmehr Sachgebieten geordnet. Als gutes Beispiel kann der Abschnitt über Domain Namen dienen, welcher die verschiedensten Rechtsgebiete umfasst (siehe Abbildung 2).

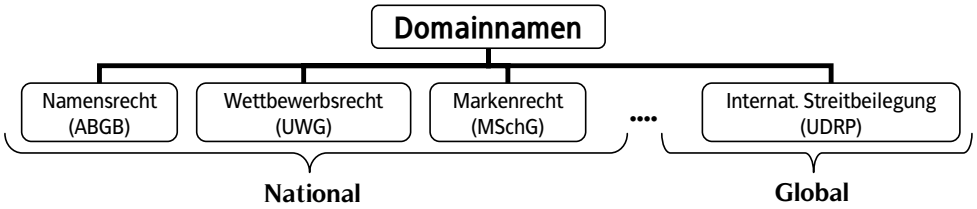


Abbildung 2: Rechtsgebiete mit Einfluss auf Domain Namen

Der allgemeine Ablauf von Geschäften im Internet dient als Vorlage für die Gliederung:

1. Ohne einem Domain Namen kann im Internet praktisch kein Geschäft getätigt werden. Im Hinblick auf Endkunden schon gar nicht, da ihnen ein leicht merkbarer Zugang zu Webseiten zur Verfügung gestellt werden muss, aber auch nicht im B2B-Bereich, da das Hantieren (relativ volatilen) mit IP-Adressen problematisch ist.
2. Über den Domain Namen sind Inhalte erreichbar, welche typischerweise über das Urheberrecht sowie ev. weitere Rechtsvorschriften geschützt sind. Nicht alles darf daher in beliebiger Form verwendet werden. Hierzu gehören insbesondere der Schutz von Webseiten und Fragen rund um Links und Providerhaftung.
3. Um von Kunden gefunden zu werden, ist Werbung unerlässlich. Diese kann aktiv erfolgen, z.B. über E-Mails oder Werbe-Banner, oder passiv über Suchmaschinen. Nicht jede Art und Form der Betätigung ist hierbei erlaubt.
4. Um dem Kunden die Ware zusenden zu können, Rechnungen zu erstellen, aber auch für Werbezwecke, müssen Daten des Kunden gespeichert und verarbeitet werden. Hierbei ist der Datenschutz zu berücksichtigen. Dies ganz besonders, sobald andere Firmen von den Daten profitieren oder diese neuen Zwecken zugeführt werden sollen.
5. Nicht immer ist der Konsument mit der Ware vollauf zufrieden, sodass es zum Rücktritt vom Vertrag kommen kann. Dieser und weitere Schutzvorschriften für Verbraucher müssen, teilweise auch schon im Vorfeld, z.B. bei AGBs, beachtet werden.
6. Ein Vertragsabschluss muss auch nachweisbar sein, insbesondere bei höherwertigen Waren bzw. Dienstleistungen. In manchen Fällen, und in Zukunft wohl häufiger, wird er daher mittels einer el. Signatur beweiskräftiger gestaltet werden.
7. Manchmal sind "schwarze Schafe" im Internet unterwegs, welche sich durch Manipulationen bereichern oder einfach nur Schaden anrichten wollen. Hierfür ist als schärfste Sanktion das Strafrecht maßgebend, wobei beachtet werden muss, dass u.U. besondere technische Vorkehrungen notwendig sind, um diesen Schutz zu genießen.

Urheberrecht und Datenschutz fallen etwas aus dem Schema der Gliederung nach Sach- anstatt Rechtsgebieten heraus. Sie werden alleine für sich besprochen, da sie auch unabhängig vom E-Business bedeutsam sind. Konkrete Anwendungen davon werden allerdings

in verschiedenen Abschnitten gestreift, siehe hierzu insbesondere die Diskussion über den Urheberrechtsschutz von Webseiten.

I.4. Abgrenzung zu hier nicht behandelten Gebieten

Das Thema dieses Werkes ist E-Business, weshalb der gesamte Bereich des E-Government ausgeklammert wurde. Dies beinhaltet sowohl die öffentliche Verwaltung mitsamt dem Kontakt zu ihr, welcher für Firmen durchaus von großer Bedeutung ist, als auch Punkte wie E-Voting oder E-Participation.

Ebenso wird hier das Telekommunikationsrecht nicht betrachtet, welches für Telekommunikationsanbieter, insbesondere aber auch für Internet-Service-Provider von Bedeutung ist.

Das Prozessrecht ist zwar auch im E-Business von essentieller Bedeutung, doch für juristische Laien eher weniger interessant: Wenn es zu einem gerichtlichen Verfahren kommt, ist ein Anwalt ohnehin unerlässlich. Ganz kurz gestreift wird jedoch die Rechtswahl und die internationale Zuständigkeit, da diese einem Prozess noch vorgelagert sind.

Auf andere Literatur ist bezüglich des Software-Vertragsrechts zu verweisen: Wie Lizenzen gestaltet werden und wie Software gekauft, geleast, lizenziert etc. wird, ist ein separates Gebiet und vor allem für Softwareproduzenten von Bedeutung. Hiermit verwandt sind weitere Schutzrechte, insbesondere das Patentrecht. Software-Patente sind ein stark diskutiertes Thema, welches jedoch für den E-Business eher von geringerer Bedeutung ist[27].

Schlussendlich wird auch das Arbeitsrecht hier ausgeklammert: Insbesondere im Bereich des Datenschutzes ist dieses bedeutsam, spielt sich jedoch innerhalb eines Betriebes ab, während der Schwerpunkt hier auf den Außenbeziehungen liegt.

Dieses Buch will und kann die Kontaktierung von professionellen Rechtsberatern in Streitfällen oder bei wichtigen Entscheidungen nicht ersetzen. Es bietet demgegenüber eine Einführung, um gewisse Probleme gleich von vornherein, z.B. beim Systementwurf, der Programmierung, oder der Verwendung von Informations- und Kommunikationstechnologie vermeiden zu können sowie das Bewusstsein für Problemgebiete zu schärfen.

[27] Siehe aber z.B. die vielen Geschäftsmethoden-Patente, wie das Amazon "1-Click" Patent (US 5960411; EP 0927945).

II. Domain Namen

Ein wichtiger Teil des E-Business sind Online- oder Web-Shops. Diese bedürfen zur Auffindbarkeit im Internet eines zu registrierenden Domain Namens, welcher weltweit eindeutig sein muss bzw. technisch eindeutig ist. Diese Anforderung der weltweiten Eindeutigkeit bringt spezifische Probleme mit sich, da bisher viele Unternehmen mit identer Bezeichnung gleichzeitig existieren konnten, solange sich ihre Geschäftsbereiche oder ihr Einzugsgebiet nicht überlappten. Es kann daher für ein Unternehmen unmöglich sein, seinen eigenen Namen als Domain Namen zu verwenden, da dieser bereits von jemandem anderen registriert wurde. Es bestehen in diesem Fall zwei Möglichkeiten: Die Verwendung eines anderen Namens für den Internet-Auftritt oder der Versuch, diesen Domain Namen zu erlangen. Letztere Variante besaß eine große praktisch Bedeutung, da es viele Personen gab, welche die Namen bekannter Firmen registrierten, um diese zu einem späteren Zeitpunkt gegen hohe Summen an diese Unternehmen zu verkaufen. Ähnliches tritt immer wieder bei neuen Top-Level Domains auf, wie etwa zuletzt bei der Einführung von „.eu“. Doch auch eine umgekehrte Möglichkeit besteht: Der Versuch, einem rechtmäßigen Inhaber den Domain Namen aufgrund eines vorgeblichen besseren Rechts wegzunehmen („Reverse Domain Name Hijacking“, RDNHJ).

II.1. Einleitung

Im ersten Abschnitt wird kurz der technische Hintergrund erläutert, darauf aufbauend die wichtigsten rechtlichen Aspekte: Namensrecht, Wettbewerbsrecht und Markenrecht. Mithilfe dieser Vorschriften ist es möglich, sich gegen Domain Grabbing, dem "Wegschnappen" eines Domain Namens, zu wehren. Anschließend werden einige besondere Aspekte untersucht, wobei insbesondere die Verwendung beschreibender Namen oder Gattungsbezeichnungen bedeutend ist. Als Abschluss wird das Streitbeilegungsverfahren der ICANN (Internet Corporation For Assigned Names and Numbers) erläutert, welches zwar weder österreichisches noch EU-Recht betrifft, jedoch enorme praktische Bedeutung besitzt. Seit der Einführung im Jahr 2000 werden durchschnittlich ca. 2200 Entscheidungen pro Jahr nach diesem Verfahren getroffen.

II.2. Technische Realisierung

Das Domain Name System (DNS) dient hauptsächlich dazu, Hostnamen in Internet-Adressen umzuwandeln, da Menschen sich Namen viel leichter merken als Zahlen. Es können noch weitere Informationen gespeichert bzw. abgefragt werden. Beispiele hierfür sind Informationen über den zuständigen E-Mail Rechner (MX-Record) bzw. über Rechner, welchen der Versand von E-Mails für diese Domain erlaubt ist (SPF[28], SenderID[29]).

[28] Sender Policy Framework: http://www.openspf.org/

[29] Sender ID Framework: http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

II.2.1. Aufbau von Domain Namen

Der Bereich aller Domain Namen ist hierarchisch in Form eines Baumes (directed acyclic graph; DAG) aufgebaut. Es handelt sich hier jedoch nur um eine logische Struktur, welche von der physikalischen Netzwerksstruktur vollständig unabhängig ist. Jeder Knoten dieses Baumes entspricht einer Ressourcen-Menge, welche auch leer sein kann, und besitzt einen Namen, der sich von allen Bruderknoten unterscheidet. Der Namen eines Knotens kann zwischen 1 und 63 Zeichen enthalten, wobei nur Buchstaben (Groß-/Kleinschreibung wird ignoriert!), Ziffern und der Bindestrich erlaubt sind. Namen müssen mit einem Buchstaben beginnen sowie mit einem Buchstaben oder einer Ziffer enden.

Ein Domain Name setzt sich aus der Folge aller Knotennamen bis zur Wurzel des Baumes zusammen, wobei die Knoten von unten nach oben gelesen und durch einen Punkt getrennt werden. Gemeinsame Wurzel ist ein leerer Knoten: Der einzige Knoten mit einem Namen der Länge 0. Wird der gesamte Weg angegeben (z.B. „www.fim.uni-linz.ac.at."), so spricht man von einem absoluten Namen, ansonsten von einem relativen (z.B. „www.fim"). Sie können dadurch unterschieden werden, dass absolute Namen immer mit einem Punkt enden[30]. Bei relativen Namen wird zur Erzeugung vollständiger (=absoluter) Namen die Standard-Domäne angehängt (z.B. ".uni-linz.ac.at.").

Auf der obersten Ebene, direkt unter dem gemeinsamen Wurzelknoten, befinden sich die so genannten "generic Top-Level Domains" (gTLD). Von diesen existieren zur Zeit 19 Stück: biz, com, info, jobs, name, net, org, pro und travel sind frei verfügbar; aero, cat, coop, edu, gov, mobi, mil, museum und int nur eingeschränkt; arpa dient zur internen Verwaltung des Namensraumes und z.B. auch für ENUM[31]. Weiters stehen mehr als 200 länderspezifische (country-code: ISO-3166-1: at, us, de, ...; ccTLD) Top-Level Domains (TLDs) zur Verfügung. Zu den ccTLD gehört auch .eu, obwohl es sich hier um einen Staatenbund und nicht einen Einzelstaat handelt. Weitere gTLDs wurden beantragt, aber entweder abgewiesen, noch nicht entschieden oder es bestehen Verhandlungen mit einem Registrar. Für die Zulassung bzw. die Zuteilung von Registrierungsstellen ist die ICANN (siehe II.2.5) zuständig. Der Domain-Baum ist in Abbildung 3 dargestellt.

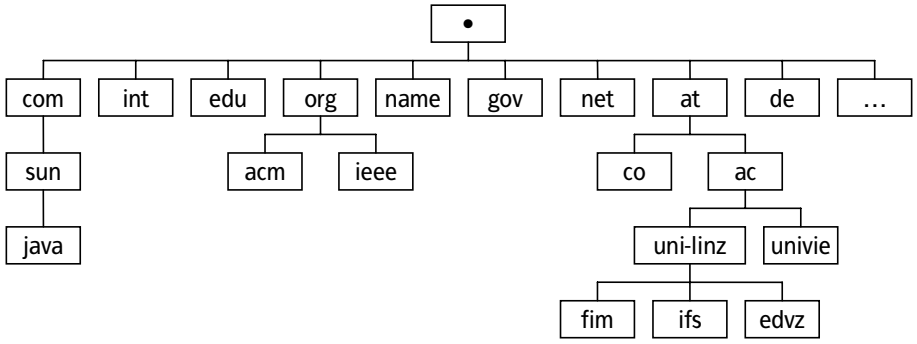


Abbildung 3: Der Domain Baum

[30] In der Praxis wird allerdings auch dieser weggelassen. Absolute Namen werden dann daran erkannt, dass entweder keine Standard-Domäne angehängt wird (Betriebssystem-Konfiguration) und der Name so verwendet wird wie er ist, bzw. indem er mit den top-level Domains verglichen wird.

[31] Adressierung von Internet-Diensten über Telefonnummern.

II.2.2. Name Server

Name Server (NS) sind jeweils für einen Teilbereich des Domain Baumes zuständig, für welchen sie "authoritative anwers" liefern und die zugehörigen Informationen speichern (siehe Abbildung 4). Weitere andere Server sind möglich; sie dienen u.a. der Ausfallsicherheit (Secondary NS) oder der Effizienz (Caching NS), beziehen aber ihren Inhalt jeweils von den Haupt-Nameservern. Die einem Authoritative NS zugeordneten Abschnitte ("zone") dürfen sich nicht überlappen. Probleme ergeben sich an den unteren Schnittstellen: Befindet sich der Nameserver für diesen Bereich selbst in genau diesem Bereich, z.B. wenn eine Firma ihre Nameserver selbst betreibt[32], so muss die darüber liegende Zone zusätzliche Informationen speichern ("glue"). Typischerweise existieren für jede Zone zumindest zwei Name Server (bei vielen Registrars eine Voraussetzung), wobei sekundäre Server ihre Daten in regelmäßigen Abständen vom primären Server aktualisieren.

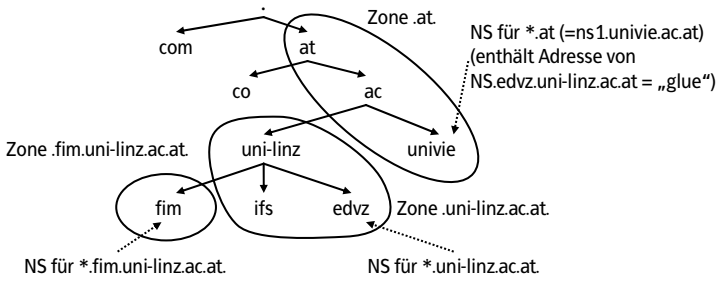


Abbildung 4: Zonenaufteilung des Domain Baumes

Bei TLDs stellt sich ein gewisses Problem: Woher erhält man die Adressen der für sie zuständigen Nameserver? Hierfür existieren ein Anzahl logischer[33] Root-Nameserver, welche über die ganze Welt verteilt sind (13 Stück; 10 x USA, England, Japan und Schweden; „a.root-server.net“ bis „m.root-server.net“). Diese werden (inhaltlich) von der ICANN kontrolliert. Die IP Adressen von diesen Wurzel-Nameservern muss jeder Nameserver „einfach kennen“. Technisch reicht ein einzelner Wurzel-Nameserver aus, von welchem dann die Liste aller anderen geholt werden kann.

Jede Domain muss bei der darüber liegenden Domain registriert werden. Hierfür existieren Registrierungsstellen, sowohl für generische als auch nationale TLDs. Eine Firma hat sich daher an eine Registrierungsstelle zu wenden, um die Domain "gadget.com" zugeteilt zu erhalten. Alternativ können auch weitere Firmen dazwischentreten, welche jedoch lediglich Vermittler gegenüber einer solchen Registrierungsstelle sind und die Domain Namen nicht tatsächlich selbst vergeben. Für die Erstellung einer Subdomain ist die Genehmigung von „höheren“, also im Baum weiter oben liegenden, Domains *nicht* notwendig und auch nicht vorgesehen. So kann etwa die obige Firma mit dem Domain Namen "gadget.com" ohne Genehmigung/Mitwirkung ihres Providers oder der Registrierungsstelle die Domains

[32] Typischerweise wird daher der Nameserver in der darüber liegenden Zone eingetragen, sowie zusätzlich unter dem Namen des Nameserver dessen IP Adresse. Um diese IP Adresse des Nameservers zu erhalten, müsste sonst genau dieser Nameserver befragt werden, von dem die Adresse noch nicht bekannt ist ....

[33] Physisch handelt es sich um eine viel größere Anzahl, siehe z.B. den K Root Server, der aktuell aus 17 weltweit verteilten Knoten besteht (http://k.root-servers.org/) oder den F Root Server (37 Knoten; http://f.root-servers.org/)

"www.gadget.com", "production.gadget.com", "www.test.production.gadget.com" oder "test.gadget.com" erzeugen[34].

II.2.3. Umwandlung Name ⇒ IP-Adresse

Hierbei handelt es sich um die häufigste Abfrage. So ist etwa der Domain Name „www.fim.uni-linz.ac.at“ der IP-Adresse 140.78.100.116 zugeordnet. Um diese Umwandlung durchführen zu können, muss ein Rechner zumindest einen einzigen Nameserver kennen, welcher meist bei der IP Client-Konfiguration eingestellt wird. Kennt dieser Nameserver den gewünschten Namen z.B. aus dem Cache oder handelt es sich um einen lokalen Namen, so liefert er sofort die Adresse zurück. Wenn nicht, so existieren zwei Möglichkeiten: Iterative und rekursive Suche:

- Iterative Suche: Der Nameserver liefert die Adresse eines anderen Nameservers zurück, welcher dem gesuchten Namen seines Wissens nach am nächsten liegt. Im schlechtesten Fall ist dies ein Wurzel-NS. Der Client muss sich dann mit seiner Anfrage selber an diesen NS wenden. Diese Suche muss von jedem NS implementiert werden.
- Rekursive Suche: Der Nameserver erkundigt sich selbst bei anderen Nameservern und liefert anschließend die Antwort an den Client zurück. Diese Suche ist optional. Nameserver weit oben in der Hierarchie führen meist keine rekursive Suche aus. Beispiele hierfür sind die Wurzel-NS, aber auch der NS der Universität Wien, welcher für die Domain "at" zuständig ist.

II.2.4. WHOIS-Datenbank

Die WHOIS-Datenbank ist eine Datenbank von Internet-Netzwerken (Zuteilung von IP-Adressen bzw. Adressräumen), deren Domain Namen, zugehöriger Kontaktpersonen und Regeln für IP-Routing. Es handelt sich nicht um eine zentrale Datenbank[35], sondern jede Registrierungsstelle stellt ihre eigene Datenbank selbst zur Verfügung oder auch nicht. Es existieren auch zentrale Anbieter, welche auf Sub-Datenbanken der einzelnen Länder zugreifen, in welchen die lokalen und jeweils gültigen Daten gespeichert sind. So sind beispielsweise die Daten über .at bei der nic.at[36] gespeichert und auch zugänglich, jedoch wie alle europäischen ccTLDs auch über http://www.ripe.net/db/index.html abfragbar.

Für Endbenutzer ist hauptsächlich die Abfrage nach einem Domain wichtig, etwa um herauszufinden, für wen diese registriert ist. Es muss beachtet werden, dass kein Standard-Format für die Antwort definiert ist!

---

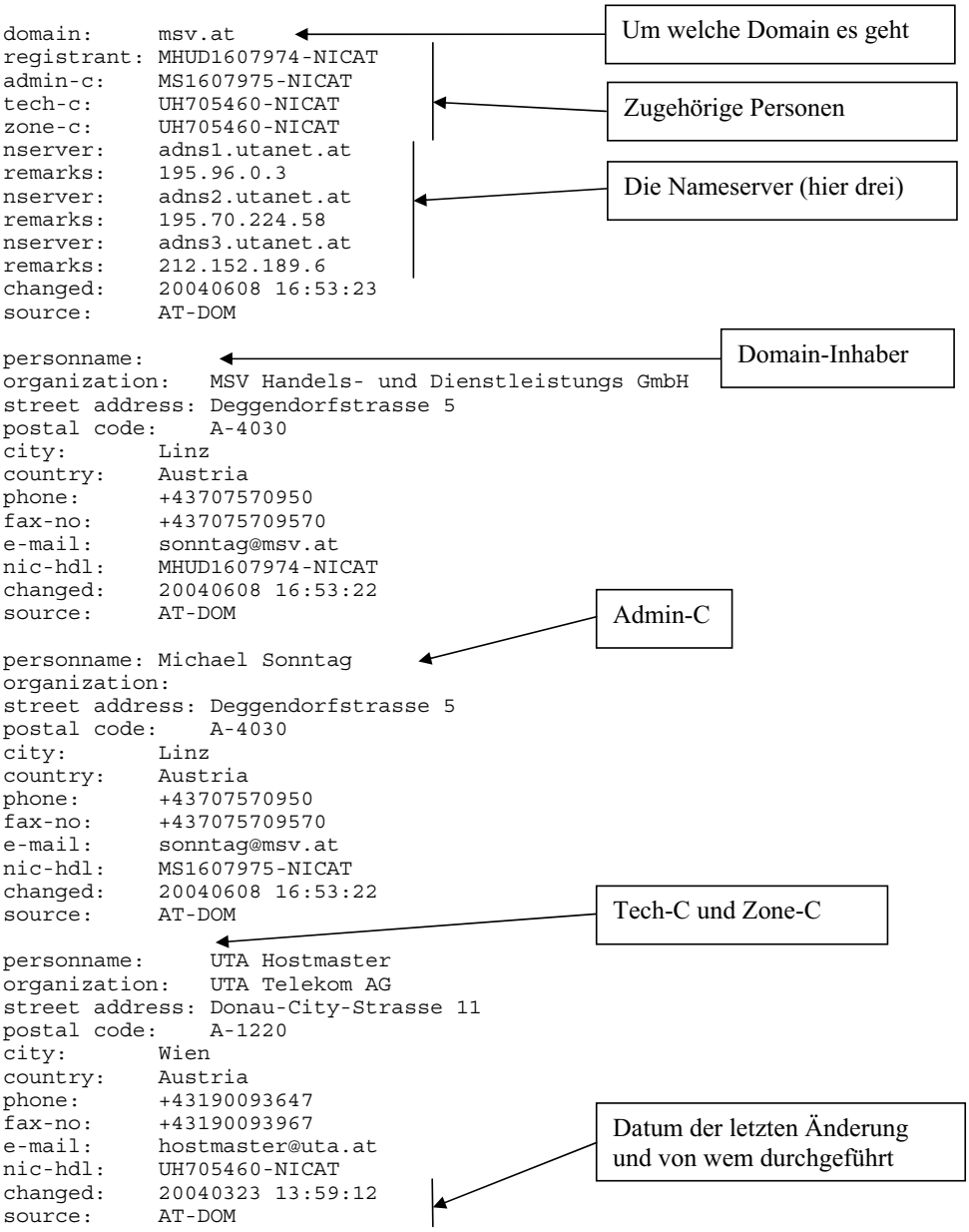
[34] Unter Umständen benötigt sie jedoch die (technische) Mitarbeit des Providers, falls sich wie üblich der Nameserver für die Domain "gadget.com" bei diesem befindet, um diese Namen dort auf dem Nameserver einzutragen. Dies ist nur erforderlich, sofern die Domains weltweit erreichbar sein sollen.

[35] Siehe http://www.iana.org/cctld/cctld-whois.htm und http://www.iana.org/gtld/gtld.htm für eine Liste aller TLDs, wo jeweils auch der WHOIS-Dienst vermerkt ist, sofern vorhanden.

[36] nic.at Internet Verwaltungs- und Betriebsgesellschaft m. b. H. (http://www.nic.at/). Es handelt sich um eine private Gesellschaft, welche zu 100% im Eigentum der gemeinnützigen "Internet Privatstiftung Austria" steht. Die technische Abwicklung, d.h. der Betrieb der Nameserver, erfolgt als bezahlte Dienstleistung durch den Zentralen Informatikdienst der Universität Wien. Die nic.at ist daher mit keiner Art von öffentlichen Aufträgen betraut und kann keine hoheitlichen Akte setzen (Bescheide ausstellen, Verordnungen erlassen etc.). Sie ist allerdings Monopolist und hat daher besondere Vorsicht walten zu lassen (Ausnutzung einer Monopolstellung ist verboten; das Monopol selbst jedoch nicht!).

II.2.4.1. Beispiels-Abfrage: msv.at (Ausschnitt):

Bei einer Abfrage nach „msv.at“ auf www.ripe.net erhält man etwa folgende Antwort:



II.2.4.2. Beschreibung einzelner Felder

Folgende Abkürzungen finden typischerweise Verwendung:

- Admin-C: Kaufmännische Ansprechperson
- Tech-C: Technische Ansprechperson für das Netzwerk der Domain
- Zone-C: Technische Ansprechperson für den Betrieb der Nameserver

- Mnt-by: Die Person, welche für die Eintragung der Daten zuständig/berechtigt ist[37]
- Nic-Hdl: Eindeutige Kurzbezeichnung einer Person (unter diesem Kürzel gespeichert)

II.2.5. ICANN

Die ICANN (Internet Corporation for Assigned Names and Numbers) wurde im Oktober 1998 gegründet. Diese gemeinnützige private Gesellschaft ist zuständig für:

- Das Internet Domain Name System
- Die Zuteilung von IP-Adressen / IP-Adressräumen
- Die Zuteilung von Protokoll-Parametern (z.B. feste Service-Nummern) und Standardisierung von Protokollen
- Management der Root-Nameserver hinsichtlich der enthaltenen Daten; Hardware und Betrieb erfolgen durch verschiedene andere Organisationen

Es werden jedoch keine konkreten Dienstleistungen für Endkunden erbracht: Es können weder Domain Namen registriert werden, noch werden Streitigkeiten über solche vor ihr ausgetragen. Sie ist vielmehr hauptsächlich für die Erstellung von Standards und die internationale Koordination zuständig.

Die Leitung von ICANN besteht aus einem 15-Personen-Vorstand, wobei acht von einem Nominierungs-Komitee gewählt werden, jeweils zwei von den drei wichtigsten Teilorganisationen (Address-, Generic Names-, Country Code Domain Name Supporting Organization) ernannt werden, sowie dem Präsidenten, welcher vom Vorstand gewählt wird (siehe auch Abbildung 5). Zusätzlich zu den 15 stimmberechtigten Mitgliedern gehören sechs weitere nicht-stimmberechtigte Personen dem Vorstand an. Jeweils einer wird von folgenden Institutionen bzw. Unterorganisationen entsandt: Governmental Advisory Committee, At-Large Advisory Committee, Security and Stability Advisory Committee, Root Server System Advisory Committee, Technical Liaison Group, und der IETF[38].

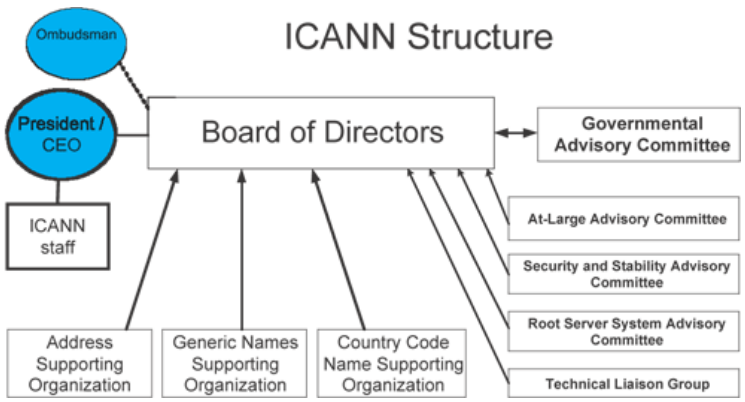


Abbildung 5: ICANN Organisation[39]

[37] Im Beispiel nicht enthalten!

[38] Internet Engineering Task Force. Nicht im (offiziellen) Bild, vermutlich da es sich um eine separate Institution handelt.

[39] Quelle: http://www.icann.org/general/icann-org-chart.htm

Die ICANN wird teilweise sehr stark diskutiert und es wird nach Alternativen gesucht, da das amerikanische Wirtschaftsministerium sehr großen Einfluss auf sie besitzt und die ICANN auch mehrere sehr kontroversielle Entscheidungen getroffen hat.

II.2.6. Internationale Domain Namen

Der derzeitige Standard (RFC[40] 3490-3492, 3454) baut auf normalem DNS auf, indem internationalen Namen eindeutig ein ASCII-Name zugeordnet wird. Hierzu werden alle speziellen Zeichen, für die Unicode zur Verfügung steht, umcodiert (Stringprep+Punycode) und eine Spezialkennung ("xn--")[41] vorangestellt. Derart muss nur die Client-Software dies unterstützen, während die NS selbst sowie die Protokolle unverändert bleiben können.

Schwierigkeiten können sich daraus ergeben, dass nun die Darstellung von Domain Namen nicht mehr eindeutig sein muss. So können zwei Domain Namen vollkommen identisch aussehen, jedoch aus verschiedenen Unicode-Zeichen bestehen und daher auch eine andere Domain bezeichnen. Beispielsweise sehen das lateinische und das kyrillische kleine a zwar exakt gleich aus, sie sind aber unterschiedliche Unicode-Zeichen. Sie ergeben daher unterschiedliche Domain Namen, die dennoch absolut identisch dargestellt werden. Teilweise wird dies durch Kanonisierungsregeln abgefangen, aber vollständig kann das Problem auf diese Weise nicht behoben werden. Dies bringt einerseits praktische Probleme, so ist etwa das Abschreiben eines Domain Namens dann eventuell nicht genug, um die entsprechende Webseite auch tatsächlich zu finden, andererseits auch neue rechtliche Fragestellungen: So wäre es nun möglich, einen Namen doppelt zu vergeben. Sollte es sich hierbei um den identischen oder stark ähnlichen Namen zweier Firmen handeln, so sind sehr schwierige Diskussionen vorprogrammiert.

Abgesehen von diesem Problem stellen sich bei internationalen Domain Namen dieselben rechtlichen Fragen wie bisher, nur eben für andere Zeichenketten[42].

II.3. Namensrechtlicher Schutz

Der namensrechtliche Schutz (§ 43 ABGB) ist ein Persönlichkeitsrecht, das sowohl natürlichen als auch juristischen Personen zusteht. Nicht nur der eigentliche bürgerliche (Nach-!) Name ist geschützt, sondern auch Decknamen und Etablissementbezeichnungen, genauso wie Abkürzungen, Vornamen und Namensbestandteile, sofern diese eigene Namensfunktion besitzen. Auch die langjährige Verwendung eines Domain Namens kann zu einem Schutz desselben über Namensrecht führen, wenn die Person/Firma darunter bekannt ist[43].

Im Falle einer Verletzung muss als Rechtsfolge mit einem Unterlassungsanspruch und bei Verschulden zusätzlich mit Schadenersatz gerechnet werden. Obwohl nicht ausdrücklich erwähnt, wird auch ein verschuldensunabhängiger Beseitigungsanspruch enthalten sein, was eine Löschung der Domain bedeuten kann, nicht bloß eine Veränderung des Inhalts.

---

[40] Request For Comments: Die inoffiziellen Internet-Standards. Siehe http://www.rfc-editor.org/

[41] Auch bisher konnten Namen mit "xn--" beginnen, was zu Problemen führen könnte. Daher sollen ab nun keine derartigen Namen mehr vergeben werden. In der Praxis dürfte dieses Problem allerdings gering sein.

[42] Siehe dazu „schlüsselbänder.de“, OLG Köln 2.9.2005, 6 U 39/05, http://www.jurpc.de/rechtspr/20050116.htm

[43] Wohl analog Etablissement-Bezeichnungen. Siehe AG Köln 24.11.2004, 136 C 161/04 http://www.justiz.nrw.de/nrwe/ag_koeln/j2004/136_C_161_04urteil20041124.html sowie OGH 14.2.2006, 4 Ob 165/05a

Zuerst stellt sich die Frage, ob die Verwendung einer Folge von Zeichen als Domain Name überhaupt in den Schutzbereich des Namensrechtes fällt. Vor allem in Deutschland (durch Gerichte; in Österreich auch durch einen Teil der Lehre) wurde früher die Meinung vertreten, dass Domain Namen nicht mit dem bürgerlichen Namen vergleichbar sind, sondern eher mit Telefonnummern, und daher keinen Schutz genießen. Sie dienen im täglichen Gebrauch jedoch vor allem dazu, die hinter den Webseiten stehende Firma bzw. Person zu identifizieren und werden auch vielfach so verwendet. Beispiel hierfür ist die Eingabe eines vermuteten Domain Namens durch einen suchenden Benutzer, welcher aus dem Firmennamen abgeleitet ist, z.B. für IBM die Eingabe von „www.ibm.com“. Sowohl in Deutschland wie auch in Österreich ist inzwischen die Namensfunktion von Domain Namen allgemein anerkannt[44].

II.3.1. Namensgebrauch

Das Namensrecht schützt sowohl gegen den Gebrauch des Namens durch jemand anderen als auch gegen die Bestreitung der Rechtmäßigkeit der Führung des eigenen Namens. Entgegen manchen Auffassungen[45] kann meines Erachtens in der Anmeldung eines Domain Namens keine automatische Leugnung des Namensrechts Dritter gesehen werden[46]. Es ergibt sich lediglich eine tatsächliche Ausschlusswirkung von der Verwendung im Internet, doch wird damit normalerweise nicht das Recht jemandes anderen bestritten, diesen Namen berechtigterweise sonst zu führen, z.B. im persönlichen Gespräch oder auf Briefpapier. Andernfalls wäre es unmöglich, einen Namen als Domain Name zu verwenden, welcher von zwei Personen geführt wird, da jeder von ihnen automatisch das Recht des anderen bestreiten würde. Es bleibt nur der tatsächliche Gebrauch des Namens als Verletzungshandlung übrig. Bereits die bloße Registrierung kann hierfür ausreichen, ohne dass sich irgendein Inhalt dahinter befindet, d.h. ohne darunter abrufbare Webseiten (siehe unten).

Ein Name wird nur dann gebraucht, wenn er zum fraglichen Namen entweder identisch oder zumindest ähnlich ist. Die äußerste Grenze sind Namen, die lediglich einen ähnlichen Klang besitzen[47]. Hier kommt es auf das Identitätsinteresse des Verletzten an: Er soll nicht mit anderen verwechselt werden und es soll keine wechselseitige Zuschreibung von Handlungen oder Leistungen erfolgen. Im Internet wird aufgrund des Namensmangels, nur eine Person kann einen bestimmten Domain Namen verwenden, wohl eher von großer Ähnlichkeit als Voraussetzung auszugehen sein, u.a. wegen der Internationalität: In anderen Sprachen können völlig unterschiedlich geschriebene Wörter ähnlichen Klang besitzen.

Ein Gebrauch eines Namens liegt zweifellos vor, wenn unter diesem Domain Namen eine Webseite erreichbar ist. Doch schon die Registrierung alleine ist ein Gebrauch[48], da der verwendete Name auf mehreren Rechnern eingetragen wird, z.B. in der WHOIS-

---

[44] Schanda: Internet Domain Names haben Namensfunktion, ecolex 1998, 565 und Schanda: § 43 ABGB bietet Anspruchsgrundlagen gegen Domain Namen, ecolex 2000, 215; OGH 21.12.1999, 4 Ob 320/99h

[45] "ufa.de II": OLG Düsseldorf 17.11.1998 20 U 162/97 http://www.aufrecht.de/index.php?id=751 erwähnt/besprochen in OGH 13. 7. 1999, 4 Ob 140/99p ecolex 1999/281 mit Anmerkungen von Schanda

[46] So inzwischen auch der OGH im Fall Adnet II: OGH 20.5.2003, 4 Ob 47/03w: http://www.eurolawyer.at/pdf/OGH_4_Ob_47-03w.pdf

[47] Etwa durch Registrierung eines Namens mit Umlaut (ü), welcher vom „echten“ Besitzer schon vorher mit „ue“ verwendet wurde: AG Köln 24.11.2004, 136 C 161/04 http://www.justiz.nrw.de/nrwe/ag_koeln/j2004/136_C_161_04urteil20041124.html

[48] graz2003.com: OGH 22.4.2002, 4 Ob 41/02m; Mayer-Schönberger/Hauer: Kennzeichenrecht & Internet Domain Namen. ecolex 1997, 947-951

Datenbank, aber auch auf den Nameservern. Dies ist analog zu dem Fall, dass ein Name als Markenzeichen registriert wird (zur umgekehrten Registrierung einer Marke als Domain siehe aber unten): Auch dort liegt bereits bei der Registrierung, also schon vor der Verwendung im Verkehr, ein Namensgebrauch vor. Die Nutzung als Überschrift einer Webseite ist im Gegensatz fast immer als bloße Namensnennung zu qualifizieren[49].

Zu beachten ist, dass der Gebrauch jedes beliebigen Namens grundsätzlich frei ist. Probleme ergeben sich erst im Zusammenhang mit einem Verwender des gleichen Namens. Existiert kein solcher, darf jede Zeichenfolge verwendet werden. Grundsätzlich dürfen auch obszöne[50] oder illegale[51] Domain Namen registriert werden, anders als z.B. Auto-Wunschkennzeichen. Dies schützt jedoch nicht vor einer etwaigen späteren Verfolgung deswegen.

Auch die Verwendung einer catch-all Funktion, d.h. alle beliebigen Subdomains werden auf eine bestimmte Web-Site abgebildet (Beispiel: www.michael.sonntag.cc, martin.sonntag.cc, xyz.sonntag.cc, … würden alle auf die Web-Site www.sonntag.cc aufgelöst) kann einen Namensgebrauch darstellen[52].

II.3.2. Unbefugtheit

Unbefugt ist der Gebrauch eines Namens dann, wenn er nicht auf einem eigenen Recht beruht, das Recht von dem bzw. einem beliebigen anderen Berechtigten eingeräumt wurde oder der eigene Name in unlauterer Absicht verwendet wird. Einschränkungen ergeben sich jedoch bei Wahlnamen (z.B. Decknamen, geschäftliche Kennzeichen): An diese werden strengere Anforderungen gestellt, da sie frei ausgewählt werden können. Sie sind daher Zwangsnamen (z.B. bürgerlicher Name) unterlegen. Dies gilt jedoch nur, sofern tatsächlich eine Wahl bestanden hat: Alteingeführte Namen müssen wohl gegenüber durch Namensänderung „geschaffenen“ nicht automatisch zurücktreten[53]. Ähnlich sind auch "berühmte" Marken privilegiert, indem Personen gleichen Namens unterscheidende Zusätze anbringen müssen. Ansonsten gilt zwischen Namen der gleichen Stufe, d.h. zwei Zwangsnamen oder zwei Wahlnamen, das Prioritätsprinzip. Dies kann problemlos auf Domain Namen übertragen werden: Besitzen beide Parteien entsprechend der Interessenabwägung gleiche Berechtigung, so gewinnt derjenige, der diesen Namen zuerst eintragen ließ, bzw. der andere muss einen unterscheidenden Zusatz hinzufügen.

---

[49] Der Beitrag in einem Blog mit der Überschrift "Sozialgericht Bremen", in welchem es um genau dieses geht, ist keine Verletzung des Namensrechts des Gerichts. U.a. deshalb nicht, da es sich nur um eine Seitenüberschrift bzw. einen URL-Bestandteil und nicht einen Domainnamen (hier: "shopblogger.de") handelt. Daran ändert auch nichts, dass die Seite bei Google bei einer Suche nach dem Gericht unter den ersten zehn Ergebnissen aufschien. Harste, Sozialgericht Bremen, http://www.shopblogger.de/blog/archives/1120-Sozialgericht-Bremen.html Kremer, § 12 BGB und das Sozialgericht Bremen http://weblawg.saschakremer.de/2005/12/30/12-bgb-und-das-sozialgericht-bremen/

[50] Siehe etwa die in OGH 18.11.2003, 4 Ob 219/03i („Pornotreff.at“) erwähnten Domainnamen.

[51] Bei jeder erfolgreichen Domainstreitigkeit handelt es sich gewissermaßen um einen „illegalen“ Domainnamen. Genau dies wird jedoch von der Registrierungsstelle, z.B. der nic.at *nicht* geprüft.

[52] "Suess.de" LG Nürnberg-Fürth 12.4.2006, 4 U 1790/05: Die Verwendung der Domain "suess.de" mit catch-all Funktion und anschließender Weiterleitung zu einer Erotikseite verletzt das Namensrecht einer Person gleichen Familiennamens. Die bloße Verwendung der Domain an sich ist jedoch keine Verletzung des Namensrechts, da keine Unterscheidungskraft vorliegt ("suess" ist ein allgemeines Adjektiv und kann daher von jedem verwendet werden). Problematisch ist hier jedoch, dass der Name nicht vom Domaininhaber verwendet wird, sondern von dem, der den Namen eingibt. Analog zu dieser Überlegung wurde in Österreich ein Markenrechtseingriff abgelehnt (siehe FN 79).

[53] Ändert Herr Müller etwa seinen Nachnamen auf Siemens und registriert „siemens.at“, so hat die Firma Siemens wohl trotzdem das bessere Namensrecht, auch wenn sie nur einen Wahlnamen besitzt und ihren Firmennamen theoretisch jederzeit ändern könnte. Markenrecht würde hier u.U. nichts helfen, wenn Herr Müller-Siemens eine rein private Homepage betreibt (siehe in Deutschland aber den Fall „shell.de“, BGH 22.11.2001, I ZR 138/99!).

II.3.3. Beeinträchtigung schutzwürdiger Interessen

Ein Abwehranspruch ist nur dann gegeben, wenn der unbefugte Gebrauch des Namens auch schutzwürdige Interessen des Verletzten beeinträchtigt. Es ist jedoch schon eine ideelle Beeinträchtigung ausreichend; eine wirtschaftliche oder rechtliche Gefährdung muss nicht gegeben sein. Der rechtliche Schutz soll zur Unterscheidung der Personen und dem Schutz ihrer Individualität dienen. Konkrete Verwechslungsgefahr ist daher nicht erforderlich, doch muss zumindest ein *Anschein* ideeller oder wirtschaftlicher Beziehungen bestehen. Entscheidend ist die Wirkung auf das Publikum, d.h. bei Domain Namen darauf, ob der "durchschnittliche"[54] Internet-Benutzer solche Beziehungen vermuten würde. Dieses Interesse muss auch schutzwürdig sein, was bei geschäftlichen Kennzeichen nur vorliegt, wenn es um Beeinträchtigungen von Geschäftsinteressen geht. Ein Hinweis auf den Webseiten selbst kann daher u.U. die Verwechslungsgefahr und damit eine etwaige darauf beruhende Interessensbeeinträchtigung verhindern[55].

Ein besonderer Aspekt existiert noch bei berühmten Namen: Eine berühmte Marke mit umfassendem Bekanntheitsgrad, die das Unternehmen selbst bezeichnet, und nicht nur Waren desselben, ist auch gegen Verwässerung geschützt (siehe dazu auch Abschnitt II.5.4). Diese Marke dient also zusätzlich als Name, weshalb das Namensrecht ebenso Anwendung findet. Es kann daher einer gleichnamigen Person die Verwendung dieses Namens als Domain Name untersagt werden, selbst wenn diese hierzu berechtigt ist[56]. Dies wurde in Deutschland auch bereits zwei Mal entschieden: Sowohl Herr Krupp als auch Herr Shell mussten die Verwendung der Domains "krupp.de" bzw. "shell.de" unterlassen[57]. Hier ist jedoch erforderlich, dass der eigene Name auf unlautere Weise verwendet wird oder es sich nur um einen ähnlichen Namen handelt, etwa um die Bekanntheit des Namens für sich auszunutzen. Dies wird jedoch auch kontroversiell diskutiert. Ansonsten kommt der wettbewerbsrechtliche Schutz in Frage, der freilich nur bei Handeln im geschäftlichen Verkehr und Gleichartigkeit der Waren greift. "Lautere" und rein private Verwendung des bürgerlichen Namens ist immer geschützt und sollte daher wohl selbst gegenüber berühmten Namen Erfolg haben.

II.4. Wettbewerbsrechtlicher Schutz

Für den wirtschaftlichen Bereich existiert ein allgemeiner Schutz durch das Gesetz gegen den unlauteren Wettbewerb (UWG). Es wurde nicht für die Anwendung auf Domain Namen geschaffen, doch ist es auch hierfür geeignet. Wichtig sind hier die § 1 (Generalklausel), § 2 (Irreführung) und § 9 Abs 1 (Schutz von Kennzeichen eines Unternehmens). Für die Anwendbarkeit des UWG ist es erforderlich, dass zwischen beiden Parteien ein Wettbewerbsverhältnis besteht. Es müssen daher beide im geschäftlichen Verkehr sowie auf einem zumindest ähnlichen Gebiet tätig sein.

---

[54] Ein deutsches Gericht führte aus, dass es keinen "durchschnittlichen" Internet-Benutzer gebe, da sehr viele verschiedene Benutzergruppen mit unterschiedlichem Verhalten existieren. Es verwendete daher zur Beurteilung eine mehr oder weniger beliebige Gruppe. Praktisch wendete es die eigenen Gewohnheiten des Gerichts zur Beurteilung an.

[55] „adnet.at": OGH 20.5.2003, 4 Ob 47/03w

[56] Siehe dazu auch „ams.at", OGH 5.11.2002, 4 Ob 207/02y, wonach auch befugter Namensgebrauch rechtswidrig sein kann, wenn das damit verfolgte Interesse wesentlich geringer zu bewerten ist als das Interesse eines Gleichnamigen, den Namen uneingeschränkt zu verwenden.

[57] „shell.de": BGH 22.11.2001, I ZR 138/99; „krupp.de": OLG Hamm 13.1.1998, 4 U 135/97

Irreführung und die Generalklausel betreffen hauptsächlich Fälle, in denen mit Hilfe der Domain vorgespiegelt wird, dass es sich bei dem Angebot auf der Webseite um eine andere Firma handelt. Insbesondere bei identischem oder sehr ähnlichem Erscheinungsbild wird dies schlagend werden. Eine zweite hierher gehörende Kategorie ist ein sehr ähnlicher Domain Name, z.B. mit oft vorkommenden Tippfehlern oder fehlerhaften Schreibweisen, um den Anschein einer Verbindung mit der bekannten Firma zu erreichen. Ebenfalls zu § 1 UWG gehört Domain Grabbing zur Behinderung eines Konkurrenten.

II.4.1. Missbrauch von Kennzeichen

Gemäß § 9 Abs 1 UWG ist es verboten, im geschäftlichen Verkehr einen Namen, eine Firma, die besondere Bezeichnung eines Unternehmens oder eine registrierte Marke so zu benützen, dass es zu einer Verwechslung mit dem Namen/Firma/Bezeichnung/Marke eines anderen Berechtigten kommen kann. Diese Benennungen sind jedoch nur insoweit geschützt, als sie unterscheidungskräftig sind, wobei die gleichen Grundsätze wie im Markenrecht gelten[58]. Die Rechtsfolge bei Verletzungen ist ein Unterlassungsanspruch und bei wissentlicher Verletzung auch Schadenersatz. Fahrlässige Unkenntnis führt ebenfalls zu Schadenersatz, da hier wohl gewisse Nachforschungspflichten bestehen, sodass bloßes "Nichtkennen" nicht schützt.

Unter "geschäftlichem Verkehr" wird jede auf Erwerb gerichtete Tätigkeit verstanden. Eine Verwendung als Domain Name reicht für die zusätzlich erforderliche kennzeichenmäßige Benützung aus, da der Name hierbei als Unternehmens- oder Dienstleistungsbezeichnung verwendet wird. Rein private Webseiten fallen ohnehin bereits mangels Anwendbarkeit des UWG weg. Die bloße Registrierung, ohne das Zurverfügungstellen von Webseiten, reicht (nur hier!) nicht, da dies zu keiner Verwechslung führen kann[59].

Letztes erforderliches Element ist die Verwechslungsgefahr. Hierfür muss der Name entweder identisch oder zumindest ähnlich sein. Für die Beurteilung ist, wieder einmal, der "normale Internet-Benutzer" maßgebend[60]. Die Verwechslungsgefahr ist jedoch ausgeschlossen, wenn sowohl Branche wie auch angebotene Waren bzw. Dienstleistungen völlig unterschiedlich sind, da der Konsument dann kaum irregeführt wird[61]. Es kommt daher nach ständiger Rechtsprechung auch auf den Inhalt der Webseiten an[62]. Dies ist umstritten, da auf Visitenkarten, Plakaten etc. der tatsächliche Inhalt der Webseite ja nicht erkennbar ist, der Domain Name aber schon. Daraus kann jedoch kein Freibrief abgeleitet werden, da auch der Anschein einer Nahebeziehung (z.B. selber Konzern; wirtschaftlicher, aber auch organisatorischer Art) für eine Verwechslungsgefahr ausreicht, sodass trotz unterschiedlichem Angebot Irreführungsgefahr vorliegen kann.

---

[58] OGH 11. 8. 2005, 4 Ob 59/05p. Der Name müsste also theoretisch als Marke eingetragen werden können, um geschützt zu sein. "Jusline I" OGH 24.2.1998, 4 Ob 36/98t Da "jusline" ein beschreibender Term ist, könnte er nur bei Verkehrsgeltung (=Bekanntheit) als Marke eingetragen werden. Eine solche wurde jedoch nicht bescheinigt.

[59] „amtskalender.at“: OGH 21.1.2003, 4 Ob 257/02a

[60] Allgemein, also nicht Internet-spezifisch: "Bei der Beurteilung der Verwechslungsgefahr kommt es auf die Verkehrsauffassung, also auf die durchschnittlichen Anschauungen eines nicht ganz unbeträchtlichen Teils der angesprochenen Verkehrskreise an." OGH 8.11.2005, 4 Ob 187/05m

[61] Gleicher Bereich, daher Verwechslungsgefahr: „internetfactory.at“ OGH 27.11.2001, 4 Ob 230/01d

[62] „gewinn.at“: OGH 17.8.2000, 4 Ob 158/00i

II.4.2. Behinderungswettbewerb und Domain Grabbing ieS

Wird ein Domain Name alleine zu dem Zweck registriert, damit er auf Grund der technischen Ausschlusswirkungen nicht von einem anderen Unternehmen verwendet werden kann, so ist dies sittenwidriger Behinderungswettbewerb[63] nach § 1 UWG. Dies geht jedoch nicht soweit, dass die Registrierung einer Gattungsbezeichnung schon Domain Grabbing wäre[64]. Der Beweis hierfür ist jedoch vielfach schwer zu erbringen, da meist ein eigenes Interesse des Registrierenden ausgeführt und - zumindest in Ansätzen - bewiesen wird. Es reicht daher aus, wenn das Fehlen eines sachlichen Grundes bewiesen wird, worauf sich die Beweislast umkehrt[65].

Wird ein Domain Name deswegen reserviert, um ihn anschließend an jemanden anderen zu verkaufen, insbesondere an den Berechtigten, oder etwa an dessen Konkurrenten, so spricht man von Domain Grabbing im engeren Sinne. Auch dies fällt unter sittenwidrigen Wettbewerb und ist verboten[66]. Auf Grund der meist einfacheren Beweisbarkeit sind diese Fälle häufiger: Oft erfolgt das Verfahren im Anschluss an Verhandlungen, in denen der Verkauf gegen eine hohe Geldsumme angeboten wurde. Dies verbietet zwar keinen Handel mit Domain Namen, schränkt ihn im Ergebnis jedoch sehr stark ein. Wird eine Domain tatsächlich anders verwendet oder dies zumindest ernsthaft versucht, so liegt auch bei späterem Verkaufsversuch kein Domain Grabbing vor[67].

Auch hier ist ein Handeln im geschäftlichen Verkehr erforderlich, doch ist bereits die Anmeldung des Domain Namens ein solches, unabhängig davon, ob eine Webseite darunter veröffentlicht wird oder sonst irgendeine Verwendung erfolgt, sofern nur schon die Anmeldung zum Zwecke der Behinderung oder des späteren Verkaufs erfolgt.

II.4.3. Abgrenzung zum Namensschutz

Der wettbewerbsrechtliche Schutz ist einerseits weiter als der namensrechtliche, andererseits jedoch auch enger:

- Weiter: Nicht nur Namen und Geschäftskennzeichen mit Namensfunktion sind erfasst, sondern auch sonstige Namen, Firmen, Unternehmens- oder Druckwerksbezeichnungen, Warenverpackungen bzw. -ausstattungen etc.
- Enger: Schutz besteht nur bei Verwendung des Namens durch den Verletztenden im geschäftlichen Verkehr. Privater Gebrauch ist hier irrelevant.

II.5. Markenrechtlicher Schutz

Für Marken existiert ein eigener Schutz im Markenschutzgesetz (MSchG), welcher allerdings ausschließlich auf das Handeln im geschäftlichen Verkehr beschränkt ist. Dieser

---

[63] "format.at" OGH 13.9.1999, 4 Ob 180/99w; Anmerkungen von Schanda, ecolex 2000, 53

[64] „autobelehnung.at“: OGH 10.2.2004, 4 Ob 229/03k http://www.eurolawyer.at/pdf/OGH_4_Ob_229-03k.pdf

[65] „taeglichalles.at“: OGH 12.6.2001, 4 Ob 139/01x

[66] "Jusline II" OGH 27.4.1999, 4 Ob 105/99s Registrierung eines DN ausschließlich dafür, um ihn später an den Betreiber eines Dienstes zu verkaufen ist sittenwidrig. Es kommt dabei nicht darauf an, ob der Dienst, und damit auch der DN, eine registrierte Marke ist oder Verkehrsgeltung besitzt: Jedes beliebige begründete Interesse an der Nutzung reicht aus.

[67] Siehe dazu „amade.at“: LG Salzburg 31.3.2004, 2 Cg 233/01s und OGH 13.3.2002, 4 Ob 56/02t Siehe auch Anmerkungen von Thiele zur Nachfolgeentscheidung OGH 14.2.2006, 4 Ob 6/06w http://www.eurolawyer.at/pdf/OGH_4_Ob_6-06w.pdf

dauert zehn Jahre und kann beliebig oft verlängert werden. Die private Verwendung eines Markennamens ist hier unerheblich. Wird er allerdings zur Werbung für die eigene Firma genutzt oder Werbefläche auf der Web-Site verkauft, so gilt dies nicht mehr als private Nutzung[68]! Zu beachten ist, dass auch bei einer eingetragenen Marke ältere Rechte bestehen können, welche vom Schutz nicht berührt werden. Grundsätzlich sind nur eingetragene Marken geschützt, doch sind diesen Kennzeichen gleichgestellt, welche aufgrund von Verkehrsgeltung Unterscheidungskraft besitzen. Verkehrsgeltung liegt vor, wenn maßgebliche Teile des geschäftlichen Verkehrs diese kennen.

Zwei Hauptfälle der Verletzung von Markenrechten sind zu unterscheiden (§ 10 MSchG): Verwechslungs- und Verwässerungsgefahr. Es besteht, neben dem Unterlassungsanspruch, jedenfalls ein Anspruch auf Schadenersatz, angemessenes Entgelt und Herausgabe der Bereicherung. Ein Übertragungsanspruch, der bei Domain Namen besonders wichtig ist, ist nicht vorgesehen, kann aber u.U. durch Analogie gewonnen werden (§ 30a Abs 3 MSchG; Schutz ausländischer Marken). Ansonsten kann hier zusätzlich das UWG Anwendung finden, indem ein sittenwidriger Wettbewerbsvorsprung durch die Verwendung der fremden Marke argumentiert wird.

Eine Marke kann sowohl national, EU-weit („EU-Gemeinschaftsmarke“) als auch international angemeldet werden. Hierfür ist das österreichische Patentamt, das Harmonisierungsamt für den Binnenmarkt bzw. die WIPO zuständig.

Bei Marken kann es zusätzlich problematisch sein, dass eine Webseite international abrufbar ist: Eine Marke kann zwar in zwei Ländern von verschiedenen Personen für die gleichen Waren registriert werden, aber nur einer von ihnen kann die Marke als Subdomain unter der gTLD ".com" verwenden. Ob dies immer und automatisch oder nur in bestimmten Fällen eine Verletzung des Markenrechts des Zweiten ist, ist umstritten[69]. In der Praxis ist eine gewisse Einschränkung wohl unumgänglich: Fehlt jeder Inlandsbezug, entweder durch den Domain Namen selbst (z.B. ccTLD) oder durch den Webseiteninhalt (Sprache, Währung etc.), könnte z.B. die internationale Zuständigkeit abgelehnt werden[70].

II.5.1. Was ist eine "Marke"?

Marken können alle Zeichen sein, die sich graphisch darstellen lassen, insbesondere Wörter einschließlich Personennamen, Abbildungen, Buchstaben, Zahlen und die Form oder Aufmachung einer Ware, d.h. auch Domain Namen. Die Zeichen müssen geeignet sein,

---

[68] LG Hamburg 1.3.2000, 315 O 219/99 http://www.netlaw.de/urteile/lghh_10.htm ("luckystrike.de"). Die Nutzung von Gratis-Webspace mit "Bezahlung" durch Bannereinblendungen bedeutet ein Handeln im geschäftlichen Verkehr.

[69] OGH 24.4.2001, 4 Ob 81/01t Anbieten einer Ware unter einer .com Domain: Abrufmöglichkeit von Österreich aus reicht als Inlandsbezug, auch wenn die Ware in Österreich nicht verkauft sondern nur produziert und exportiert wird. Etwas vorsichtiger OGH 29.5.2001, 4 Ob 110/01g Werbung für eine Slowenische Zigarettenmarke auf Deutsch unter einer ausländischen Domain ist zumindest auch nach Österreich gerichtet, sodass es nicht auf die bloße Abrufbarkeit ankommt. OGH 22.3.2001, 4 Ob 39/01s "rechnungshof.com": Rechtssatz: "Wird ein Name für eine im Ausland registrierte Internet Domain verwendet, so liegt darin ein Namensgebrauch im Inland, weil jede Internet Domain von einem inländischen Internetzugang aus angewählt werden kann." Im Urteil selbst wird jedoch wieder darauf abgestellt, dass der Inhalt der Webseite direkt auf Österreich ausgerichtet ist, da ja für eine Markenrechtsverletzung auch eine Verletzungshandlung im Inland erforderlich ist. Die Registrierung der Domain alleine ist daher anscheinend *keine* solche Verletzungshandlung.

[70] Die Behauptung einer möglichen Verletzung reicht daher für ein Gerichtsverfahren im Ausland aus. Materiell muss jedoch über die bloße Abrufbarkeit im Inland hinaus zusätzlich eine gewisse und intendierte Auswirkung auf das Inland vorliegen. Siehe dazu BGH 13.10.2004, I ZR 163/02 "hotel-maritime.dk", wonach eine Markenrechtsverletzung einen wirtschaftlich relevanten Inlandsbezug aufweisen muss. Siehe auch die Anmerkungen von Thiele zu diesem Urteil unter http://www.eurolawyer.at/pdf/BGH_I_ZR_163-02.pdf

Waren oder Dienstleistungen des Unternehmens von denjenigen anderer zu unterscheiden. Sie darf daher insbesondere nicht das Produkt beschreiben oder eine allgemeine übliche Bezeichnung sein. So ist z.B. "E-Commerce Shop" keine zulässige Marke für einen Internet-Shop. Für Domain Namen ist allerdings rein der Text bedeutsam; die graphische Gestaltung, z.B. bei Wort-Bild-Marken, bleibt mangels Darstellung im WWW außer Betracht.

Eine Marke soll der Unterscheidung von Waren und Dienstleistungen dienen, sodass der Kunde das Produkt eindeutig identifizieren und auf den Markeninhaber Rückschlüsse ziehen kann. Auf diesem Wege soll es ihm auch ermöglicht werden, die Beschaffenheit, Ausstattung und eventuell eingehaltene Qualitätsstandards schnell zu beurteilen.

Marken werden nach dem darunter betriebenen Wirtschaftsbereich bzw. vertriebenen Produkten oder Dienstleistungen in "Klassen" eingeteilt[71]. Eine Anmeldung hat die Klassen exakt zu bezeichnen, für welche die Marke später verwendet werden soll, und in welchen Bereichen sie dann geschützt ist. Innerhalb einer Klasse darf eine Marke nur einmal verwendet werden, bei verschiedenen Klassen jedoch auch von unterschiedlichen Personen[72]. Zu beachten ist, dass sich dies nur nach der Markeneintragung richtet, welche nicht notwendigerweise mit der aktuellen Verwendung übereinstimmen muss: Oft wird breiter registriert, um spätere Änderungen oder Ausweitungen des Geschäfts zu ermöglichen.

II.5.2. Benutzung der Marke

Um ein rechtliches Problem zu erzeugen, muss eine Marke auch "benützt" werden. Dies kann einerseits durch Registrierung einer zweiten Marke erfolgen, falls diese zu ähnlich ist, oder andererseits durch die Verwendung im Verkehr, etwa den Aufdruck auf Verpackungen oder in Form von Werbung. Immer erlaubt ist die Verwendung der Marke, um damit die „echten“ Produkte zu beschreiben, die "Namensnennung". So darf etwa ein Reinigungsunternehmen damit werben, dass es Staubsauger einer bestimmten Marke verwendet, sofern kein Anschein einer besonderen Beziehung zu dieser Firma geweckt wird.

Hier könnte schon die bloße Registrierung der Marke als Domain Name eine Benützung sein, sodass das Markenrecht schon verletzt würde, bevor noch eine Webseite unter dem Namen erreichbar ist. Dies wird zumindest in Österreich[73] jedoch vom OGH abgelehnt, was dem Gedanken entspricht, dass Marken nur für bestimmte Waren/Dienstleistungsgruppen geschützt sind. Bei der bloßen Registrierung ist kein echter Vergleich möglich, sondern erst bei den darunter zu findenden Webseiten, welche die Verwendung näher präzisieren[74]. In Deutschland[75] und der Literatur[76] wird eine abweichende Meinung vertreten: Die bloße Registrierung für sich alleine ist schon eine Benützung, da dadurch jeder andere,

---

[71] Beispiel: Klasse 10 beinhaltet u.a. Magnetaufzeichnungsträger, Schallplatten, Verkaufsautomaten und Mechaniken für geldbetätigte Apparate, Registrierkassen, Rechenmaschinen, Datenverarbeitungsgeräte und Computer, Feuerlöschgeräte.

[72] Siehe „computerdoktor.com“: OGH 24.6.2003, 4 Ob 117/03i http://www.eurolawyer.at/pdf/OGH_4_Ob_117-03i.pdf Die Marke wurde exakt am selben Tag (!) für jeweils verschiedene Klassen registriert, sodass im Endeffekt im Hinblick auf den Domain Namen die frühere tatsächliche Benutzung und damit § 9 UWG ausschlaggebend war.

[73] "Cyta.at": OGH 30.1.2001, 4 Ob 327/00t

[74] Daher auch keine Markenrechtsverletzung im Inland, wenn eine Österreichische Marke als DN verwendet wird, ohne dass der Inhalt der Webseite eine Verbindung zu Österreich besitzt (siehe auch oben).

[75] "Shell.de": BGH 22.11.2001, I ZR 138/99; http://www.jurpc.de/rechtspr/20020139.htm

[76] Siehe Burgstaller: Domainübertragung auch im Provisorialverfahren? http://www.multimedia-law.at/db8/profverf.html mit weiteren Nachweisen

inklusive dem Markeninhaber, an der Nutzung gehindert wird[77]. Ist keine Webseite unter dem Markennamen erreichbar, so kann eine Benützung auch darin liegen, den Domain Namen in E-Mail Adressen zu verwenden, da hierfür schon die Nameserver-Eintragung alleine ausreicht und diese technische Verwendung auch an die Öffentlichkeit tritt. Anhand des darunter betriebenen Geschäfts ist dann auch ein Vergleich der Klassen möglich. Selbst in Österreich ist jedoch die bloße Registrierung schon für eine einstweilige Verfügung, im Sinne der Vorbeugung bei Gefahr der entsprechenden Nutzung, ausreichend[78].

Die Verwendung einer catch-all Funktion, d.h. alle beliebigen Subdomains werden auf eine bestimmte Web-Site abgebildet (Beispiel: www.sonntag.fim.jku.at, sonntag.fim.jku.at, xyz.fim.jku.at, … werden alle auf die Web-Site www.fim.jku.at aufgelöst), beeinträchtigt in der Praxis Markenrechte. Hier wird eine Marke jedoch nicht tatsächlich verwendet, da sie nirgendwo direkt eingetragen ist. Dies ist daher im Hinblick auf den Markenschutz zulässig, stellt aber u.U. unlauteren Wettbewerb (§ 1 UWG) dar[79].

II.5.3. Verwechslungsgefahr

Eine identische Marke darf nicht für identische Waren bzw. Dienstleistungen verwendet werden. Gleiche oder ähnliche Marken dürfen aber auch bei Verwechslungsgefahr, also lediglich ähnlichen Waren/Dienstleistungen, nicht verwendet werden. Diese besteht dann, wenn für das Publikum durch die Verwendung die Gefahr besteht, die beiden Produkte zu verwechseln oder mit dem anderen gedanklich in Verbindung zu bringen[80], z.B. durch den Anschein einer Zusammenarbeit. Sind aber die Produkte bzw. Tätigkeiten völlig unterschiedlich, so besteht keine Verwechslungsgefahr und dieselbe Marke kann für beide registriert und verwendet werden[81].

Umstritten ist hier, ob sich bei Domain Namen die Verwechslungsgefahr lediglich auf den Domain Namen bezieht, oder auch die darunter abrufbaren Webseiten, und damit die angebotenen Waren, zu untersuchen sind. In einer deutschen Entscheidung[82] wurde festgestellt, dass lediglich der Name relevant ist und es auf den dahinter stehenden Inhalt nicht ankommt. Hierfür spricht auch, dass man Domain Namen vielfach auch Offline begegnet, z.B. auf Briefpapier, Firmenwagen etc. Dagegen spricht, dass der Domain Name meist kein eigenes Produkt ist, sondern es um die darunter angebotenen Inhalte geht. Der OGH hat im Fall "sattler.at"[83] hingegen auf die völlige Branchenunterschiedlichkeit abgestellt, und damit die Verwechslungsgefahr, wenn auch nicht im Hinblick auf den Markenschutz,

---

[77] Dem Argument ist entgegenzuhalten: Welcher Markeninhaber? Es können mehrere Berechtigte in verschiedenen Klassen nebeneinander bestehen. Jeder von diesen verhindert dann ja auch die Verwendung durch die anderen, sodass keiner von ihnen die Marke als Domain verwenden dürfte!

[78] „amade.net“: OGH 9.4.2002, 4 Ob 51/02g

[79] „whirlpools.at“: OGH 12.7.2005, 4 Ob 131/05a Die Klägerin verwendet „armstark-whirlpools.at“, die Beklagte „whirlopools.at“. Die Beklagte hat eine catch-all Funktion eingerichtet, sodass bei der (fehlerhaften) Eingabe von „armstark.whirlpools.at“ (Punkt statt Bindestrich) anstatt einer Fehlermeldung die Webseite der Beklagten erscheint.

[80] „wohnbazar.at“: OGH 19.8.2003, 4 Ob 160/03p

[81] Ein sehr geringer Unterschied der Marken kann durch größeren inhaltlichen Unterschied ausgeglichen werden: Kennzeichnungskraft der Marke, Zeichenähnlichkeit und Werk-/Produktähnlichkeit sind in Beziehung zu setzen. DN "oesterreich.de" und Titel "Österreich.de" vs. DN "österreich.de" ist erlaubt, da die Webseiten unterschiedlich genug sind. OLG München 20.10.2005, 29 U 2129/05 http://www.bonnanwalt.de/entscheidungen/OLG-Muenchen29U2129-05.html

[82] "epson.de" LG Düsseldorf 4.4.1997, 34 O 191/96 http://www.uni-muenster.de/Jura.itm/netlaw/epson.html; Brandl/Fallenböck, Zu den namens- und markenrechtlichen Aspekten der Domain Namen im Internet, wbl 1999, 481

[83] Gewerbliche Interessensvertretung der Lederwarenerzeuger, Taschner, Sattler und Riemer ⇔ Rechtsanwalt mit Familienname "Sattler";

verneint. Da der Name identisch war, wurde offensichtlich der Inhalt der Webseiten berücksichtigt. Dies wurde vom OGH inzwischen auch mehrfach ausdrücklich festgestellt[84].

II.5.4. Verwässerungsgefahr

Besteht keine Ähnlichkeit der Produkte, so kann trotzdem eine Rechtsverletzung möglich sein: Ist die Marke weithin bekannt und erfolgt die Verwendung eines gleichen oder ähnlichen Namens, um die Unterscheidungskraft und Wertschätzung der Marke in unlauterer Weise auszunutzen oder ist sie geeignet, diese zu beeinträchtigen, so kann der Markeninhaber die Verwendung untersagen[85]. Hier ist zusätzlich die besondere Bekanntheit der Marke (§ 10 Abs 2 MSchG) erforderlich. Diese wird von der Verkehrsgeltung unterschieden, welche, im Gegensatz zu diesem Fall, für nicht eingetragene Marken Bedeutung hat.

II.6. Besondere Aspekte

In diesem Abschnitt werden verschiedene andere Aspekte des Schutzes von Bezeichnungen behandelt: Beschreibende Namen, an denen niemandem ein besonderes Recht zusteht und daher auch kein individuelles Abwehrrecht möglich ist, sowie Ortsnamen als Domain. Von geringerer Bedeutung in diesem Zusammenhang sind (und werden daher nur kurz behandelt) der firmenrechtliche und der urheberrechtliche Schutz. Abschließend wird kurz erläutert, wie ein Urteil auf Übertragung eines Domain durchgesetzt werden kann.

II.6.1. Der Einfluss der Top-Level Domain auf die Verwechselbarkeit

Nach der derzeitigen Judikatur[86] ist die Top-Level-Domain eines Domain Namens bei der Beurteilung der Verwechselbarkeit wegzulassen, ebenso Zusätze wie „www". Ob „www.rtl.at" daher verwechslungsfähig mit RTL ist, richtet sich danach, ob „~~www.~~rtl.~~at~~", also „rtl" ähnlich zu „RTL" ist. In verschiedenen anderen Fällen wurde dies demgegenüber nicht so eindeutig ausgesprochen und etwa der Rechnungshof auf „rechnungshof.*gv.*at"[87] verwiesen. In Deutschland ist die Judikatur großteils ähnlich. Ein Teil der Lehre[88] meint jedoch, dass dies nicht so allgemein gilt und macht für besondere Fälle Ausnahmen.

So wird ein Internetnutzer unter „rechnungshof.com" wohl eher ein kommerzielles Angebot erwarten und nicht den „echten" Rechnungshof, im Gegensatz zu „rechnungshof.gv.at". Bei weitem nicht so eindeutig ist die Lage bei „rechnungshof.org", da auch der österreichische Rechnungshof zweifellos als „Organisation", wenn auch nicht als internationale wie z.B. die WIPO, zu bezeichnen ist. Es existieren aber noch weitere problematische Fälle. Beispielsweise kann die TLD auch direkt Teil des Namens sein: „parmal.at" für

---

[84] Zuletzt „amade.at", OGH 13.3.2002, 4 Ob 56/02t sowie „amade.at Neu": OGH 14.2.2006, 4 Ob 6/06w

[85] Beispiel: Die Marke "Firn" wurde auch für ein Cafe verwendet. "firn.at" OGH 25.5.2004, 4 Ob 36/04d

[86] „rtl.at": OGH 25.3.2003, 4 Ob 42/03k: „Die Netzbezeichnungen "www." und die Top-Level-Domains (TLD, zB ".at" und ".com") sind namensrechtlich ohne Belang. […] Die TLD tritt deshalb in ihrer Bedeutung für den von der Second-Level-Domain (Domainname) bestimmten Gesamteindruck zurück […]"

[87] „rechnungshof.com, -.net, -.org": OGH 22.3.2001, 4 Ob 39/01s

[88] Siehe etwa Thiele, kennzeichen.egal – Zur Unterscheidungskraft von Top-Level-Domains. http://www.eurolawyer.at/pdf/kennzeichen_egal.pdf

die Marke „Parmalat“, oder die Webseiten von Aktiengesellschaften unter der ccTLD von Antigua und Barbuda: „.ag“[89].

Generell ist wohl auf das allgemeine Verkehrsverständnis abzustellen und eine Gesamtbetrachtung vorzunehmen. Normalerweise wird der TLD keine Unterscheidungskraft zukommen, in besonderen, extra zu begründenden Fällen ausnahmsweise sehr wohl. Hierbei ist weitgehend die Verkehrsauffassung, d.h. der „normale Internettnutzer“, und die tatsächliche Praxis, wo/wie Firmen ihre Domain Namen reservieren, zu berücksichtigen: So werden unter „.com“ eher keine nationalen Behörden zu erwarten sein, aber umgekehrt nicht ausschließlich kommerzielle Angebote. Auch Privatpersonen oder gemeinnützige Organisationen besitzen aus historischen und anderen Gründen unter dieser TLD Webseiten.

II.6.2. Gattungsbegriffe und beschreibende Namen

Sowohl Gattungsbegriffe als auch beschreibende Namen stellen ein besonderes Problem im Internet dar, da sie alle Mitbewerber von der Verwendung ausschließen[90]. Im Markenrecht ist daher festgelegt, dass solche Namen nicht als Marke reserviert werden können (§ 4 Abs 1 Z 5 MSchG), da ein allgemeines Freihaltebedürfnis vorliegt[91]. Im Gegensatz zu einer Marke ist bei einem Domain Namen der Hauptzweck die Identifizierung des Anbieters, und nicht des dahinter stehenden Angebotes und dessen Unterscheidbarkeit von ähnlichen Produkten. Auch kann das Markenrecht nicht analog angewendet werden, da dort für solche Fälle ein besonderes hoheitliches Verfahren zur Prüfung vorgesehen ist, welches bei Domain Namen fehlt.

Das Standardargument für die Möglichkeit der Reservierung solcher Namen ist, dass durch eine leichte Abwandlung jederzeit auch andere Unternehmen einen äquivalenten Namen verwenden könnten. Da jedoch der normale Internet-Benutzer praktisch immer die einfachste Form verwenden wird, kann diesem Standpunkt wohl nicht gefolgt werden. Nur die wenigsten Benutzer werden noch abgewandelte Bezeichnungen versuchen, wenn sie mit der Grundform bereits Erfolg hatten[92]. Es kann daher eine wettbewerbswidrige Kanalisierung der Kundenströme erfolgen (§ 1 UWG; ein Übertragungsrecht ist hier nicht enthalten, da es dann ja auch dem Kläger verboten ist, diesen Namen zu verwenden!). Entsteht durch die Verwendung *keine* Irreführung der Kunden, z.B. indem eine Art "Alleinstellung" vermittelt wird, so ist die Verwendung zulässig[93]. Bei der Beurteilung, ob es sich um eine derartige "Konkurrenz-Verdrängung" handelt, ist wieder der Inhalt der Webseiten relevant. Meiner Meinung nach sollte dies jedoch streng geprüft werden, da in der Praxis die Kana-

---

[89] Siehe dazu das Urteil OLG Hamburg 16.6.2004, 5 U 162/03 http://www.aufrecht.de/3351.html, wonach bei der Verwendung des Domainnamens „tipp.ag“ diese TLD eine Täuschung von Kunden ist, da unter „.ag“ (zumindest in diesem Zusammenhang) eine Aktiengesellschaft, und damit die staatliche Lotteriegesellschaft, vermutet würde, und nicht eine „Tipp-Abgabengemeinschaft“.

[90] Brandl/Fallenböck, Der Schutz von Internet Domain Namen nach UWG, RdW 1999, 186; Hartmann, OLG Hamburg: Branchenbezeichnung als Domain Name. CR 12/1999, 779-783

[91] So würden etwa große Schwierigkeiten entstehen, wenn jemand sich "Fernseher" oder gar "cm" oder "kg" als Marke eintragen ließe. Siehe jedoch auch "Walkman", was eine geschützte Produktbezeichnung von Sony war, aber praktisch als Gattungsbegriff verwendet wird und dadurch den Markenschutz verlor. Hieraus ergeben sich viele Probleme. Weniger Fragen wirft etwa "Tixo" → "Klebeband" auf.

[92] Außerdem: Auf welche Art sollte die Abwandlung erfolgen? Der Grundname ist relativ eindeutig, die (möglichen und sinnvollen) Abwandlungen in der Regel jedoch von sehr großer Zahl.

[93] „mitwohnzentrale.de“: BGH 17.5.2001, I ZR 216/99, http://www.jurpc.de/rechtspr/20010219.htm sowie OLG Hamburg 6.3.2003, 5 U 186/01, http://www.jurpc.de/rechtspr/20030165.htm

lisierung wohl oft vorliegen wird[94]. Im Urteil „mitwohnzentrale.de“[95] wurde entschieden, dass ein Hinweis genüge, dass auf der Webseite nur Vereinsmitglieder angeführt sind; ein expliziter Verweis bzw. Link auf Konkurrenten sei jedoch nicht notwendig.

Auch eine Reservierung zum späteren Verkauf ist möglich. Siehe „kettenzüge.de“[96], wonach die Registrierung von Domains zum späteren Verkauf eine anerkannte geschäftliche Betätigung ist. Dieses Urteil erlaubt die Registrierung von beschreibenden Domain Namen, sofern Konkurrenten dadurch nicht systematisch blockiert würden, d.h. diese keinen beschreibenden Begriff zur gleichen Thematik reservieren könnten. Obwohl im gegenständlichen Fall vertretbar, da die Klägerin bereits „kettenzuege.de“ reserviert hatte, sollte dieses Urteil eher einschränkend gesehen werden. Konkret wurde darauf verwiesen, dass ein Auftreten unter anderer TLD, z.B. „.com“, weiterhin möglich ist.

II.6.3. Ortsnamen

Vielfach wurde versucht, den Namen von Orten zu reservieren. Dies geschah einerseits in Form von Domain Grabbing, was aber rechtlich inzwischen geklärt ist[97]. Andererseits besteht die Möglichkeit, dass Private einerseits über die Gemeinde berichten, d.h. die Webseite ist im weiteren Sinne im Interesse der Gemeinde, oder andererseits private/geschäftliche Zwecke verfolgen, z.B. dort ansässig sind.

Im letzteren Fall könnte zwar ein Hinweis eine Verwechslungsgefahr verhindern, doch können immer noch berechtigte Interessen des Ortes beeinträchtigt werden[98]. In diesem Fall handelt es sich um eine unberechtigte Namensanmaßung, da versucht wird, mit dem Namen der Gebietskörperschaft für Dinge zu werben, zu welchen diese keinerlei Verbindung hat. Dies ist unabhängig davon, ob die Gemeinde die Domain selber nutzen möchte.

Wird über die Gebietskörperschaft berichtet, z.B. durch ein regionales Informationsportal, so besteht zumindest laut OGH kein Problem und dies ist zulässig, siehe den Fall "adnet.at II". Da jedoch auch hierbei sehr oft ein kommerzieller Hintergrund besteht, z.B. Verkauf von Werbung auf der Seite, welcher sonst der Gemeinde zukommen würde, ist dies meiner Meinung nach eher fraglich[99]. Gegenüber der Gemeinde, welche die Bezeichnung als "bürgerlichen Namen" verwendet, besitzt der Verwender meist keinerlei eigene Berechtigung, sodass eher von einer Namensanmaßung auszugehen wäre. Noch diffiziler ist der Fall, wenn sich hinter der Webseite z.B. eine Gesellschaft befindet, welche nun ebenfalls

---

[94] Der Vergleich von Polishuk, Dirk: Gedanken zum Urteil des BGH vom 17.05.2001 - Az.: I ZR 216/99 - mitwohnzentrale.de http://www.jurpc.de/aufsatz/20020014.htm der generischen Domain mit einem Geschäft an der Hauptstraße ist jedoch verfehlt: An der Hauptstraße befinden sich viele praktisch gleichwertige Geschäftslokale und es existieren auch noch andere Städte; eine generische Domain ist jedoch absolut und weltweit einzigartig. Jeder auch nur geringfügig andere bzw. mit Zusätzen versehene Namen ist demgegenüber mit Wertverlust und stark verringerter Auffindbarkeit verbunden. Auch eine andere TLD hilft hier meist nicht. Suchmaschinen können den Nachteil ebenfalls nicht wettmachen.

[95] "mitwohnzentrale.de" BGH 17.5.2001 I ZR 216/99

[96] „kettenzüge.de“: LG Leipzig, 24.11.2005, 05 O 2142/05 http://www.jurpc.de/rechtspr/20060035.htm, Bestätigend das OLG Dresden 7.3.2006, 14 U 2293/05 http://www.rechtsanwalt.de/Urteile/OLG-Dresden_Domainrecht-Kaufangebot_generischer_Domains.html Für Domain-Grabbing ist eine Zwangslage erforderlich, welche bei Umlaut-Domains meist nicht vorliegen wird.

[97] „aistersheim.at“: OGH 20.1.2004, 4 Ob 258/03z

[98] "serfaus.at" OGH 16.12.2003, 4 Ob 231/03d mit Anmerkungen Thiele, wbl 2004/95, http://www.eurolawyer.at/pdf/OGH_4_Ob_231-03d.pdf

[99] Dieses Urteil wird auch von anderen kritisiert, z.B. Thiele, Anmerkungen zu adnet II (OGH 20.5.2003, 4 Ob 47/03w http://www.eurolawyer.at/pdf/OGH_4_Ob_47-03w.pdf

ein Namensrecht geltend machen kann. Dieses ist jedoch späteren Datums als das der Gemeinde und meist wohl in Anlehnung an diese ausgewählt, sodass auch hier die Gebietskörperschaft Vorrang besitzen sollte.

Trotz der Entscheidung im Fall „adnet.at“ stehen der Orts- oder Gebietsnamen daher wohl vorrangig den jeweiligen Gemeinden oder Körperschaften zu. Siehe dazu auch die EU-VO betreffend der Reservierung verschiedenster Schreibweisen von Ländernamen, welche nur den jeweiligen Staaten zustehen[100].

II.6.4. Firmenrechtlicher Schutz

Der § 37 Handelsgesetzbuch (HGB) schützt die Firma eines Kaufmannes, gewährt jedoch nur einen Unterlassungsanspruch. Dieser beinhaltet zwar eine Beseitigung, also die Löschung bei Domain Namen, jedoch *kein* Übertragungsrecht. Mit der Firma wird ein vollkaufmännischer Unternehmensträger bezeichnet, also nicht das Unternehmen als Sachgesamtheit, sondern dessen Rechtsträger. Nur Vollkaufleute können eine Firma besitzen und *müssen* diese auch verwenden.

Voraussetzung ist ein unbefugter Gebrauch der Firma, also der Bezeichnung des Unternehmens, z.B. im Firmenbuch oder im Geschäftsverkehr, der jemanden in seinen Rechten verletzt. Nicht nur den Inhaber der Firma, sondern auch andere in ihren Rechten, z.B. dem Namensrecht des Besitzers sofern davon abgeleitet, Verletzte können klagen. Die Verletzung rechtlicher Interessen wirtschaftlicher Art reichen aus, wobei diese nicht im Geschäftsverkehr erfolgen muss, nicht jedoch bloß ideelle[101]. Die Befugnis und der Gebrauch sind analog zum Namensrecht zu beurteilen.

Dieser Schutz besitzt keine praktische Bedeutung, da der Firmenname auch über das Namens- bzw. Wettbewerbsrecht geschützt ist.

II.6.5. Urheberrechtlicher Schutz

Der Titelschutz nach § 80 UrhG[102] schützt Werke der Literatur oder der Kunst, daher auch Software, selbst wenn für diese kein urheberrechtlicher Schutz (mehr) besteht. Es kommt hier darauf an, dass andere Werke gehindert werden, einen gleichen oder gleichartigen Titel oder eine Bezeichnung, aber auch eine äußere Ausstattung eines Werkes, z.B. eine bestimmte Umschlaggestaltung, zu verwenden, die geeignet sind, Verwechslungen hervorzurufen. Um geschützt zu sein, muss der Titel selbst (alleine, ohne Rest des Werkes) Kennzeichnungs- und Unterscheidungskraft[103] besitzen, also bereits eine gewisse Bekanntheit erlangt haben.

---

[100] Verordnung Nr. 1654/2005 der Kommission vom 10.Oktober 2005 zur Änderung der Verordnung Nr. 874/2004 zur Festlegung von allgemeinen Regeln für die Durchführung und die Funktionen der Domäne oberster Stufe „.eu“ und der allgemeinen Grundregeln für die Registrierung, ABl L 266/35 vom 11.10.2005, http://www.bmvit.gv.at/telekommunikation/tld/downloads/vo2005de1654.pdf

[101] Schuhmacher in Straube, Kommentar zum Handelsgesetzbuch, Wien: Manz 1995, I/§ 37

[102] In Deutschland in § 5 Abs 1, 3 MarkenG geschützt; Fälle hierzu: "freundin.de" (OLG München I 2.4.1998, 6 U 4798/97), "bike.de" (LG Hamburg 13.8.1997, 315 O 120/97, MMR 1998, 485ff), "welt-online.de" (LG Hamburg 13.1.1999, 315 O 478/98), "kueche-online.de" (OLG München 6 U 5719/99; http://www.domain-recht.de/magazin/werktitel.php). Österreich: „domainbox.at“ (LG Salzburg 22.11.2002, 5 Cg 144/01z), „amtskalender.at“ (OGH 21.1.2003, 4 Ob 257/02a), „steuerprofi.at“ (OGH 19.12.2000, 4 Ob 256/00a)

[103] Rein beschreibende Titel z.B. "Handbuch Netzwerktechnik", sind daher nicht geschützt.

Für Domain Namen bedeutet dies, dass Titel von Büchern, Zeitschriften oder Kunstwerken und ähnliche Bezeichnungen nur von Berechtigten als Domain Namen verwendet werden können. Der Name an sich ist wohl ohne Rücksicht auf eine etwaige Verwechslungsgefahr des Inhalts der Webseiten geschützt[104], da das Gesetz neben dem Titel auch explizit die „äußere Ausstattung“ erwähnt. Hieraus kann man schließen, dass es mehr auf den äußeren Anschein ankommt, als auf das, was bei genauerer Betrachtung (=Lesen einer Zusammenfassung/Klappentext) erkennbar wäre. Die Eingabe des Domain Namens im Internet und Abruf der zugehörigen Webseite entspricht etwa dem Aufschlagen des Buches und Lesen der ersten Seiten und ist daher "zuviel". Es kommt hier nicht auf eine Verwechslungsgefahr bei genauerer Untersuchung an, als vielmehr auf den ersten Blick. Dies umso mehr, als Domain Namen auch auf Papier (z.B. Briefen) vorkommen, und daher eine sofortige Prüfung des Inhalts u.U. nicht möglich ist, was Abbildungen des Buchumschlags ähnelt.

II.6.6. Übertragung von Domain Namen

Wurde vor einem österreichischen Gericht die Übertragung eines Domain Namens erreicht oder ist ein entsprechendes ausländisches Urteil vollstreckbar, so stellt sich die Frage, wie es in die Realität umgesetzt werden kann. Dies kommt in der Praxis in Österreich nur selten vor, da kein allgemeiner Anspruch auf einen bestimmten Domain Namen besteht[105], sondern nur eine im Verhältnis zu anderen Personen unrechtmäßige Verwendung. D.h. jemand anderer, also der Beklagte, darf den Namen nicht verwenden, weil der Kläger ein besseres Recht besitzt. Ein Dritter kann jedoch noch bessere Rechte daran besitzen als der Kläger, sodass dieser keine absolute Position hat. Das gleiche Problem stellt sich jedoch, wenn der Beklagte zur Löschung verpflichtet wurde, worauf die normale Folge die Registrierung durch den Kläger ist bzw. sein soll.

Eine direkte Übertragungsanweisung beinhaltet das schwere Problem, dass das Urteil aus einem Streit zwischen dem derzeitigen Inhaber der Domain und einem (zukünftigen) neuen ergeht. Nicht Partei des Verfahrens, und daher auch nicht an das Urteil gebunden, ist die Registrierungsstelle. Da es sich bei der Domainregistrierung um einen privatrechtlichen Vertrag handelt, kann die Registrierungsstelle nicht einfach dazu gezwungen werden, einen Wechsel ihres Vertragspartners zu akzeptieren. Es bliebe daher als einzige Lösung übrig, den bisherigen Inhaber zur Löschung durch Nicht-Fortsetzung oder Beendigung des Vertrages zu zwingen. Befindet sich bereits ein anderer auf der Warteliste für diesen Domain Namen (sofern eine solche existiert) oder ist ein Dritter bei der Neu-Registrierung schneller, so führte dies zu keiner Übertragung der Domain.

Zur Lösung dieses Problems verpflichten sich die Registrierungsstellen (z.B. nic.at; AGB’s Punkt 3.6), einen Domain auf Antrag des derzeitigen Inhabers auf jemanden anderen zu übertragen und mit diesem einen Vertrag zu schließen, sofern er die allgemeinen Voraussetzungen (Volljährigkeit, Angabe der notwendige Informationen wie der IP-Adressen der Nameserver etc.) erfüllt. Dieses Recht des Inhabers kann nun im schlimmsten Fall auf Grund des gegen ihn ergangenen Urteils nach Exekution vom Kläger selbst ausgeübt werden und es erfolgt eine Übertragung der Domain.

---

[104] Andere Meinung Thiele in den Leitsätzen zu „amtskalender.at“: http://www.i4j.at/entscheidungen/ogh4_257_02a.htm, was aber meiner Meinung nach so aus dem Urteil nicht hervorgeht, da dort nur über wettbewerbsrechtliche Aspekte geurteilt wurde.

[105] „omega.at“: OGH 8.2.2005, 4 Ob 226/04w. Etwas anderes gilt natürlich im Verhältnis zu einem Dienstleister, der für jemanden anderen eine Domain auf dessen Namen registrieren sollte, dies jedoch auf seinen eigenen vornahm. Hier ist eine Verurteilung auf Übertragung, beruhend auf dem Vertrag, natürlich jederzeit möglich.

II.6.7. Wartestatus

Um einer Verurteilung zu entgehen bzw. die Domain zu behalten, besteht die Möglichkeit, diese während des Verfahrens an jemanden anderen zu übertragen. Dies verhindert zwar nicht unbedingt eine Verurteilung, aber jedenfalls die Übertragung der Domain an den Kläger im Erfolgsfall. Das gleiche Ergebnis kann auftreten, wenn eine Löschung angeordnet wurde, und jemand anderer bei der Neu-Registrierung schneller war als der Kläger. Dieses unbefriedigende Ergebnis kann durch Sperren von Verfügungen über die Domain vermieden werden. Ein einfaches gerichtliches Verbot an den Beklagten reicht hier nicht, da dies zwar zu Schadenersatz bei Missachtung führt, aber die Domain dennoch von Dritten rechtswirksam erlangt werden kann, sofern diese nichts von dem Verbot wussten. Ein Verbot an einen unbeteiligten Dritten, die Registrierungsstelle, ist hier nicht möglich.

Die nic.at stellt hierfür den Wartestatus 1 und 2 zur Verfügung. Für jeden Streitfall[106] kann dies nur ein einziges Mal erfolgen. Um eine Domain in den Wartestatus 1 zu versetzen reicht eine schriftliche Bescheinigung der Anspruchsgrundlagen aus. In diesem Zustand kann die Domain weiterhin verwendet oder gekündigt werden (und auf diese Weise auch an einen Dritten gelangen), aber nicht *direkt* an einen Dritten übertragen werden. Eine Aufhebung erfolgt durch gemeinsamen Antrag der Parteien. Der Wartestatus 1 bleibt für maximal ein Monat aufrecht. Auf Aufforderung einer Partei kann dieser Status um ein Monat verlängert werden.

Ist bereits ein Gerichts- oder Schiedsverfahren anhängig und wird dies nachgewiesen, so kann die Domain in den Wartestatus 2 versetzt werden. Dieser Status ist zeitlich unbegrenzt und dauert bis zur Beendigung des Verfahrens. In dieser Zeit ist die Domain weiterhin nutzbar, kann aber nicht übertragen werden. Eine Kündigung ist hier dennoch möglich, sodass ein Eigentümerwechsel nicht unbedingt verhindert wird, u.a. auch, da der Vertrag ebenso durch Nichtzahlung der Gebühr enden kann.

Obwohl der Wartestatus keine absolute Garantie ermöglicht, ist es in einem Streitfall dennoch äußerst wichtig, diese Maßnahme zu ergreifen - insbesondere da praktisch kostenlos - um im Falle eines positiven Urteils dieses dann auch tatsächlich und erfolgreich umsetzen zu können. Der Wartestatus stellt jedoch keine Reservierung dar: Nach dem Ende des Wartestatus, aus welchem Grund auch immer, wird die Domain an den ersten Antragsteller vergeben, was nicht unbedingt der Beantrager des Wartestatus sein muss.

II.7. UDRP: Das Streitbeilegungsverfahren der ICANN

Bei der "Uniform Domain Name Dispute Resolution Policy" handelt es sich um einen Modell-Vertrag, welcher von der ICANN erarbeitet wurde und von allen Registrierungsstellen für gTLDs (mit Einschränkungen bei manchen) sowie verschiedenen ccTLD Registrierungsstellen verwendet wird. Sie ist über die AGBs Teil des Vertrages zwischen dem Inhaber der Domain und der Registrierungsstelle, woraus sich ihre Gültigkeit ergibt[107]. Die ICANN

[106] Was vermutlich bedeutet: Selbe Domain, selbe Streitparteien, aber Unerheblichkeit der Anspruchsgrundlagen.

[107] Problematisch könnte sein, ob dies auch gegenüber Konsumenten gilt: Die Schiedsabrede ist aber wohl eher keine überraschende bzw. (gröblich) benachteiligende (§ 864a, § 879 Abs 3 ABGB) Klausel. Da das Verfahren für den Beklagten gratis, ansonsten günstig, sowie schneller ist als ein Gerichtsverfahren und immer noch die nationalen Gerichte angerufen werden können, ist eine Benachteiligung nur schwer möglich. Beispielsweise die Verfahrenssprache, meist Englisch, könnte jedoch Fragen aufwerfen. Ebenso sind manche verfahrensrechtliche Elemente zumindest diskussionswürdig, z.B. dass der Kläger die Schiedsstelle auswählt, welche daher ev. nicht ganz unparteiisch ist (um weitere Fälle und damit Einkommen an sich zu ziehen). Siehe dazu und weiteren Fragen Hestermeyer, Holger, The Invalidity of ICANN's UDRP

hat keine hoheitlichen internationalen Befugnisse und kann daher keine weltweit gültigen Gesetze erlassen. Zur Zeit stehen vier Organisationen zur Verfügung, welche Schiedsverfahren nach dieser Policy durchführen.

Ein Domainbesitzer ist nur dann diesem Verfahren und diesen Regeln unterworfen, wenn er ihm entweder freiwillig zustimmt, was bei allen Domainstreitigkeiten möglich ist, auch wenn dies nicht in der Registrierung enthalten war, oder er durch seinen Vertrag mit der Registrierungsstelle dazu verpflichtet ist.

II.7.1. Verpflichtungen der Registrierungsstelle

Eine Registrierungsstelle verpflichtet sich, Änderungen bei Domain-Registrierungen ausschließlich in folgenden Fällen vorzunehmen[108]:

- Aufforderung durch den Inhaber der Domain
- Entscheidung eines *zuständigen*[109] Gerichts- oder Schiedsgerichts
- Entscheidung eines Verfahrens nach der Policy der ICANN, bei welchem der Inhaber der Domain Partei war
- Sondervereinbarungen oder lokale Gesetze sehen dies vor

II.7.2. Streitgegenstand

Es werden nur sehr eng begrenzte Streitigkeiten nach dieser Policy ausgetragen. Der Beschwerdeführer muss nachweisen, dass alle drei folgenden Elemente kumulativ zutreffen:

- Der Domain Name ist identisch oder verwechslungsfähig ähnlich zu einem Warenzeichen oder einer Dienstleistungsmarke[110], auf das der Beschwerdeführer ein Recht hat[111], und die bereits bei der Domain-Registrierung[112] bestand.
- Der Inhaber der Domain hat weder Recht noch berechtigtes Interesse in Bezug auf den Namen.
- Der Domain Name wurde bösgläubig registriert *und* wird bösgläubig verwendet[113].

Under National Law. Minnesota Intellectual Property Review 1 (3) 2002, 1-57 http://mipr.umn.edu/archive/v3n1/hestermeyer.pdf

[108] Siehe aber z.B. Anderl: Streitbeilegung nach der UDRP – Endstation Cheoranam-do oder zurück zum Start? ecolex 2006, 38-41 http://www.dbj.at/publ332.pdf

[109] Nach eigener Beurteilung der Registrierungsstelle!

[110] Dies wird meist eine eingetragene Marke sein. In manchen Ländern sind jedoch auch "common law" Marken geschützt: Diese sind nicht registriert, aber aufgrund langer/weit verbreiteter/… Verwendung bekannt.

[111] D.h. ein Markeninhaber kann gegen einen Domaininhaber vorgehen. Ohne (eingetragene; siehe aber die Möglichkeit von Marken mit Verkehrsgeltung; FN 110) Marke ist die UDRP nicht anwendbar, ebenso wie ein Domaininhaber nicht gegen einen Markeninhaber vorgehen kann. Alle diese und anderen Fälle sind daher wie bisher von den zuständigen Gerichten, Verwaltungsbehörden etc. nach nationalem Recht zu beurteilen.

[112] Siehe aber den Fall "Delikomat" (WIPO D2001-1447; http://arbiter.wipo.int/domains/decisions/html/2001/d2001-1447.html), wo die Bekanntheit zu diesem Zeitpunkt bereits ausreichte. Dies wurde als "common-law" Marke angesehen, obwohl dort (=Österreich) Markenrecht mit *expliziter* Registrierung gilt.

[113] Hier besteht bei den Entscheidungen keine Einigkeit: Nach manchen Entscheidungen ist statt des "und" ein logisches "oder" zu lesen. Die UDRP ist hier leider nicht ganz klar. Siehe dazu auch Fußnote 115!

II.7.3. Rechtsfolgen

Ausschließlich die Löschung oder der Transfer eines Domain Namens an den Beschwerdeführer kommen als Ergebnis eines erfolgreichen Verfahrens in Frage.

Handelt es sich um einen Fall von RDNHJ (Reverse Domain Name Hijacking; Versuch, dem rechtmäßigen Inhaber eines Domain Namens diesen per UDRP zu entziehen), so ist dies im Urteil explizit anzumerken, was u.U. für spätere Schadenersatzprozesse wichtig ist. Dies ist in der Praxis jedoch äußerst selten.

II.7.4. Beispiele für bösgläubige Registrierung und Benutzung

Es ist erforderlich, dass *sowohl* die Registrierung bzw. der Erwerb *als auch* die Verwendung einer Domain[114] bösgläubig erfolgen müssen, oder dass bereits *eines* dieser beiden Elemente vorliegt. Manchmal wird auch die Verwendung mit einer Unterlassung begründet: überhaupt nichts tun wird mit bösgläubiger Verwendung gleichgesetzt. Die Entscheidungen in konkreten Fällen divergieren[115]. Meiner Meinung nach ist beides erforderlich, was durch den klaren Text und den Sinn der UDRP begründet ist. Fehlt bei dieser Meinung einer der beiden Teile, z.B. bei gutgläubigem Erwerb und späterer bösgläubiger Benützung, so ist abweisend zu entscheiden und Abhilfe über nationale Gerichte zu suchen.

U.a. in folgenden Fällen wird eine bösgläubige Registrierung und Benützung angenommen (*demonstrative* Aufzählung in der UDRP!):

- Registrierung bzw. Erwerb erfolgten hauptsächlich für den Verkauf, die Vermietung oder eine sonstige Übertragung des Domain Namens an den Inhaber des Warenzeichens oder der Dienstleistungsmarke oder an einen Wettbewerber desselben, und zwar für eine Gegenleistung, welche die tatsächlichen Kosten übersteigt.
- Die Registrierung erfolgte, um den Inhaber der Marke an der Verwendung des Domain Namens zu hindern. Zusätzlich müssen derartige Registrierungen gehäuft („pattern of conduct“) erfolgen.
- Die Registrierung erfolgte hauptsächlich, um einen Wettbewerber zu schädigen.
- Die Verwendung des Domain Namens erfolgt wissentlich, um einen geschäftlichen Nutzen durch Webseitenbesucher zu erzielen, indem die Wahrscheinlichkeit einer Verwechslung mit der Marke des Beschwerdeführers, dessen Mitarbeit, oder dessen Verbindung zu dieser Webseite, einem Produkt oder einer Dienstleistung hergestellt wird.

---

[114] Zu einem beliebigen Zeitpunkt: Einmal bösgläubig, immer bösgläubig. Sonst könnte z.B. eine Modifikation der Webseiten während des Verfahrens den Ausgang verändern, wonach die alten Inhalt sofort wiederhergestellt würden. Hierzu existieren auch andere Meinungen (dissenting opinion in Hearst vs. Spencer; esquire.com; http://www.arbforum.com/domains/
decisions/93763.htm)!

[115] Siehe z.B. "Telstra.org" (WIPO D2000-0003; http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0003.html), wo alleine aus der böswilligen Registrierung auf die böswillige Verwendung geschlossen wurde, ohne dass zusätzliche Elemente behauptet oder nachgewiesen wurden.

II.7.5. Beispiele für berechtigte Interessen

Mögliche berechtigte Interessen für die Verwendung eines Domain Namens, welche daher eine Übertragung ausschließen, sind u.a. (*demonstrative* Aufzählung in der UDRP!):

- Bevor die Streitigkeit dem Inhaber bekannt wurde, wurde der Name von diesem bereits für echte Angebote zum Verkauf von Waren oder Dienstleistungen verwendet, oder es bestanden nachweisbar schon damals Vorbereitungen für eine solche Nutzung.
- Der Beschwerdegegner ist als Person, Unternehmen oder Organisation unter dem Domain Namen bekannt, auch wenn hierfür kein Markenrecht besteht.
- Der Domain Name wird für einen berechtigten nicht-kommerziellen oder erlaubten Zweck verwendet, und es besteht keine Absicht, wirtschaftlichen Gewinn aus der Umleitung von Kunden zu ziehen oder die Marke zu verwässern.

II.7.6. Wichtige Elemente des Prozesses

Die Entscheidung erfolgt durch einen einzelnen Schiedsrichter. Auf Verlangen einer der Parteien kann auch ein Senat von drei Schiedsrichtern bestellt werden. In diesem Fall kann jede Partei einen Dreiervorschlag für jeweils einen Richter erstellen. Der dritte Schiedsrichter wird über einen Fünfervorschlag der Schiedsstelle von den Parteien gewählt. Die konkrete Auswahl des/der ersten beiden Schiedsrichter, sowie subsidiär auch des dritten, erfolgt durch die Streitschlichtungsstelle, welche die Vorschläge der Parteien nach Möglichkeit befolgen soll. Die Parteien haben kein Ablehnungsrecht; Richter haben etwaige Umstände welche auf eine mangelnde Unparteilichkeit hinweisen der Streitschlichtungsstelle mitzuteilen, die dann eigenständig über eine Auswechslung entscheidet.

Es handelt sich in der Regel um ein reines Aktenverfahren. Eine mündliche Verhandlung (auch per Videokonferenz, Telefon etc.) ist nur in Sonderfällen und ausschließlich auf Anordnung des Schiedsgerichts vorgesehen. Das Schiedsgericht kann den Gang des Verfahrens frei bestimmen, hat jedoch auf Gleichheit der Parteien und einen raschen Ablauf zu achten. Es besteht freie Beweiswürdigung.

Die Sprache des Verfahrens ist die Sprache des Registrierungsvertrages, sofern dort, oder mittels Parteienvereinbarung, nicht eine andere vorgesehen wird[116].

Versäumt eine Partei eine Frist, so hat das Schiedsgericht ein Versäumnisurteil zu fällen, wobei keine Wiedereinsetzung vorgesehen ist. Über die allgemeine Verfahrensgewalt sollte dies dennoch möglich sein; die Anforderungen werden jedoch in der Praxis hoch sein.

Es existieren keine Zwangsmöglichkeiten. Kommt eine Partei einer Aufforderung des Schiedsgerichts, beispielsweise zur Vorlage bestimmter Dokumente, nicht nach, so hat es sich damit zu begnügen und daraus seine Schlüsse zu ziehen.

Für die Kommunikation zwischen den Parteien, der Registrierungsstelle und dem Schiedsgericht bestehen besondere Vorschriften, welche genau einzuhalten sind. So ist etwa keine "geheime" Kommunikation einer Partei mit dem Schiedsgericht erlaubt. Alle Mitteilungen sind immer sowohl an das Schiedsgericht als auch an die Gegenpartei zu richten.

---

[116] Dies kann unangenehme Konsequenzen nach sich ziehen: Siehe den in Anderl, Streitbeilegung nach der UDRP – Endstation Cheonranam-do oder zurück zum Start? ecolex 2006, 38-41 geschilderten Fall, bei welchem die Verfahrenssprache Koreanisch war, was zu entsprechenden Verzögerungen und Kosten für Übersetzungen führte.

Bei der Einbringung einer Beschwerde muss eine Unterwerfungserklärung unter einen "gemeinsamen Gerichtsstand" für Streitigkeiten über ein abänderndes Urteil (Entzug oder Transfer eines Domain Namens) abgegeben werden. Hierbei handelt es sich in Sonderfällen um den Hauptsitz der Registrierungsstelle, bei welcher der Domain Name registriert wurde und sonst um die Adresse des Inhabers der Domain nach der Datenbank der Registrierungsstelle (WHOIS) zum Zeitpunkt der Einbringung der Beschwerde.

Alle Entscheidungen werden ausnahmslos, komplett und im Internet veröffentlicht, wobei keine Anonymisierung der Beteiligten oder der Domain Namen erfolgt, anders als z.B. beim Österreichischen OGH.

Um Missbrauch vorzubeugen, ist eine Übertragung der Domain während des Verfahrens und bis 15 Tage nach dessen Abschluss (wegen der Option, anschließend ein Gerichtsverfahren zu beginnen) nicht möglich.

II.7.7. Gerichtsentscheidungen

Ein Verfahren nach dieser Policy schließt ein normales Gerichtsverfahren zu keinem Zeitpunkt aus. Nach der Entscheidung bleiben zehn Werktage, um ein solches Verfahren anhängig zu machen. Erfolgt dies innerhalb dieser Frist *und* wird dies der Registrierungsstelle mitgeteilt, so wird die Entscheidung des Schiedsgerichts bis zur Entscheidung des Gerichts nicht umgesetzt. Das bedeutet, bei Einstellung des Gerichtsverfahrens ohne Endurteil wird es später vollzogen.

II.7.8. Kosten

Alle Kosten des Verfahrens[117] trägt der Beschwerdeführer, es sei denn der Beschwerdegegner wählt einen Dreiersenat, obwohl der Beschwerdeführer nur einen Einzelrichter verlangte. In diesem Fall werden die Gesamtkosten gleichmäßig (50:50) geteilt.

Diese Kosten können jedoch später z.B. innerstaatlich als Schadenersatz geltend gemacht werden[118], da es sich bei der UDRP, zumindest nach Österreichischem Recht, nicht um ein Schiedsverfahren handelt, bei welchem dies ausgeschlossen wäre[119]. Der Grund hierfür ist, dass im Anschluss an die UDRP immer noch die Gerichte angerufen werden können, was bei einem (nach österreichischem Verständnis) „echten“ Schiedsverfahren nicht mehr möglich wäre.

II.7.9. Bewertung

Es handelt sich bei der UDRP um eine rasche, da typischerweise binnen 45-60 Tagen abgeschlossene, und kostengünstige Möglichkeit, gegen unberechtigte Domainbesitzer vorzugehen. Eine Konsequenz der Internationalität ist jedoch, dass der Anwendungsbereich recht eng ist: Nur Streitigkeiten im Zusammenhang mit Marken werden entschieden. Das liegt daran, dass das Markenrecht weltweit relativ einheitlich ist (gleiche Grundprinzipien), während z.B. das Namensrecht sehr unterschiedlich sein kann.

---

[117] Beispiel WIPO (seit 2002 unverändert; für 1 Richter bzw. 3er-Senat): 1-5 Domain Names = US$ 1.500/4.000, 6-10 = US$ 2.000/5.000, >10 = Nach Vereinbarung mit WIPO

[118] Siehe "Delikomat", das österreichische "Gegenstück" im Anschluss an die WIPO Entscheidung zum selben Domainnamen; (siehe Fußnote 112), wo es um genau diese Kosten ging. OGH 16.3.2004, 4 Ob 42/04m

[119] Dort müssten die Kosten im Verfahren zugesprochen werden, was jedoch bei der UDRP nicht vorgesehen ist.

In Bezug auf die Entscheidungen wird angemerkt, dass starke Divergenzen zwischen den verschiedenen Richtern bestehen, da kein einheitlicher Auswahlprozess und keine übergeordnete Stelle zur Vorgabe von Leitentscheidungen, wie etwa ein „Berufungsgerichtshof“, existieren. Ein anderes Problem ist, dass die meisten Fälle von der WIPO (World Intellectual Property Organization) verhandelt werden, welche aufgrund ihres Hintergrunds eher "Markeninhaber-freundlich" ist. Dies hängt auch damit zusammen, dass der Beschwerdeführer (=der Markeninhaber) den Einzelrichter auswählt, wobei verständlicherweise eher markenfreundliche Richter ausgewählt werden. Dies ist das so genannte "Forum shopping". Hier wäre daher eine feste Geschäftsverteilung für ein garantiert faires Verfahren unbedingt erforderlich.

II.8. Sonstige Schiedsverfahren

Für bestimmte TLDs existieren besondere Schiedsverfahren. Hier werden nur zwei ganz kurz erwähnt: Für die neue TLD der Europäischen Union (.eu) und für Österreich (.at).

II.8.1. Streitschlichtung für .eu Domains

Für diese spezielle Domain existiert ein eigenes Schiedsverfahren[120], das zwar dem der UDRP ähnelt, jedoch einige kleine, aber bedeutende Abweichungen besitzt. So ist etwa eindeutig, dass böswillige Registrierung *oder* böswillige Verwendung jeweils auch für sich ausreichen. Darüber hinaus besteht keine Beschränkung auf Markenrecht alleine, sondern auch Wettbewerbs- und Namensrecht wird hierbei in bestimmten Aspekten behandelt. Bösgläubigkeit liegt u.a. bei Registrierung zum Verkauf, Behinderung, zweijähriger Nicht-Nutzung, sechsmonatiger Nichtnutzung nach Ankündigung der Nutzung in einem Streitbeilegungsverfahren, Behinderungswettbewerb, Irreführung von Internet-Nutzern, sowie Registrierung eines Personennamens ohne Verbindung zum Inhaber der Domain vor. Weitere Unterschiede und Details werden hier nicht näher erläutert. Die tatsächliche Durchführung von Schiedsverfahren obliegt dem Tschechischen Schiedsgericht in Prag[121].

II.8.2. Streitschlichtung für .at Domains

Die Nic.at hat für .at Domänen nicht die UDRP herangezogen, sondern es wurde mit 1.3.2003 eine eigene Streitschlichtungsstelle mit eigenen Regeln gegründet. Diese hat allerdings bisher (April 2006) erst zwei Fälle entschieden.

Im Gegensatz zur UDRP wird das gesamte Recht angewendet (UWG, MSchG, UrhG, ...). Ein weiterer Unterschied ist, dass bei einer Domainregistrierung keine Unterwerfungserklärung abgegeben wird. Um diese Streitschlichtung in Anspruch zu nehmen, müssen sich beide Parteien freiwillig dem verfahren unterwerfen, wie bei jedem anderen Schiedsverfahren auch.

---

[120] Verordnung 874/2004 der Kommission vom 28. April 2004 zur Festlegung von allgemeinen Regeln für die Durchführung und die Funktionen der Domain oberster Stufe „.eu“ und der allgemeinen Grundregeln für die Registrierung, ABl L 162/40 vom 30.4.2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0874:DE:HTML

[121] http://www.adreu.eurid.eu/

II.9. Literatur

II.9.1. Allgemein

Aicher, Josef in Rummel, Peter: Kommentar zum ABGB[2], Wien: Manz 1990, I/§ 43

Anderl: Streitbeilegung nach der UDRP – Endstation Cheonranam-do oder zurück zum Start? ecolex 2006, 38-41

Bettinger, Torsten: ICANN's Uniform Domain Name Dispute Resolution Policy, CR 4/2000, 234-239

Brandl, Margit, Fallenböck, Markus: Der Schutz von Internet Domain Namen nach UWG, RdW 1999, 186

Brandl, Margit, Fallenböck, Markus: Zu den namens- und markenrechtlichen Aspekten der Domain Namen im Internet, wbl 1999, 481

Burgstaller, Peter: Domainübertragung auch im Provisorialverfahren? http://www.multimedia-law.at/db8/profverf.html

Dillenz, Walter: Praxiskommentar zum österreichischen Urheberrecht und Verwertungsgesellschaftenrecht. Wien: Springer 1999

Geist, Michael: Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP. http://www.udrpinfo.com/resc/fair.pdf

Geist, Michael: Fundamentally Fair.com? An Update on Bias Allegations an the ICANN UDRP. http://aix1.uottawa.ca/~geist/fairupdate.pdf

Gravenreuth, Günter Frhr. von: OLG Dresden: "cyberspace.de" CR 9/1999, 589-592

Hartmann, Matthias: OLG Hamburg: Branchenbezeichnung als Domain Name. CR 12/1999, 779-783

Helm, Günther: Domain Grabbing und andere Tatbestände im Internet. Diplomarbeit. Universität Linz, 2000.

Hestermeyer, Holger: The Invalidity of ICANN's UDRP Under National Law. Minnesota Intellectual Property Review 1 (3) 2002, 1-57 http://mipr.umn.edu/archive/v3n1/hestermeyer.pdf

The Internet Corporation for Assigned Names and Numbers (ICANN): http://www.icann.org/

Liste der Schiedsgerichts-Organisationen: http://www.icann.org/dndr/udrp/approved-providers.htm

Mayer-Schönberger, Viktor, Hauer, Karin: Kennzeichenrecht & Internet Domain Namen. ecolex 1997, 947-951

Mockapetris, P.: Domain Names - Concepts and Facilities (RFC 1034) http://www.faqs.org/rfcs/rfc1034.html

N. N.: "Domain Grabbing" als sittenwidriger Behinderungswettbewerb. ecolex 1999, 559f

Polishuk, Dirk: Gedanken zum Urteil des BGH vom 17.05.2001 - Az.: I ZR 216/99 - mitwohnzentrale.de. http://www.jurpc.de/aufsatz/20020014.htm

Schanda, Reinhard: Internet Domain Names haben Namensfunktion, ecolex 1998, 565

Schanda, Reinhard: Internet Domain Names und Namensrecht, ecolex 1999, 703-705

Schanda, Reinhard: § 43 ABGB bietet Anspruchsgrundlagen gegen Domain Namen, ecolex 2000, 215

Schuhmacher, Wolfgang in Straube, Manfred: Kommentar zum Handelsgesetzbuch[2], Wien: Manz 1995, I/§ 37

Thiele, Clemens: Privatrechtlicher Schutz von Ortsnamen im Internet. Österreichische Gemeindezeitung 11/99, 4-13

Thiele, Clemens: kennzeichen.egal – Zur Unterscheidungskraft von Top-Level-Domains. http://www.rechtsprobleme.at/doks/kennzeichen_egal-thiele.pdf

UDRPinfo.com: http://www.udrpinfo.com/

UDRPLaw.net: http://udrplaw.blogspot.com/

Uniform Domain Name Dispute Resolution Policy Database (UDRP-DB): http://udrp.lii.info/udrp/index.php

UDRP Opinion Guide (Unverbindliches Restatement der Harvard Law School): http://cyber.law.harvard.edu/udrp/opinion/index.html

WHOIS Abfrage nach Ländern: http://www.iana.org/cctld/cctld-whois.htm

II.9.2. Rechtsvorschriften

ABGB: Allgemeines bürgerliches Gesetzbuch (ABGB) vom 1. Juni 1811 JGS

UWG: Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG. BGBl 448/1984

MSchG: Markenschutzgesetz 1970 BGBl 260/1970

HGB: Handelsgesetzbuch vom 10. Mai 1897 dRGBl S 219/1897

UrhG: Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (BGBl 1936/111)

UDRP (=Materielles Recht): http://www.icann.org/dndr/udrp/policy.htm

UDRP Rules (=Prozessrecht): http://www.icann.org/dndr/udrp/uniform-rules.htm

II.9.3. Registrierungsstellen

nic.at (.at): http://www.nic.at/

Network Solutions (.biz, .com, .info, .name, .net, .org, .pro): http://www.networksolutions.com/

eNIC (.cc): http://www.nic.cc/

Liste für generische TLDs: http://www.icann.org/registrars/accredited-list.html

III. Urheberrecht

Im Bereich des E-Business treten an vielen Stellen urheberrechtliche Fragen auf, beginnend mit Grafiken auf Webseiten, welche von anderen Web-Sites übernommen wurden. Weiter Probleme sind die Lizenzierung der verwendeten Programme zur Erstellung der Webseiten bzw. dem Webserver sowie der Datenbank, aus der die angezeigten Informationen entnommen werden. Besondere Aufmerksamkeit benötigt auch die Einbindung von Daten aller Art wie Grafiken, Musik, Animationen, Programm-Module etc. in selbst erstellte Programme, die anschließend verkauft werden sollen.

Das Urheberrecht gehört allgemein zu den Immaterialgüterrechten (auch IPR – Intellectual Property Rights – genannt), wozu insbesondere noch das Patent- sowie die Geschmacks- und Gebrauchsmusterrechte zählen. Aufgrund deren geringerer Bedeutung für E-Business selbst, im Gegensatz zu den darüber vertriebenen Gegenständen oder Dienstleistungen, werden sie hier nicht behandelt.

III.1. Einleitung

Für das österreichische Urheberrecht ist auch in Hinblick auf den oft internationalen E-Business eine Vielzahl von Rechtsvorschriften von Bedeutung, wobei besonders die EU auf diesem Gebiet stark rechtsvereinheitlichend tätig ist[122]:

1. Das österreichische Urheberrechtsgesetz (UrhG)
2. Die Computer-Richtlinie der EU (eingearbeitet in das UrhG)
3. Die Datenbank-Richtlinie der EU (eingearbeitet in das UrhG)
4. Die Urheberrechts-Richtlinie der EU (eingearbeitet in das UrhG)
5. Die Urheberrechts-Durchsetzungs-Richtlinie der EU (eingearbeitet in das UrhG)
6. Die Berner Übereinkunft in der Pariser Fassung[123], welche in Österreich unmittelbar anzuwenden ist. Sie besitzt fast universelle Geltung und legt einen Mindeststandard an Rechten für Urheber fest, der von allen Vertragsstaaten zu garantieren ist. Jeder Urheber aus einem Mitgliedsland hat einen Korrekturanspruch selbst gegenüber der Gesetzgebung anderer Staaten direkt aus der Übereinkunft. Für Österreich ist dies praktisch von geringerer Bedeutung, da das Urheberrechtsgesetz darüber hinausgeht.
7. Das TRIPS-Abkommen (Trade-Related Aspects of Intellectual Property Rights) legt einen Mindeststandard für Immaterialgüterrechte fest, was auch das Urheberrecht betrifft. Es besitzt keine direkte Geltung, sondern ist durch nationales Recht umzusetzen.

[122] Weitere Rechtsvorschriften sind die Vermiet-RL (92/100/EWG vom 19.11.1992, ABl. L 346/61, 27.11.1992), die Kabel- und Satelliten-RL (93/83/EWG vom 6.10.1993, ABl. L 248/15, 6.10.1993), Schutzfristen-RL (93/98/EWG vom 29.10.1993, ABl. 290/9, 24.11.1993) sowie die Folgerechts-RL (2001/84/EG vom 27.9.2001, ABl. 272/32, 13.10.2001)

[123] Berner Übereinkunft zum Schutze von Werken der Literatur und Kunst, BGBl 1982/319 idF BGBl 1985/133, 1986/612

III.2. Begriffsbestimmungen

In diesem Abschnitt wird erläutert, was unter den verschiedenen Ausdrücken zu verstehen ist. Von besonderer Wichtigkeit ist die Definition von "Werk", da an diesem der Schutz des Urheberrechts anknüpft: Nur Werke sind rechtlich geschützt. Für anderes existieren verwandte Schutzrechte, z.B. die Leistungsschutzrechte oder etwa der sui-generis Datenbankschutz. Diese sind aber meist schwächer als das Urheberrecht oder anders gestaltet.

III.2.1. Werk

§ 1 Abs 1 UrhG: Werke im Sinne dieses Gesetzes sind eigentümliche geistige Schöpfungen auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste und der Filmkunst.

Ein Werk setzt voraus, dass es von seinem Urheber in besonderer Weise geprägt ist. Es muss sich von den Werken anderer Personen dadurch unterscheiden, dass die Persönlichkeit des Urhebers einen besonderen Einfluss auf das Ergebnis hat ("eigentümlich"). Hierbei ist ein niedriger Maßstab anzulegen: Es ist weder Einzigartigkeit noch die Unmöglichkeit der Herstellung durch andere gefordert.

Geschützt sind jedoch nicht Ideen und Einfälle, sondern immer nur eine bestimmte Festlegung davon[124]. Ein Beispiel im Bereich der Informatik sind Algorithmen. Es ist daher grundsätzlich jeder frei, eine von jemandem anderen stammende Idee auf seine eigene Weise zu bearbeiten. Nicht erlaubt ist im Gegensatz, die besondere Form zu übernehmen. Eine Planung oder körperliche Festlegung ist nicht notwendig: Auch "zufällig" entstehende oder transiente Werke, z.B. Musik-Improvisationen, Chats oder Vorträge können urheberrechtlich geschützt sein, selbst wenn von letzteren weder Noten, Logs noch sonstige Aufzeichnungen vorhanden sind. Dies führt jedoch zu einem gewissen Beurteilungsproblem: Wann entsteht ein Werk? Eine Idee allein ist nicht geschützt, kurze Notizen zu einem Roman basierend auf dieser auch noch nicht, eine Rohfassung hingegen schon, und das fertige Werk auf jeden Fall. Oder in Bezug auf die Informatik: Die Idee für ein Programm ist kein Werk, ein kurzer Ablaufplan wohl auch noch nicht, eine detaillierte Spezifikation der Prozeduren ziemlich sicher, und das fertige Programm mit Sicherheit. Der Punkt, ab dem eine "Schöpfung" vorliegt, ist daher für jeden Fall einzeln zu betrachten.

Für ein Werk ist ein Gebrauchszweck unschädlich: Nicht nur „echte Kunst“ im Sinne von Gemälden oder Symphonien werden geschützt, sondern beispielsweise auch eine ansprechende Gestaltung von Werkzeugen aller Art. Auch was nützlich ist, kann ein Werk sein. Voraussetzung ist jedoch, dass die Gestaltung über die durch den Verwendungszweck vorgegebene Gestaltung hinausgeht. Eine Uhr muss z.B. die Zeit anzeigen; dies alleine reicht daher für ein Werk nicht aus. Die Art und Weise der Darstellung, durch Zeiger, Digitalziffern, Schatten, Lichtprojektion etc. und die Gehäusegestaltung, kann sie zu einem Werk machen. Auch hier ist wieder zu beachten, dass keine Idee geschützt ist, sondern nur die konkrete Ausgestaltung: So kann nicht eine "Digitaluhr" als Werk dem Urheberrecht unterliegen, jedoch u.U. die besondere Form und Gestaltung der einzelnen Ziffern. Als Informatik-Beispiel kann wieder ein Algorithmus dienen: Er selbst kann nicht durch das Urheberrecht geschützt werden, ein bestimmtes Programm, das diesen Algorithmus ausführt, sehr wohl. Dem gegenüber stehen der Patent- und der Musterschutz, bei denen Ideen, hier etwa Algorithmen unter zusätzlichen Bedingungen, geschützt werden können.

---

[124] "Schutzobjekt des Urheberrechts ist die bestimmte Formung eines Stoffes, nicht aber der dem Werk zu Grunde liegende, noch ungeformte Gedanke als solcher", OGH 11.2.1997, "Wiener Aktionismus", MR 1997, 98

Die Werkhöhe, also das Ausmaß der Formung des Werkes, wird relativ niedrig angesetzt (Juristisch: die „kleine Münze“). Besondere künstlerische Qualität oder Außergewöhnlichkeit ist nicht notwendig. Die Grenze kann in etwa dort gezogen werden, wo noch eine Prägung durch die Persönlichkeit des Urhebers vorliegt und das Werk noch eindeutig dem Urheber zuordenbar ist. Lässt sich aufgrund des Ergebnisses alleine nicht mehr feststellen, von wem es stammt, ohne freilich eine konkrete Identifizierbarkeit des Urhebers zu verlangen, so liegt kein Werk vor. Kurze, allseits bekannte Liedzeilen, Werbejingles, Plakate oder Stadtpläne mit Hervorhebung von Sehenswürdigkeiten wurden alle von der Judikatur als Werke angesehen. Auch naturalistische Bilder (Foto-Imitationen) sind Werke, obwohl in ihnen keine persönliche Formung zu stecken scheint: Die Auswahl des Motivs und die Art der Ausführung genügen in diesem Fall (Beispiel: Dürer-Hase).

Auch Teile von Werken sind als Teilwerke geschützt. Hier ist freilich eine Abgrenzung notwendig: Aus einer Symphonie sind einzelne Sätze Werke, ebenso einzelne Zeilen oder Motive, einzelne Noten alleine jedoch nicht mehr. Ein geschütztes Teilwerk liegt dann vor, wenn es noch zu einem bestimmten (Haupt-)Werk zuordenbar ist. Dadurch, dass ein Teil noch eindeutig seinem Eltern-Werk zuordenbar sein muss, lässt sich ableiten, dass es selbst auch ein Werk sein muss: Ist eine Zuordnung unmöglich, so liegt auch keine Prägung durch den Urheber mehr vor und damit weder ein Werk noch ein Teilwerk. Umgekehrt sind auch sehr kleine Teile, welche besondere künstlerische Qualität aufweisen noch Werke und damit Teilwerke und sind vom Urheberrecht umfasst.

In Österreich besteht ein numerus clausus an Werkkategorien. Vier Stück existieren: Literatur, Tonkunst, bildende Künste und Filmkunst. Was darüber hinausgeht unterliegt nicht dem Urheberrecht. Dennoch ergibt sich daraus kein lückenhafter Schutz, da auch neue "Werkkategorien" den vier Bereichen zugeordnet werden können bzw. explizit wurden, so beispielsweise Computerprogramme unter die Werke der Literatur, oder ein kunstvoll angelegter Garten unter die bildenden Künste (Hauptgedanke hier: plastische Kunst)[125].

III.2.1.1. Werke der Literatur

In dieser Kategorie finden sich neben dem Hauptinhalt (Sprachwerke) auch noch einige sonstige Arten von Werken, die aufgrund der geschlossenen Gruppen irgendwo eingeordnet werden mussten:

1. Computerprogramme (Details siehe unter III.5)
2. Bühnenwerke, deren Ausdrucksmittel Gebärden und andere Körperbewegungen sind (choreographische und pantomimische Werke)
3. Werke wissenschaftlicher und belehrender Art, die in bildlichen Darstellungen in der Fläche oder im Raum bestehen: Landkarten, Globen, Darstellungen von Körperhaltungen bei verschiedenen Sportarten etc. Ist die Darstellung auch künstlerisch ausgestaltet, so handelt es sich hingegen um Werke der angewandten oder bildenden Kunst.

Unter Sprachwerken ist alles zu verstehen, was durch den Einsatz von Sprache eine Idee transportiert. Ob diese dauerhaft festgehalten ist (Buch) oder nicht (Vortrag), ist für den

[125] Zum Werkbegriff für Webseiten siehe Schramböck, Urheberrechtsschutz von Internet-Websites und anderen Bildschirmdarstellungen von Computerprogrammen. ecolex 2/2000, 126: Sammelwerk, Einzelschutz der Elemente, Schutz als Ausgabe eines Computerprogramms. Ev. kommt auch noch der Schutz als Datenbank(-werk) hinzu. Es ist genau zwischen (einzelnen) Webseiten und Web-Sites (=Sammlung einzelner Seiten mit Verlinkung untereinander) zu unterscheiden. Siehe zu diesem Thema im Detail Kapitel IV Rechtsaspekte von Web-Sites.

Werkscharakter unerheblich. Um als Werk zu gelten, werden keine besonderen Ansprüche gestellt: Auch Vertragsentwürfe sind geschützt, sofern sie über einen normalen Standard-Vertrag hinausgehen und z.B. besondere Klauseln enthalten. Welche Sprache verwendet wird, ist unerheblich. Dies ist insbesondere für Computerprogramme von Bedeutung, da hierdurch jede Ausdrucksform (Maschinenprogramm, Assemblercode, Hochsprache, ...) gleichermaßen geschützt ist. Lesbarkeit mit freiem Auge wird nicht gefordert, daher sind ebenso Programme auf Datenträgern oder im Speicher geschützt und nicht nur Ausdrucke, wie es die Einordnung in die Kategorie der Literatur vermuten ließe.

III.2.1.2. Werke der bildenden Künste

Der Hauptinhalt dieser Kategorie sind Bilder, Gemälde, Skulpturen und Ähnliches. Auch hier ist keine Dauerhaftigkeit gefordert, sodass Eisskulpturen oder Bilder aus gestreutem Sand ebenso geschützt sind wie Ölbilder und Marmorstatuen.

In diese Kategorie fallen jedoch auch alle Lichtbildwerke. Da kein bestimmtes technisches Verfahren vorausgesetzt wird, sind auch mittels digitaler Kamera aufgenommene Bilder geschützt. Problematisch ist die Abgrenzung zwischen Lichtbildwerk (Urheberrecht) und einfachem Lichtbild (lediglich Leistungsschutzrecht, siehe später): Bei einem Lichtbildwerk wird wiederum eine besondere Prägung durch den Urheber vorausgesetzt, wie etwa durch Auswahl des Motivs, besondere Art der Erstellung (z.B. überlange Belichtungszeit, Bewegung während der Belichtung, ...), Beleuchtung oder den Bildausschnitt. Dem steht jedoch nicht entgegen, dass auch ein schneller Schnappschuss ein Werk sein kann: Der Herstellungsaufwand ist unerheblich, nur das Resultat zählt. Die Abgrenzung kann immer nur im Einzelfall erfolgen und ist sehr kasuistisch.

Weiters enthalten sind hier Werke der Baukunst wie Häuser, Brücken oder auch deren Teile: Fassade, Außengestaltung etc. Hier ist der künstlerischen Freiheit naturgemäß eine enge Grenze gesetzt, daher sind lediglich reine Zweckbauten ohne jegliche künstlerische Gestaltung keine Werke, wie rein zweckmäßige Lagerhallen. Am oberen Ende der "Kunstskala" befinden sich herausragende Bauwerke wie ausgefallene Brücken oder beispielsweise das Hundertwasserhaus in Wien.

Als letztes Element zählt zu dieser Gruppe die angewandte Kunst (= Kunstgewerbe). Im Gegensatz zu den anderen Werkarten, ev. mit Ausnahme der Baukunst, steht hier, wobei das Werk sonst u.U. auch zusätzlich gewissen praktischen Zwecken dient, die praktische Nutzung im Vordergrund, zu der noch eine künstlerische Gestaltung hinzutritt. Beispiele dieser Kategorie sind Juwelen, Möbel im weitesten Sinne, Porzellan, Besteck etc. Der Gebrauchswert dieser Objekte schadet nicht. Doch ist hier, wie bei den Lichtbildwerken, die Schwelle, ab der ein Werk entsteht, schwierig zu bestimmen. Allgemein ist das Niveau bei angewandter Kunst niedriger anzusetzen, da der künstlerische Freiraum durch den praktischen Zweck naturgemäß eingeengt ist.

III.2.1.3. Werke der Filmkunst

Bei einem Filmwerk handelt es sich um eine Abfolge von Bildern, sodass sich eine Bewegung ergibt: Eine Darstellung der den Gegenstand des Werkes bildenden Vorgänge und Handlungen. Wie diese hergestellt werden, als Zeichentrick-, Schwarzweiß- oder Farbfilme, in 3D-Verfahren, ... ist unerheblich, genauso wie die Technik, die zur Herstellung bzw. Wiedergabe verwendet wird. Analog den Lichtbildwerken wird zwischen Filmwerken und Laufbildern unterschieden: Letztere erreichen nicht die notwendige Werkhöhe (Ur-

laubsvideos, Naturszenen etc.)[126]. Es ist jedoch zu beachten, dass auch bei vom Hersteller des Filmwerkes völlig ungestaltetem Inhalt, z.B. Filmen einer öffentlichen Kundgebung (⇒ keine persönliche "Färbung" durch den Urheber und daher eigentlich kein Werk), dennoch ein Werk vorliegen kann. Die Auswahl der Motive, Ausschnitte, Überblendungen, Zusammenstellung verschiedener Ausschnitte usw. kann im Ergebnis trotz allem die notwendige Werkhöhe erreichen.

Auch bei Filmwerken ist es nicht notwendig, dass das Werk auf einem Träger festgehalten wird: Live-Übertragungen im Internet ohne Aufzeichnung sind ebenso geschützt wie der Kinofilm, von dem sehr viele Kopien existieren.

Eine weitere Besonderheit bei Filmwerken besteht darin, dass die Musikspur unabhängig von den Bildern zu betrachten ist. Die Rechte für die Filmmusik sind gesondert zu erwerben[127]. Bei einem Filmwerk handelt es sich um eine Bearbeitung (siehe III.2.3) der zugrunde liegenden Werke wie beispielsweise dem Roman und dem Drehbuch. Auch hierfür sind die Rechte zu erwerben. Da es sich um unabhängige Rechte handelt, kann es vorkommen, dass das Recht am Drehbuch verloren geht, und daher das Filmwerk ab diesem Zeitpunkt nicht mehr aufgeführt werden darf.

In Bezug auf die Informatik stellen sich zu Filmwerken einige besondere Fragen, da neue oder andere Kategorien und neue Verwendungen entstehen:

- Animierte Werbebanner werden regelmäßig keine Filmwerke sein, im Gegensatz z.B. zu Film- oder Fernseh-Werbespots, da die Werkhöhe nicht ausreicht. Oft handelt es sich lediglich um eine Folge verschiedener Bilder ohne zugrunde liegende Handlung. Bei so genannten "narrative Bannern", in denen eine Kurzgeschichte erzählt wird, könnte hingegen die notwendige Werkhöhe u.U. erreicht werden. Laufbilder kommen hier nicht in Frage, da kein der Fotographie ähnliches Verfahren zum Einsatz kommt.
- Einfache animierte Bilder (funkelnde Kugeln, bewegte Linien etc.), die zur Gestaltung von Webseiten verwendet werden, sind ebenso keine Filmwerke, da sie keinerlei Handlung besitzen oder irgendwelche Vorgänge darstellen. Bei ihnen ist jedoch, trotz der Animation, an Bildwerke oder Gebrauchsgraphik zu denken[128].
- Mit Shockwave Flash[129] oder anderen Produkten erstellte interaktive Grafiken/Filme können sehr wohl Filmwerke sein: Interaktion, welche die weitere Bildfolge bestimmt, ist kein Hindernis für ein Filmwerk und verlangt keine Einordnung in eine andere Kategorie. Es kommt wiederum nur auf die Werkhöhe an. Aufgrund der Technik-Indifferenz schadet es nicht, wenn Bilder aus Vektordaten erzeugt oder berechnet werden, da die "Miniaturisierung" auf Bildträger wie Celluloid für Filmwerke keine Voraussetzung ist.
- Auch rein berechnete Darstellungen wie Bildschirmschoner können Filmwerke sein. Es muss jedoch darauf geachtet werden, ob durch die Art der Berechnung/Auswahl der Formeln etc. noch eine persönliche Prägung durch den Urheber erfolgt. Eine Apfelmännchen-Animation mit zufälligen Zooms wird kein Filmwerk darstellen, ein komplexer Bildschirmschoner mit Handlung (z.B. AfterDark) hingegen schon.

---

[126] Achtung: Im Gegensatz zu Lichtbildern und Filmwerken ist bei Laufbildern ein der Fotographie ähnliches Verfahren Voraussetzung, sodass digitale, eben nicht ganz die nötige Werkhöhe erreichende, "Filme" hier nicht darunter fallen!

[127] Die Tonspur (=Dialoge, Texte) ist jedoch enthalten!

[128] Burgstaller: Schutz von Computeranimationen. MR 2003/5, http://www.multimedia-law.at/db11/cr5.html

[129] http://www.shockwave.com/

- Auch eine ganze Webseite kann in Ausnahmefällen ein Filmwerk darstellen, falls etwa Flash extensive Verwendung findet oder viele Animationen enthalten sind, die aufeinander abgestimmt sind. Statische Teile dazwischen sind kein Hindernis.
- Computerspiele fallen üblicherweise ebenfalls unter die Filmwerke: Es ist unerheblich, ob die Handlung fest vorbestimmt ist wie bei klassischen Filmen, oder diese vom Konsumenten in gewissen Grenzen beeinflusst werden kann. Es kommt lediglich auf eine graphische bewegliche Darstellung einer Handlung an[130]. Der Quellcode ist natürlich auch geschützt (→ Literatur), ebenso eventuell vorhandene andere graphische Elemente (→ Lichtbilder/Lichtbildwerke), sofern sie die normalen Voraussetzungen, insbesondere hinsichtlich der Werkhöhe, erfüllen.

III.2.2. Sammelwerke

Bei Sammelwerken handelt es sich um eine Kollektion von einzelnen Teilen, die durch ihre besondere Zusammenstellung zu einem eigenständigen Werk werden. Die Einzelteile selbst können, müssen jedoch nicht, Werke sein. Sind sie es, ist das Urheberrecht an ihnen zu beachten, das unabhängig von den Rechten am Sammelwerk weiter besteht. Eine bloße Menge an Elementen ohne Ordnung, oder wenn diese lediglich nach äußeren Kriterien wie Größe, Farbe, Nummer etc. erfolgt, stellt kein Sammelwerk dar. Erst wenn in der Sortierung, dem Arrangement, der Reihung, usw. eine persönliche Prägung vorhanden ist, entsteht ein neues Werk, das Sammelwerk. Auswahl oder Anordnung müssen daher eine Eigentümlichkeit und Originalität aufweisen, wobei jedoch auch hier keine besonders hohen Anforderungen gestellt werden. Auszuscheiden sind jedoch alle Einflüsse, die durch externe Merkmale diktiert sind, z.B. Sachzwänge[131].

Auch Datenbanken können Sammelwerke sein, doch bestehen für diese zusätzlich noch Sondervorschriften, die einen weiteren Schutz bieten, wenn die Eigentümlichkeit nicht für ein Sammelwerk ausreicht (siehe Abschnitt III.6). Weiters von Bedeutung hinsichtlich der Informatik sind Web-Sites, die aus einer Vielzahl von einzelnen Webseiten bestehen. Eine konventionelle und übliche Anordnung, z.B. in Baumstruktur, wird so nicht ein Sammelwerk schaffen, eine besondere Vernetzung nach Schlagwörtern oder Ähnlichem hingegen kann ein Sammelwerk ergeben[132]. Typische Sammelwerke im Internet sind weiters Themen für Webseiten, die aus zusammenpassenden Grafiken, Schriftformatierungen, Hintergründen, Musikstücken etc. bestehen sowie besonders geordnete oder nach bestimmten Gesichtspunkten zusammengestellte Linksammlungen.

Unter dem Aspekt des E-Commerce stellt ein reiner Produktkatalog kein Sammelwerk dar, da es an einem besonderen Ordnungsprinzip fehlt[133], es wird sich hierbei meist um eine „bloße“ Datenbank handeln. Auch eine Sammlung von Kundendaten (=Adress-Datenbank) ist kein Sammelwerk, sondern rechtlich gesehen allenfalls bloße Datenbank.

---

[130] "Fast Film" OGH 6.7.2004, 4 Ob 133/04v

[131] Siehe dazu auch die im US-Recht entwickelte Methode "Abstraction – Filtartion – Comparison" zur Prüfung von Urheberrechtsverletzungen bei Computerprogrammen, wo insbesondere hinsichtlich der Filterungsstufe als auszuscheiden angeführt wird: Effizienzgründe, externe Faktoren (scènes à faire, merger, Interoperabilität), öffentliche Elemente, Fakten, Ideen etc. Hollaar, Lee, Legal Protection of Digital Information. BNA Books, 2002. http://digital-law-online.info/ Mills, Laurin, Abstraction-Filtration-Comparison Analysis Guidelines for Expert Witnesses. http://nixonpeabody.com/copyright_article.asp?ID=86&PubType=A

[132] Vorsicht: Dadurch wird nicht die Struktur der Hyperlinks geschützt, da diese als reine Idee nicht schutzfähig ist. Nur die konkrete Ausprägung bei diesen einzelnen Elementen wird als Sammelwerk geschützt.

[133] Bloße Gliederung nach Produktgruppen ist zu offensichtlich, als dass dies eine persönliche Prägung wäre.

III.2.3. Bearbeitung

Bei einer Bearbeitung wird aus einem oder mehreren bestehenden Werken ein neues Werk geschaffen. Im Gegensatz zu einem Sammelwerk ist hier jedoch Voraussetzung, dass es sich tatsächlich um Werke handelt, die umgewandelt oder integriert werden. Keine Bearbeitung sondern getrennte Werke liegen dann vor, wenn das neue Werk nur aus einer trennbaren Verbindung besteht, z.B. der Vertonung eines Gedichtes. Bearbeitungen sind in allen Werkkategorien denkbar. Ein Beispiel für die Informatik ist die Erweiterung oder Umarbeitung eines Programms, inkl. der Behebung von komplexen Fehlern[134].

Da es sich bei einer Bearbeitung wieder um ein Werk handeln muss, ist ein signifikanter neuer Teil erforderlich: Ein eigener Beitrag des (Nach-)Urhebers ist notwendig, beispielsweise die Übersetzung von Menüs, Dialogboxen oder der Dokumentation eines Programms. Rein technische Umwandlungen, z.B. die Restaurierung eines Bildes, Compilierung eines Computerprogramms, Behebung trivialer Programmfehler, Aufhellung einer Grafik, Dateiformat-Konvertierung, ... begründen für sich kein neues Werk. Es liegt nur eine "Umwandlung", aber keine „Bearbeitung“ im Sinne des Urheberrechts vor. Als Kriterium kann verwendet werden, ob eine gleichartige Transformation durch verschiedene Personen das gleiche Ergebnis liefern würde (= Umwandlung) oder nicht (= Bearbeitung). Geht hingegen die Bearbeitung zu weit über das ursprüngliche Werk hinaus, war dieses also nur eine Anregung aber keine Vorlage, so liegt ein eigenständiges Werk und keine Bearbeitung vor. Es handelt sich daher bei einer Bearbeitung um eine Zwischenstufe, die im Bereich „Ursprüngliches Werk“ ⇔ „Bearbeitung“ ⇔ „Neues Werk“ einzuordnen ist.

Die Veröffentlichung oder Verwertung von Bearbeitungen ist grundsätzlich unzulässig, im Gegensatz zur rein privaten Bearbeitung als solcher. Es ist daher erforderlich, die Zustimmung des (ursprünglichen) Urhebers für eine öffentliche Nutzung zu erlangen. Dahinter steht der Grundsatz des Werkintegritätsschutzes: Jeder Urheber hat das Recht, Veränderungen seines Werkes zu verbieten, wenn diese der Öffentlichkeit zugänglich sind. Ebenso ist ja jede Verwertung der Bearbeitung auch eine Verwertung, zumindest eines Teils, des Originalwerkes, wodurch sich das Zustimmungserfordernis ergibt. Dies ist insbesondere finanziell von Bedeutung, da in solchen Fällen Nutzungs-/Lizenzgebühren abzuführen sind.

Für den Bereich des Internet ist zu beachten, dass die vielfach vorgenommenen geringen Änderungen z.B. an Grafiken nicht genügen, ein neues Werk zu schaffen. Meistens wird die dafür notwendige Werkhöhe nicht erreicht werden, ja oft nicht einmal die für eine Bearbeitung notwendige. Ebenso wird normalerweise keine Zustimmung des Urhebers des Originalwerkes vorliegen.

III.2.4. Veröffentlichung

Ein Werk ist dann veröffentlicht, wenn es der Öffentlichkeit mit Einwilligung des Berechtigten zugänglich gemacht worden ist. "Öffentlichkeit" liegt nur dann vor, wenn das Werk für die Allgemeinheit bereitgestellt wird, also potentiell jeder Kenntnis davon nehmen könnte. Eine Mitteilung an einen sehr eng begrenzten Kreis, z.B. die Vorlage bei Gericht als Beweisstück, eine Erläuterung in der Familie, die Verteilung an alle Vorstandsmitglie-

[134] Ausbessern von Tippfehlern oder sonstigen Kleinigkeiten sind demgegenüber keine Bearbeitung, da keine persönliche Prägung hinzukommt. Erst wenn die Ausbesserung einen persönlichen Umsetzungsspielraum lässt, liegt eine Bearbeitung vor. Beispiel: Korrektur von einheitlichem Umsatzsteuersatz auf mehrere mögliche Sätze für verschiedene Produktgruppen oder die Einführung von Synchronisation zur Verhinderung von race conditions.

der, ist nicht als Veröffentlichung anzusehen. Im Gegensatz zum Erscheinen ist eine Veröffentlichung nicht an körperliche Exemplare gebunden: Es genügt, wenn eine unkörperliche Mitteilung erfolgt, z.B. eine Film-Premiere oder das Ausstellen eines Werkes in einem Museum mit allgemeinem Zutritt. Einige Rechte von Dritten hängen von der Veröffentlichung ab, beispielsweise das Recht, einzelne Stellen aus dem Werk zu zitieren (Kleinzitat).

Im Zusammenhang mit dem Internet besteht eine Veröffentlichung aus dem Zurverfügungstellen mit allgemeinem Zugriff; siehe aber zusätzlich das neue „Recht der Zurverfügungstellung“. Eine Präsentation auf Webseiten oder in einer öffentlichen Datenbank ist daher eine Veröffentlichung (und u.U. auch ein Erscheinen; siehe nächster Abschnitt). Hierbei wird zu beachten sein, dass eine gewisse Mindestwirksamkeit der Öffentlichkeit gegeben sein muss. Die Veröffentlichung auf einer Webseite, zu der keinerlei Links führen, oder das Einspeisen in eine Datenbank unter einem anonymen Schlüssel, etwa einer laufenden Nummer, ohne weitere Suchmöglichkeit, wird keine ausreichende Öffentlichkeit darstellen. Im Gegensatz dazu ist es nicht notwendig, dass die Allgemeinheit das Werk *tatsächlich* wahrnimmt: Besucht niemand die Webseite/das Museum oder fragt keiner genau dieses Werk in der Datenbank ab, so ist es dennoch veröffentlicht. Ebenso sind versteckte Daten nicht veröffentlicht, auch wenn die zugrunde liegenden Daten oder Webseiten öffentlich zugänglich sind. Beispiele hierfür sind Steganographie oder Webseiten mit schwarzer Schrift auf schwarzem Hintergrund.

Im Hinblick auf das Internet ist hier zu erwähnen, dass eine Veröffentlichung keine Zustimmung zur allgemeinen oder freien Nutzung bedeutet, die über die Wahrnehmung der Veröffentlichung selbst hinausgeht. Das Kopieren von Teilen oder der ganzen Information ist daher nur im Rahmen der freien Werknutzungen oder der mit der Veröffentlichung erteilten Genehmigung erlaubt. Eine Veröffentlichung ist keine Zustimmung zur unbegrenzten Nutzung[135]! Eine solche umfasst typischerweise das individuelle Betrachten, hingegen das Ausdrucken oder Abspeichern jedoch vermutlich bereits nicht mehr[136], und sicher nicht die Weitergabe/den Verkauf dieser Kopien. So werden gratis zur Verfügung gestellte Programme auch nicht „frei“, sondern dürfen nur in dem freigegebenen Ausmaß und Umfang verwendet werden.

III.2.5. Erscheinen

Ein Werk ist erschienen, wenn es mit Einwilligung des Berechtigten der Öffentlichkeit zugänglich gemacht wird, indem Werkstücke in genügender Anzahl angeboten oder in Verkehr gebracht werden. Ob die Werkexemplare tatsächlich verkauft werden ("angeboten") oder nicht, ist unerheblich. Auch genügt es, wenn sie in anderer Weise (Miete, Tausch, Schenkung, ...) verbreitet werden ("in Verkehr gebracht"). Die „genügende Anzahl“ ist nicht genau festgelegt und variiert je nach Werkart: Zeitungen benötigen eine höhere Auflage als Textbücher für Theateraufführungen. Ist ein Werk erschienen und nicht nur veröffentlicht, so steht es der Öffentlichkeit in größerem Umfang zur Verfügung, beispielsweise durch zusätzliche freie Werknutzungen oder das Großzitat.

Im Unterschied zur Veröffentlichung ist beim Erscheinen eine körperliche Form notwendig. In Bezug auf Musik ist das mittels Tonträgern oder Notenblättern möglich. Eine Auf-

[135] Siehe den Fall "Fast Film" (FN 130), wo zwar das Einstellen auf eine Webseite, privater Download und das Spielen erlaubt war, der Verurteilte das Spiel jedoch auf CD brannte und diese am Flohmarkt für € 2 pro Stück verkaufte.

[136] Zweifelsfall je nach Zweck der Webseite; hier wird aber meist eine freie Werknutzung zutreffen.

führung ist hingegen bloß als eine Veröffentlichung anzusehen. Beim Erscheinen ist eine Veröffentlichung implizit enthalten, da es durch allgemeines in Verkehr bringen immer eine Mitteilung an die Öffentlichkeit beinhaltet.

Teilweise umstritten ist in Bezug auf das Internet, ob eine Darstellung z.B. auf Webseiten das Erscheinen bewirkt oder lediglich eine Veröffentlichung ist. Das Hauptproblem liegt darin, ob mit dem Download eine körperliche Form entsteht, also ein "Werkstück". Eine genügende Anzahl liegt mit Sicherheit vor, da unbegrenzt viele Exemplare hergestellt werden können. Neben der physikalischen Betrachtung, dass jede Speicherung immer auch eine physische Festlegung und damit eine körperliche Form ist, lässt sich ein Erscheinen auch teleologisch begründen: Das Ziel des Erscheinens eines Werkes besteht darin, dieses Werk einer großen Anzahl von Personen zugänglich zu machen und eine freie Übertragbarkeit im Sinne einer Weitergabe zu ermöglichen. Das Werk soll der Öffentlichkeit in hohem Maße übergeben werden: Die Veröffentlichung ist eine Aufgabe der Geheimhaltung, ein Erscheinen hingegen die möglichst weite Verbreitung. Dies entspricht auch genau dem Zugänglichmachen im Internet, wo viele Personen Zugang erlangen (können) und freie Weitergabe möglich wird. So "erscheint" eine Skulptur etwa durch Ausstellung in einem öffentlich zugänglichen Museum. Weiters ist es für den Urheber auch gleichzuhalten, ob sein Gemälde im Internet veröffentlicht, oder jedem Interessierten auf einer Postkarte zugeschickt wird. Im zweiten Fall handelt es sich jedenfalls um ein Erscheinen, das sich aber von einer Internet-Einspeisung nicht wesentlich unterscheidet. Vielfach werden z.B. die Postkarten vernichtet werden, doch besteht die Möglichkeit, sie weiterzugeben, genau wie im Internet eine Weitergabe auf Disketten oder in elektronischer Form per E-Mail möglich ist. Bei einer Darstellung im Internet wäre daher eher von einem Erscheinen auszugehen.

Zumindest für Deutschland wird dies jedoch großteils abgelehnt und strikt auf die Körperlichkeit im Sinne von Angreifbarkeit abgestellt, sodass beim Einstellen ins Internet kein Erscheinen, sondern nur eine Veröffentlichung vorliegt. In Österreich wurde auch bei der Urheberrechtsnovelle zur Einführung des Rechts der Zurverfügungstellung das Problem, obwohl bekannt, nicht explizit geklärt. Das Zurverfügungstellen wird aber *nicht* dem Erscheinen gleichgesetzt. Da eher nicht von einem Versehen des Gesetzgebers auszugehen ist, muss als Konsequenz angenommen werden, dass die Verbreitung im Internet kein "Erscheinen" begründet. Dies ist insbesondere wichtig für Großzitate, welche ja an das Erscheinen des Werkes gebunden sind, im Gegensatz zum "normalen" oder Kleinzitat, das nur eine Veröffentlichung erfordert. Wird ein Werk daher ausschließlich im Internet zur Verfügung gestellt, so darf es nur im Rahmen von Kleinzitaten verwendet werden.

III.2.6. Urheber/Miturheber

Ursprünglicher Urheber eines Werkes ist ausschließlich diejenige physische Person, welche das Werk tatsächlich geschaffen hat. Wer Vorarbeiten, Anregungen oder Ideen geliefert hat, aber nicht an der Formung derselben mitgewirkt hat, ist kein Urheber. Die Mitwirkung am Programmentwurf alleine hingegen schon, da auch solche Materialien schon zum Computerprogramm zählen. Allein dem Urheber stehen anfangs alle Rechte zu. Diese Rechte können, auch schon im Voraus, übertragen werden, die Stellung als Urheber jedoch niemals; ein Verzicht darauf ist unwirksam. Eine juristische Person kann also niemals Urheber sein. Daher sind "Werke" von Firmen oder Behörden niemals die Werke dieser, sondern immer der einzelnen Mitarbeiter, welche sie hergestellt haben. Davon ist streng zu unterscheiden, wem die (wirtschaftlich bedeutsamen) Verwertungsrechte zustehen: Diese

liegen ursprünglich beim Urheber, doch bei einem Dienstverhältnis gehen sie regelmäßig aufgrund des Arbeitsvertrags auf den Dienstgeber, also die juristische Person, über[137].

Es kann jedoch auch vorkommen, dass mehrere Personen gemeinsam ein Werk schaffen. Hier sind zwei Subkategorien zu unterscheiden: Sind die Teile unabhängig, so handelt es sich um separate Werke, die jeweils für sich alleine geschützt sind. Bildet jedoch das Ergebnis eine untrennbare Einheit, was typischerweise daran zu messen ist, ob eine gesonderte Verwertung der Einzelteile möglich ist, so wird Miturheberschaft begründet. Alle Personen sind dann gleich als Urheber anzusehen. Persönliche Rechte daraus stehen jedem Miturheber einzeln zu, die Verwertungsrechte nur allen zusammen. Anteile können nur einvernehmlich festgesetzt werden, ansonsten steht jedem Miturheber ein gleicher Teil zu, unabhängig vom Ausmaß seines Beitrages zum Ergebnis.

Wichtig ist auch die Abgrenzung zur Bearbeitung. Wird ein fertiges Werk umgewandelt, so liegt eine Bearbeitung vor, welche der Zustimmung des Urhebers bedarf. Dieser kann daher ganz nach seinem Belieben mit den Rechten an seinem Werk verfahren. Wird hingegen originär ein Werk von mehreren Personen zusammen geschaffen, so liegt Miturheberschaft vor und *alle* Beteiligten müssen einer Veränderung der Rechte, und daher jeder Vervielfältigung, Bearbeitung etc., zustimmen. Jeder Miturheber besitzt damit ein Vetorecht und Verfügungen sind nur einstimmig möglich.

In Bezug auf die Informatik ergeben sich wenige besondere Gesichtspunkte. So ist etwa ein gemeinsam geschaffenes Programm differenziert zu betrachten: Ein tatsächlich gemeinsamer Entwurf/Programmierung schafft Miturheberschaft, während die Zusammenstellung gesondert programmierter und relativ eigenständiger Module dies nicht erzeugt. Jeder bleibt dann Urheber seines Teils und es entsteht ev. ein Sammelwerk. Dies hat in der Praxis geringe Bedeutung, da derartige Werke normalerweise in Unternehmen produziert werden, welche alle Verwertungsrechte, direkt per Gesetz oder über den Dienstvertrag, in sich vereinen.

Im Bereich der Open Source Software (OSS), sofern nicht von einer Firma entwickelt und von dieser zur Verfügung gestellt, besitzt dies jedoch immense Bedeutung. So ist etwa der Linux Kernel ein Werk vieler Autoren, welche allesamt Miturheber sind. Hierbei ist es unerheblich, dass diese nicht gleichzeitig, sondern sukzessive und verzahnt an dem Gesamtwerk gearbeitet haben. Da der Kernel nicht „teilbar“ ist, liegt auch kein Sammelwerk vor. Von sehr vielen weiteren einzelnen Personen wurden Bugfixes, Verbesserungen etc. eingebracht, welche für sich alleine nicht die erforderliche Werkhöhe erreichen und vielfach auch nicht zusammen für eine Miturheberschaft ausreichen. Es dürfte darum äußerst schwer sein, mit Sicherheit und tatsächlich alle Urheber ausfindig zu machen[138]. Dies stellt jedoch durch die spezielle Konstruktion der GPL (Gnu Public License) kein Problem dar. Wünschte man eine andere Lizenz für den Kernel, müsste genau dieses Problem gelöst werden und *ausnahmslos* von *allen* (im Sinne von Miturheberschaft maßgeblichen) Autoren die Zustimmung eingeholt werden, was in der Praxis illusorisch ist.

---

[137] Anders z.B. in den USA: Bei Auftrags- oder Angestelltenwerken ist der Auftraggeber der originäre Urheber. Dies resultiert aus einem anderen, mehr wirtschaftlich und weniger künstlerisch geprägten, Verständnis des Urheberrechts: „Urheber“ –recht vs. „Kopier“ –recht (copyright).

[138] Eine große Menge an einzelnen "unwichtigen" Bugfixes könnte als Gesamtes auch zur Miturheberschaft ausreichen! Dies auch nur einigermaßen verlässlich zu beurteilen, ist wohl ebenso aussichtslos.

III.3. Rechte des Urhebers

Dem Urheber stehen eine Reihe von Rechten zu, die durch das Schaffen des Werkes entstehen. Großteils ist eine Übertragung auf Andere möglich[139]. Diese Rechte, hauptsächlich die wirtschaftlich bedeutsamen Nutzungsrechte, werden im Folgenden näher erläutert.

In Österreich sind fünf verschiedene Verwertungsmöglichkeiten für Werke vorgesehen:

1. Vervielfältigung: Multiplikation der Exemplare
2. Verbreitung: Verwertung durch körperliche Werkstücke
3. Sendung: Drahtlose oder drahtgebundene Weiterleitung, E-Mail, … ("Öffentliche Wiedergabe")
4. Aufführung (hier nicht näher besprochen): Vortrag oder Aufführung, z.B. Theater, Konzert etc.
5. Öffentliche Zurverfügungstellung (EU-Richtlinie: „Zugänglichmachung“): Anbieten an die Öffentlichkeit, sodass selbige es von beliebigen Orten aus und zur Zeit ihrer Wahl abrufen kann.

Durch diese erschöpfende Aufzählung und die jeweils unterschiedliche Regelung ist es notwendig, jeden Akt der Verwertung einer dieser Kategorien zuzuordnen, was manchmal Probleme aufwirft[140]. Vervielfältigung und Verbreitung betreffen jeweils eine körperliche Nutzung, während Sendung, Aufführung und Zurverfügungstellung unkörperliche Verwertungshandlungen erfassen.

Die Verwertungsrechte sollen dem Urheber ermöglichen, alle Akte der Verwendung seines Werkes wirtschaftlich zu nutzen. Dazu wäre es theoretisch notwendig, jede Nutzung gesondert zu verrechnen, z.B. jedes Umblättern in einem Buch, jeden Blick auf ein Bild, jedes Abspielen einer CD, ... Da dies praktisch unmöglich ist bzw. war und zu sehr in die Privatsphäre eingreifen würde, wurde das "Stufensystem zur mittelbaren Erfassung des Endverbrauchers" geschaffen. Die "Besteuerung" zugunsten des Urhebers wird um eine Stufe vorgelagert auf denjenigen, der dem Werk-Endverbraucher genau diese Nutzung ermöglicht. Dies ist einerseits derjenige, der Kopien des Werkes herstellt, welche anschließend verkauft und dann benutzt werden, andererseits aber auch jeder, der das Werk der Öffentlichkeit in anderer Weise zugänglich macht, etwa der Disc-Jockey, der eine CD abspielt, sodass Personen der Musik zuhören können. Genau dieses Konzept wird in letzter Zeit insbesondere von der Musikindustrie angegriffen, welche zum Grundprinzip zurück möchte: Jeder gesonderter Nutzungsvorgang soll zu bezahlen sein. Dies kann nun technisch in weiten Bereichen durch Digital Rights Management (DRM) auch tatsächlich realisiert bzw. durchgesetzt werden. Allerdings regt sich starke Gegenwehr von Verbrauchern, welche gewisse Rechte oder Gewohnheiten, z.B. dass ein einmaliger Kauf einer CD zu ei-

[139] Dies kann im Vorhinein per Vertrag erfolgen. Ansonsten ist § 27 Abs 2 UrhG zu beachten, wonach die Zustimmung zu einer Übertragung im Wege der Sondernachfolge, z.B. eines Verkaufs, nur aus wichtigen Gründen verweigert werden kann. Auf schriftliche Anfrage an den Urheber hat dieser die Übertragung binnen zwei Monaten explizit abzulehnen, ansonsten gilt sie als erteilt. Der Veräußerer haftet weiter für die Vertragserfüllung hinsichtlich Entgelt und Schaden als Bürge und Zahler.

[140] Bekannter Fall mit großer praktischer Bedeutung über den Anlassfall hinaus: "Sex-Shop" SZ 60/9 OGH 27.1.1987, 4 Ob 393/86. Das Betrachten eines zentral abgespielten Films in den Kabinen eines Sexshops ist eine öffentliche Aufführung und keine drahtgebundene Sendung. Es kommt daher das Aufführungsrecht und nicht das Senderecht zur Anwendung. Daraus wurde das Konzept der "sukzessiven Öffentlichkeit" entwickelt: Mehrere Personen unabhängig hintereinander können auch "Öffentlichkeit" darstellen.

ner beliebigen Anzahl von kostenfreien Abspielvorgängen auf beliebigen Medien bzw. an beliebigen Orten berechtigt, sowie ihre Privatsphäre[141] nicht aufgeben möchten. Eine gewisse Einschränkung erfährt eine derart detaillierte Verrechnung auch durch die so genannte „Erschöpfung“ (siehe III.3.7), welche u.a. den freien Warenverkehr sichern soll.

III.3.1. Vervielfältigung

Allein der Urheber besitzt das Recht, Vervielfältigungen seines Werkes herzustellen oder herstellen zu lassen. Die Form dieser Vervielfältigung ist unerheblich. Es kommt lediglich darauf an, dass das Werk dadurch für andere Personen sinnlich erfahrbar wird. Beispiele sind Kopien literarischer Werke oder Aufzeichnungen von Reden oder Musikstücken. Ob dabei eine Transformation auf einen anderen Sinn erfolgt (Buch → Blindenschrift; Vortrag → Mitschrift, ...) ist unerheblich. Nach seinem Ursprung wird dies als das "mechanische Recht" bezeichnet, da bei der Schaffung des Gesetzes an eine Vervielfältigung durch Drehorgeln oder ähnliche Apparate auf rein mechanischem Weg gedacht wurde.

Im Hinblick auf die Informatik ergeben sich bis auf einen Sonderfall keine Besonderheiten. Inzwischen nicht mehr umstritten ist, ob die Zwischenspeicherung von Webseiten auf Proxies eine Vervielfältigung darstellt oder nicht: Es handelt sich um eine, doch ist sie gesetzlich erlaubt. Zu beachten ist aber, dass dieses Recht stark eingeschränkt ist (siehe III.4.2).

III.3.2. Verbreitung

Das Verbreitungsrecht ist dem Vervielfältigungsrecht in der Weise untergeordnet, dass es verbietet, körperliche Werkstücke[142] der Öffentlichkeit zugänglich zu machen. Da eine Verbreitung aber ohne vorherige Vervielfältigung nur selten denkbar ist[143], beschränkt sich die Anwendung auf einige Fälle.

Dies sind unter anderem:

- Ein zeitlich begrenztes Vervielfältigungsrecht ist ausgelaufen und es sind noch (daher legal vervielfältigte) Werkstücke vorhanden. Diese dürfen der Öffentlichkeit nun nur mehr angeboten werden, wenn das Verbreitungsrecht vorhanden ist.
- Die Vervielfältigung erfolgte legal, aber ohne Zustimmung des Urhebers. Ein Beispiel hierfür wäre das Kopieren in einem Staat, in welchem die Schutzfrist bereits abgelaufen ist. Der Urheber kann mit seinem Vervielfältigungsrecht dann verhindern, dass die Werkstücke im Inland in Verkehr gebracht werden.

Das Verbreitungsrecht kann territorial und zeitlich eingeschränkt jeweils verschiedenen Personen eingeräumt werden. In anderen Gebieten ist diesen Personen dann eine Verbreitung nicht gestattet. Hier ist jedoch der Erschöpfungsgrundsatz (siehe III.3.7) zu beachten.

---

[141] Eine tatsächlich komplette Durchsetzung ist derzeit technisch nur möglich, wenn bei jedem einzelnen Verwertungsvorgang bei einer zentralen Stelle eine Genehmigung eingeholt wird: Diese erfährt dadurch bei jedem Nutzungsvorgang Zeit und Benutzer, teilweise auch Ort, verwendetes Gerät etc.

[142] Siehe OGH 23.5.2000, 4 Ob 30/00s, wonach auch beim Erwerb von Software-Lizenzen eine Erschöpfung eintritt, selbst bei entgegenstehenden Vertragsbedingungen. Dies wohl deshalb, da es sich um physische Datenträger handelte. Anders bei reinem Online-Verkauf, und damit Download des Exemplars, von Software (siehe weiter unten)!

[143] Der Verkauf von Büchern setzt etwa deren Druck voraus, welcher eine Vervielfältigung ist.

III.3.3. Senderecht

Beim Senderecht wird eine Werk durch Rundfunk oder auf eine ähnliche Art, z.B. über Leitungen[144], verbreitet. Wegen des Bezugs auf den Rundfunk ist davon auszugehen, dass dem Gesetzgeber eine Art unbeschränkte Verbreitung vorschwebte, bei welcher die einzelnen Empfänger nicht bekannt sind. Das Werk wird sozusagen aktiv und synchron dem Publikum über ein vermittelndes Medium zur Verfügung gestellt, wobei es technisch praktisch unmöglich ist, die genauen Empfänger (bzw. Nicht-Empfänger) festzustellen. Diese Empfänger wissen auch nichts voneinander. Auf welcher Weise die Verbreitung erfolgt, Lichtwellen, elektromagnetische Wellen, Rauchzeichen etc., ist unerheblich. Auch eine Weiterleitung per Kabel ist inbegriffen. Rechte für die Sendung sind, da eine gesonderte Verwertungskategorie, separat zu erwerben und wegen der Vielzahl der Konsumenten teuer. Für Satellitenübertragungen bestehen Sonderregelungen.

Für das Internet ist das Senderecht im Hinblick auf Webseiten und E-Mails nicht anzuwenden, da hier 1:1-Beziehungen vorliegen, selbst wenn viele Kommunikationsvorgänge innerhalb kurzer Zeit mit einer großen Empfängeranzahl stattfinden. Da es sich jedoch immer um einen genau bekannten einzelnen Partner handelt, liegt keine Sendung vor[145].

Davon zu unterscheiden sind Broadcasts oder Multicasts, worauf z.B. Internet-Radio aufbauen kann: Hier erfolgt typischerweise eine An- und Abmeldung beim Quell-Server, sodass die einzelnen Teilnehmer genau bekannt sind. Dennoch wird technisch nur ein einziger Datenstrom „gesendet“, welcher durch die technischen Zwischenkomponenten vervielfältigt und auf die Empfänger verteilt wird. Dies rückt zwar schon in die Nähe einer Sendung, doch da der "Sender" noch immer jeden einzelnen Kunden kennt und daher eine gesonderte Abrechnung und auch Überprüfung des Rechts an diesen zu verbreiten, möglich wäre, handelt es sich wohl noch nicht um eine Sendung. Erst wenn die Anmeldung nur mehr an Zwischen-Verteilstationen und nicht mehr beim Ausstrahlenden erfolgen würde, z.B. moderne Multicasts mit entsprechender Hardware, wäre von einer echten Sendung auszugehen. Da die Übermittlung synchron erfolgt, wird auch nicht das Recht der Zurverfügungstellung in Anspruch genommen.

III.3.4. Das Recht der Zurverfügungstellung

Dies ist das Recht, der Öffentlichkeit ein Werk so anzubieten, dass Personen es zu der von ihnen gewünschten Zeit und an einem selbst gewählten Ort abrufen können. Hiermit wird besonders das Internet angesprochen, wo das Problem bisher darin bestand, dass der "Endverbraucher" selbst die Vervielfältigung vornahm, und dies fast immer unter das Privileg der Privatkopie fiel. Auch das Recht der Zurverfügungstellung liegt ausschließlich beim Urheber, daher ist das Anbieten von Informationen, selbst wenn legal erlangt, ohne Zustimmung verboten. Hierunter fallen z.B. das Einstellen von MP3‘s oder Videos in Filesharing-Systeme aller Art, wobei dann aber schon die Herstellung der Kopie für das Anbieten verboten ist; siehe unten. Wie dieses Angebot erfolgt, drahtgebunden oder drahtlos, ist nicht ausschlaggebend. Aus dieser sonst wohl eher überflüssigen Formulierung wird aber auch klar, dass es z.B. nicht auf das technische Format ankommt.

---

[144] Übertragung des Radio-/Fernsehprogramms im Kabelfernsehen.

[145] Siehe dazu näher Thiele: Rechtsfragen beim Betrieb von Webradios. http://www.eurolawyer.at/pdf/Rechtsfragen_Webradios.pdf

Dieses Recht unterliegt *nicht* der Erschöpfung: Werden Webseiten legal abgerufen, dürfen diese dennoch nicht weitergegeben werden[146]. Dies beinhaltet auch das Einstellen einer absolut identischen Kopie auf die eigene Webseite als „Cache“[147]. Jeglicher Wiedergabevorgang bedarf hier der Zustimmung des Inhabers der Rechte. Das (erlaubte: implizite Genehmigung durch das Einstellen!) Speichern und ev. Ausdrucken von Webseiten berechtigt daher nicht zur Weitergabe, bzw. nur im Rahmen expliziter vertraglicher oder gesetzlicher Ausnahmen, wie etwa der Kopie für den privaten/eigenen Gebrauch. Immer möglich ist die Weitergabe eines Links, sodass jeder individuell die erlaubten Nutzungen vornehmen kann: Sofern das Werk an der Quelle noch vorhanden ist.

III.3.5. Bezeichnungsrecht

Der Urheber selbst kann bestimmen, ob sein Werk anonym bleiben soll oder ob er es mit seinem Namen oder einem persönlichen Zeichen versehen will. Ebenso besitzt der Urheber das Recht, sein Werk, welches fälschlicherweise einer anderen Person zugeschrieben wird, als seine Schöpfung zu reklamieren. Umgekehrt besteht jedoch eine Lücke: Wird ein Werk fälschlicherweise einer bestimmten Person als Urheber zugeordnet, so hat diese keine rechtliche Möglichkeit, dies zu verhindern, außer ev. über das Namensrecht nach ABGB. Auf das Recht, direkt auf dem Werkstück als Urheber genannt zu werden (Namensnennung), kann verzichtet werden. Im Gegensatz dazu ist das Recht, sich allgemein als Urheber zu bezeichnen, unverzichtbar, unübertragbar und kann immer geltend gemacht werden.

Für die Informatik bedeutend ist ein Sonderfall: Der Urheber eines Programms ist nur dann berechtigt, seine Bezeichnung auf das Werk zu setzen, wenn dies mit dem Dienstgeber ausdrücklich vereinbart wurde: Eine Umkehrung der normalen Regelung. Hiermit wird nur das Recht der Namens*nennung* (About-Boxen, Quellcode etc.) beseitigt; die Urheber-Eigenschaft darf der Programmierer weiterhin für sich reklamieren (*Bezeichnungs*recht).

III.3.6. Dauer der Urheberrechte

Das Bezeichnungsrecht besteht für den Urheber Zeit seines Lebens, die anderen Rechte sind zeitlich begrenzt. Für Werke der Literatur, der Tonkunst und der bildenden Künste[148] bestehen die Urheberrechte bis 70 Jahre nach dem Tod des letzten Miturhebers. Für vorverstorbene Miturheber treten deren Erben ein. Wurde ein Werk anonym geschaffen, d.h. fehlt eine Urheberbezeichnung oder ein sonstiger Anknüpfungspunkt, so wirkt der Schutz 70 Jahre ab der Werkschaffung. Wird es *vor* Ablauf dieser Zeit veröffentlicht, so beginnen die 70 Jahre jedoch ab der Veröffentlichung neu zu laufen ($\Rightarrow$ maximal 140 Jahre).

Um einen länger dauernden Schutz zu erreichen, vergeben viele Verwertungsgesellschaften einige Jahre vor Ablauf der Schutzfrist nur mehr Rechte für eine (neu erstellte) Bearbeitung des Originalwerks, um das Publikum an den Genuss dieser zu gewöhnen. Da Bearbeitungen selbst Werke sind, besteht für sie ebenfalls eine Schutzfrist. Diese läuft jedoch, da später geschaffen, auch später aus. Ein Beispiel hierfür ist der Radetzky-Marsch

---

[146] Im Unterschied etwa zu Büchern: Einmal gekauft, kann es beliebig (zumindest EU-weit) weiterverkauft oder verschenkt werden, ohne dass der Urheber dies verhindern kann.

[147] Der Berechtigte soll ein Werk auch wieder entfernen können, was durch solche Kopien unmöglich würde.

[148] Für Filmwerke besteht eine Sonderregelung: Wegen der vielen Urheber werden für die Berechnung der Schutzfrist ausschließlich (!) die folgenden vier Personen als Urheber festgelegt: Hauptregisseur, Drehbuchautor, Dialogautor und der Komponist der Filmmusik.

von J. Strauss, der immer nur in einer geschützten Bearbeitung aufgeführt wird. Das Original könnte zwar jederzeit ohne Lizenzgebühren aufgeführt werden, doch sind keine Noten dafür erhältlich. Weiters erwartet das Publikum inzwischen die etwas andere Fassung.

III.3.7. Die Erschöpfung

Wurde an einem Werkstück innerhalb der EU oder des EWR[149] mit Einwilligung des Berechtigten das Eigentum übertragen, so kann dieses einzelne Werkstück in der gesamten Europäischen Union/dem EWR (weiter-) verbreitet werden. Es kann also keine Verkaufsdifferenzierung nach Ländern innerhalb der EU vorgesehen werden. Parallelimporte von außerhalb der EU in diese hinein können jedoch verboten werden. Sonderregelungen bestehen für das Vermieten und den Verleih.

In diesem Zusammenhang von Bedeutung ist OEM-Software[150], z.B. Betriebssysteme, welche zusammen mit Festplatten oder Computern verkauft werden. Diese sind meist billiger als die technisch ansonsten identischen Vollversionen, welche unabhängig und einzeln verkauft werden. Inzwischen wurde entschieden[151], dass eine (dingliche) Bindung der Software an das Gerät nicht möglich ist. Lediglich der Händler kann (vertraglich!) verpflichtet werden, beide Elemente ausschließlich zusammen zu verkaufen. Dies bedeutet, dass ein Kunde die Software anschließend selbst, bzw. bei fehlender vertraglicher Bindung auch der Händler, ebenso ohne den Computer/Festplatte weiterverkaufen darf, da die "Erschöpfung" des Rechtes bereits durch den Verkauf an ihn eingetreten ist. Ansonsten bliebe die Software in alle Ewigkeit an das Gerät gebunden. Dies wurde jedoch u.a. als zu große Beschränkung des freien Warenverkehrs angesehen und daher abgelehnt. Natürlich darf in keinem Fall eine Kopie der Software zurückbehalten werden. Werden bloße Lizenzen verkauft, also z.B. Rechte zur Nutzung bereits vorhandener Software auf weiteren Computern, so tritt im Gegensatz dazu mangels physischer Exemplare *keine* Erschöpfung ein[152].

Im Bereich des E-Commerce ist dieser Erschöpfungsgrundsatz besonders wichtig: Wird etwa das Verbreitungsrecht an einem (körperlichen) Buch nur für ein bestimmtes Gebiet eingeräumt, so ist ein Verkauf über das Internet nur in diesem erlaubt. Genau zu beachten ist diesfalls, wo das Werkstück "in Verkehr gebracht" wird: Handelt es sich um einen Verkauf in dem genehmigten Gebiet mit anschließendem "Privatimport" durch den Konsumenten[153], so ist das Verbreitungsrecht nicht beeinträchtigt. Erfolgt jedoch der Verkauf am Ort des Käufers[154], so würde das Verbreitungsrecht verletzt.

Besonders bedeutsam ist, dass die Erschöpfung nur bei *körperlicher* Verbreitung („Werkstück“) eintritt: Wird Software daher auf CD-ROM erworben, so kann das Programm, d.h. die CD mit dem daran hängen Nutzungsrecht, später weiterverkauft werden. Bei Kauf und

---

[149] Achtung: Früher galt in Österreich internationale Erschöpfung. Daher unterliegt z.B. ein in den USA verkauftes Produkt, welches in die EU eingeführt wird, nicht der Erschöpfung nach EU-Recht!

[150] OEM = Original Equipment Manufacturer, d.h. Software, welche direkt vom Erzeuger der Hardware zusammen mit dieser verkauft wird.

[151] „OEM-Software“ BGH 6.7.2000, 1 ZR 244/97, http://www.flick-sass.de/oem_soft.html

[152] Siehe „Handel mit gebrauchten Softwarelizenzen“: LG München I 19.1.2006, 7 O 23237/05 (nicht rechtskräftig) http://www.aufrecht.de/4679.html

[153] Der Standardfall bei Versandkauf ist die Schickschuld: Der Verkauf erfolgt am Ort des Händlers, dieser ist jedoch zusätzlich verpflichtet, die Ware per Post/Spedition/… auf Gefahr des Empfängers an diesen abzusenden.

[154] Ein Hinweis darauf könnte z.B. die Lieferung frei Haus sein, sofern nicht explizit anderes vereinbart wurde. Dies kommt sehr selten vor. Ein Beispiel hierfür ist der Haustürverkauf, welcher aber nicht zum E-Commerce gehört.

Download über das Internet tritt keine Erschöpfung ein, da kein körperlicher Gegenstand vorliegt, und ein Weiterverkauf ist *nicht* möglich! Die erworbene Lizenz ist daher "höchstpersönlich" und nicht übertragbar, sofern nicht explizit vertraglich gestattet. Fehlende Erschöpfung betrifft insbesondere Musikdownloads, sowie alle anderen durch das Urheberrecht geschützten Werke (z.B. E-Books).

III.4. Freie Werknutzung

Im Interesse der Allgemeinheit besteht eine Einschränkung der ausschließlichen Rechte des Urhebers: Manche Zwecke wie beispielsweise die Verfolgung von Straftätern, z.B. die Veröffentlichung eines von einem Fotografen hergestellten Fotos als Fahndungsfoto, stehen höher als der Schutz der Rechte des Urhebers. Hierfür hat der Urheber in den meisten Fällen keinen Vergütungsanspruch und kann die Nutzung auch nicht verhindern. Um eine Entwertung der Urheberrechte zu verhindern, ist der Katalog der Ausnahmen jedoch restriktiv auszulegen. Hier wird nur die freie Werknutzung allgemeiner Art und das Zitatrecht an Sprachwerken behandelt. Es bestehen jedoch auch an Werken der anderen Kategorien freie Werknutzungen, z.B. das Ton-Zitat oder die Freiheit des Straßenbildes.

III.4.1. Staatliche Zwecke

Ein Werk kann immer als Beweis vor Gericht oder einer Verwaltungsbehörde verwendet werden. Ebenso ist ein Zugriff darauf für parlamentarische Verfahren und für die öffentliche Sicherheit möglich.

III.4.2. Begleitende Vervielfältigungen

Für Telekommunikationsunternehmen wurde eine spezielle zwingende, d.h. vertraglich nicht ausschließbare, Ausnahme eingeführt. Hiernach sind Vervielfältigungen erlaubt, sofern folgende Voraussetzungen kumulativ erfüllt sind:

- Flüchtige oder begleitende Vervielfältigung: z.B. Zwischenspeicherung während der Decodierung oder Caching zur Erhöhung der Zugriffsgeschwindigkeit.
- Die Vervielfältigung ist integraler und wesentlicher Teil eines technischen Verfahrens.
- Ihr einziger Zweck ist eine Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder eine rechtmäßige Nutzung.
- Sie besitzt keine eigenständige wirtschaftliche Bedeutung.

Damit ist also Caching sowohl in Vermittlungsrechnern (Proxies) als auch in Browsern, Hauptspeicher etc. wie auch sonstigen ähnlichen Vorgängen erlaubt. Die Voraussetzungen sind streng zu prüfen[155].

III.4.3. Eigener/Privater Gebrauch

Für den *eigenen* Gebrauch dürfen einzelne Vervielfältigungsstücke von Werken hergestellt werden, sofern dies auf Papier oder "ähnlichem Träger" erfolgt, z.B. Fotokopien oder Mikrofilme. Im Gegensatz zu Deutschland gilt dies in Österreich auch für juristische Personen,

[155] Die Entscheidung "Radio Melody III" (OGH 26.1.1999, 4 Ob 345/98h) bleibt daher weiter gültig, da es sich hierbei um dauerhafte Kopien handelte, die auch keinen integralen Teil eines technischen Verfahrens darstellen.

da diese ebenso einen "eigenen" Gebrauch haben können, im Gegensatz zu "privaten"; siehe sogleich. Einzelne derartige Vervielfältigungsstücke dürfen auch unentgeltlich[156] für den eigenen Gebrauch eines anderen hergestellt werden (=Kopien für Freunde).

Für den *privaten* Gebrauch dürfen natürliche Personen, also keine Firmen, da diese juristische Personen sind, auch einzelne Vervielfältigungsstücke auf anderen Trägern herstellen. Diese Kopien müssen daher nicht auf Papier-ähnlichen Medien erfolgen, was insbesondere Digitalkopien beinhaltet[157]. Solche Kopien dürfen weder unmittelbar noch mittelbar kommerziellen Zwecken dienen. El. Fachbücher dürfen daher nicht zu privater Weiterbildung kopiert werden[158]. Hier besteht keine Ausnahme zur Vervielfältigung für andere, weshalb nur Analog- aber nicht Digitalkopien für Freunde erstellt werden dürfen! Eine Weitergabe ist nur im engsten Kreis, z.B. Familie, erlaubt, aber nicht mehr an Freunde, Bekannte etc.

Ob für die Vervielfältigung zum eigenen/privaten Gebrauch eine legale Vorlage erforderlich ist oder nicht, ist umstritten, aber eher zu verneinen[159].

Diese Vervielfältigungen sowohl zum eigenen wie auch privaten Gebrauch dürfen niemals dazu verwendet werden, das Werk der Öffentlichkeit zugänglich zu machen. Schon die ursprüngliche Vervielfältigung ist dann illegal. Ein Beispiel hierfür ist das Einstellen in ein Filesharing-Netzwerk. Der Umfang des Gebrauchs muss vielmehr auf den Eigentümer des Werkes beschränkt bleiben. Die Anzahl der Vervielfältigungsstücke ist nicht explizit festgelegt, doch müssen alle Exemplare tatsächlich für den eigenen/privaten Gebrauch verwendet werden. Die Grenze dürfte, je nach Zweck, zwischen 1 und ausnahmsweise bis zu 20 liegen; als ungefährer Richtwert kann eine Anzahl von etwa sieben gelten. Die Urheber werden hierfür durch die Reprographie-Vergütung entschädigt. Dies ist eine Abgabe auf Vervielfältigungsgeräte, wie Kopierer und Scanner, sowie Leermedien, wie CD-Rohlinge oder Leerkassetten.

Bei diesem Recht bestehen einige Ausnahmen, von denen eine besonders wichtig ist: Ganze Bücher, Zeitschriften sowie Musiknoten dürfen nur dann zum eigenen oder privaten Gebrauch vervielfältigt werden, wenn sie erschienen und bereits vergriffen, oder nicht erschienen aber zumindest veröffentlicht (d.h. verfügbar, jedoch nicht in körperlichen Werkstücken) sind. Hier wird der Verbreitung des Inhalts im Sinne des Interesses der Öffentlichkeit Vorrang gegenüber dem Recht der Urheber eingeräumt. Die Weitergabe, und damit die Nutzung des Inhalts, soll nicht dadurch unmöglich werden, dass die potentiellen Nutzer keine Möglichkeit haben, ein Werkexemplar zu erwerben. Ist das Werk nicht erschienen oder bereits vergriffen, so bestehen keine oder nur sehr schwierig zu nutzende Möglichkeiten, ein Werkexemplar zu erlangen und damit an den Urheber ein angemessenes Entgelt zu entrichten. Dadurch soll das Werk jedoch nicht "auf Eis" liegen, sondern trotzdem genutzt werden können. Hinzuzufügen ist, dass sich ein Urheber auch dagegen

---

[156] Auch entgeltlich, falls es sich (neben anderen Fällen) um Vervielfältigungen mit Reprographie oder ähnlichen Verfahren handelt, da dann die Urheberrechtsabgabe auf Geräte bzw. Medien anfällt. Dies betrifft etwa Copyshops.

[157] Beispielsweise das Abspeichern einer Webseite auf der Festplatte: Die Anzeige ist bei frei zugänglichen Webseiten immer erlaubt; für das Abspeichern gilt dies jedoch nicht allgemein. Existiert ein spezieller Download-Link, so kann von einer Erlaubnis ausgegangen werden. Ansonsten ist dies verboten.

[158] Dies ist indirekt ein kommerzieller Zweck, da die Verbesserung der eigenen Qualifikation das Lohnniveau bzw. die Chancen bei einer Stellensuche verbessert.

[159] Siehe Thiele/Laimer, Die Privatkopie nach der Urheberrechtsgesetznovelle 2003, ÖBl 2004, 17. In Deutschland wurde dies explizit geregelt: § 53 Abs 1 dUrhG: Es dürfen keine "offensichtlich rechtswidrig hergestellte[n] Vorlage[n]" verwendet werden, sodass wohl ein Großteil der Downloads aus dem Internet hiermit ausgeschlossen werden.

wehren kann (§ 29 UrhG), wenn ein Verleger sein Werk nicht ausreichend produziert und damit diese freie Vervielfältigung ermöglicht. Er kann diesem Verleger die Rechte trotz bestehenden Vertrages entziehen und einem anderen überlassen, der dann hoffentlich das Werk verbreitet. Eine Vervielfältigung durch Abschreiben mit der Hand ist immer erlaubt.

Zu beachten ist, dass das Recht der Vervielfältigung zum eigenen oder privaten Gebrauch zwar grundsätzlich auch für Computerprogramme als Werke der Literatur gelten würde, dieses jedoch in § 40d Abs 1 UrhG explizit ausgeschlossen wird. Solche Vervielfältigungen sind damit verboten, werden im Gegenzug aber etwa um Sicherungskopien erweitert. Siehe dazu III.5.3!

III.4.4. Pressespiegel

Für den eigenen Gebrauch, also auch innerhalb von Firmen, dürfen einzelne Vervielfältigungsstücke der Berichterstattung über Tagesereignisse hergestellt werden (§ 42 Abs 3 UrhG)[160]. Dies gilt jedoch ausschließlich für "analoge"[161] Nutzung. Es ist daher erlaubt, Zeitungsausschnitte zusammenzukleben und zu fotokopieren. Einscannen und Weiterleiten auf el. Wege ist ebenso möglich[162]. Das Einstellen der eingescannten Berichte in ein Intra- oder gar das Internet sind dagegen nicht erlaubt[163]. Texterkennung per OCR-Software[164] und Weiterleiten als Text ist ebenso verboten, da sich hier die Nutzungsmöglichkeiten, etwa durch die mögliche Volltextsuche, erweitern.

Im Gegensatz dazu ist eine Zusammenstellung von Links zu Online-Artikeln mit kleiner Textvorschau erlaubt[165]. Dies kann auch auf Bestellung für einen anderen und sogar entgeltlich erfolgen (§ 42a Abs 3 UrhG).

III.4.5. Schulgebrauch

An Schulen und Universitäten dürfen Werke, sogar ganze Bücher[166], zu Zwecken des Unterrichts und der Lehre in Klassenstärke, also jeweils nur für eine ganz bestimmte konkrete Klasse oder Lehrveranstaltung, kopiert und verbreitet werden. Von diesem Recht nicht betroffen sind Werke, die nach ihrer Beschaffenheit für den Schul- oder Unterrichtsgebrauch bestimmt und als solche bezeichnet sind, d.h. auch Skripten. Eine freie Kopierbarkeit würde eine sinnvolle Verwertung solcher Werke verhindern, daher dürfen hiervon an Schulen bzw. in Lehrveranstaltungen nur Originale verwendet werden. Für digitale Kopien, also

---

[160] Siehe Fallenböck/Nitzl: Urheberrechtliche Rahmenbedingungen für el. Pressespiegel. MR 2003, 102

[161] Dieses Wort kommt sonst nirgends im UrhG vor, ist also wohl etwas anderes als eine Vervielfältigung „auf Papier oder einem ähnlichen Träger“.

[162] Dittrich, Medienbeobachtung - ihre Möglichkeiten und Grenzen nach der UrhG-Nov 2003, ÖBl 2003, 61 Anderer Meinung Fallenböck/Nitzl: Urheberrechtliche Rahmenbedingungen für el. Pressespiegel. MR 2003, 102 ebenso Wiebe, Das neue "digitale" Urheberrecht - Eine erste Bewertung, MR 2003, 309. Für eine Zulässigkeit der el. Übermittlung BGH 11.7.2002, I ZR 255/00 (im deutschen UrhG jedoch keine Einschränkung auf "analoge Nutzung"!), sofern nur dieselben Funktionen und Nutzungspotentiale wie bei herkömmlichen Pressespiegeln dadurch verfügbar sind.

[163] Dabei ergeben sich deutlich mehr und bessere Nutzungen, z.B. Suchfunktionen und Zugriffsmöglichkeiten als bei einem Pressespiegel auf Papier.

[164] Optical Character Recognition = Umwandlung von Schrift in einem Bildformat in Text

[165] Deutschland: Entscheidung „Paperboy“: BGH 17.7.2003, I ZR 259/00 http://www.jurpc.de/rechtspr/20030274.htm Dies gilt wohl identisch in Österreich, da beides auf denselben EU-RL beruht.

[166] Die Änderung von § 42 Abs 8 UrhG erster Satz nimmt wohl nicht nur, wie anscheinend intendiert, Musiknoten aus, sondern auch das Verbot der Vervielfältigung ganzer Bücher für den Schulgebrauch.

nicht auf Papier oder ähnlichem Träger, darf die Vervielfältigung zum Schulgebrauch aber nur für nicht-kommerzielle Zwecke Anwendung finden[167].

III.4.6. Forschung

Jedermann darf einzelne Vervielfältigungsstücke, sogar digitale, zum eigenen Gebrauch der Forschung anfertigen, solange kein kommerzieller Hintergrund vorliegt. Entwicklungsabteilungen in Firmen fallen daher heraus, genauso wie Selbständige oder Drittmittelforschung an Universitäten. Es ist aber keine Verbindung zu einer besonderen (Forschungs-) Institution wie Schulen, Universitäten, … erforderlich. Dies wurde von Verlagen als "Einfallstor" für praktisch unbeschränkte Vervielfältigungen erfolglos bekämpft, da sich eine beliebig zusammengesetzte Gruppe als "private Forschungsgemeinschaft" deklarieren und dann innerhalb dieser frei kopieren könnte. Diese Gefahr besteht natürlich, doch wird auch tatsächlich eine ernsthafte Forschung und Auswertung gewissen Ausmaßes erfolgen und im Zweifelsfalle nachgewiesen werden müssen, um sich erfolgreich auf diese Ausnahme berufen zu können. Da es sich um Vervielfältigung zum eigenen Gebrauch handelt, ist auch eine unentgeltliche Herstellung und Weitergabe an Dritte erlaubt, sofern diese die sonstigen Anforderungen erfüllen[168].

III.4.7. Zitate

Bei Zitaten (§ 46 UrhG) wird in zwei Untergruppen unterschieden: Kleinzitate und wissenschaftliche Großzitate. Bei einem Kleinzitat handelt es sich um einzelne kurze Passagen, während bei einem Großzitat auch ganze Werke, z.B. Gedichte, wiedergegeben werden können. Zitate müssen als solche in Erscheinung treten, also durch Angabe von Quelle und Urheber und als solche[169] besonders gekennzeichnet sein. Weitere Voraussetzung für die Zulässigkeit eines Zitates ist, dass die aufnehmende Einheit selbst ein Werk ist und das Zitat als Beleg bzw. zur Erläuterung des eigenen Inhaltes dient, jedoch nicht als Ersatz einer eigenen Leistung. Eine Kollektion von Zitaten alleine[170] erreicht nicht die Werkhöhe und ist daher keine Rechtfertigung für die einzelnen Zitate: Ohne die Zitate muss immer noch ein (Rest-) Werk übrig bleiben.

- Kleinzitat: Aus einem veröffentlichten, aber nicht unbedingt erschienenen oder bereits vergriffenen, Sprachwerk dürfen einzelne Stellen verwendet werden. Die Quelle ist mit Titel und Urheberbezeichnung anzugeben sowie die Stelle so genau zu bezeichnen, dass sie leicht aufgefunden werden kann. Dies ist typischerweise eine Seitenangabe oder Nummerierung. Bei Online-Werken wird ein Link alleine nicht ausreichen: Urheber und Titel sind zusätzlich erforderlich, sofern vorhanden.
- Wissenschaftliches Großzitat: Im Gegensatz zu einem Kleinzitat muss das Ursprungswerk hier schon erschienen sein; eine bloße Veröffentlichung ist nicht ausreichend. Achtung: Das Zurverfügungstellen im Internet ist zwar eine Veröffentlichung, aber kein Erscheinen! Zusätzlich muss es sich beim aufnehmenden Werk um ein *wissenschaftliches* Werk handeln, was deutlich höhere Qualität und eine besondere Natur[171] voraus-

[167] Kommerzielle Schulungen sind zwar Unterrichtsgebrauch, dürfen deshalb aber nur analoge Nutzungen vornehmen.

[168] Also die Erstellung einer Digitalkopie für einen anderen Forscher zu dessen Forschungszwecken.

[169] Einrückungen, Schriftart, Anführungszeichen etc.

[170] Dies kann ein Sammelwerk darstellen, wobei aber dann für die Verwertung die Rechte der Urheber der Einzelwerke erforderlich sind.

[171] Gekennzeichnet durch ernsthafte, methodische Suche nach Erkenntnis.

setzt. Auch ist hier eine größere Menge an Zitaten möglich, sofern das Rest-Werk weiter seinen Werks- sowie wissenschaftlichen Charakter behält.

Da es sich bei Computerprogrammen um Sprachwerke handelt, sind auch bei ihnen Zitate möglich, z.B. die Übernahme einzelner Code-Abschnitte in Diplomarbeiten, Bücher etc. Deshalb ist dann eine exakte Quellenangabe notwendig. Ein wissenschaftliches Großzitat, also die Übernahme ganzer Programme oder großer Teile davon, z.B. ganzer Module oder Klassen, wird jedoch nur selten möglich sein. Der Einsatz von Programmteilen als Ersatz für eigenen Code wird nicht vom Zitatrecht umfasst: Ein Zitat darf nicht um seiner selbst willen eingefügt werden, sondern muss als Beleg, Hinweis, Erklärung, Beispiel etc. dienen.

Links selbst sind keine Zitate sondern nur Verweise, da sie keinen eigenen Inhalt darstellen, sondern nur auf diesen verweisen (siehe dazu auch IV.5 und IV.7).

III.5. Sondervorschriften für Computerprogramme

Bei Computerprogrammen bestehen einige Abweichungen im Vergleich zu anderen Werkarten, daher sind hier separate Regelungen erforderlich. Das beste Beispiel hierfür ist die freie Werknutzung der Vervielfältigung für den privaten Gebrauch: Würde sie auch für Computerprogramme gelten, wäre beispielsweise eine wirtschaftliche Verwertung von Betriebssystem- oder Textverarbeitungssoftware im Privatbereich faktisch unmöglich. Diese Regelungen basieren auf der Computer-Richtlinie der EU.

III.5.1. Computerprogramme als Werke

Computerprogramme sind dann Werke, wenn sie „das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers" sind. Diese Definition gilt, wie bereits erwähnt, als Voraussetzung für Werke allgemein. Wegen der strengen Syntax-Bindung von Programmen und der limitierten Anzahl von Basiselementen (=Sprachkonstrukten) ist besonders die Anordnung und die dahinter stehende Idee, welche (als solche) aber ebenso wenig wie ein Algorithmus[172] nicht über das Urheberrecht geschützt ist, zu beachten. Der Charakter als Werk kann sich auch aus für die Ausführung irrelevanten Zusatzdaten ergeben, etwa Variablennamen oder Kommentaren. In dieser gesetzlichen Definition fehlt jedoch die für sonstige Werke erforderliche „Eigentümlichkeit“, welche durch „eigene geistige Schöpfung“ ersetzt wurde. Daraus wird geschlossen, dass der Standard für Programme noch niedriger liegt als für andere Erzeugnisse. Alles, was über Trivialprogramme hinausgeht, ist daher ein Werk, wodurch also auch schon recht kleine Programmteile Teilwerke sein können.

Ein Programm ist in allen seinen Ausdrucksformen geschützt. Jede Art von Programmcode einschließlich Maschinensprache stellt dasselbe Werk dar und ist als Einheit geschützt. Zum Programm zählt auch "das Material zur Entwicklung des Computerprogramms", was sich auf Struktogramme oder ähnliche programmnahe Darstellungen bezieht. Spezifikationen und Anforderungshefte sind davon jedoch eher nicht umfasst und stattdessen als eigenständige Werke der Literatur geschützt. Die Grenze ist hier fließend und an Hand der Nähe zur formalen Strenge einer Programmiersprache zu ziehen.

[172] So ist auch die Idee "Fenster" zu verwenden nicht schutzfähig, sehr wohl jedoch eine konkrete Anordnung von Fenstern. Algorithmen können jedoch durch Patente bzw. Gebrauchsmuster geschützt werden.

III.5.2. Computerprogramme von Dienstnehmern

Wird ein Computerprogramm von einem Dienstnehmer in Erfüllung seiner Dienstpflichten geschaffen, so erhält der Dienstgeber daran ein unbeschränktes Werknutzungsrecht, außer es wurde anderes vereinbart. Dieser Rechtsübergang ist notwendig, da sich sonst eine Interessenskollision ergeben könnte: Laut Dienstvertrag stehen die Früchte der Arbeit dem Dienstgeber zu, nach dem Urheberrecht könnte jedoch der Dienstnehmer darüber verfügen. Normalerweise wird sich aber auch für andere Werke aus dem Dienstvertrag, explizit oder implizit, eine Pflicht ergeben, die Nutzungsrechte an den Dienstgeber zu übertragen.

Darüber hinaus erhält der Dienstgeber weitere Rechte: Er kann bestimmen, ob bzw. mit welcher Urheberbezeichnung das Programm versehen wird. Dies betrifft sowohl den Code selbst (Kommentare) als auch für den Benutzer sichtbare Elemente wie "Credits", eine About-Box, Datenträger oder die Dokumentation. Weiters ist er berechtigt, sowohl Werk, Titel als auch Urheberbezeichnung zu verändern, was insbesondere im Hinblick auf Weiterentwicklungen und Korrekturen von Bedeutung ist. Ein Recht bleibt dem Urheber jedenfalls erhalten, sich als Urheber zu bezeichnen, wenn auch nicht direkt im/am Werk.

III.5.3. Freie Übertragbarkeit

Da es sich bei Computerprogrammen im Gegensatz zu anderen Werken praktisch nie um echte Kunstwerke handelt, sondern kommerzielle Aspekte im Vordergrund stehen, gelten für die Übertragung der Rechte daran zwei Besonderheiten. Ist nichts anderes vereinbart, so können die Nutzungsrechte an einem Computerprogramm auch ohne Einwilligung des Urhebers auf andere Personen übertragen werden. Ein (Weiter-) Verkauf eines Programms ist daher ohne Zustimmung der Programmierer möglich[173]. Auch Änderungen am Programm, also z.B. die Weiterentwicklung, kann der Erst-Urheber nicht verhindern, selbst wenn das Ergebnis der Öffentlichkeit zugänglich gemacht wird[174].

Die zweite Besonderheit ist, dass im Gegensatz zu normalen Werken bei einer Nicht-Ausübung des Werknutzungsrechtes (="auf Eis legen") dieses nicht entzogen und an andere Personen übertragen werden kann. Entsprich das Werk daher nicht den Standards des Unternehmens oder wird aus strategischen Gründen ein späterer Veröffentlichungszeitpunkt gewählt, so liegt dies im freien Ermessen der Firma. Der Urheber eines Programms sollte daher darauf achten, dass er beim Einräumen der Rechte an einem Programm entweder eine endgültige Entschädigung erhält (=Verkauf des Programms), oder sich eine ordentliche Vermarktung im Vertrag zusichern lässt, wenn er in Folge an jedem lizenzierten Exemplar beteiligt ist. Handelt es sich um das Werk eines Dienstnehmers, besitzt ohnehin der Dienstgeber normalerweise alle Verwertungsrechte[175].

Wichtig ist zu beachten, dass ein einmal verkauftes Programm in allen seinen Teilen übergeht. Wenn daher nicht ein besonderer Vorbehalt vereinbart wurde, kann z.B. auch eine als Grundlage für das Endprodukt entwickelte Klassenbibliothek nicht für weitere Projekte

---

[173] Diese Vorschrift ähnelt ein wenig dem Erschöpfungsgrundsatz, der ja sonst nur für Werkstücke, also physische Exemplare, gilt. Im Gegensatz dazu kann jedoch die freie Übertragbarkeit von Programmen vertraglich verboten werden. Dieser Ausschluss betrifft aber nur rein el. Versionen oder (Sub-)Lizenzen; wird das Programm rechtmäßig auf CD gebrannt und verkauft, so tritt ganz normale Erschöpfung ein.

[174] Ciresa, Softwareentwicklung durch Arbeitnehmer. ZAS 2006/3

[175] Siehe hierzu auch Schwarz, Software- und Datenbankerstellung durch Arbeitnehmer: Welche rechtlichen Aspekte sind zu beachten? http://www.dbj.at/phps/start.php?noie=1&lang=de&content=publikationen_show.php&navi=publikationen&publikation_nr=307 Weiters: OGH 28.10.1997, 4 Ob 304/97b (=wbl 1998/144)

verwendet werden. Es sollte daher immer genau festgelegt werden, welche Rechte an welchen Teilen übergehen und welche vorbehalten bleiben bzw. wo nur lizenziert und nicht verkauft wird.

III.5.4. Freie Werknutzungen

Für Computerprogramme gilt die Vervielfältigung zum privaten Gebrauch nicht[176]. Darunter fällt nicht nur die "klassische" Form, sondern auch das Kopieren in Klassenstärke für Unterrichtszwecke[177] und einige weniger wichtige bzw. hier nicht bedeutsame Arten, wie etwa das Kopieren zu Ausstellungszwecken in Museen.

Dieser Einschränkung stehen einige besondere zusätzliche Rechte gegenüber, auf die auch nicht wirksam verzichtet werden kann. Selbst wenn diese Rechte in wirksamen Lizenzbedingungen ausgeschlossen wurden, bleiben sie bestehen (Unwirksamkeit entgegenstehender Regelungen).

Dazu zählen im Einzelnen:

- Es dürfen Sicherungskopien erstellt werden. Es besteht keine Beschränkung auf eine bestimmte Anzahl, doch dürfen diese Kopien ausschließlich zur Sicherung dienen, und dies muss für die Nutzung des Programms notwendig sein[178]. Je wertvoller ein Programm ist, desto mehr Sicherungskopien werden erlaubt sein. Darin ist etwa das so genannte "Hot-Standby", ein Rechner wird parallel mitbetrieben, um im Fehlerfall sofort auf diesen Zweitrechner umschalten zu können, nicht inbegriffen: „Sicherung“ ist ausschließlich der Schutz vor *Verlust* des Programms, beinhaltet daher nicht eine jederzeitige Nutzungsmöglichkeit oder andere Zwecke.
- Ein Computerprogramm darf soweit vervielfältigt und bearbeitet (= Eingriff in den Code) werden, als dies für die bestimmungsgemäße Nutzung durch den Berechtigten notwendig ist. Das Kopieren auf eine Festplatte (Installation) und der Start (Kopie in den Hauptspeicher) sind typische Beispiele. Diese Erlaubnis schließt Lizenzierungsvorschriften, welche eine Begrenzung auf bestimmte Rechner oder eine feste Anzahl vorsehen, nicht aus. Die Bearbeitung bezieht sich typischerweise darauf, das Programm an bestehende Programme oder Daten anzupassen bzw. zu konfigurieren, wozu manchmal ein Eingriff in das Programm selbst nötig ist. Nicht davon erfasst ist eine Erweiterung oder Weiterentwicklung des Programms, da dies eine andere Nutzung als die bestimmungsgemäße ist. Diese Erlaubnis ist mehr oder minder eine Generalklausel zum Ersatz fehlender Regelungen in Kauf- bzw. Nutzungsverträgen, in denen meistens zumindest die "bestimmungsgemäße Nutzung" festgelegt wird. Zusätzlich kann sich diese auch aus dem Programm selbst ergeben.
- Der Benutzer kann das Programm untersuchen, beobachten und testen, um die Funktionsweise und die verwendeten Ideen, Grundsätze, Algorithmen etc. herauszufinden. Hier ist aber eine Beschränkung der Mittel zu berücksichtigen: Eine Untersuchung darf

---

[176] Zum Problem, ob die freie Werknutzung nach § 42a (Reprographieabgabe) erlaubt ist, siehe Wachter/Winter, Computerrecht für die Praxis. Schutz von Computerprogrammen Datenschutzrecht Bildschirmarbeitsplätze. Wien: Weiss 1996. Eigener Gebrauch wäre ohnehin relativ sinnlos, da dieser ja nur auf Papier und ähnlichen Medien, aber nicht digital, erlaubt ist. Das Programm könnte daher nur mit Papier und Bleistift ausgeführt werden, jedoch niemals auf einem Computer, da schon die Eingabe eine digitale Vervielfältigung ist.

[177] Also keine Verteilung von Software nur für die Verwendung in einer bestimmten Lehrveranstaltung!

[178] Bei Zusage der Zusendung eines Ersatzdatenträgers fällt dieses Recht also wohl weg.

nur durch normale Handlungen erfolgen, zu denen der Benutzer auch berechtigt ist (Laden, Speichern, Ausführen, ...). Hierfür ist keine Zweckbindung festgelegt. Ergebnisse können also, im Gegensatz zur Dekompilierung (siehe unten), auch dazu verwendet werden, Informationen für die Schaffung eines Konkurrenzproduktes zu erlangen. Ein Programm darf daher fast beliebig als "Black-Box" getestet werden.

- Gegenüber dem vorigen Punkt bestehen für die Dekompilierung, einem Testen als "White-Box", besondere zusätzliche Einschränkungen: Es müssen auf diese Weise nicht ohne weiteres erhältliche Informationen, insbesondere nicht vom Urheber, gesammelt werden, um die Interoperabilität mit einem unabhängig geschaffenen Programm zu ermöglichen. Dekompilierung ist nur dann erlaubt, wenn es durch einen Nutzungsberechtigten an einem legalen Vervielfältigungsstück erfolgt. Sie darf nur in dem zu diesem Zweck notwendigen Ausmaß erfolgen, also nur soweit Informationen nötig sind, und nur an diesen Programmteilen. Für die dadurch erlangten Informationen bestehen besondere Geheimhaltungsvorschriften: Die extrahierten Informationen dürfen nur für die Anpassung an andere Programme verwendet, nicht an Dritte weitergegeben werden, außer genau dies ist für die Interoperabilität erforderlich, und nicht zur Schaffung eines ähnlichen Produktes[179] oder der Begehung einer Urheberrechtsverletzung verwendet werden.

III.5.5. Umgehungsschutz

Werden Computerprogramme[180] durch technische Maßnahmen wie beispielsweise Kopierschutz auf Programm-CD's, Verschlüsselung, Passwörter etc. geschützt, so sind diese Schutzmaßnahmen selbst ebenfalls geschützt. Als Rechtsfolge bei Verletzungen kommen Unterlassung und Beseitigung in Frage. Verboten ist das in Verkehr bringen oder der Besitz zu Erwerbszwecken von speziellen Mitteln zur Umgehung dieser technischen Schutzmaßnahmen. Diese müssen *allein* dazu bestimmt sein, die Umgehung von technischen Schutzmechanismen zu erleichtern bzw. zu ermöglichen. Beispiele sind nachgebaute Dongles, Kopierschutz-Knack-Programme oder Programme zur Generierung von Lizenzschlüsseln. Derartige Mittel dürfen daher zwar privat besessen und verwendet[181], jedoch nicht in Verkehr gebracht werden, etwa durch Verkauf, Verschenken oder Anbieten auf Webseiten. Dies umfasst beispielsweise nicht die Weitergabe von *Anleitungen* zum Selbstbau. Verboten sind Mittel, die allein (=ausschließlich) dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung der technischen Maßnahmen zu erleichtern oder zu ermöglichen. Eine besondere Bedeutung dürfte diesem Paragraphen aufgrund der Beschränkung auf die Ausschließlichkeit des Zweckes nicht zukommen.

Zum viel interessanteren Schutz technischer Maßnahmen, welcher allgemein, aber mit Ausschluss der Rechte an Computerprogrammen, gilt, siehe Abschnitt III.8.

---

[179] Ein Problem etwa für Samba, die Open-Source Alternative zu Windows Datei (Drucker-, …) Servern. Siehe hierzu auch das Verfahren vor der EU, in dem Microsoft zur Bekanntgabe der Protokolle verpflichtet wurde, um genau solche Interoperabilität zu ermöglichen.

[180] Also nicht DVDs, Audio-CDs, ..., da diese keine Computerprogramme enthalten. Hierfür ist § 90c UrhG vorgesehen.

[181] Sofern die Nutzung ansonsten erlaubt ist! Ein Programm mit Kopierschutz darf also „gecrackt" werden, um auch ohne Einlegen des Datenträgers zu funktionieren. Die dadurch mögliche Verwendung auf zwei Computern gleichzeitig bleibt jedoch nach wie vor verboten.

III.6. Sondervorschriften für Datenbanken

Nicht nur für Programme, sondern auch für Datenbanken existieren Sonderregelungen. Sie wären jedoch auch ohne diese in begrenztem Umfang als Sammelwerke geschützt. Die folgenden Regelungen basieren auf der Datenbank-Richtlinie der EU.

Neben den hier erläuterten Punkten gelten für Datenbanken dieselben Vorschriften wie für Dienstnehmerwerke und die freie Übertragbarkeit bei Computerprogrammen (siehe III.5.2 und III.5.3), da es sich ebenfalls eher um wirtschaftliche als künstlerische Werke handelt.

III.6.1. Datenbankwerke

Eine Datenbank ist eine Sammlung von Daten, welche systematisch angeordnet und einzeln zugänglich sind. Die „einzelne Zugänglichkeit“ bezieht sich darauf, dass das Abfragen oder ein Aufsuchen individueller Elemente möglich sein muss; zusätzliche Mengen- oder Gesamtabfragen sind unschädlich. Die einzelnen enthaltenen Elemente müssen selbst keine Werke sein. Um ein Datenbankwerk darzustellen, ist zusätzlich erforderlich, dass das/ein Ordnungskriterium eigentümlich ist. Für eine (bloße) Datenbank reicht also eine laufende zufällig vergebene Nummer aus. Für ein Datenbankwerk hingegen muss diese Nummer zumindest in einer bestimmten, originellen oder in sonstiger Weise "besonderen", Reihung bestehen[182]. Genau genommen handelt es sich hier lediglich um eine neue Bezeichnung: Erfüllt eine Datenbank das Kriterium der eigentümlichen Auswahl oder Anordnung, so handelt es sich um ein Sammelwerk.

Analog dem, allerdings neueren, Datenschutzgesetz müssen Datenbankwerke nicht el. gespeichert oder zugänglich sein; auch Zettelkarteien sind von diesen Regelungen betroffen. Wichtig ist die Abgrenzung der Datenbankwerke selbst von dem Zugriffsmechanismus: Er zählt nicht zum Datenbankwerk, sondern ist ev. selbst als Computerprogramm geschützt. Es geht hier also ausschließlich um die Zusammenstellung und Organisation des Dateninhalts, nicht aber die konkrete Zugriffsmöglichkeit oder deren Umsetzung.

III.6.2. Öffentliche Wiedergabe

Nur der Urheber hat das Recht, ein Datenbankwerk öffentlich wiederzugeben. Dies schließt Wiedergabe, Vor- und Aufführung ein. Hervorzuheben ist, dass das Zugänglichmachen eines Datenbankwerkes z.B. über Internet explizit dem Urheber vorbehalten ist[183]. Der konkrete Inhalt einer "öffentlichen Wiedergabe"[184] ist jedoch etwas unklar.

---

[182] Eine „Datenbank“ ist eine bloße Menge. Mit der Existenz eines Kriteriums alleine ändert sich noch nichts, erst wenn dieses „kreativ“ ist, sich also nicht typischerweise aus den Daten ergibt, entsteht ein Datenbankwerk. Ein Beispiel wäre die Sortierung einer Adressliste nach dem Nachnamen: Dies ist nichts Besonderes und ergibt sich direkt aus den Daten, erzeugt also kein Datenbankwerk. Besteht die Sortierung in der Bedeutung der Personen am Kunstmarkt, so ist dies ein eigentümliches Kriterium, was in einem Werk resultiert.

[183] Beispiel: Erwerb einer Telefonnummern-Datenbank, lokale Installation derselben und Erstellung von Webseiten, sodass Abfragen der lokalen Datenbank über das Internet möglich sind.

[184] Das Recht der Zugänglichmachung wird hier nicht erwähnt, obwohl es an anderen Stellen explizit eingefügt wurde: Es gilt für alle "Werke". Daher auch die explizite Einfügung bei den bloßen Datenbanken, für welche die Liste der Verwertungsrechte nicht standardmäßig gilt, da diese ja keine Werke sind; siehe unten! Unter öffentlicher Wiedergabe wird sonst eine unkörperliche Verwertung verstanden, welche typischerweise durch Aufführung, Vortrag oder Vorführung erfolgt. Diese ist jedoch für die verschiedenen Werkarten jeweils separat bestimmt (z.B. Literatur: Vortrag oder Aufführung; bildende Kunst: optische öffentliche Darstellung). Da in einer Datenbank grundsätzlich jedes beliebige Werk enthalten sein kann, musste dies hier (Alternative: Einfügen in § 18) generell festgelegt werden.

III.6.3. Freie Werknutzungen

Auch bei Datenbankwerken sind die wichtigsten Regeln die freien Werknutzungen. Hier bestehen zwei Einschränkungen und eine Erweiterung.

Die freie Vervielfältigung zum eigenen und zum privaten Gebrauch (siehe III.4.2) ist bei Datenbankwerken ebenso wie bei Computerprogrammen ausgeschlossen. Vervielfältigung zur wissenschaftlichen Forschung ohne Erwerbszweck ist jedoch erlaubt, sowohl durch digitale Kopien als auch auf Papier. Demgegenüber dürfen von Datenbankwerken, deren Teile nicht el. zugänglich sind (i.e. Karteien), zusätzlich noch einzelne Vervielfältigungsstücke zum privaten nicht-kommerziellen Gebrauch hergestellt werden.

In einer Generalklausel wird jede Verwertungshandlung erlaubt, die notwendig ist, um die bestimmungsgemäße Nutzung zu erreichen. Es dürfen daher beliebige Vervielfältigungen (z.B. auf Proxy-Servern) und Verbreitung (z.B. innerhalb der Firma) erfolgen, wenn dies für den Zugang unvermeidlich ist. Derartige Kopien sind jedoch auf diejenigen Personen eingeschränkt, die zur Benutzung ermächtigt sind. Vervielfältigungen dürfen also nur auf firmeninternen Proxies, aber nicht auf jenen Dritter, erfolgen[185]. Hier handelt es sich um ein unverzichtbares Recht, das vertraglich nicht ausgeschlossen werden kann. Wie bei Computerprogrammen kann auch hier der Umfang der Nutzung frei festgelegt werden, z.B. die Anzahl der gleichzeitigen Zugriffe, der berechtigten Personen, oder die Vervielfältigung von Abfrageergebnissen, etwa durch Ausdruck.

III.6.4. Datenbanken („Bloße Datenbanken“)

Analog zu der Unterscheidung Lichtbildwerke ↔ Lichtbild existieren auch etwas "geringere" Datenbanken, welche keinen Werkscharakter aufweisen. Dies ist deshalb von Bedeutung, da bei Datenbanken oft großer Wert auf Vollständigkeit gelegt wird, was jedoch das Werkskriterium der besonderen Auswahl aus der Grundgesamtheit unmöglich macht[186].

Bei einer "bloßen" Datenbank handelt es sich wieder um eine Sammlung einzeln zugänglicher Elemente, doch muss hier zusätzlich für die Beschaffung, Überprüfung oder Darstellung derselben eine wesentliche[187] Investition erfolgt sein. Der Schutz solcher Sammlungen ist daher weniger ein echter Urheberrechtsschutz, als vielmehr ein Investitionsschutz. Wichtig zu beachten ist, dass der Aufwand für die Generierung der Daten nicht als Investition zählt[188]! Erst wenn ohnehin bereits bestehende Daten mit zusätzlichem Aufwand in eine Datenbank umgewandelt werden, entsteht dieser neue Schutz[189].

---

[185] Siehe jedoch die allgemeine Erlaubnis von Caching in § 41a UrhG („Flüchtige und begleitende Vervielfältigungen“)

[186] Eine Liste aller subjektiv von einer Person als „*gut*“ beurteilten Webseiten für Kinder ist daher ein Datenbankwerk, eine Auflistung *aller* für Kinder gedachten Webseiten jedoch nicht. „Alle“ ist nicht eigentümlich/kreativ!

[187] Was genau "wesentlich" ist, wird wohl nur durch das Gericht im Einzelfall zu klären sein!

[188] Siehe die EuGH-Urteile vom 9.11.2004 mit den Nummern C-46/02, C-203/02, C-338/02, C-444/02 ("Sport-Datenbank"): Die Erstellung eines Spielplanes ist „Erzeugung“ und zählt nicht für die Beurteilung des Schutzes. Eine mühevolle Sammlung internationaler Spielpläne und Abgleich derselben würde jedoch wohl ausreichen, da die Spielpläne schon unabhängig existieren.

[189] Siehe dazu „Bettercom“ LG Berlin, Einstweilige Verfügung vom 22.12.2005, 16 O 743/05 http://www.bettercom.de/ebay-bettercom/ev-urteil-20051222 (Berufung läuft, noch kein Hauptverfahren), wo u.a. die Datenbankqualität der eBay-Bewertungen zu beurteilen ist: Welche Investitionen tätigt E-Bay in die Bewertungs-"Datenbank", wo die Daten ja von den Kunden eingegeben werden? Die Software selbst kann hier nicht zählen, da das Datenbankprogramm explizit nicht zur Datenbank zählt und Investitionen dafür also nicht anrechenbar sind. Der Betrieb der Software (="Server-Miete", im Gegensatz zu Erstellung und Wartung) ist jedoch ein Aufwand zur Datenbeschaffung.

Dieser für das System des Urheberrechts ungewöhnliche Schutz besitzt eine weitere Besonderheit: Es ist möglich, dass er nie abläuft. Eine nach Art oder Umfang wesentlich geänderte Datenbank gilt komplett, also auch hinsichtlich der alten Teile, als neue Datenbank, wenn hierfür wesentliche Investitionen erforderlich waren. Diese können auch durch mehrere kleinere Aktualisierungen zusammen erreicht werden, sodass auch sukzessive Updates ausreichen. Wird die Datenbank kontinuierlich aktualisiert, bleibt daher der Schutz für sie als Ganzes bestehen. Ansonsten erlischt er schon nach 15 Jahren ab der Herstellung bzw. der letzten Aktualisierung. Auch bei diesem Recht ist aber zu beachten, dass der Schutz der Datenbank als solcher unabhängig vom Schutz der enthaltenen Elemente ist.

Der Datenbankschutz umfasst das ausschließliche Recht, die Datenbank als ganzes oder einen nach Art oder Umfang wesentlichen Teil davon zu vervielfältigen, zu verbreiten, zu senden, wiederzugeben oder der Öffentlichkeit zur Verfügung zu stellen. Unwesentliche Vervielfältigungen sind daher jedem erlaubt, aber nur mit der Einschränkung, dass wiederholte und systematische Verwertungshandlungen von unwesentlichen Teilen[190] der Datenbank verboten sind, sofern diese der normalen Verwertung entgegenstehen oder die berechtigten Interessen des Herstellers unzumutbar beeinträchtigen. Auch hier wird die genaue Abgrenzung wohl noch viele Probleme mit sich bringen.

III.7. Verwandte Schutzrechte

Leistungsschutzrechte sind sozusagen der "kleine Bruder" des Urheberrechts. Mit diesen werden Leistungen geschützt, die zu einem Werk hinzukommen, wie die Aufführung eines Musikstückes durch ein Orchester. Ähnlich hierzu werden Erzeugnisse behandelt, welche die notwendige Werkhöhe nicht ganz erreichen. Letzteres betrifft insbesondere die Lichtbilder: Erreichen sie keine Werkhöhe, sind sie also keine Lichtbildwerke, so bleiben sie immer noch durch das verwandte Schutzrecht für eine gewisse Zeit geschützt.

Im Gegensatz zu Werken wird die Schutzfrist von 50 Jahren bei den verwandten Schutzrechten nicht beginnend mit dem Tod des Urhebers berechnet, sondern ab der Erzeugung des geschützten Elements, also dem Vortrag, der Aufführung bzw. der Herstellung des Lichtbildes. Erfolgt innerhalb dieser Zeit eine Veröffentlichung, so besteht der Schutz analog zu anonymen Werken weiter bis 50 Jahre nach dieser, wenn auch mit kürzerer Frist.

Ein weiterer Unterschied besteht darin, dass im Gegensatz zu Werken verwandte Schutzrechte negativ definiert sind: Bei Werken ist eine explizite Genehmigung erforderlich, alles andere verbleibt dem Urheber. Hinsichtlich der verwandten Schutzrechte ist grundsätzlich alles erlaubt, was nicht explizit dem Urheber vorbehalten ist. Insbesondere betrifft dies die verschiedenen Verwertungsarten, welche jeweils einzeln aufzuführen sind.

III.7.1. Briefschutz

Nach § 77 UrhG dürfen "Briefe, Tagebücher und ähnlich vertrauliche Aufzeichnungen" nicht verbreitet werden, wenn dies berechtigte Interessen des Verfassers bzw. seiner nahen

[190] Ein Online-Zeitungsdienst, der Deep-Links zu Meldungen anbietet, sowie zusätzlich ein kurzer Ausschnitt der eigentlichen Meldung verletzt das Recht nicht. Es erfolgt zwar eine wiederholte und systematische Auswertung, diese behindert aber nicht die normale Verwertung: Wollen Benutzer die Meldung lesen, müssen sie direkt zur Quell-Webseite gehen. Dies wurde als "Anregung" zur Nutzung der Datenbank qualifiziert. "Paperboy" BGH 17.7.2003, I ZR 259/00. Stadler, Thomas, Die Zulässigkeit sog. Deep-Links - Eine Anmerkung zur Paperboy-Entscheidung des BGH http://www.jurpc.de/aufsatz/20030283.htm

Angehörigen nach seinem Tode oder des Adressaten bzw. dessen nahen Angehörigen verletzen würde. Solche berechtigten Interessen sind typischerweise der Privatbereich einer Person, also familiäre oder höchstpersönliche Tatsachen, oder auch die politische Orientierung. Zu beachten ist dabei jedoch, dass bei bereits öffentlich bekannten Tatsachen kein berechtigtes Interesse mehr verletzt werden kann.

Im elektronischen Bereich betrifft dies E-Mails sowie sonstige private Aufzeichnungen.

III.7.2. Bildnisschutz

Es handelt sich hier um ein analoges Recht zum Briefschutz, das auch "Recht am eigenen Bild" genannt wird (§ 78 UrhG). Bildnisse einer Person dürfen danach nicht verbreitet (hier nach allgemeinem Sprachgebrauch und nicht nach der Definition im Urheberrecht zu verstehen!) werden, wenn dadurch berechtigte Interessen des Abgebildeten verletzt werden. Beispiele sind das Einstellen von Klassenfotos[191] oder Fotos von Mitarbeitern[192] in das Internet. Eine Ausnahme besteht nur für die Rechtspflege (siehe III.4.1; Klassischer Fall ist das Fahndungsfoto). Praktisch bedeutsam sind heute u.a. Kamera-Handys: Fotografieren, insbesondere, aber nicht ausschließlich, in peinlichen Szenen, und Senden an andere Personen ist verboten[193]!

III.8. Technische Schutzmaßnahmen

Für alle Werkarten *außer Rechte an Computerprogrammen* werden technische Maßnahmen zur Verhinderung oder Einschränkung der Verletzung von Ausschließlichkeitsrechten unter Schutz gestellt (Unterlassung, Beseitigung, Schadenersatz, Gewinnherausgabe, Urteilsveröffentlichung, Rechnungslegung). Solche Maßnahmen sind Technologien (z.B. Verschlüsselungsprogramme, DRM) oder Vorrichtungen (Hardware-Kopierschutz wie Dongles), die bei normalem Betrieb dazu bestimmt und auch tatsächlich in der Lage sind, derartige Rechtsverletzungen zu verhindern oder einzuschränken. Hierunter fallen also nicht nur Hardwaregeräte, sondern auch Informationen wie etwa Lizenzschlüssel-Generatoren. Unwirksame Methoden, sofern existent, dürfen umgangen werden[194], was ein wenig tautologisch anmutet. Weiters muss es sich entweder um eine Zugangskontrolle (z.B. Passwörter), eine Umcodierung (z.B. Verschlüsselung, Verzerrung) oder einen Mechanismus zur Vervielfältigungskontrolle (Digital-Kopie-Bit bei Minidisks, Broadcast-Flag) handeln.

---

[191] Verboten, sofern die einzelnen Schüler darauf erkennbar sind, da kein besonderes Interesse der Schule oder der Öffentlichkeit erkennbar ist.

[192] Grundsätzlich verboten. Handelt es sich jedoch um Mitarbeiter mit Außenkontakt, z.B. Kundenbetreuer für persönliche Gespräche, so kann das Interesse der Firma höher stehen als das Interesse der betroffenen Person, sodass diese nach dem Arbeitsvertrag zu einer Zustimmung verpflichtet sein kann. Immer separat zu beachten ist das Urheberrecht an den Fotos, das z.B. für Veröffentlichungen im Internet beim Fotografen verblieben sein kann!

[193] Das Veröffentlichen; Die Aufnahme des Fotos selbst ist urheberrechtlich erlaubt, aber ev. ein Datenschutzproblem.

[194] Bei sehr alten CD-Kopierschutzverfahren ist diese Wirksamkeit wohl nicht mehr gegeben, wenn jedes moderne CD-Laufwerk den Schutz einfach mitkopiert oder ignoriert. Ansonsten ist das Niveau allerdings sehr niedrig: Normaler Betrieb, d.h. bloßes Einlegen ohne zusätzliche Aktionen. Wenn dann das Kopieren, Abspielen etc. nicht funktioniert, ist der Kopierschutz wirksam und daher geschützt. Dies betrifft also wohl hauptsächlich Kopierschutz-Varianten, die so fehlerhaft erzeugt/konfiguriert/… sind, dass sie ihre Funktion nicht erfüllen, bzw. welche für andere Betriebssysteme erstellt wurden. Dass dann kein Bedarf für eine Umgehung und daher auch kein Bedarf für einen Schutz der Maßnahmen besteht, führt jedoch zu einem rechtlichen Auslegungsproblem! Eine mögliche Variante wäre das Betreffen von „Features“, die tatsächlich das Kopieren verhindern, aber nicht hierfür gedacht sind.

Strafbar ist die

- vorsätzliche oder fahrlässige Umgehung solcher Maßnahmen. Beispiel: Drücken der Shift-Taste, um den Autostart-Mechanismus der CD zu umgehen, welcher den Kopierschutz prüft oder ein Kopierschutzprogramm installiert[195].
- Herstellung, Einfuhr, Verbreitung, Verkauf und Vermietung sowie Besitz von Umgehungsmitteln zu kommerziellen Zwecken. Besitz zu privaten Zwecken, z.B. Forschung, ist daher erlaubt, nicht aber die tatsächliche Verwendung, siehe voriger Punkt. Beispiel: CD-Kopierprogramme mit Features zum Knacken von Kopierschutz-Mechanismen[196] dürfen zum Vervielfältigen ungeschützter CDs besessen und verwendet werden, nicht jedoch für kopiergeschützte.
- Werbung für Verkauf oder Vermietung von Umgehungsmitteln[197]. Beispiel: Werbung für den Verkauf von CD-/DVD-Kopierprogrammen mit dem Hinweis, dass hiermit Kopierschutzmechanismen umgangen werden können[198].
- Erbringung von Umgehungsdienstleistungen (Cracken/Kopieren gegen Bezahlung). Beispiel: Verkauf von auf Anfrage berechneten Freischalt-Schlüsseln.

Derartige Umgehungsmittel sind Vorrichtungen oder Dienstleistungen, die zur Umgehung von Schutzmaßnahmen angepriesen werden, selbst wenn sie tatsächlich dazu nicht in der Lage sein sollten. Weiters fallen darunter Mittel, die außer der Umgehung von Schutzmaßnahmen nur begrenzten wirtschaftlichen Zweck oder Nutzen haben (keine relevanten anderen Verwendungsmöglichkeiten), oder die *hauptsächlich* entworfen, hergestellt oder angepasst wurden, eine Umgehung zu erleichtern oder zu ermöglichen. Im Gegensatz zum speziellen Schutz von Computerprogrammen ist hier eine geringfügige erlaubte Nutzungsmöglichkeit kein Schutz; diese müsste schon eine gewisse praktische Relevanz besitzen.

Diese Bestimmung, welche fast wörtlich der EU-Richtlinie entstammt, war sehr umstritten. Hiermit ist z.B. die Verwendung von DeCSS[199] strafbar[200], was für viele schwer einsichtig ist. CD-/DVD-Kopierprogramme sind nur solange erlaubt, als sie nicht mit der Möglichkeit der Vervielfältigung geschützter Datenträger werben bzw. hierfür tatsächlich eingesetzt werden (können). Das Ergebnis ist, dass fast alle am Markt erhältlichen CD-Brennprogramme dadurch illegal wären und daher eigentlich nicht mehr verkauft werden dürften[201].

---

[195] Siehe Bell, Dan, BMG album copy protection is thwarted with the shift key? http://www.cdfreaks.com/news/8143. Sollte der Autostart-Mechanismus grundsätzlich ausgeschaltet sein, was durchaus auch aus anderen erlaubten und nachvollziehbaren Gründen üblich ist, so kann aber wohl nicht von einer fahrlässigen Umgehung ausgegangen werden.

[196] Siehe http://www.heise.de/newsticker/meldung/49741 allerdings nach amerikanischem Recht (DMCA).

[197] Werbung für Herstellung, Einfuhr, Verbreitung oder Besitz ist daher wohl erlaubt, sofern dies praktisch möglich oder bedeutsam sein sollte!

[198] Siehe das Urteil LG München 1 7.3.2005, 21 O 3220/05 sowie Berufungsurteil OLG München 28.6.2005, 29 U 2887/05; eine Verfassungsbeschwerde läuft. Die Entscheidungen gehen aus mehreren Gründen wohl klar zu weit: Hier lag kaum Werbung vor, es wurde nichts erleichtert, und zusätzlich wird mit dem Urteil eine (verfassungsrechtlich geschützte!) freie journalistische Berichterstattung zumindest behindert. Siehe auch http://www.heise.de/heisevsmi/

[199] Ein Programm zur Entschlüsselung von DVDs, die praktisch ausnahmslos mit einem, wenn auch eher schwachen, Kopierschutz versehen sind. Das Programm wurde ursprünglich dazu geschrieben, DVDs auch unter Linux abspielen zu können, da für dieses Betriebssystem keine Abspielprogramme, die den Schlüssel zur Decodierung enthalten müssen, vorhanden waren.

[200] Die Umgehung des Schutzes, also das normale Abspielen, war die hauptsächliche Absicht der Erstellung. Dies ist unabhängig davon, dass die DVD legal erworben wurde.

[201] Siehe dazu das in http://www.urheberrecht.org/news/1486/ erwähnet Gutachten (inzwischen nicht mehr online verfügbar) wonach entsprechende Software dennoch verkauft werden darf. Siehe aber auch http://www.heise.de/newsticker/

Problematisch ist insbesondere, dass es nicht darauf ankommt, ob damit vorgenommene Vervielfältigungen auch erlaubt wären oder nicht[202]. Es kommt einzig und allein auf die Absicht des Erzeugers an, und ob es sich um einen vom Rechteinhaber geplanten Vorgang/Gerät/Maßnahme handelt (keine Umgehung) oder nicht[203]. Damit kann der Urheber völlig frei bestimmen, auf welchen Geräten seine Werke dargestellt werden können, wodurch sich eine starke Monopolbildungsgefahr ergibt[204]: Nutzung des Urheberrechtes zur Monopolbildung auf dem Markt der Abspielgeräte. Mit diesem Umgehungsschutz können ansonsten ohne weiteres erlaubte Kopien für den Privat- oder Eigengebrauch, selbst wenn technisch problemlos möglich, verhindert werden. Da jedoch kein *Recht* auf die Privatkopie existiert, sondern nur eine *Erlaubnis*, kann diese Möglichkeit durch die Einführung von Kopierschutztechnologien komplett ausgehebelt werden.

In der Richtlinie ist zwar vorgesehen, dass die Einzelstaaten darauf achten müssen, dass z.B. Vervielfältigungen zum Schulgebrauch dadurch nicht unmöglich werden, und sie diese Rechte gegebenenfalls per Gesetz durchzusetzen haben. Dies gilt jedoch für die private Kopie nur optional (freiwillig!), wobei zusätzlich der Schutz im Hinblick auf die Zahl der Vervielfältigungen immer erlaubt bleiben muss. In den Erläuterungen zum österreichischen Gesetzesentwurf wird die Ansicht vertreten, dass mit einer solchen Regelung auf einen Bedarf gewartet werden soll, bevor entsprechende Regelungen erlassen werden. Man hofft in diesem Bereich auf eine Selbstbeschränkung der Urheber bzw. Verleger.

Eine Einschränkung besteht jedoch (§ 91 Abs 1 UrhG): Erfolgt die Vervielfältigung zum eigenen Gebrauch oder unentgeltlich zum eigenen Gebrauch eines anderen, so besteht keine strafrechtliche Verantwortung (sonst: bis zu 6 Monaten/360 Tagessätzen)[205]. Private werden dadurch also entkriminalisiert. Nicht vergessen werden darf jedoch, dass die zivilrechtlichen Vorschriften davon unberührt sind: Unterlassung, Beseitigung, Schadenersatz etc. können in jedem Fall auch bei rein privater Nutzung geltend gemacht werden!

III.9. Schutz von Metadaten

Gewisse Kategorien von Metadaten werden ebenfalls geschützt (Unterlassung, Beseitigung, Schadenersatz, Gewinnherausgabe, Urteilsveröffentlichung, Rechnungslegung), da diese dazu dienen, die Rechte der Urheber zu kennzeichnen oder sie durchzusetzen. Kon-

meldung/56197 http://www.heise.de/newsticker/meldung/55297 und http://www.netzwelt.de/news/69963-slysoft-vs-musikindustrie-softwareschmiede-schlaegt.html Ob dies tatsächlich so hart gesehen würde kommt wohl darauf an, wie Gerichte ihren Hauptzweck beurteilen würden. Wurden die Kopierprogramme "hauptsächlich" zur Umgehung von Kopierschutzmaßnahmen oder für andere Zwecke hergestellt?

[202] Was natürlich bei Verkauf oder Einfuhr noch nicht beurteilt werden kann: Die Mittel würden explizit nur zu legalen Zwecken verkauft werden, sodass der Verkauf nicht im Mindesten behindert würde, was ja eigentlich der Zweck der Regelung ist: Die Verbreitung derartiger Mittel einzuschränken oder zu verhindern.

[203] Sonst wäre jedes Abspielgerät für verschlüsselte Daten, z.B. der offizielle Premiere-Decoder, verboten, da es erlaubt, diese Daten anzuzeigen. Das Beispielgerät wurde schließlich genau dafür entworfen und der Konsument weiß auch, dass das Programm verschlüsselt ist und er es sonst nicht betrachten kann.

[204] Z.B. der Verkauf von Musikstücken, welche sich nur auf Geräten einer bestimmten Marke abspielen lassen: Beispiel iTunes, betreffend das proprietäre Format. Würde die Musik eines großen Labels ausschließlich in dem iTunes Format angeboten, wäre dies wohl rechtlich bedenklich. Allgemeiner Verkauf, auch kopiergeschützter, CDs dieser Titel würde jedoch wohl als „Gegenmaßnahme“ ausreichen.

[205] Dieser Strafrahmen betrifft auch Inhaber und Leiter eines Unternehmens, die nicht verhindern, dass ein Bediensteter einen solchen Eingriff im Betrieb begeht.

kret geschützt sind el. Angaben, in welcher Form auch immer, d.h. auch verschlüsselte[206], die mit einem Vervielfältigungsstück verbunden oder gemeinsam verschickt bzw. zur Verfügung gestellt werden. Das bedeutet, dass auch Zusatzinformationen unter einem gesonderten Link, etwa externe Dublin-Core Metadaten, geschützt sind.

Betroffen sind folgende Inhalte:

- Bezeichnung des Werkes, Urhebers oder jedes sonstigen Rechteinhabers (Verlag, Webseitenbetreiber, Firma, …), sofern sie vom Rechtsinhaber stammen. Erstellen daher Dritte derartige Metadaten, so sind diese zwar ununterscheidbar, aber nicht geschützt!
- Modalitäten und Bedingungen für die Werknutzung: Kopierbeschränkungen, Lesen, aber nicht Ausdrucken etc.

Verboten ist die Änderung, z.B. durch Rücksetzen des Kopierzählers, oder Entfernung, etwa das Digital-Kopie-Bit bei Mini-Disks, derartiger Informationen sowie die Verbreitung, Einfuhr, Sendung, öffentliche Wiedergabe oder öffentliche Zurverfügungstellung von Vervielfältigungsstücken mit entfernten oder geänderten Metadaten. Ansprüche bestehen jedoch nur gegen Personen, welche dies unbefugt und wissentlich durchführen und denen zusätzlich bekannt oder fahrlässigerweise unbekannt ist, dass hierdurch eine Urheberrechtsverletzung veranlasst, ermöglicht, erleichtert oder verschleiert wird. Diese Voraussetzungen reduzieren den Anwendungsbereich beträchtlich, da Wissentlichkeit selten vorliegen wird und auch nicht einfach nachweisbar ist.

Problematisch sind hier alle Medien- oder Format-Änderungen. Sind etwa in einem Webdokument Metadaten enthalten (META-Tags), so verschwinden diese bei einem Ausdruck und darauf folgenden Vervielfältigungen, oder bei einer Konvertierung in Plaintext. Dies betrifft z.B. auch XML-Dokumente, bei denen besonders oft Metadaten vorkommen. Diese sind unverändert zu übernehmen, auch wenn ihr Inhalt unbekannt ist. Eine Unterdrückung ist nicht erlaubt. Es besteht jedoch auch keine Pflicht zur Anzeige oder zu einem besonderen Hinweis darauf. Sie müssen lediglich unverändert erhalten werden.

III.10. Rechtsdurchsetzung

In diesem Abschnitt wird besprochen, was gegen eine erfolgte oder drohende Verletzung des Urheberrechts unternommen werden kann. Da es sich vielfach um ein besonders leicht zu verletzendes Recht handelt, sind die vorgesehenen Instrumente sehr wirksam.

III.10.1. Unterlassung

Hierbei handelt es sich um ein Ausschließungsrecht, mit dem geltend gemacht werden kann, dass eine andere Person kein Recht besitzt, eine bestimmte Handlung, typischerweise irgendeine Verwertungshandlung wie Vervielfältigung oder Verbreitung, vorzunehmen. Eine Berufung auf den "guten Glauben" ist nicht möglich, ebenso ist eine Wiederholungsgefahr nicht Voraussetzung: Eine solche wird schon bei einmaligem Verstoß angenommen, selbst bereits erfolgte Beseitigung hilft nicht. Auch rein vorbeugend kann eine Unter-

[206] Obwohl dann wohl meist keine Wissentlichkeit mehr vorliegt und die Strafbarkeit wegfällt: Sobald ein Feld jedoch als derartiges deklariert wird, ist eine Veränderung verboten!

lassungsklage erhoben und eine einstweilige Verfügung erwirkt werden[207]. Überdies haftet ein Unternehmer für seine Bediensteten und Beauftragten. Der Anspruch ist unabhängig von Verschulden, doch Beihilfe (⇒ Provider!) ist nur durch *bewusste Förderung* möglich. Wichtig ist festzustellen, dass es sich beim Anspruch auf Unterlassung um ein absolutes Recht handelt, welches daher nicht an Vertragsverhältnisse gebunden ist.

III.10.2. Beseitigung

Im Gegensatz zum auf die Zukunft gerichteten Unterlassungsanspruch bezieht sich der Anspruch auf Beseitigung auf die Vergangenheit bzw. Gegenwart. Voraussetzung ist die Verletzung eines Ausschließungsrechtes, z.B. die Unterdrückung oder Fehlerhaftigkeit einer Urheberbezeichnung. Die Folge ist, dass Vervielfältigungsstücke vernichtet oder Herstellungsmittel zerstört werden. Es ist hierbei jedoch eine strenge Subsidiarität zu beachten: Kann der gesetzwidrige Zustand auch durch einen geringeren Eingriff beseitigt werden, so ist nur dieser erlaubt, z.B. durch Korrektur der Urheberbezeichnung. Dieser Anspruch kann nur gegen Eigentümer von Werkstücken gerichtet werden, benötigt jedoch keinerlei Form von Verschulden: Das Eigentum und die objektive Rechtsverletzung alleine genügen[208]. Dieser Anspruch endet mit dem Ablauf der Schutzfrist.

Im Hinblick auf E-Business sind sowohl Suchmaschinen als auch Internet-Archive[209] von Bedeutung: Auch bei diesen ist in zumutbarer Weise eine Beseitigung vorzunehmen.

III.10.3. Urteilsveröffentlichung

Hat ein Anspruchsberechtigter durch eine Verletzung seiner Rechte einen Nachteil erlitten, der durch Aufklärung der Öffentlichkeit zumindest gemildert werden kann, so hat er das Recht, zusätzlich zu einer Unterlassungs-, Beseitigungs- oder Feststellungsklage auch die Veröffentlichung des Urteils zu verlangen. Eine Urteilsveröffentlichung kann auch ein Beklagter verlangen, wenn sich herausstellt, dass er keinen Eingriff begangen hat. Dieses Recht intendiert keine Strafe, doch kann es praktisch genau diese ergeben[210]. Durch das Urheberrechtsgesetz werden Medienunternehmer verpflichtet, solche Veröffentlichungen ohne unnötigen Aufschub vorzunehmen. Diese Pflicht ist Technik-neutral und betrifft auch das Internet, sodass sich dort ebenso eine Urteilsveröffentlichung erwirken und durchsetzen lässt, insbesondere wenn die Verletzung gerade dort begangen wurde. Beispiele hierzu kamen bereits vor[211], z.B. auf www.orf.at.

III.10.4. Angemessenes Entgelt

Wurde ein Werk wirtschaftlich genutzt ohne dass dafür notwendige Rechte erworben wurden kann der Berechtigte, also der Urheber bzw. wer die Verwertungsrechte erworben hat,

---

[207] Betreffende Inhalte sind daher z.B. vom Netz zu nehmen: Aktives Tun trotz bloßer Unterlassung. Eine weitergehende Entfernung der Inhalte, z.B. in Caches, Proxies, Suchmaschinen etc., ist jedoch nicht erforderlich. Derartiges ist nur bei einer Verurteilung zur Beseitigung erforderlich. Siehe OGH 25.2.2004, 3 Ob 261/03h ("Proxy-Berichtigung")

[208] Raubkopien werden daher, selbst wenn gutgläubig erworben, entschädigungslos vernichtet. Schadenersatzansprüche müssen an den Verkäufer des illegalen Vervielfältigungsstückes gerichtet werden.

[209] Siehe z.B. Wayback Machine http://www.archive.org/web/web.php

[210] Beispiel aus Dillenz, Praxiskommentar: Die Veröffentlichung eines Unterlassungsurteils 1998 in Kurier, Kronen Zeitung, Fachzeitschrift und Ö3 kostete insgesamt 440.000,- ATS.

[211] Siehe "BOSS III": OGH 15.10.2002, 4 Ob 174/02w http://www.rechtsprobleme.at/doks/urteile/bossIII.html

ein angemessenes Nutzungsentgelt verlangen. Auch hier ist Verschulden nicht notwendig. Unter angemessenem Entgelt ist normalerweise der übliche Marktpreis zu verstehen.

III.10.5. Schadenersatz/Gewinnherausgabe

Damit es im Fall der Nicht-Einholung einer Genehmigung oder jeder anderen Schädigung durch Verletzung des Urheberrechtsgesetzes tatsächlich zu einer "Bestrafung" des Täters kommt und er nicht einfach auf Nicht-Entdeckung spekuliert, ist er weiters verpflichtet, Schadenersatz zu leisten[212] bzw. den durch die Verletzung erlangten Gewinn herauszugeben, letzteres allerdings nur bei bestimmten Verletzungen. Der entstandene Schaden ist exakt nachzuweisen, andernfalls gebührt pauschal das Doppelte des angemessenen Entgelts. Im Gegensatz zu den vorherigen Durchsetzungsmöglichkeiten ist hier Verschulden notwendig. Zu dieser Sanktion und beim angemessenen Entgelt besteht auch ein Rechnungslegungsanspruch, da sonst eine genaue Bezifferung des Schadens, Gewinns bzw. Entgeltes unmöglich wäre.

III.10.6. Auskunftsanspruch

Die Umsetzung der EU-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums wurde kürzlich abgeschlossen. Demgegenüber stärker eingeschränkte Rechte auf Auskunft über bestimmte Daten existierten jedoch auch schon vorher[213].

Bisher bestanden Auskunftsansprüche, um u.a. gefälschte Produkte zum ursprünglichen Erzeuger bzw. Importeur zurückverfolgen zu können. Durch die Novelle wurde dies konkretisiert und ausgeweitet. Betroffen von der Auskunftspflicht sind Personen, welche Urheberrechte verletzt haben, sowie zusätzlich Personen, die gewerbsmäßig rechtsverletzende Waren besessen, rechtsverletzende Dienstleistungen in Anspruch genommen oder Dienstleistungen erbracht haben, welche für Rechtsverletzungen genutzt wurden. Dienstleistungen im letzten Fall müssen daher nicht *selbst* illegal gewesen sein! Insbesondere nicht erfasst sind Privatpersonen: Es müssen keine Angaben über die Quelle rechtsverletzender Gegenstände gemacht werden bzw. wo illegale Dienstleistungen in Anspruch genommen wurden[214], sofern nicht selbst Verletzungen begangen werden. Eine weitere Ausnahme besteht, wenn gesetzliche Verschwiegenheitspflichten bestehen, z.B. bei Ärzten, oder die Auskunft unverhältnismäßig im Vergleich zur Schwere der Verletzung wäre, etwa bei Bagatellverletzungen wie dem illegalen Download eines einzigen Musikstückes.

Anzugeben sind Name und Anschrift der Quellen sowie die der gewerblichen Abnehmer und Verkaufsstellen. D.h. auch hinsichtlich der Empfänger[215] sind Private privilegiert, deren Name nicht offenbart werden muss, aber kann. Weiters ist Menge und Preis mitzuteilen.

---

[212] Dies betrifft insbesondere auch immaterielle Schäden.

[213] OGH 26.7.2005, 11 Os 57/05z: Ein Provider hat Name und Adresse des Inhabers einer IP-Adresse zu einem bestimmten Zeitpunkt an Gerichte herauszugeben, da es sich um Stamm- und nicht um Verkehrsdaten handelt. Die IP-Adresse ist ja bereits bekannt und nicht erst festzustellen: Zweiteres wäre eine Telekommunikationsüberwachung mit besondern rechtlichen Anforderungen. Das Fernmelde- bzw. Kommunikationsgeheimnis greift hier nicht. Name und Adresse zu einer IP-Adresse unterliegen nicht dem § 149a StPO, der ein Straftat mit einer Strafdrohung *größer* als 6 Monate fordert, worunter Urheberrechtsdelikte mit 6 Monaten Maximum *nicht* fallen würden. Anmerkung von Daum, MR 2005, 352

[214] Beispiele könnten Raubdrucke sein: Der Besitzer und Leser eines solchen Buches muss seine Erwerbsquelle nicht angeben. Bei Raubkopien dürfte die Rechtslage jedoch anders sein: Hier ist der Besitzer selbst ein Verletzer, da er für den Einsatz Vervielfältigungen des Programms (Installation auf Festplatte, Kopie in Hauptspeicher bei Aufruf etc.) vornimmt.

[215] Gewerbliche Aufkäufer von Privaten müssen jedoch die Name und Adresse von diesen (Privat-) Personen angeben!

Hinsichtlich des Internets besteht eine Sonderregelung: Internet-Service-Provider sind zwar zur Auskunft verpflichtet, da diese gewerbsmäßig Dienstleistungen erbringen, die für Rechtsverletzungen, z.B. illegalen Upload in File-Sharing-Netzwerke, verwendet werden. Sie könnten jedoch argumentieren, dass sie nicht wüssten, ob der Anschlussinhaber selbst die Verletzung begangen habe oder eine andere Person, welche den Computer benutzt hat. Damit würde jede Auskunftspflicht wegfallen. Sie werden daher verpflichtet, die Informationen bereitzustellen, die erforderlich sind, um die Identität des Verletzers festzustellen, also hier die Daten des Anschlussinhabers.

Wichtig ist weiters, dass vorher eine erfolgte Rechtsverletzung nachzuweisen bzw. zu bescheinigen ist. Eine bloße Behauptung reicht nicht aus, sondern das (schriftliche!) Auskunftsbegehren hat u.a. hinreichend konkretisierte Angaben über die den Verdacht der Rechtsverletzung begründenden Tatsachen zu enthalten[216]. Die angemessenen Kosten der Auskunft hat (vorläufig) der Verletzte zu tragen und dem Vermittler zu ersetzen.

III.10.7. Einstweilige Verfügungen

Auch dieser Abschnitt beruht auf der Umsetzung der EU-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums. Schon bisher konnten durch Gerichte einstweilige Verfügungen, wenn auch in etwas geringerem Ausmaß, erlassen werden[217].

Sie sollen dazu dienen, schon vor einem Verfahren schnell und wirksam eine Sicherung von Beweisen zu erreichen sowie eine spätere Durchsetzung von Ansprüchen nach erfolgreichem Hauptverfahren zu garantieren. Insbesondere im el. Bereich mit leichter Löschbarkeit von Daten ist eine solche "Vorbeugung" besonders wichtig.

Eine Neuigkeit ist, dass in manchen Fällen die Verfügung ohne Anhörung des Betroffenen zu ergehen hat, während dies bisher im Ermessen des Richters stand. Würde der gefährdeten Partei durch die Anhörung wahrscheinlich ein nicht wieder gut zu machender Schaden entstehen oder bestünde die Gefahr, dass Beweise vernichtet werden, so darf keine Anhörung des Gegners erfolgen, sondern eine Verfügung muss sofort erlassen werden[218].

III.11. Literatur

III.11.1. Allgemein

Burgstaller, Peter: Schutz von Computeranimationen. MR 2003/5, http://www.multimedia-law.at/db11/cr5.html

Ciresa, Meinhard: Softwareentwicklung durch Arbeitnehmer. ZAS 2006/3

Daum, Anmerkungen zu OGH 26.7.2005, 11 Os 57/05z, MR 2005, 352

Dillenz, Walter: Praxiskommentar zum österreichischen Urheberrecht und Verwertungsgesellschaftenrecht.. Wien: Springer 1999

---

[216] Beispielsweise Auszüge eines Logs, dass bestimmte Musikdateien up-/downgeloaded wurden sowie ein Nachweis der Berechtigung an diesen Musikstücken.

[217] Wie und in welchem Ausmaß ist jedoch sowohl in Lehre als auch Rechtsprechung umstritten und sollte daher zumindest bezüglich des Urheberrechts explizit klargestellt werden.

[218] Natürlich nur, insofern alle Voraussetzungen gegeben sind und Notwendigkeit bzw. Gefahren bescheinigt wurden!

Fallenböck, Markus, Nitzl, Stephan: Urheberrechtliche Rahmenbedingungen für el. Pressespiegel. MR 2003, 102

Gruber, Angelika: Urheberrechtlicher Schutz von Datenbanken. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther, Liebwald, Doris (Hg.): Zwischen Rechtstheorie und e-Government. Wien: Verlag Österreich 2003, 479-486

Hollaar, Lee A.: Legal Protection of Digital Information. BNA Books 2002. http://digital-law-online.info/

Kochinke, Clemens, Tröndle, Rüdiger: Links, Frames und Meta-Tags: Urheber- und markenrechtliche Implikationen im Internet. Computer und Recht 3/99 (15. Jahrgang) 190ff (zur amerikanischen Rechtslage)

Koch, Frank: Handbuch Software- und Datenbank-Recht. Berlin: Springer 2003

Mills, Laurin: Abstraction-Filtration-Comparison Analysis Guidelines for Expert Witnesses. http://nixonpeabody.com/copyright_article.asp?ID=86&PubType=A

Rössel, Markus: Der Wettlauf um Suchmaschinen. CR 5/2003, 349

Schramböck, Michael: Urheberrechtsschutz von Internet-Web-Sites und anderen Bildschirmdarstellungen von Computerprogrammen. ecolex 2/2000, 126ff

Schwarz, Winfried: Software- und Datenbankerstellung durch Arbeitnehmer: Welche rechtlichen Aspekte sind zu beachten? http://www.dbj.at/phps/start.php?noie=1&lang=de&content=publikationen_show.php&navi=publikationen&publikation_nr=307

Sonntag, Michael, Chroust, Gerhard: Legal protection of component metadata and APIs. In: Trappl, Robert (Ed.): Cybernetics and Systems 2004. Proc. of the 17th European Meeting on Cybernetics and Systems Research. Wien: Austrian Society for Cybernetic Studies 2004, 445ff

Stadler, Thomas: Die Zulässigkeit sog. Deep-Links - Eine Anmerkung zur Paperboy-Entscheidung des BGH http://www.jurpc.de/aufsatz/20030283.htm

Thiele, Clemens: Rechtsfragen beim Betrieb von Webradios. http://www.eurolawyer.at/pdf/Rechtsfragen_Webradios.pdf

Thiele, Clemens, Laimer, Barbara: Die Privatkopie nach der Urheberrechtsgesetznovelle 2003, ÖBl 2004, 17 http://www.eurolawyer.at/pdf/privatkopie-laimer-thiele.pdf

Wachter, Heinz-Peter, Winter, Arthur: Computerrecht für die Praxis. Schutz von Computerprogrammen Datenschutzrecht Bildschirmarbeitsplätze. 3. Auflage. Wien: Weiss 1996

Walter, Michel: Digitalisierung von Musikwerken für Sendezwecke ("Radio Melody III"). Medien und Recht 2/1999, 94ff

Walter, Michel: Computerprogramme - Raubkopie - Rechnungslegungsanspruch - Einstweilige Verfügung. Medien und Recht 7/1999 (17. Jahrgang) 167ff

Wiebe, Andreas: Das neue "digitale" Urheberrecht - Eine erste Bewertung, MR 2003, 309

Wittman, Heinz: Die EU Urheberrechts-Richtlinie – ein Überblick. MR 3/01, 143

III.11.2. Rechtsvorschriften

UrhG: Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (BGBl 1936/111 idF BGBl I 81/2006)

Urheberrechts-RL der EU: Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. ABl. L 167/10 vom 22.6.2001: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:DE:HTML

Datenbank-RL: Richtlinie 96/9/EG des Europäischen Parlamentes und des Rates vom 11.3.1996 ABl. Nr. L 77/20 vom 27.3.1996 über den rechtlichen Schutz von Datenbanken http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:DE:HTML

Computer-RL: Richtlinie 91/250/EWG des Rates vom 14.5.91 über den Rechtsschutz von Computerprogrammen ABl. Nr. L 122/42 vom 17.5.1991 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:DE:HTML

Urheberrechts-Durchsetzungs-RL:Richtlinie 2004/48/EG des Europäischen Parlamentes und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums. ABl. L 195/16 vom 2.6.2004 (Berichtigung). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R(01):DE:HTML

IV. Rechtsaspekte von Web-Sites

Webseiten sind heute für fast alle Firmen eine Notwendigkeit: Einerseits zur Unternehmenspräsentation, andererseits zur Geschäftsabwicklung, z.B. durch die Entgegennahme von Bestellungen oder für Terminreservierungen. Die "höchste" Form ist, die Dienstleistung durch die Webseite direkt und komplett abzuwickeln, z.B. kostenpflichtige Informationsangebote mit Lieferung durch Online-Anzeige oder Download. In diesem Kapitel werden hierbei relevante rechtliche Aspekte dargestellt: Informationspflichten, der Schutz von Inhalten und die Haftung für diese sowie Rechtsfragen rund um Links und Framing.

IV.1. Anwendbarkeit

Viele der Themen in den folgenden Abschnitten sind im E-Commerce-Gesetz (ECG) geregelt, welches nur für einen eingeschränkten Bereich anwendbar ist. Es betrifft den el. Geschäfts- und Rechtsverkehr, berücksichtigt also nicht eine rein private Nutzung. Zu beachten ist hierbei, dass ein Handeln im Geschäftsverkehr sehr schnell vorliegt: Werbung auf den Webseiten für eigene Produkte, auch ohne dass diese online bestellt oder gar erworben werden können, oder für das Unternehmen als solches reicht bereits aus. Aber auch sonstige Tätigkeiten, beispielsweise eine private Webseite mit Verkauf von Bannerwerbung, können darunter fallen.

Konkret gilt das Gesetz für Diensteanbieter. Ein solcher ist eine natürliche oder juristische Person, welche einen "Dienst der Informationsgesellschaft" anbietet. Hierbei handelt es sich um einen elektronischen[219] Dienst, welcher "normalerweise gegen Entgelt im Fernabsatz auf individuellen Abruf des Empfängers" zur Verfügung gestellt wird. Dies bedeutet im Detail:

- Normalerweise gegen Entgelt: Es handelt sich um ein kommerzielles Angebot. Ausnahmsweise gratis angebotene Dienste, z.B. zu Werbezwecken, fallen ebenfalls darunter. Lediglich Dienste, die praktisch immer gratis sind, also auch bei fast allen anderen Anbietern, fallen heraus. Es kommt hierbei nicht darauf an, dass das Entgelt durch den direkten Endbenutzer bezahlt wird, sondern es kann auch von Dritten stammen[220].
- Im Fernabsatz: Dies hat nichts mit der Fernabsatz-RL zu tun. Dienstleistungen im Fernabsatz werden hier als Dienstleistungen definiert, die ohne gleichzeitige physische Anwesenheit erbracht werden. Gegenbeispiel ist die Suche in einem el. Katalog in einem Geschäft, wobei dem Kunden vom Verkäufer assistiert wird, oder die el. Buchung eines Flugtickets bei persönlichem Erscheinen im Reisebüro.

[219] D.h. nicht Sprachtelephonie oder darüber erbrachte Dienste sowie der Verkauf von Programmen als Datenträger. Sehr wohl jedoch der Verkauf von Programmen als Download über das Internet.

[220] Beispiel: Der Versand von Online-Grußkarten, der normalerweise für die Benutzer kostenlos ist. Wird jedoch für die Werbung, z.B. bestimmte Sujets, von Firmen bezahlt, so reicht dies bereits aus, dass es sich um einen "normalerweise gegen Entgelt" erbrachten Dienst handelt. Siehe OGH 18.8.2004, 4 Ob 151/04s. Erste und zweite Instanz bejahten dies (zweite Instanz: im konkreten Fall aber kein Hinweis auf eine solche Bezahlung durch Firmen), der OGH lehnte die Beschwerde aus einem anderen Grund ab und behandelte dieses Thema nicht.

- Auf individuellen Abruf des Empfängers: Der Kunde kann entscheiden, wann und wo er den Dienst in Anspruch nimmt. Es fallen daher Broadcasts wie etwa Radio heraus[221].

Haftungserleichterungen für Provider und Links gelten zusätzlich auch für die *unentgeltliche* Bereitstellung el. Dienste (§ 19 Abs 2 ECG). Dies hat den Sinn, dass Private nicht schlechter gestellt werden sollen als Unternehmen, welche Dienste kommerziell betreiben.

IV.2. Informationspflichten

Für Webseiten und Newsletter (=Werbe-E-Mails) müssen verschiedenste Informationspflichten erfüllt werden. Die Vorschriften nach dem ECG werden hier im Kurzüberblick dargestellt. Weiterhin zu beachten sind allgemeine Vorschriften über Werbung, z.B. deren Kennzeichnung als solche, sowie die Informationspflichten nach der Fernabsatz-RL[222].

IV.2.1. Informationspflichten nach dem E-Commerce Gesetz

Nach § 5 ECG müssen auf E-Commerce Webseiten, d.h. beim Verkauf von Waren oder Dienstleistungen, ständig, leicht und unmittelbar bestimmte Informationen zur Verfügung gestellt werden. Leicht und unmittelbar bedeutet, dass diese Daten nicht versteckt werden dürfen, heißt aber nicht, dass sie direkt auf der Startseite zu platzieren sind. Ständig bezieht sich auf die Dauer der Pflicht, d.h. eine entsprechende Webseite darf nicht nur "ab und zu" online sein. Nicht gefordert ist daher, die Daten auf jeder einzelnen Webseite direkt oder über einen Link, was aber sehr sinnvoll ist, z.B. in der Fußzeile, anzubieten.

IV.2.1.1. Anzuführende Informationen

Details dazu wurden schon oben im Kapitel über Konsumentenschutz besprochen, daher erfolgt hier nur mehr ein Kurzüberblick:

- Name/Firma
- Ladungsfähige Anschrift
- Angaben für rasche und unmittelbare Kommunikation
- Firmenbuchnummer und Firmenbuchgericht
- Zuständige Aufsichtsbehörde
- Umsatzsteuer-Identifikationsnummer
- Gewerbe- oder berufsrechlichte Vereinigungen sowie entsprechende Vorschriften mit Zugang zu diesen

In Österreich existiert zur Erleichterung der Erfüllung dieser Vorschriften eine Aktion der Wirtschaftskammer[223]. Auf deren Webseite sind die meisten Informationen schon eingetragen, da bei der (Zwangs-)Mitgliedschaft bereits der Großteil anzugeben ist. Restliche In-

---

[221] Webradio dürfte jedoch sehr wohl darunter fallen: Es wird zwar allgemein ausgestrahlt ohne auf den Einzelnen Rücksicht zu nehmen, doch ist für die tatsächliche Zuleitung eine individuelle Anforderung (=Abruf) notwendig. Technisch handelt es sich eben gerade nicht um Broadcasts, sondern eine Vielzahl von Einzelzuleitungen eines unveränderlichen Programms. Siehe Handig: Downloads aus dem Internetradio. ecolex 2005, 921

[222] Siehe Abschnitte VII.2.2.2 und VII.2.2.3 des Kapitels VII, Vertragsabschluss und Konsumentenschutz im Fernabsatz!

[223] Siehe http://firmena-z.wko.at/

formationen müssen selbst eingetragen werden, was Online möglich ist. Durch einen entsprechenden Link (siehe Abbildung 6 für das als Link-Anker vorgeschlagene Bild) kann dann diese Pflicht sehr einfach erfüllt werden.

Abbildung 6: Link-Button zum Firmen A-Z der Wirtschaftskammer

IV.2.1.2. Sondervorschriften für Preise

Spezielle für Preise gilt, dass diese den Produkten leicht les- und zuordenbar sein müssen. Hierbei soll ein "durchschnittlich aufmerksamer Betrachter" als Vergleichssubjekt dienen, wodurch die Aufmerksamkeitsschwelle wohl relativ niedrig liegen dürfte und daher ein enger räumlicher Zusammenhang erforderlich ist. Darüber hinaus ist eindeutig anzugeben, ob[224] es sich um Brutto- oder Nettopreise (Umsatzsteuer, Abgaben, Zuschläge etc.) handelt. Selbst reine Business-to-Business Anbieter müssen explizit auf das Fehlen der USt. hinweisen. Eine bloße Anmerkung in den AGBs reicht nicht aus. Weiters ist explizit anzugeben, ob Versandkosten enthalten sind oder nicht.

IV.2.1.3. Konsequenzen bei Verstößen

Eine unvollständige oder fehlende Information unterliegt gem. § 26 Abs 1 Z 1 ECG einer Verwaltungsstrafe mit einem Strafrahmen von bis zu € 3.000. Jeder kann eine derartige Anzeige erstatten. Sollten diese Pflichten verletzte werden, so ist aber noch § 27 ECG zu beachten, wonach die Behörde zuerst auch mit einer kostenfreien Abmahnung unter Setzung einer Frist zur Behebung reagieren kann[225].

Viel teurer werden kann hingegen eine ebenfalls und parallel dazu mögliche Klage nach dem UWG[226], da es sich hierbei um einen Wettbewerbsvorteil durch Rechtsbruch handeln kann, beispielsweise durch die Unterfälle Verschleierung der eigenen Person, Behinderung der Kontaktaufnahme durch Kunden etc.[227]. Hierzu ist allerdings ein Wettbewerbsverhältnis erforderlich[228] und der Verstoß muss den Wettbewerb beeinträchtigen können[229].

---

[224] Achtung: Bei B2C-Shops muss es sich zusätzlich zwangsweise um Inklusiv-Preise handeln (§ 9 Abs 1 PreisauszeichnungsG). Siehe für Deutschland LG Berlin 26.1.2006, 16 O 543/05: Angabe von Netto-Preisen und dem Hinweis am unteren Webseitenrand in kleiner Schrift "Alle Preise verstehen sich zuzüglich 16 % MwST." reicht nicht aus.

[225] Bei Korrektur innerhalb der Frist darf keine Strafe erfolgen. In den meisten Fällen wird wohl hiermit vorgegangen werden, außer es handelt sich um einen besonders eklatanten Fall. Filzmoser: Gewerbe- und berufsrechtliche Aspekte des E-Commerce-Gesetzes, RdW 2002/337, plädiert mit guten Argumenten für eine Auslegung als „muss“, wonach die Behörde *immer* zuerst eine Abmahnung aussprechen *muss*.

[226] Simon: Ist ein Verstoß gegen die Informationspflichten des § 5 ECG UWG-widrig? RdW 2004/105

[227] Dies ist nicht ganz unumstritten. Im Fall 3-Pagen-Katalog wurde jedoch ein sehr ähnlicher Verstoß (Postfach anstatt Straßenadresse auf Bestellkarten, daher keine "ladungsfähige Anschrift"; § 5c Abs I Z 1 KSchG) vom OGH als wettbewerbsrelevant anerkannt. Anmerkung von Thiele zu "3 Pagen" OGH 23.9.2003, 4 Ob 175/03v http://www.eurolawyer.at/pdf/OGH_4_Ob_175-03v.pdf

[228] Oder es handelt sich um eine besonders klagslegitimierte Organisation zum Schutz von Konsumenteninteressen (Verbandsklage: § 29 KSchG). Siehe dazu "Werico" http://normative.zusammenhaenge.at/faelle/velawe.html (derzeit nicht verfügbar). Dazu zählen u.a. die Wirtschaftskammer, die Arbeiterkammer und der Verein für Konsumenteninformation.

[229] Fehlen der Aufsichtsbehörde ist nicht unbedingt hierfür geeignet: OLG Koblenz 25.04.2006, 4 U 1587/04

IV.2.2. Impressumspflichten

Auf allen Web-Sites müssen verschiedene Informationen zur Verfügung gestellt werden, selbst wenn es sich um eine ausschließlich und rein private handelt. Hierzu gehören insbesondere Informationen nach dem Mediengesetz. Unter den Daten für das „Impressum“ bzw. die „Offenlegung“ versteht man allgemein jene Informationen, die den Anbieter/Inhaber/Redakteur und die Zielrichtung des Mediums, hier der Webseite, beschreiben. Zu unterscheiden ist zwischen der "großen" Offenlegung und dem "kleinen" Impressum, welche teilweise unabhängig, teilweise gemeinsam erforderlich sind.

IV.2.2.1. Offenlegung: Inhalt

Folgende Daten sind allgemein auf allen Webseiten, also selbst auf nicht-kommerziellen, anzuführen. Hierbei handelt es sich um die Offenlegungspflicht aus § 25 Mediengesetz, die umfangreicher als die in § 24 vorgeschriebenen Impressumspflicht ist. Im Einzelnen sind folgende Informationen bereitzustellen:

1. Name oder Firma: Wie beim Betreibernamen nach den anderen Informationspflichten! Anzugeben ist der Medieninhaber, d.h. der Betreiber bzw. Gestalter der Web-Site.
2. Unternehmensgegenstand: Welche Tätigkeit die Firma ausübt, beispielsweise „Warenhandel“ zusammen mit einer groben Angabe der Warenart.
3. Wohnort, Sitz oder Niederlassung: Damit ist nur die Angabe des Ortes gemeint, nicht jedoch eine genaue Anschrift, was insbesondere für private Web-Sites wichtig ist.
4. Art und Höhe der Beteiligung der Medieninhaber: Sofern mehrere Personen die Web-Site gemeinsam betreiben, sind diese mit Anteilen anzugeben[230]. Für Firmen bedeutet dies eine Offenlegung der Beteiligungsverhältnisse von großen „Gesellschaftern“. Für Gesellschaften oder Vereine sind im Detail anzuführen:
   a) Der oder die Geschäftsführer
   b) Die Mitglieder des Vorstandes und, falls vorhanden, Aufsichtsrates
   c) Die Gesellschafter, deren Einlage oder Stammeinlage 25% übersteigt
   d) Sind Gesellschafter wiederum Gesellschaften, so sind auch deren Gesellschafter mit mehr als 25% anzugeben
   e) Besitzt jemand mittelbar mehr als 50%, so ist auch diese Person anzuführen
5. Weitere Beteiligungen: Wenn eine anzugebende Person (Betreiber, Geschäftsführer, Vorstand, Aufsichtsrat, ...) Inhaber eines weiteren Medienunternehmens ist, so ist auch von diesem Unternehmen Firma, Unternehmensgegenstand und Sitz anzugeben.
6. Blattlinie: Eine Erklärung über die grundlegende Richtung des Mediums. Zu erläutern ist, welcher Inhalt präsentiert und welche Zielsetzung verfolgt werden soll.

Eine gewisse Erleichterung besteht für Webseiten, deren Inhalt nicht über die Darstellung des persönlichen Lebensbereichs oder die Präsentation des Medieninhabers (=Webseiten-Autor) hinausgeht. Zu diesen zählen sowohl rein private Webseiten als auch die bloße Präsentation einer Firma inklusive einem eventuellen Waren- oder Dienstleistungsverkauf. Erst wenn auch allgemeine Themen unabhängig von dem Unternehmen erörtert werden, z.B. Wirtschaftspolitik, ist die volle Offenlegung erforderlich.

[230] Dies betrifft etwa OHG, KG, OEG, KEG und GmbH, nicht jedoch die AG, d.h. die Aktieninhaber.

Bei der erleichterten (=reduzierten) Offenlegung sind nur Name/Firma, der Unternehmensgegenstand, sofern zutreffend, sowie der Wohnort/Sitz des Medieninhabers anzugeben (d.h. die Punkte 1-3 obiger Aufzählung), nicht jedoch die Beteiligungsverhältnisse und die Blattlinie (Punkte 4-6). Im Gegensatz zu Web-Sites existiert bei regelmäßigen Newslettern keine Privilegierung für „unbedeutendere" Varianten, z.B. bloße Eigenwerbung: Es sind immer alle Informationen, d.h. inkl. der Beteiligungsverhältnisse, anzugeben.

IV.2.2.2. Offenlegung: Position

Auf einer Web-Site muss die Offenlegung ständig leicht und unmittelbar auffindbar sein. Leicht bedeutet, dass sie unter einem klaren Hinweis zu finden ist, z.B. „Impressum", „Offenlegung gemäß MedienG", ... aber etwa nicht unter „Über uns". Eine bestimmte Bezeichnung ist in Österreich nicht vorgeschrieben. Mit unmittelbar ist gemeint, dass die Daten unabhängig von der derzeitigen Position auf der Web-Site zugreifbar sein müssen. Das kann beispielsweise über einen Link in einer immer enthaltenen Fußzeile („Footer") erfolgen. Für Deutschland wird vertreten[231], dass maximal zwei Links zwischen jeder beliebigen Seite und den Informationen liegen dürfen, was meist folgendermaßen realisiert wird: Auf jeder Seite ist ein Link auf die Homepage, und dort befindet sich dann der Link zur Offenlegung. „Ständig" hat bei Webseiten geringere Bedeutung, da dies nur bei andersgearteten Medien wie Zeitungen wichtig wäre, die eine Offenlegung nur ein mal pro Jahr durchführen müssen. Die Webseite mit den Informationen muss also das ganze Jahr über vorhanden und vollständig sein und nicht nur während eines kleinen Zeitraums.

Bei Newslettern (siehe unten) kann die Offenlegung direkt in jeder Ausgabe erfolgen oder auch durch einen Link auf eine Web-Site erfüllt werden.

IV.2.2.3. Impressum: Inhalt

Bei einem *wiederkehrenden* el. Medium ist zusätzlich zur Offenlegung ein Impressum anzuführen (§ 24 MedienG). Ein solches Medium wird wenigstens vier mal pro Jahr in vergleichbarer Gestaltung verbreitet. Anzugeben sind also z.B. bei regelmäßigen Newslettern:

1. Herausgeber – Name/Firma: Name bzw. Firma des Herausgebers. Herausgeber ist die Person, welche die grundlegende Richtung des periodischen Mediums bestimmt.
2. Herausgeber – Anschrift: Die volle Postanschrift des Herausgebers. Hier ist die Angabe eines Postfaches zulässig, da keine „ladungsfähige Adresse", sondern nur eine „Anschrift" gefordert ist.
3. Medieninhaber – Name/Firma: Name bzw. Firma des Medieninhabers. Dieser besorgt die inhaltliche Gestaltung und führt Herstellung und Verbreitung entweder selbst durch oder veranlasst diese. Im Web fällt dies meist mit dem Herausgeber zusammen.
4. Medieninhaber – Anschrift: Die volle Postanschrift; siehe oben.

IV.2.2.4. Impressum: Position

Das Impressum ist direkt in jeder einzelnen Ausgabe, d.h. in jeder einzelnen Aussendung anzuführen. Ein bloßer Link zu diesen Informationen auf einer Web-Site reicht im Gegensatz zur Offenlegung nicht aus.

---

[231] OLG München 11.9.2003, 29 U 2681/03 Erreichbarkeit über zwei Links: "Kontakt" – "Impressum" reicht aus. Siehe auch http://www.wettbewerbszentrale.de/de/verhaltensregeln/el..asp (Teil 3 - Zugänglichkeit). Dem entgegen jedoch Urteil OLG München 12.2.2004, 29 U 4564/03: Ist der (direkte) Link im Footer erst nach Scrollen über vier Bildschirmseiten erreichbar, so ist dies nicht ausreichend.

IV.2.3. Checklisten zu Informationspflichten

Für verschiedene Konstellationen wird hier kurz zusammengefasst, welche Informationen anzugeben bzw. bereitzustellen sind. Details hierzu sind oben sowie in den anderen Kapiteln dieses Buches angeführt.

- Private Web-Site: Name, Wohnort
- Firmen-Web-Site: Name/Firma, Anschrift, Unternehmensgegenstand, Kommunikationsangaben, Firmenbuchdaten, Aufsichtsbehörde, Kammer/Berufsverband/…, UID
- E-Mail Newsletter:
  - Intern: Name/Firma und Anschrift des Herausgebers, Name/Firma und Anschrift des Medieninhabers
  - Zugehörige Web-Site: Name/Firma und Sitz des Medieninhabers, Unternehmensgegenstand, Geschäftsführer/Vorstand/Aufsichtsrat, Beteiligungsverhältnisse, weitere Beteiligungen, Blattlinie
- Web-Site mit Verkauf (Shop), aber ohne Einfluss auf die öffentliche Meinungsbildung: Name/Firma, Anschrift, Unternehmensgegenstand, wesentliche Eigenschaften von Ware/Dienstleistung, Preis-Informationen, Lieferkosten, Zahlungs- und Lieferdetails, RücktrittsrechtsiInformation, Kommunikationskosten, Bindungsdauer von Angebot/Preis, Mindestlaufzeit, Vertragsabschluss-Technik, Vertragstext-Speicherung, Eingabefehler-Berichtigung, Vertragssprachen, Kommunikationsangaben, Firmenbuchdaten, Aufsichtsbehörde, Kammer/Berufsverband/…, UID, Reklamationsadresse, Kundendienst/Garantiebedingungen, Kündigungsbedingungen, Datenschutzhinweise

IV.3. Urheberrechtsschutz von Web-Sites

Dieser Abschnitt erörtert, auf welche Arten eine Webseite bzw. eine Web-Site nach dem Urheberrecht geschützt sein kann. Aufgrund der Vielfalt enthaltener Elemente, Texte, Bilder, Musik, Videos, Programme etc. können sie in fast allen Werkkategorien untergebracht werden und auch mehrfach in einer Art Schichtenmodell geschützt sein. Webseiten sind hinsichtlich des Urheberrechts besonders vielfältig, da diverse Anwendungsformen bestehen, z. B. der "ewige" Schutz bei Datenbanken (ganze Web-Sites können in diese Kategorie fallen) oder der Schutz des Gesamtaussehens (Layout-Schutz für eine Webseite).

In Hinblick auf etwaige Rechtsstreitigkeiten ist zu empfehlen, sich auf alle möglichen Schutzarten zu berufen (einzelne Elemente, einzelne Webseiten, ganze Web-Site), um so die Möglichkeit einer positiven Feststellung als Werk zu erhöhen: Was von einem konkreten Gericht als "eigentümlich" angesehen wird, ist äußerst schwer vorherzusagen[232].

IV.3.1. Elemente einer Webseite

Unabhängig vom Schutz der Webseite/-Site als Ganzes genießen natürlich die einzelnen Elemente urheberrechtlichen Schutz, sofern sie als Werke einzustufen sind. Falls nicht, kommen noch die verwandten Schutzrechte in Frage.

---

[232] Siehe etwa "Telering" OGH 24.4.2001, 4 Ob 94/01d: Sachbereiche sind als Menü horizontal gegliedert, die einzelnen Unterkapitel links vertikal. Rollover von schwarzem auf roten Text und Markierung links davon mit einem roten Pfeil. Eine derartige Gestaltung ist laut OGH originell, dürfte aber selbst 2001 schon relativ weit verbreitet gewesen sein.

Dies betrifft insbesondere:

- Bilder und graphische Elemente: Schutz als Lichtbild (-werk) oder Gebrauchsgraphik
- Text: Schutz als Werk der Literatur
- (Hintergrund-)Musik: Schutz als Musikwerk
- Animationen: Schutz in Ausnahmefällen als Filmwerke
- JavaScript Code (oder ähnliches): Schutz als Computerprogramm. Diese müssen streng von dem dadurch erzeugten Ergebnis unterschieden werden (siehe unten).
- Sammlung von Daten (z.B. Linkliste): Schutz als (bloße) Datenbank bzw. Sammelwerk

IV.3.2. Webseite/Web-Site als Sammelwerk

Eine Webseite als Ganzes kann auch als Sammelwerk geschützt sein, wenn Auswahl und Anordnung der einzelnen Elemente Individualität ausdrücken. Ein "klassisches" Layout ist daher nicht geschützt, sondern es müssen besondere Gestaltungen hinzukommen, z.B. durch die Platzierung von Bildern oder sonstigen Elementen in Verbindung mit dem Text. Auch die Auswahl[233], d.h. welche Texte/Bilder/Graphiken/etc. gezeigt werden, kann eine Schutzwürdigkeit begründen. Siehe hierzu weiters den Schutz als (bloße) Datenbank, falls die Auswahl/Sammlung zwar Kosten verursacht, aber nicht eigentümlich genug ist.

Ähnliches gilt für ganze Web-Sites, wobei die "Anordnung" sowohl durch eine Menüstruktur als auch durch verbindende Links erfolgen kann. Da jedoch oft eine umfassende Darstellung eines Gebietes erfolgt, ist das Kriterium der "Auswahl" wohl nur selten erfüllt. Details dazu werden bei den Dankbankwerken erläutert.

IV.3.3. Web-Site als Datenbank(-werk)

Eine einzelne Webseite kann in der Regel kein Datenbankwerk sein, da die Elemente nicht unabhängig und einzeln zugänglich sind (Gegenbeispiel: Rezeptliste mit Index nach Geschmacksrichtungen). Eine Menge an Webseiten (=eine Web-Site) hingegen kann sehr wohl ein Datenbankwerk darstellen[234].

Voraussetzung ist, dass unabhängige Elemente (jede Webseite kann für sich alleine stehen und besitzt auch so gewissen Sinn) systematisch/methodisch angeordnet (Verbindungen dazwischen, d.h. die Link-Struktur) sind. Damit eine Datenbankwerk vorliegt, müssen Auswahl oder Anordnung dieser Elemente eine eigentümliche Schöpfung sein. Hinsichtlich zweiter ist daher eine "kreative" Menüstruktur bzw. Verlinkung erforderlich.

---

[233] Siehe LG Berlin 26.1.2006, 16 O 543/05: Aufbau und Untergliederung waren kreativ. Die gewählte "... strikte Einteilung [der Webseite] in gesonderte Kapitel liegt nicht notwendig in der Logik der Sache, sondern stellt den Ausdruck einer individuellen Nutzung eines zwar kleinen, aber gleichwohl vorhandenen Gestaltungsspielraums dar." Als möglicher Entkräftungsbeweis wird angeführt, dass Beispiele von anderen Anbietern beigebracht würden, die eine gleiche Einteilung verwenden (hier nicht erfolgt). Geringfügige Änderungen der Worte führen nicht zu einem eigenen Werk, da die schutzbegründenden Elemente unverändert übernommen wurden.

[234] "Caribbean Villas": OGH 20.7.2001, 4 Ob 155/01z. Auch wenn der Fall nach der Sachverhaltsbeschreibung wohl sehr stark an, wenn nicht überhaupt jenseits, der Grenze liegt (Auswahl: die Villen waren durch die Betreibergemeinschaft vorgegeben; die Anordnung scheint nicht übermäßig "besonders" gewesen zu sein): Eine Qualifikation als allgemeines Sammelwerk (Gesamt-graphische Darstellung, Grundidee über alle Seiten durchgezogen) hätte meiner Einschätzung nach dem Sachverhalt mehr entsprochen.

Wird eine Web-Site als Datenbankwerk geschützt, so ist diese Anordnung bzw. Auswahl geschützt, unabhängig vom konkreten Inhalt[235]. Würden daher in der angeführten Entscheidung die zur Miete angebotenen Villen vollständig (Text, Bilder etc.) durch andere ersetzt, so würde immer noch das Recht am Datenbankwerk verletzt werden.

Vom Datenbankwerk zu unterscheiden ist die "bloße" Datenbank: Obwohl sie fast gleich heißt, ist der Schutzbereich deutlich anders. Hierbei wird die Reproduktion des Inhalts (Verbreitung, Zurverfügungstellung etc.) geschützt, selbst wenn dieser einem separaten Schutz unterliegt. Zusätzliche Voraussetzung zur systematischen Anordnung einzelner Elemente ist jedoch, dass Beschaffung, Überprüfung oder Darstellung eine wesentliche Investition darstellen. Dies wird wohl bei jeder mittleren bis größeren Web-Site vorliegen. Ein Beispiel hierfür wäre etwa eine Menge an Webseiten mit Rezepten, welche nach Anfangsbuchstaben sortiert sind. Werden alle Rezepte einer bestimmten Gegend gesammelt, so liegt kein Datenbankwerk vor, da keine besondere Auswahl erfolgte. Dafür ist sicherlich die Sammlung dieser Rezepte mit Kosten verbunden, woraus sich der Schutz als bloße Datenbank ergibt. Werden sie noch auf Korrektheit, z.B. Angabe in metrischen Maßen, überprüft, so wäre ein zweiter Grund gegeben. Die Kosten der Produktion neuer Rezepte wären jedoch nicht relevant, da es sich um Kosten für die Erzeugung der Daten handeln würde. Siehe dazu Abschnitt III.6.4.

Resultat einer Qualifikation als Datenbank ist, dass deren, auch falls sonst freie, Elemente nicht einfach übernommen werden dürfen[236]. Ausnahmen bestehen nur für unwesentliche Teile der Datenbank; im Beispiel dürften einzelne Rezepte übernommen werden, eine ganze Gruppe jedoch nicht.

IV.3.4. Web-Site als Gebrauchsgraphik

Des gesamte Aussehen (äußeres Erscheinungsbild) einer Web-Site kann als Gebrauchsgraphik geschützt sein[237]. Dies ist z.B. dann von Bedeutung, wenn die einzelnen Elemente nicht schutzfähig sind, etwa Buttons oder Icons. Voraussetzung ist, dass das Erscheinungsbild als Ganzes individuell und originell ist. Es kommt daher hier auf den Gesamteindruck an (ähnliche Formgebung, Farben, Anordnungen, ähnliche Texte etc.), wodurch gewisse Parallelen zum Sammelwerk bestehen: Auch dort kommt es auf Auswahl und Anordnung der einzelnen Elemente an. Hier ist jedoch ein konkretes Grundkonzept als solches geschützt, während ein Sammelwerk eine einzelne Webseite bzw. die Navigationsstruktur schützt.

Aus dem Schutzbereich fallen daher u.a. alle Standard-Layouts heraus, z.B. die mitgelieferten Layouts bei Webseitenerstellungsprogrammen. Umso "ungewöhnlicher" das Ergebnis ist, desto eher wird Schutz beansprucht werden können: Links die Navigation, oben eine Überschrift und unten eine Fußzeile sind so üblich, dass hierfür kein Schutz besteht. Ebenso wenig sind übliche Icons (Brief für E-Mail) oder Buttons (rechteckiger Rand der optisch einen erhabenen Knopf darstellt) ausreichend.

---

[235] Die einzelnen Webseiten können daher vollkommen "gewöhnlich" und aus freien Teilen bestehen. Die einzige Konsequenz ist, dass dann *nur* noch der Schutz als Datenbankwerk übrig bleibt und keine Schichtung des Schutzes besteht.

[236] Unabhängige Datensammlung, d.h. nicht durch Extraktion aus der Datenbank, bleibt bei freien Elementen zulässig.

[237] "Telering" OGH 24.4.2001, 4 Ob 94/01d

IV.3.5. Webseite als Computerprogramm

Bei einer Webseite ist im Hinblick auf den Schutz als Computerprogramm genau zu unterscheiden: Geht es um das Programm, also den Quellcode an sich, oder um das Ergebnis des Programms, d.h. die Ausgabe, welche dem Benutzer präsentiert wird? Nur ersteres ist als Programm geschützt; für Ausgaben kommen die anderen Werkarten in Frage.

Der Quellcode von Webseiten selbst, also HTML, ist einerseits ein Werk der Literatur (sofern nicht vollständig automatisch generiert[238] oder trivial), andererseits ev. ein Computerprogramm[239]. Gegen letzteres spricht, dass es sich hierbei rein um eine Markierungssprache handelt, und keinerlei Verzweigungen, Schleifen etc. vorhanden sind. Auch ist die Intention nicht ein bestimmter Ablauf mit ev. sichtbarem Ergebnis, sondern ein rein visuelles Resultat. Allerdings besteht eine große Ähnlichkeit zu funktionalen Programmiersprachen: Die Tags könnten als "Klammern" angesehen werden und der Tag-Name als Funktion, welche auf den Parameter anzuwenden ist. Da jedoch keinerlei Kontrollstrukturen (Verzweigung, Schleife) vorgesehen sind und damit keine universelle Programmierbarkeit im Sinne einer Turingmaschine besteht, ist meiner Meinung nach der Quellcode einer Webseite kein Computerprogramm[240].

Das besagt nicht, dass nicht zwei verschiedene "Quellcodes", z.B. einmal als Applet und bei einer anderen Webseite statisches HTML, identischen "Output" (=das sichtbare Ergebnis im Browser) produzieren können[241]. Geschützt als Programm sind zwar alle dessen Ausdrucksformen, was jedoch weder die Ein- noch die Ausgabe des Programms beinhaltet. Ein Applet ist daher selbst und zusammen mit seinen Entwurfsmaterialien geschützt, seine Ausgabe aber separat zu beurteilen: Text, Grafik, HTML oder eventuell auch wieder ein Programm.

IV.4. Provider-Haftung

Für Internet-Provider bestand lange Zeit eine große Unsicherheit bezüglich ihrer Haftung: Haften sie als Beitragstäter für *alle* illegalen Handlungen ihrer Kunden im Internet bzw. welche Maßnahmen sind wann zu setzen, um dies auszuschließen? Auch hier hat die E-Commerce-RL bzw. das ECG Klarheit gebracht.

Dabei ist insbesondere nach der Art des Providers zu unterscheiden:

- Access-Provider: Ermöglicht den Zugang zu einem Kommunikationsnetz oder ist eine Zwischenstation der Daten, bietet aber ausschließlich Transportleistungen an.

---

[238] Dann kommen aber die Grunddaten für die Generierung als Programm in Betracht.

[239] Dafür: OGH in "Telering", ohne allerdings darüber zu entscheiden, Schramböck, Urheberrechtsschutz von Internet-Websites und anderen Bildschirmdarstellungen von Computerprogrammen. ecolex 2000, 126. Dagegen: Thiele, Comments on the OGH decision "Telering.at". WBl 2001, 318; Waß, Freie Werke (§ 7 UrhG) im Internet. Diplomarbeit. Salzburg 2000. http://www.rechtsprobleme.at/doks/clemens-wass-freie-werke.pdf

[240] Siehe dazu auch Sonntag: A small product line needing requisitely holistic management. Case study of a call-center application and its legal protection. In: Robert Trappl (Ed.): Cybernetics and Systems 2006. Wien: Austrian Society for Cybernetic Studies 2006, 454-459

[241] Siehe dazu "Baumarkt.de" OLG Düsseldorf 29.6.1999, 20 U 85/98 http://www.netlaw.de/urteile/olgd_02.htm, wo dies ebenso dargestellt wird. Dort wird jedoch der Urheberrechtsschutz verneint, was aber darauf zurückzuführen ist, dass für das *optische Erscheinungsbild* der Schutz als *Computerprogramm* beansprucht, und daher korrekterweise abgelehnt, wurde. Da es sich bei dem Sachverhalt um Übernahme durch Framing und keine Kopie durch den Anbieter handelte, war ein Schutz des Quellcodes als Computerprogramm nicht relevant.

- Caching-Provider: Speichert Daten für gewisse kurze Zeiten, um die Effizienz des Abrufs zu steigern. Diese Kategorie kommt in der Praxis nur als Teilaspekt eines der anderen Providerarten vor.
- Hosting-Provider: Ermöglicht es Kunden, Daten auf ihren Rechnern abzulegen. Es handelt sich daher für ihn um "fremde" Daten. Beispiele sind die Betreiber von E-Mail- oder Webservern.
- Content-Provider: Stellt den eigentlichen Inhalt zur Verfügung. Für ihn bestehen keine Haftungserleichterungen[242], sondern er ist voll für den Inhalt seiner Webseiten, E-Mails bzw. sonstige Informationen verantwortlich (und wird daher im Folgenden nicht mehr behandelt). Hierbei handelt es sich normalerweise nicht um einen "Provider", sondern vielmehr um den Endnutzer. Für sie kommt jedoch auch keine Zusatzhaftung, z.B. wegen besonderer "Gefährlichkeit" des Internets, hinzu.

Eine ähnliche Privilegierung wie für Access-Provider besteht für Betreiber von Suchmaschinen, die ebenfalls nicht für abgefragte Informationen haften müssen[243].

Eine Haftung kann auch noch weitere Personen treffen, insbesondere solche, die mit der Domain, auf welcher sich illegale Inhalte befinden, in einem besonderen Zusammenhang stehen. Dies ist einerseits der Inhaber, der naturgemäß sehr weitgehend haftet. Viel geringer ist jedoch die Haftung des Admin-C[244] bzw. des Zone-C[245] oder des Tech-C[246]. Der bloße Betrieb eines Nameservers fällt weder unter Access- noch Hosting-Provider, sondern unterliegt den normalen Haftungsregeln ohne irgendwelche Privilegien.

IV.4.1. Access-Provider

Bei Access-Providern handelt es sich typischerweise um Internet-Service-Provider (ISP), welche den Zugang zum Internet herstellen bzw. für andere ISP die Daten weiterleiten. Diese Firmen bzw. Personen sind dann nicht verantwortlich, wenn sie die Übertragung nicht veranlasst haben, z.B. selbst abgeschickte Daten (Push-Dienste von ihnen zum Kunden) im Gegensatz zu bloß weitergeleiteten. Keine Haftung besteht weiters, wenn sie den Endempfänger der Informationen nicht auswählen, was beispielsweise durch die explizite Zuleitung nicht angeforderter Daten an bestimmte Personen ihrer Wahl erfolgen könnte.

---

[242] OGH 19.2.2004, 6 Ob 190/03i

[243] Details dazu in Strasser: § 14 ECG - Paradies auf Erden für Napster & Co? ecolex 2002, 241

[244] "Haftung des Admin-C" OLG Stuttgart 1.9.2003, 2 W 27/03. Der Admin-C haftet als Gehilfe unabhängig vom Verschulden für Verletzungen durch den Domainnamen (hier: Kennzeichenrecht), da er "willentlich und adäquat kausal" an der Registrierung eines Domainnamens mitwirkt. Achtung: In Österreich ist hier "bewusste Förderung" erforderlich! Eine Ausnahme besteht dann, wenn es sich beim Admin-C um eine abhängige Hilfsperson handelt, die lediglich eine untergeordnete Stellung in einem fremden Unternehmen bekleidet. Siehe auch; Junkers: Haftung des Admin-C - Anmerkung zu OLG Stuttgart. http://www.jurpc.de/aufsatz/20040098.htm Für Spam aus der Domain haftet der Admin-C ebenfalls: LG Berlin 26.9.2005, 16 O 718/05. Ob dies tatsächlich haltbar ist, darf insbesondere für Österreich bezweifelt werden. Im Ergebnis jedoch korrekt, da der Admin-C auch im Newsletter-Impressum als Vertreter angegeben war.

[245] "Haftung des Zone-C" LG Bielefeld 14.5.2004, 16 O 44/04. Der ISP (Zone-C; anscheinend *nur* Domain Name-Server und *nicht* Hosting-Provider!) ist erst zu einer Dekonnektierung der Domain verpflichtet, um einer Haftung als Gehilfe zu entgehen, wenn "die Verletzung der Rechte Dritter für sie ohne weiteres feststellbar ist". Er haftet also analog wie die DENIC, die deutsche Vergabestelle für Domainnamen. Im konkreten Fall ging es um das Tabaksteuergesetz, welches so komplex ist, dass erst das Vorliegen eines rechtskräftigen (!) gerichtlichen Titels zur Entfernung aus dem DNS verpflichtet. Allgemein ist vorrangig der Domaininhaber haftbar.

[246] Hanseatisches OLG 4.11.1999, 3 U 274/98. Wer als Zone-C eingetragen ist, hilft mit, einen Domainnamen "aktiv" zu erhalten, da diese Ansprechperson bei einer Registrierung vorhanden sein *muss*. Daher haftet sie auch für etwaige Rechtsverletzungen durch den Domainnamen ab deren Kenntnis. Keine Haftung besteht wohl für den Web-Site-Inhalt.

Die bloße Entscheidung, an welchen weiteren Rechner die Daten geroutet werden sollen, ist damit nicht gemeint, da dies nicht auf seiner Entscheidung beruht, sondern er nur die Wünsche Dritter erfüllt. Ein Grund für eine Haftung ist, wenn die übermittelten Daten ausgewählt werden, etwa wenn der Provider dafür sorgt, dass beim Browser-Start von ihm bestimmte Werbe-Webseiten angezeigt werden. Weiters von der Befreiung ausgenommen ist die Veränderung der Daten[247]. Erfolgt eine irgendwie geartete inhaltliche Bearbeitung, z.B. Ersetzen von Teilen (Beispiel: Entfernen von Werbebannern), so entfällt das Privileg.

Selbst die positive Kenntnis von Rechtsverletzungen führt nicht zu einer Haftung, sofern nicht eine der erläuterten Gegenausnahmen vorliegt.

Ein gewisser Cachinganteil (siehe sogleich im Detail) ist auch hier enthalten: Kurzzeitige Speicherungen *ausschließlich* zur *Durchführung* der Übermittlung, z.B. in einem Store-and-Forward-Switch, die anschließend sofort verworfen werden, bleiben unberücksichtigt.

Dieser Haftungsausschluss betrifft sowohl Zivil- wie auch Strafrecht (gerichtliche wie auch Verwaltungsstrafen). Besondere andere Ansprüche, z.B. Unterlassung, sind jedoch ausgenommen! Siehe hierzu Kapitel IV.6.

IV.4.2. Caching

Caching ist die automatische und zeitlich begrenzte Speicherung von Informationen Dritter. Zusätzlich muss eine Zweckbindung eingehalten werden: Sie darf ausschließlich dazu dienen, den Zugriff durch andere Nutzer effizienter zu gestalten. Der typische Fall ist der Betrieb eines Web-Proxies, nicht jedoch eines E-Mail Servers (siehe unten).

Auch hier bestehen Ausnahmen von der Privilegierung:

- Keine Informationsveränderung: Es darf keine Veränderung der Informationen erfolgen, sondern ausschließlich eine zeitverzögerte identische Weiterleitung. Auch hier betrifft die Veränderung wieder den Informationsgehalt und nicht technische Modifikationen (Umcodierung, Komprimierung etc.)
- Bedingungen für den Zugang zu den Informationen beachten: So darf etwa eine Webseite mit Zugangsschutz, d.h. nur über Username und Passwort erreichbar, entweder nicht gespeichert oder ausschließlich mehrmals an dieselbe Person weitergegeben werden[248]. Caching soll nicht dazu dienen, Schutzmaßnahmen auszuhebeln, indem einmal autorisiert weitergegebene Daten anschließend ohne Kontrolle weiterverbreitet werden.
- Aktualisierungsregeln aus Industriestandards sind einzuhalten: Ist angegeben, wie lange eine Seite zwischengespeichert werden darf, z.B. durch die Meta-Tags "expires" oder "cache-control" oder in HTTP Headern, so ist diese Angabe zu beachten. Dadurch soll es u.a. möglich sein, Änderungen an Seiten vorzunehmen und sicherzustellen, dass diese für alle Abrufenden übernommen werden. Wenn aus rechlichten Gründen Informationen verändert werden müssen, z.B. durch Entfernen eines Links oder Verändern des Inhalts, muss die Ersetzung der alten Version für alle Besucher sichergestellt sein.
- Sammlung von Nutzungsdaten nicht behindern: Die Sammlung von Daten über die Nutzung, die nach anerkannten und verwendeten Industriestandards erfolgt, darf nicht

[247] Dies betrifft nur ihren Informationsgehalt: Datenkompression fällt daher nicht unter "Veränderung". Siehe Erwägungsgrund 43 der EC-RL

[248] Durch z.B. NAT ist dies oft nicht feststellbar: Es darf daher in der Praxis keinerlei Caching derartiger Daten erfolgen!

behindert werden[249]. Dies betrifft beispielsweise Zugriffszähler, da nach diesen in manchen Fällen etwaige Werbung abgerechnet wird.

- Unverzügliche Entfernung oder Sperrung des Zugangs zu Informationen, sobald tatsächliche Kenntnis besteht, dass die Daten an der Quelle entfernt wurden, der Zugang zu Ihnen gesperrt ist, oder ein Gericht/Verwaltungsbehörde eine Sperre angeordnet hat: Es muss sichergestellt sein, dass veraltete bzw. unerwünschte Informationen auch tatsächlich und in allen Kopien entfernt werden können.

Dieser Haftungsausschluss betrifft sowohl Zivil- wie auch Strafrecht (gerichtliche wie auch Verwaltungsstrafen). Besondere andere Ansprüche, z.B. Unterlassung, sind jedoch ausgenommen. Siehe hierzu Kapitel IV.6.

IV.4.3. Hosting-Provider

Werden von einem Anbieter fremde Informationen gespeichert, so ist, natürlich neben dem eigentlichen Urheber, der Hosting-Provider ebenso verantwortlich, sofern nicht eine besondere Privilegierung greift. Im Gegensatz zu Access- und Caching Providern ist hier der Grundsatz umgekehrt: Standardmäßig besteht eine Haftung, welche in besonderen Einzelfällen aber nicht gilt, während bei den "niedrigeren" Stufen normalerweise keine Verantwortung vorliegt, außer zusätzliche Umstände treten hinzu. Dies ist insbesondere hinsichtlich der Beweislast wichtig: Bei Access- bzw. Caching-Providern ist z.B. vom Gegner zu beweisen, dass sie Daten verändert haben. Der Hosting-Provider muss jedoch selbst beweisen, dass er tatsächlich unverzüglich tätig wurde.

Zu beachten ist, dass die Eigenschaft als Hosting-Provider unabhängig von irgenwelchen Dienstleistungen oder einem Veröffentlichen von Informationen ist. Selbst eine ausgelagerte rein private "Festplatte" im Sinne von externem Speicherplatz fällt darunter, wenn auch der typische Fall der eines Anbieters von Webseiten-Speicherplatz sowie der zugehörigen Internetanbindung (+Server etc.) ist.

Keine Verantwortlichkeit besteht ausnahmsweise hinsichtlich straf- und zivilrechtlichen Folgen, wenn keine tatsächliche Kenntnis von rechtswidrigen Tätigkeiten oder Informationen vorliegt. Tatsächliche Kenntnis wird entsprechend der Wissentlichkeit auszulegen sein. Die Rechtswidrigkeit muss weiters für Laien offensichtlich sein (z.B. Kinderpornographie oder Wiederbetätigung). Diensteanbieter sind nicht verpflichtet, Rechtsgutachten über die Zulässigkeit einzuholen[250]. Die Offensichtlichkeit geht nicht soweit, dass ein rechtskräftiges Urteil o.Ä. erforderlich wäre[251]. Im Sonderfall von Schadenersatzansprüchen ist die Anforderung für eine Freistellung jedoch höher: Diesfalls schadet auch Kenntnis von Tatsachen oder Umständen, aus welchen eine Rechtswidrigkeit offensichtlich wird. Dies ist analog zu

---

[249] Dies kann technisch äußerst schwierig zu erkennen sein und darf daher nicht überbewertet werden. Wird etwa der bloße Abruf eines "statischen" Bildes ("counter.gif"), selbst wenn schlussendlich dynamisch erzeugt, zum Zählen verwendet, so ist dies für externe Personen nicht erkennbar und das Bild darf gespeichert werden. Handelt es sich erkennbar um ein dynamisch generiertes Bild (URL enthält z.B. Parameter: "counter.cgi?id=3"), so dürfte kein Caching erfolgen.

[250] Siehe "Megasex.at" OGH 6. 7. 2004, 4 Ob 66/04s: Keine oder teilweise ungültige AGBs, fehlendes Impressum, Mehrwertnummern ohne Preisangabe, Verwendung von "gratis" zur Beschreibung von Mehrwertnummern sind alle für juristische Laien nicht offensichtlich. Dazu auch Hasberger/Semrau-Deutsch: Host-Provider als Richter? ecolex 2005, 197

[251] Anders "Zone-C Verantwortlichkeit" (Dekonnektierung einer Domain erst bei Vorlage eines rechtskräftigen Titels): LG Bielefeld 14.5.2004, 16 O 44/04. Dieser Fall wurde nach allgemeinem deutschen Recht entschieden. Es handelte sich jedoch um eine besonders komplexe Gesetzesmaterie (Tabak-Import), und um einen besonders schweren Eingriff (Löschen der Domain: Webseiten sind unerreichbar). Allgemein wird daher ein niedrigeres Niveau ausreichend sein, um Rechtswidrigkeit annehmen zu können bzw. müssen und deswegen zu einer Handlung verpflichtet zu sein.

Fahrlässigkeit, wird meiner Meinung nach jedoch etwas strenger als diese zu beurteilen sein: Positive Kenntnis von gewissen Tatsachen oder Umständen ist erforderlich ("bewusst ist": fahrlässige Unkenntnis reicht nicht aus!) und aus diesen muss die Rechtswidrigkeit offensichtlich (wie oben; bloße Vermutungen oder Möglichkeiten reichen nicht) werden[252]. Für die Praxis ist daher eher zu empfehlen, die Daten der Kunden erst gar nicht zu überprüfen, da ansonsten ev. der zweite Fall (Haftung auf Schadenersatz) eintreten könnte.

Eine Haftung ist weiters dann ausgeschlossen, wenn der Diensteanbieter auf derartige Informationen aufmerksam wurde (oder aufmerksam gemacht wurde) und er daher nunmehr Kenntnis oder Hinweise auf offensichtlich rechtswidrige Informationen besitzt, sofern er unverzüglich[253] zur Beseitigung dieses Zustandes tätig wird. Gefordert ist entweder die Entfernung der Informationen (=Löschung), oder die Sperrung des Zugangs zu ihnen. Aus Sicht des Providers ist jedoch anzuraten, die Daten nur zu sperren. Denn sollten sich die Informationen als nicht rechtswidrig erweisen, so können sie einfach (bzw. überhaupt, da noch vorhanden) durch Freigabe "wiederhergestellt" werden, was ev. Schadenersatz für Vertragsverletzungen[254] vermindert.

Diese Privilegierung entfällt, wenn es sich beim Nutzer (=dem Einsteller der Informationen) um einen Weisungsempfänger des Diensteanbieters handelt oder er von ihm beaufsichtigt wird. Gehilfen werden daher dem Provider voll zugerechnet, wobei es hier auf die Qualifikation des Gehilfen (Untüchtigkeit, Gefährlichkeit etc.) nicht ankommt. Er haftet daher auch für Handlungen bestens geeigneter Mitarbeiter[255]. Gleicherweise besteht auch eine Haftung für Sub-Firmen, wohl aber nur, wenn diese tatsächlich kontrolliert werden. Eine geringfügige Beteiligung alleine reicht nicht aus.

IV.4.4. Sonderproblem E-Mail

In Bezug auf E-Mail stellt sich die Frage, wie ein E-Mail-Relay (SMTP-Relay) zu behandeln ist: Werden durch das Hinzufügen einer Header-Zeile die übermittelten Informationen verändert oder nicht? Zwar bleiben die eigentlichen Nutzdaten gleich, also der sichtbare Text und damit der zu transportierende Gedankeninhalt, aber dies kann nicht mit Datenkomprimierung oder IP-Paketen verglichen werden, bei denen jeder Router die MAC-Adresse[256] des nächsten einträgt. Bei letzteren handelt es sich rein um Transferdaten, welche zum Inhalt auf dem Weg hinzugefügt und am Ende wieder entfernt werden (Encapsulation). Dies trifft nicht auf E-Mails zu, da die angefügten Header auch vom Endempfänger gelesen werden können und einen eigenen wichtigen Inhalt enthalten. Sie besitzen auch eine praktische Bedeutung, da vielfach Spam-Filter derartige Header überprüfen, um etwaige Fäl-

---

[252] Beispiel: Ankündigung auf der Startseite einer Web-Site, die vermuten lässt, dass sich weiter unten in der Seitenhierarchie ehrenbeleidigendes Material befindet. Nicht-Weitersurfen und daher fehlende Kenntnis der tatsächlichen Rechtsverletzungen würde hier nicht schützen.

[253] AG Winsen a.d. Luhe 06.06.2005, 23 C 155/05. Einer Aufforderung zur Entfernung binnen 24 Stunden wurde wegen Abwesenheit nicht nachgekommen. AG: "Im Zeitalter der schnellen E-Mails war der Beklagte verpflichtet, die von dem Kläger gesetzte Frist einzuhalten". Dies geht, insbesondere bei Privaten, wohl eindeutig zu weit. Dagegen auch Gramespacher: "Abwesenheit schützt vor Haftung nicht!" http://www.jurpc.de/aufsatz/20050122.htm

[254] Sofern überhaupt Fahrlässigkeit oder Verschulden vorliegt, z.B. bei der Beurteilung der Rechtswidrigkeit. Ein Beispiel hierfür ist, wenn offensichtlich erlaubte Daten gelöscht/gesperrt werden. Siehe dazu AG Charlottenburg 11.01.2002, 208 C 192/01: Die Nicht-Abrufbarkeit ist ein Mangel der Mietsache.

[255] Eventuell zusätzlich zu diesen, soweit nicht das Dienstnehmer-Haftpflichtprivileg eingreift.

[256] Die weltweite eindeutige (mit gewissen Ausnahmen) Adresse jeder Netzwerkkarte (MAC = Media Access Control).

schungen festzustellen[257]. Hier ist daher meiner Meinung nach von einer Inhaltsveränderung auszugehen, sodass es sich nicht um Caching[258] sondern Access handelt, wobei aber die Privilegierung nicht greift. Freilich wird praktisch nie eine tatsächliche Kenntnis des Diensteanbieters vorliegen, da der Vorgang der Weiterleitung vollkommen automatisch erfolgt. Auch betrifft die Haftung nur die veränderten Informationen[259], d.h. den Header. Für den unverändert weitergeleiteten Teil ist die Haftungsbefreiung weiterhin gültig.

IV.4.5. Überwachungspflicht

Gemäß § 18 Abs 1 ECG besteht für Provider keine generelle Überwachungs- oder Nachforschungspflicht. Werden Informationen gespeichert oder weitergeleitet, so muss der Inhalt nicht im Vorhinein kontrolliert werden. Jedoch ist auch keine regelmäßige Nachkontrolle erforderlich, z.B. in Foren oder Chat-Räumen.

Ausgeschlossen sind allerdings nur generelle Überwachungspflichten. In besonderen Fällen, z.B. im Auftrag eines Gerichts, kann eine Überwachung dennoch vorgeschrieben werden. Auch Spezialpflichten, etwa Minderjährigenschutz, z.B. Lehrlinge, könnte eine gewisse Kontrolle, beispielsweise durch automatische Programme, in manchen Fällen erfordern.

In Deutschland wurde hingegen entschieden[260], dass eine allgemeine Überwachungspflicht vorliegt, allerdings erst, nachdem bereits vorher mehrere beleidigende Postings vorgekommen sind. Also erst ab Kenntnis einer besonderen Gefahr wäre eine aktive Kontrolle erforderlich. Eine Haftung tritt grundsätzlich erst dann ein, wenn tatsächliche Kenntnis über die rechtswidrigen Einträge besteht, ansonsten kommt nur die Unterlassungspflicht in Frage. In einem anderen Fall[261] wurde eine Überwachung aller Beiträge eines Diskussionsforums im Vorhinein gefordert, was jedoch klar nicht dem Gesetz entspricht. Eine differenziertere Meinung[262] erfordert im Einzelfall eine Abwägung zwischen der technischen und der wirtschaftlichen Zumutbarkeit für den Betreiber (Aufwand, zu erwartender Erfolg, Vorteile des Anbieters aus den Diensten, Vorhersehbarkeit) und den betroffenen Rechtsgütern (Sicherheitserwartungen, Schwere der Verletzung).

In Österreich ist eine einstweilige Verfügung auf Unterlassung möglich[263], wenn keine regelmäßige Kontrolle eines Gästebuchs stattfindet. Eine Löschung erst nach einer Aufforderung reicht hiernach nicht.

---

[257] Etwa wenn ein Header eingefügt wird um vorzutäuschen, dass ein vertrauenswürdiger Rechner der Absender ist, oder zur Verschleierung des tatsächlichen Senderechners.

[258] Ein SMTP-Relay dient auch nicht der effizienteren Gestaltung des Abrufs für andere Nutzer, sodass Caching keinesfalls in Frage kommen kann.

[259] Dass eine winzige Änderung zur Haftung für den gesamten Inhalt führen würde, ginge eindeutig zu weit. Sie besteht daher nur für den neu hinzugekommen bzw. den weggefallenen Gedankeninhalt. Nur wenn ausnahmsweise eine (wenn auch winzige) Änderung die Bedeutung des gesamten Inhalts verändert, erstreckt sich die Haftung auf alles. Konkret wird wohl auf die Sicht eines verständigen Empfängers abzustellen sein.

[260] LG Düsseldorf 25.01.2006, 12 O 546/05 http://www.lexexakt.de/glossar/lgduesseldorf-2006-01-25.php

[261] LG Hamburg 2.12.2005, 324 O 721/05. Noch nicht rechtskräftig! http://www.r-archiv.de/article2379.html Anmerkung von Bahr http://www.dr-bahr.com/haftung-fuer-foreneintraege-auswirkungen-des-heise-urteils.html sowie von Hansen http://www.r-archiv.de/article2380.html Das Berufungsgericht schränkte die Kontrollpflichten deutlich ein (noch kein schriftliches Urteil verfügbar): Eine Überwachung hat nur dann stattzufinden, wenn konkret auf bereits stattgefundene Rechtsverstöße hingewiesen wurde.

[262] "Pornokönig" OLG Düsseldorf 7.6.2006, I-15 U 21/06

[263] LG Feldkirch 5.5.2004, 3 R 142/04m http://www.i4j.at/entscheidungen/lg_f_3r142_04m.htm

IV.5. Links

Bei Links ist mehrfach zu unterscheiden: Am wenigsten problematisch ist die Verantwortlichkeit des Surfenden für die Informationen, die unter einem angeklickten Link erreicht werden. Alleine das Klicken auf den Link (=das verfolgen) könnte bereits rechtswidrig sein. Außer bei Daten, bei denen schon der Besitz strafbar ist, besteht hier jedoch im Allgemeinen keine Haftung. Gefährlicher ist das Setzen des Links als solchen, d.h. die Erleichterung der Bewegung zum Ziel des Links durch Besucher. Nicht immer ist es zulässig, einen derartigen Link zu setzen. Der letzte Punkt ist die Verantwortung des Link-Setzers für die Informationen, welche unter dem Link zu finden sind.

Im Gegensatz zum Setzen von Links existieren im umgekehrten Fall, also dass (bloße, d.h. nicht bei Framing, Einbettung etc. in die fremde Seite) Links auf die eigene Seite als Ziel gesetzt werden, kaum rechtliche Möglichkeiten. Dies ist grundsätzlich erlaubt, sofern damit nicht Abrufbeschränkungen umgangen werden oder eine besondere Nahebeziehung suggeriert wird (siehe unten bei Framing).

IV.5.1. Verantwortlichkeit des Surfenden für den Inhalt verlinkter Seiten

Hier stellen sich keine großen Schwierigkeiten: Problematisch ist eventuell, falls es sich um Kinderpornographie, Zugangsdaten und Programme entsprechend § 126c StGB, oder Ähnliches handelt, bei denen schon bloßer Besitz verboten ist. Hinsichtlich Links bedeutet dies, dass Verweise auf derartige verbotene Angebote nicht verfolgt werden dürfen. Gelangt man über "unverfängliche" Links dorthin oder werden sie ohne eigenes Zutun geöffnet, z.B. über Pop-ups, so fehlt der Vorsatz und dieser "Fehltritt" ist nicht strafbar.

Im Hinblick auf das Urheberrecht entstehen normalerweise ebenfalls keine Schwierigkeiten. Mehrere Begründungen für die Zulässigkeit des Abrufs, nicht unbedingt jedoch des Speicherns, Ausdruckens etc., beliebiger Werke stehen zur Verfügung:

- Implizite Zustimmung: Durch das Zugänglichmachen der Inhalte auf einem Server wird implizit die Einwilligung gegeben, dass diese Seiten auch abgerufen werden dürfen. Eine entgegenstehende Erklärung wäre wirkungslos, da die tatsächlich relevante Vervielfältigung ja auf dem Server (=Machtbereich des Urhebers) stattfindet und er daher selbst, wenn auch vom Benutzer veranlasst, zur Vervielfältigungshandlung beiträgt und diese ermöglicht (siehe dazu sowie anderen temporären Kopien jedoch sogleich). Dies gilt jedoch dann nicht, wenn keine Zustimmung des Urhebers zur Veröffentlichung vorliegt (z.B. Raubkopien oder Veröffentlichung durch hierzu nicht berechtigte Dritte). In diesem Fall fehlt aber wiederum beim Endbenutzer oft das Wissen um diese Umstände, sodass eine Verantwortung des Benutzers ausscheidet oder zumindest stark reduziert wird: Er durfte auf die Zustimmung vertrauen[264]. Eine weitere Ausnahme sind Bereiche mit Zugangsschutz, welche z.B. erst nach Anmeldung mit Name und Passwort erreichbar sind, da diese ja gerade nicht der Öffentlichkeit angeboten werden.
- Privater Gebrauch: Der private Abruf von Webseiten ist über die Vervielfältigung zum privaten Gebrauch (§ 42 Abs 4 UrhG) legitimiert, welche auch digital erfolgen darf. Es liegt daher keine Urheberrechtsverletzung vor. Weitere Bedingung ist, dass nur nichtkommerzielle Nutzung erlaubt ist. Diese Begründung reicht daher nicht aus, wenn ein Firmenmitarbeiter eine Webseite kopiert, um diese dann weiteren Mitarbeitern zur Ver-

[264] Nicht z.B. bei den meisten Tauschbörsen.

fügung zu stellen (=für eine juristische Person), oder ein Freiberufler die Webseite im Rahmen seiner Berufstätigkeit besucht (kommerzielle Nutzung).

- Caching: Durch § 41a UrhG sind flüchtige Vervielfältigungen privilegiert, sodass Kopien auf dem Server, Proxies, Webcaches, Video-RAMs etc. allesamt rechtmäßig erfolgen. Der Weg selbst vom Server zum Bildschirm ist daher per Gesetz erlaubt (→ ISP).

Zusammenfassend kann gesagt werden, dass es sich bei der bloßen gutgläubigen Anzeige von Webseiten im Browser fast niemals um eine Urheberrechtsverletzung handeln kann: Selbst wenn es sich um ein unautorisiertes Original auf dem Server handelt, so ist der Abruf damit gleichzusetzen, dass der Text illegal auf eine Mauer geschrieben wird und Passanten diese direkt betrachten. Es kommt dann nur Unterlassung und kein Schadenersatz in Frage. Anders jedoch, wenn schon beim Link darauf hingewiesen wird oder erkennbar ist, dass das dahinter befindliche Angebot illegal ist, z.B. eine Raubkopie. Hier kommt das volle Instrumentarium zur Anwendung.

Dies darf nicht darüber hinwegtäuschen, dass die Vielzahl der obigen Begründungen dennoch ihre Berechtigung besitzt: So ist etwa das Speichern der Webseite auf einer Festplatte oder ihr Ausdruck nicht mehr als flüchtige Vervielfältigung zu bezeichnen und somit verboten. Hierfür kann jedoch auf die anderen Begründungen zurückgegriffen werden. So kann z.B. meiner Meinung nach für einfaches Ausdrucken eine implizite Zustimmung oder eine analoge Vervielfältigung zum eigenen Gebrauch angenommen werden, was etwa für das Abspeichern oder gar Weiterverbreiten von Digitalkopien nicht mehr gegeben ist.

Für Computerprogramme ist der private Gebrauch ausgeschlossen. Auch kann hier nicht mehr von Caching gesprochen werden, da praktisch alle Programme zuerst auf der Festplatte gespeichert und erst anschließend installiert bzw. gestartet werden. Auch eine implizite Zustimmung wird fehlen, sobald von vornherein erkennbar ist, dass es sich um eine Raubkopie handelt (anders bei Applets oder Plugins!). Bereits das Anklicken des Links ist daher in diesem Fall verboten, da sonst eine illegale Vervielfältigung stattfindet.

IV.5.2. Verantwortlichkeit des Erstellers für den Link an sich

Da ein Benutzer beim Verfolgen eines Links meist keine Urheberrechtsverletzung begeht, kann in diesem Fällen auch das Einfügen eines solchen in eine Webseite keine Beihilfe zu einer Urheberrechtsverletzung darstellen. In Frage kommt höchstens, den Link als "Zurverfügungstellung" nach § 18a UrhG zu klassifizieren. Dies scheitert allerdings daran, dass der Linksetzer in Wirklichkeit nichts zur Verfügung stellt: Wird das Ziel verändert oder entfernt, geht der Link ins Leere und das Werk ist unerreichbar. Ebenso ist ein Link nicht sehr hilfreich, wenn sich das Ziel überhaupt nie im Internet befunden hat. "Zurverfügungstellung" betreibt daher ausschließlich derjenige, der ein Werk auf einem Webserver anbietet. Links bieten nur eine "Verbreitung" (nicht urheberrechtlich!) der Kenntnis, wo es möglich ist, dieses individuell abzurufen[265]. Dies kann als äquivalent dazu angesehen werden, dass jemand den Ort eines Straßenkunstwerkes bekannt macht: Jeder kann hingehen und die Zeichnung betrachten. Darin, im Gegensatz ev. zum Bild selbst, wird kein Urheberrechtsverstoß gesehen, daher kann dies auch im Internet nicht der Fall sein.

Ebenso analog zur Straßenzeichnung ist aber, dass es sich beim Setzen eines Links um unlauteren Wettbewerb handeln kann. Hierbei ist jedoch weniger der Link selbst das Problem

[265] Siehe dazu ausführlich "Paperboy": BGH 17.7.2003, I ZR 259/00

als vielmehr der Eindruck, der mit ihm hervorgebracht wird. Siehe dazu auch den nächsten Abschnitt. Für den bloßen Link ist hier § 2 UWG (Irreführung) einschlägig. Wird durch den Link bzw. Linktext der Eindruck erweckt, bei der verlinkten Seite handelt es sich um ein eigenes[266] Angebot oder Werk[267], so kann dies im geschäftlichen Bereich eine verbotene Irreführung darstellen. Beispiele hierfür könnten direkte Links auf einzelne Subframes oder Deep-Links in besonderen Konstellationen mit zusätzlichen Elementen sein, da bei Links auf die Homepage oder das volle Frameset die "Fremdheit" meist offensichtlich sein wird. Als Hinweise auf fremden Inhalt können dienen:

- Die Adresszeile des Browsers: Dies funktioniert nur, wenn das Element in einem eigenen oder dem ganzen Fenster geöffnet wird. Doch auch dann ist dies nur ein geringer Hinweis, da bei normaler Navigation über Links dort nur selten hingeblickt wird. Sollten die Domain Namen auch noch ähnlich sein, liegt kein Hinweis mehr vor, da ein genauer Vergleich nicht erwartet werden kann.
- Statuszeile: Der URL wird, sofern nicht über Skripts verhindert, in der Statuszeile des Browsers angezeigt, wenn sich der Mauszeiger über dem Link befindet. Dies ist jedoch nur eine sehr kurzzeitige und kleine Anzeige. Auch blenden manche Benutzer die Statuszeile aus, sodass dies überhaupt wegfällt. Als alleiniger Hinweis auf die Fremdheit reicht die Statuszeile daher sicherlich nicht aus.
- Icons/Hinweis bei Link: Ein Hinweis, dass es sich um einen externen Link handelt, ist sehr nützlich und kann hier u.U. als Rechtfertigung dienen. Allerdings ist er nur im vorhinein sichtbar, denn ist das Ziel erst einmal erreicht, besteht kein Hinweis mehr auf den (fremden) Ursprung.

Weiters kann angeführt werden, dass der normale Link selbst nichts bewirkt: Der gesamte Datenaustausch findet zwischen dem (Ziel-)Server und dem Benutzer statt, ohne dass der Server der Seite mit dem Link auch nur irgendwie davon erfährt oder daran beteiligt ist. In dieser Hinsicht sind deswegen spezielle Links, mit Ziel auf dem eigenen Server, von wo aus anschließend ein "redirect" auf den fremden Server erfolgt, gefährlicher. Analog sind Links zu beurteilen, welche per JavaScript auf dem Client-Rechner, aber nach Regeln des Seiten-Produzenten und nicht des Betrachtenden, zusammengestellt werden. Dann wird bewusst das Linkziel vom Seitenersteller ausgesucht, sodass von einem größeren Beitrag auszugehen ist und eine Haftung als Gehilfe in Betracht kommt[268]. Dies wird jedoch nur dann schlagend, wenn eine *verbotene* Haupttat existiert, so etwa bei Links auf Raubkopien von Computerprogrammen: Ein Beitrag zu *rechtmäßigem* Tun ist nicht strafbar.

IV.5.3. Verantwortlichkeit des Erstellers für den Inhalt verlinkter Seiten

Die dritte Gruppe betrifft die Verantwortlichkeit des Linksetzers für den Inhalt der Seiten, auf welche verlinkt wird, bzw. ev. sogar für die Seiten, welche von der verlinkten Seite aus über weitere Links indirekt erreichbar sind. Als Grundsatz besteht *keine* Verantwortlichkeit für den Inhalt verlinkter Seiten, da diese eben von jemandem anderen stammen.

---

[266] "Jobmonitor": OGH 19.12.2000, 4 Ob 274/00y http://www.rechtsprobleme.at/doks/urteile/jobmonitor-linksII.html

[267] Direkt als Link hat dies allerdings wohl kaum Bedeutung und ist meist offensichtlich. Die praktischen Fälle betreffen Frames oder Bilder, welche in die eigenen Frames/Webseiten eingebunden werden.

[268] Als Beitragstäter haftet nicht, wer nur adäquat verursacht (wie in Deutschland), sondern erst wer bewusst fördert (OGH 19.9.1994, 4 Ob 97/94): Ein "bloßer" Link ist wohl nur adäquate Verursachung und daher oft nicht ausreichend (anders: so genannte "Warez"-Seiten, welche Verzeichnisse von Links zu Raubkopien sind), während die dargestellten Linkformen eher als bewusste Förderung zu werten sind.

In besonderen Fällen kann jedoch sehr wohl eine Haftung eintreten:

- Bewusste Förderung strafbarer Handlungen (Haftung als Gehilfe): Links zu illegalen Seiten, um diesen neue Besucher zuzuführen, sind verboten. Dies wird jedoch meist schwer zu beweisen sein, da es auf die innere Einstellung des Linksetzers ankommt. Ist dies erkennbar, liegt aber meist auch der nächste, viel klarere, Fall vor.
- "Zu-eigen-Machen" verlinkter Inhalte: Wird der Inhalt der Seite, auf welche der Link zeigt, explizit gutgeheißen oder gar als eigener bezeichnet oder in die eigene Web-Site gleichsam integriert[269], d.h. identifiziert sich der Linksetzer mit diesem Zielinhalt, so haftet er für ihn wie für eigene Inhalte. Wann dies genau der Fall ist, kommt auf die Formulierung bzw. die näheren Umstände an[270]. Dies kann weiters dadurch erfolgen, dass die Zielseiten so erscheinen[271], als ob es sich um eigene handeln würde.

IV.5.3.1. Haftungsausschlüsse

Der Versuch, eine Haftung für den Inhalt der Seiten dadurch abzuwenden, indem ein "Disclaimer" (Haftungsausschluss) auf der Webseite angebracht ist, bleibt zumindest in Österreich erfolglos. Einerseits findet er sich meist nur auf der Startseite und dort eher unauffällig, sodass er bei direktem Aufruf von Unterseiten durch (erlaubte!) Deep-Links gar nicht sichtbar wird, andererseits kann eine einseitige Erklärung rechtliche Vorschriften nicht aushebeln: Wird der Inhalt einer fremden Seite durch den Text zum Eigenen gemacht, so hilft auch explizites Abstreiten nichts. Weiters wäre daran zu denken, dass dies ein widersprüchliches Verhalten ist. Ganz im Gegenteil kann ein Disclaimer sogar eher nachteilig sein, da man sich dann kaum mehr auf guten Glauben berufen kann: Man vermutete ja offensichtlich bereits, dass nicht alle Ziele von Links einwandfrei sind...

IV.5.3.2. Haftungsprivileg für Links nach § 17 ECG

Rechtlich kodifiziert ist die Haftung für fremde Inhalte bei Links im § 17 ECG sowie dem ähnlichen § 14 ECG für Suchmaschinen. Danach besteht keine (straf- und zivilrechtliche) Verantwortlichkeit, wenn keine tatsächliche Kenntnis[272] von der Rechtswidrigkeit der Tätigkeit oder der Informationen auf der Zielseite vorliegt. Nachträgliche Änderungen sind deshalb, zumindest bis zur tatsächlichen Kenntnis, unerheblich. In Bezug auf Schadenersatz ist der Maßstab allerdings höher; es reicht das Wissen um Umstände, aus welchen die Rechtswidrigkeit offensichtlich wird. Da es sich meist um juristische Laien handelt, ist deren Beurteilung nur grob vorzunehmen. Nur bei einer Offensichtlichkeit der Rechtswidrigkeit, d.h. ohne größere Nachprüfungen für jedermann klar erkennbar, kann eine Haftung eintreten. Wird diese Kenntnis über die Rechtswidrigkeit nachträglich erlangt, z.B. durch Mitteilung von Dritten, so besteht die Verpflichtung, den Link unverzüglich zu entfernen.

---

[269] Siehe den Fall "Pornotreff" als Beispiel: OGH 18.11.2003, 4 Ob 219/03i: "Gliedert der auf seiner Website einen Link setzende Anbieter den Inhalt der über den Link erreichbaren fremden Website so räumlich und sachlich in seine eigene Website ein, dass sie zu deren Bestandteil wird, bringt er auf diese Weise zum Ausdruck, dass seine Website ohne die fremde Leistung nicht so vollständig wäre, wie dies aus Sicht des Anbieters erforderlich ist. Er hat deshalb für den Inhalt der fremden Seite zu haften."

[270] Insbesondere ein Standard-Disclaimer, siehe IV.5.3.1, reicht hierzu nicht aus. Aber auch eine wörtliche Distanzierung kann unerheblich bleiben, wenn sich aus den Gesamtumständen anderes ergibt.

[271] Beispielsweise durch eine identische graphische Gestaltung. Eine andere URL in der Adresszeile alleine wird wohl nicht ausreichen. Hier sind z.B. graphische Symbole zur Kennzeichnung externer Links hilfreich.

[272] Dies soll laut Erläuterungen ungefähr der Wissentlichkeit entsprechen. Der exakte Unterschied zu dieser ist jedoch nicht klar, sodass meiner Meinung nach genau diese Haftungsvoraussetzung ist.

Analog zur Haftung des Hosting-Providers besteht auch hier eine Haftung für eigene Mitarbeiter und Subfirmen. Weiters wird gehaftet, wenn die verlinkten Informationen als eigene ausgegeben werden (siehe oben: "zu eigen machen").

IV.5.3.3. Haftung für Folge-Links

Hier wird meiner Einschätzung nach wieder zu differenzieren sein: Links innerhalb der verlinkten Seite und externe Links zu Seiten Dritter. Eine genaue Grenze kann zwar nicht gezogen werden, doch wird die Haftung mit zunehmender "Distanz" abnehmen: Inhalte an anderen Stelle auf der verlinkten Seite werden noch meist zurechenbar sein, auf anderen Seiten derselben Site nur mit Einschränkungen, doch Inhalte auf Seiten Dritter nur unter ganz besonderen Umständen, beispielsweise, wenn die Site nur zur Umgehung zwischengeschaltet wird[273] oder der Link direkt auf einen Link zu Folgesites führt.

IV.5.3.4. Überwachungspflicht

Gemäß § 18 Abs 1 ECG besteht keine generelle Überwachungs- oder Nachforschungspflicht. Wird ein Link gesetzt, sollte einmal der Inhalt der direkten Zielseite kontrolliert werden; anschließend kann er unbeobachtet bleiben. Dass keine Nachforschungen erforderlich sind besagt nicht, dass diese Initialprüfung unnotwendig ist, sondern dass keine weiteren Nachforschungen, z.B. auf anderen Seiten der Web-Site, oder rechtliche Untersuchungen nötig sind. Wieder sind nur generelle Überwachungspflichten ausgeschlossen.

IV.5.3.5. Inhaltliche Ausnahmen der Privilegierung

Ausgenommen von der Privilegierung und daher immer voll verantwortlich ist der Ersteller der Webseiten für Links, die auf seine eigenen Seiten, Seiten von Personen, die ihm unterstehen oder von ihm beaufsichtigt werden (Mitarbeiter, jedoch nicht deren Privat-Seiten; Sub-Unternehmen; etc.), führen, sowie bei Übernahme der verlinkten Informationen als Eigene. Letzteres ist aber einschränkend so auszulegen, dass die Übernahme den rechtswidrigen Teil der Seiten betreffen muss. Wird auf unbedenkliche Teile verlinkt, besteht keine Verantwortlichkeit. Da hier jedoch das Privileg generell entfällt, bleibt die Haftung bestehen, wenn der rechtmäßige und zu eigen gemachte Inhalt gegen rechtswidrigen ausgetauscht wird[274]. Hier bleibt dann nur mehr die Berufung auf Unkenntnis, soweit anwendbar, sowie das Problem des Nachweises des anfänglich rechtmäßigen Inhalts.

IV.6. Ausnahmen der Privilegierung bei Providern und Links

Zwar besteht keine zivil- oder strafrechtliche Verantwortung für Links bzw. Inhalte, doch werden diese Ausnahmen in § 19 ECG explizit für Unterlassung, Beseitigung und Verhinderung[275] ausgeschlossen, sodass in dieser Hinsicht die normalen Regeln gelten. Gerichte oder Verwaltungsbehörden können deshalb jederzeit, also z.B. auch bei Unkenntnis des Linksetzers von Rechtsverletzungen auf den verlinkten Seiten, entsprechende Anordnungen erlassen. Dies betrifft insbesondere Unterlassungsklagen, da diese kein Verschulden voraussetzen. So ist daher zwar keine Schadenersatzpflicht gegeben, aber die Kosten der

---

[273] Beispielsweise wie im Sachverhalt des Falles „Pornotreff“: OGH 18.11.2003, 4 Ob 219/03i

[274] Dies kann ev. dadurch vermieden werden, dass speziell auf den Inhalt eingegangen wird (z.B. "Ich stimme mit der unter ... zu findenden Ansicht ... überein."), anstatt ihn nur generell einzubinden (Beispiel: "Stimme mit ... voll überein").

[275] Nach Wiebe: Auskunftsverpflichtung der Access Provider MR 2005 H 4 Beilage, 1, betrifft dies auch Auskunftsansprüche nach dem Urheberrechtsgesetz (§ 87 Abs 3 UrhG).

Unterlassungsklage verbleiben. Es sollte daher beim Setzen eines Links oder dem Speichern fremder Informationen sehr wohl darauf geachtet werden, worum es sich handelt!

Es existiert jedoch auch die Meinung, dass selbst Unterlassungsklagen nicht so ohne weiteres zulässig sind[276]: Wie oben erwähnt setzt die Haftung als *Mit*störer[277], und damit Subjekt einer Unterlassungsklage, eine bewusste Förderung voraus. Bei Unkenntnis kann diese jedoch nicht vorliegen, sodass auch hier kein Problem entsteht und eine Unterlassungsklage nicht erfolgreich ist. Denn es kann wohl nicht ernstlich angenommen werden, dass die Haftungsprivilegien des ECG intendiert waren, die verschuldens*un*abhängige Haftung zu verschärfen, wenn die *Verschulden*shaftung verringert wurde! Deshalb ist auch für eine Unterlassungsklage die Kenntnis der Rechtsverletzung bzw. bewusstes Fördern[278] und Wiederholungsgefahr erforderlich, d.h. die sonst geltenden allgemeinen Regeln[279]. Meiner Meinung nach ist das ECG so zu verstehen, dass eben bei Unterlassungsansprüchen lediglich der, z.B. für Schadenersatzansprüche existierende, zusätzliche Schutz durch die §§ 13ff ECG verloren geht. In allen Fällen, d.h. sowohl bei Schadenersatz wie auch bei Unterlassung, sind jedoch die normalen Voraussetzungen zu prüfen[280]. So erklären die § 13-17 ECG niemanden für haftbar, sondern beschreiben lediglich, in welchen Ausnahmefällen jemand, trotz ansonsten vorliegender Haftung nach normalen Regeln, ausnahmsweise dennoch nicht haften soll.

In Deutschland gilt nach einer Entscheidung für besondere Foren ("Meinungsmarkt", also eher politisch/gesellschaftlich orientierter Inhalt) nur ein Anspruch auf Distanzierung[281] und nicht einmal auf Unterlassung. Solche Ansprüche sind dort *nur* gegen den Äußernden möglich, außer bei anonymen Beiträgen[282]. Weiters besteht auch keine allgemeine Überwachungspflicht[283]. Auch in Deutschland besteht keine Privilegierung hinsichtlich Unterlassungsansprüchen[284], doch ist für solche ebenfalls eine Haftung als Gehilfe[285] erforderlich.

IV.7. Framing und Einbettung

Bei Verwendung von Frames und ähnlichen Techniken kann es zu vielen technischen, benutzerspezifischen (Usability) und rechtlichen Folgen kommen, wobei der Großteil davon

---

[276] Schmidbauer, Franz: Hilfe, Gehilfe! http://www.internet4jurists.at/news/aktuell56.htm

[277] Für eigene Inhalte besteht ohnehin immer eine Haftung!

[278] Siehe OGH 19.12.2005, 4 Ob 194/05s. Die Verwendung eines fremden Markennamens bei Google AdWords führt nicht zu einer Haftung von Google. Eine Gehilfenhaftung könnte nur bei bewusster Förderung bestehen. Hierzu gehört jedoch Kenntnis und Offenkundigkeit der Rechtsverletzung für Laien. Die Privilegierung für Suchmaschinenbetreiber (§ 14 ECG) ist nicht zum Tragen gekommen, da es sich bei bezahlter Werbung nicht um Suchergebnisse handelt.

[279] Siehe auch Ebensperger, Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132

[280] So auch OGH 11.12.2003, 6 Ob 218/03g, 6 Ob 274/03t "Haftung von Online-Archiven". Siehe auch Anmerkungen von Thiele http://www.eurolawyer.at/pdf/OGH_6_Ob_274-03t.pdf

[281] OLG Düsseldorf 26.04.2006, I-15 U 180/05 http://www.jurpc.de/rechtspr/20060064.htm

[282] Die IP-Adresse reicht zur Identifizierung nicht aus, also müsste wohl eine Art Vorab-Ausweiskontrolle stattfinden. Im Ergebnis haftet daher der Forenbetreiber (wiederum) immer hinsichtlich Unterlassung direkt, da er die Identität des eigentlichen Verletzers nicht genau und sicher genug preisgeben kann!

[283] Sehr wohl u.U. im Einzelfall, nachdem ein Hinweis erfolgte: Rechtsgüter, Aufwand und zu erwartender Erfolg sind für den Umfang gegeneinander abzuwägen.

[284] "Pornokönig": OLG Düsseldorf 7.6.2006, I-15 U 21/06

[285] Achtung: In Deutschland wird die Gehilfenhaftung anders, vor allem deutlich weiter, definiert: wer "in irgendeiner Weise willentlich und adäquat kausal zur Verletzung eines geschützten Guts beiträgt"!

unerwünscht ist. Daher sollte der Einsatz von Frames vermieden werden, wo immer nur irgendwie möglich. Mittels statischer Includes oder dynamischer Seitengenerierung können praktisch alle Anwendungen von Frames ersetzt werden: Es besteht heute keine Notwendigkeit (mehr) für ihre Verwendung.

Aus rechtlicher sicht soll dies hier dennoch erläutert werden, weil die Praxis oft noch anders aussieht und mit Frames auch das rechtlich sehr ähnliche Gebiet der Einbettungen verbunden ist, welches, im Gegensatz zu Frames, auch in Zukunft Bedeutung besitzen wird. Unter Einbettungen versteht man alle eingebetteten Objekte wir Inline-Frames, Bilder, Videos oder Applets, da diese separat geladen werden. Sie stammen nicht notwendigerweise vom selben Server wie die Hauptseite.

In diesem Abschnitt wird immer davon ausgegangen, dass Framing bzw. die Einbettung durch einen direkten Link an die "ursprüngliche" Quelle erfolgt. Wird eine Kopie des Ziels auf dem eigenen Server gespeichert und auf diese verlinkt, so liegt fast immer eine verbotene Vervielfältigung und damit eine Urheberrechtsverletzung vor.

IV.7.1. Frames

Einzelne Frames fremder Seiten können entweder als ganze Webseite in einem neuen Fenster dargestellt werden (Variante A: Link), oder als Subframe in ein eigenes Frameset eingebaut werden (Variante B: Einbettung; Siehe Abbildung 7 für beide Möglichkeiten). Letzteres kann technisch durch entsprechende Skripts verhindert werden[286]. Die technische Möglichkeit einer Verhinderung sagt jedoch nichts über die Zulässigkeit aus. Rechtlich gesehen ist Variante A großteils unbedenklich, während Variante B sehr "gefährlich" ist.

Für das Anzeigen fremder Inhalte in einem neuen bzw. dem gesamten Fenster (Variante A) sind dieselben Vorschriften wie für Links im Allgemeinen anzuwenden (siehe oben).

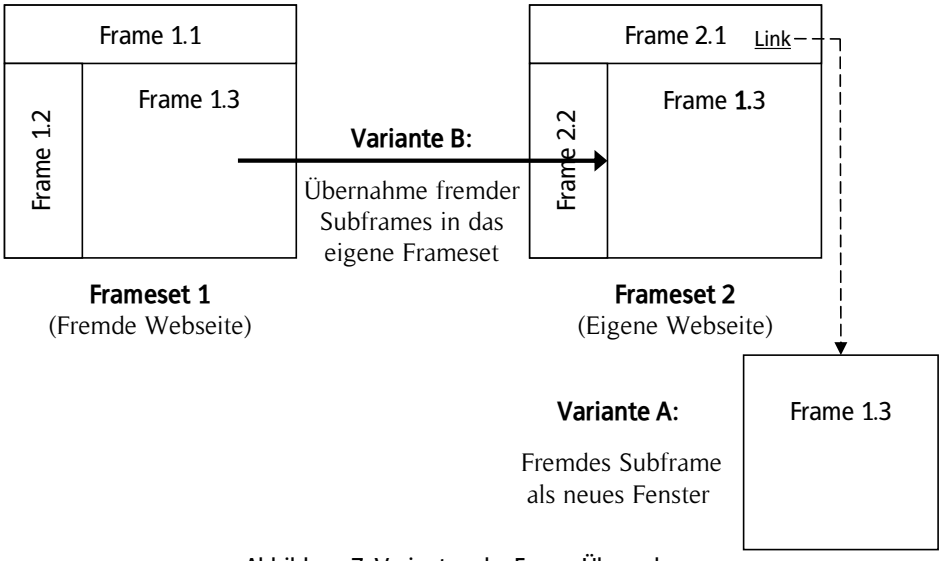


Abbildung 7: Varianten der Frame-Übernahme

[286] So genannte "Framebuster"-Skripts. Werden Webseiten eingebettet, ist dies relativ einfach. Bei anderen Elementen z.B. Bildern, ist dies jedoch äußerst schwierig.

IV.7.2. Einbettungen

Hierbei handelt es sich einerseits um so genannte "Inline Frames"[287] sowie um sonstige eingebettete Elemente (z.B. Bilder, Videos, Applets).

Im Gegensatz zu Links auf Frames als ganzes Fenster (Variante A) ist die Quelle bei der Einbindung derartiger Elemente für den Benutzer vollkommen unsichtbar: Lediglich durch genaue Inspektion des HTML-Codes oder spezielle Browser-Einstellungen, z.B. Bilder nur von dem Server der Hauptseite laden, wird dies erkennbar. Einbettungen entsprechen daher exakt der Variante B bei Frames: In beiden Fällen ist für den Betrachter nicht ohne weiteres erkennbar, dass die Inhalte aus verschiedenen Quellen stammen. Die Gefahr einer Irreführung ist daher hier besonders groß.

Weiters ist bei Einbettungen eine Berufung auf eine Zustimmung des Rechtsinhabers durch das Stellen ins Internet nicht möglich. Praktisch niemand wird derartige Dateien zur Verfügung stellen, ohne dass sie auf einer Webseite präsentiert werden, zu der sie dazugehören. Dass sie ansonsten für beliebige andere Zwecke und in einem anderen Kontext verwendet werden dürfen, entspricht sicher nicht der Intention des Einstellenden und kann auch von Dritten so nicht vermutet werden.

IV.7.3. Rechtsfragen bei Frames und Einbettungen

Einbettungen und direkte Links auf besondere Elemente, d.h. abgesehen von Deep-Links auf Webseiten (siehe oben IV.5.2), sind hauptsächlich im Hinblick auf Urheber- und Wettbewerbsrecht problematisch. Diese beiden Gebiete werden daher hier näher untersucht.

Weiters ist zu bedenken, dass sich durch eine Einbettung die Verantwortlichkeit für den verlinkten Inhalt erhöht: Da für Dritte die wahre Quelle verborgen bleibt, ist grundsätzlich davon auszugehen, dass der eingebettete Inhalt zum eigenen gemacht wird. Nur durch ganz besondere Hinweise könnte dies vermieden werden. Die bloße Erkennbarkeit als externer Inhalt, was an sich schon fast immer eine explizite Markierung voraussetzen wird, würde hier wohl nicht mehr genügen. Möglichkeiten zur Kennzeichnung sind:

- Texthinweis: Die beste und zuverlässigste Art ist, direkt beim eingebetteten Objekt einen klaren Texthinweis anzubringen, dass es sich um fremde Inhalte handelt sowie deren Quelle. Dadurch ist u.U. eine zusätzliche Berufung auf das Zitatrecht möglich.
- Hinweise auf dem eingebetteten Objekt: Diese können z.B. bei Bildern aus Symbolen oder URLs bestehen bzw. bei Dokumenten aus Copyright-Vermerken. Hierbei sollte jedoch berücksichtigt werden, dass Eindeutigkeit erforderlich ist. So ist etwa einem "Stempel" eines Symbols, z.B. dem Logo des originären Anbieters, auf einem Bild meist kein Erklärungswert zuzuweisen, sofern dieses nicht besondere Bekanntheit besitzt: Weder dass es sich hierbei um einen Urheberhinweis handelt noch von wem er stammt ist ansonsten klar erkennbar. Ähnliches gilt für textuelle Hinzufügungen, z.B. Urheberhinweise[288]. So ist etwa ein kleiner Hinweis am Ende einer langen Seite, wel-

[287] Realisiert durch den <iframe> oder <object> Tag.

[288] Siehe "Meteodata" OGH 17.12.2002, 4 Ob 248/02b, http://www.eurolawyer.at/pdf/OGH_4_Ob_248-02b.pdf wo ein Copyrighthinweis mit Link zur Quelle am Ende des eingebetteten Dokuments als ausreichend angesehen wurde. Dieser war nach Sachverhaltsfeststellung klar und deutlich sichtbar (also wohl ohne Scrolling und in entsprechend großer Schrift; meiner Einschätzung nach jedoch an unterster Grenze!). Dabei ging es allerdings nicht um eine Haftung für verbotene Inhalte, sondern um die wettbewerbsrechtlich und ev. unzulässige Übernahme fremder Inhalte. Doch in beiden Fällen ist Hauptfrage, ob Inhalte als "eigene" oder als "fremde" dargestellt bzw. von Besuchern wahrgenommen werden.

cher nur durch Scrollen sichtbar wird, meiner Meinung nach nicht mehr ausreichend. Zu berücksichtigen ist hier auch, dass diese Hinweise an der Quelle entfernt werden könnten, wodurch plötzlich die eigene Rechtsposition unbemerkt verändert würde!

Hinsichtlich Werbe-Bannern, die üblicherweise genau eine solche Einbettung darstellen, wird der Hinweis, dass es sich um Werbung handelt, wohl nicht ausreichen. Selbst wenn erkennbar für eine dritte Firma geworben wird oder dies sogar explizit angeführt ist, wurde die konkrete Werbung vom Ersteller der Webseiten an genau diese Stelle platziert, um seine eigene Seite zu vervollständigen[289].

IV.7.3.1. Urheberrecht

Bei einer Einbettung könnte es sich um eine Vervielfältigung handeln, welche einer Zustimmung bedürfte. Dies wurde auch tatsächlich vom OGH so gesehen[290], ist jedoch falsch. Dabei könnte es sich höchstens um eine Beihilfe zu unerlaubter Vervielfältigung handeln, da der tatsächliche Kopiervorgang erst durch den Abruf eines Benutzers erfolgt. Der Webserver, auf dem sich die Einbettung (und damit der Link) befindet, ist hierbei überhaupt nicht involviert. Jegliche Kommunikation diese Vervielfältigung betreffend erfolgt direkt zwischen Endbenutzer und Server des eingebetteten Objektes. Eine Haftung könnte also nur bei bewusster Förderung eines fremden Rechtsverstoßes eintreten. Das setzt jedoch voraus, dass der Besucher der Webseite selbst keine Vervielfältigung vornehmen dürfte. Hier ist auf die Ausführungen zu Links (IV.5.1) zu verweisen, wonach dies fast immer erlaubt sein wird, sodass auch eine Gehilfenhaftung dann nicht in Frage kommt.

Das Recht der Zurverfügungstellung ist hier nicht anwendbar/verletzt, da eine Einbettung nur solange funktioniert, als das eingebettete Objekt an der Quelle noch existiert.

Weiters ist daran zu denken, dass durch eine Einbettung der Eindruck entstehen kann, dass der Urheber der einbettenden Seite auch der Urheber des eingebetteten Objektes ist. Hierin könnte man eine Bestreitung der Urhebereigenschaft vermuten[291]. Die bloße falsche Behauptung der Urhebereigenschaft ist jedoch nicht strafbar. Bei direkten Links wird dies jedoch wohl kaum mehr vertretbar sein.

Urheberrechtlich relevanter ist, dass es sich um eine unzulässige Bearbeitung bzw. Störung der Werkintegrität der Quelle handeln kann. So werden einzelne Elemente (Subframe, Bild etc.) aus dem Gesamtwerk, d.h. der Webseite bzw. –Site, herausgelöst und unabhängig präsentiert (Varianten A und B). Voraussetzung ist natürlich, dass die Quelle ein Werk ist. Die Voraussetzung der öffentlichen Zugänglichkeit ist bei Webseiten ohne Zugangsschutz jedenfalls gegeben.

IV.7.3.2. Wettbewerbsrecht

Praktisch von großer Bedeutung ist das UWG, auch wenn es nur im Bereich von konkurrenzierenden Unternehmen Anwendung findet, was aber wohl in den meisten relevanten

---

[289] Schließlich erhält er eine Gegenleistung dafür: Geld oder Einblendungen eigener Banner auf anderen Seiten.

[290] Fall "vol.at"; Einbindung von Wetterkamerabildern (vermutlich über <img>) wurde als Vervielfältigung angesehen. OGH 1.2.2000, 4 Ob 15/00k

[291] Dies wird wohl eher nicht zutreffen, da zwar vielleicht eine Urheberschaft angemaßt wird, aber nichts darauf hinweist, dass eine bestimmte andere Person nicht der (Mit-)Urheber sei. Für eine Bestreitung müsste daher wohl entweder eine explizite Abstreitung oder eine zusätzliche Reklamation als eigenes Werk, beispielsweise über einen Autorenvermerk, erfolgen. Eine kommentarlose Übernahme alleine reicht dafür nicht aus.

Fällen vorliegen dürfte, da dies sehr weit verstanden wird[292]. In Betracht kommen hier insbesondere, neben weniger wichtigen oder selteneren Elementen, Irreführung und Ausbeutung fremder Leistung.

Irreführung liegt dann vor, wenn fremde Elemente als eigene ausgegeben werden und so (potentielle) Kunden einem Missverständnis unterliegen. Auch reicht es aus, wenn zwar die Elemente als "fremd" erkennbar sind, jedoch über das Vorliegen einer Berechtigung zur Nutzung getäuscht wird. Beispiel hierfür sind das Anzeigen von Informationen Dritter in einem eigenen Subframe. Um dies sicher auszuschließen ist wieder ein expliziter Hinweis auf die Fremdheit des Angebots erforderlich, welcher wie oben bei der Haftung erwähnt gestaltet sein kann.

Eine schmarotzerische Ausbeutung fremder Leistung[293] (=Leistungsübernahme) liegt dann vor, wenn durch die Einbindung fremder Frames in die eigene Web-Site Leistungen des anderen, welche schutzwürdig sein müssen (was jedoch fast immer zutreffen wird), für sich verwendet werden. Es handelt sich also um eine Ersparnis eigener Aufwendungen. Ein Beispiel ist die Übernahme von zusammengestellten Informationen, etwa technischen Spezifikationen oder Linksammlungen zu einzelnen Produkten, selbst wenn weder die einzelnen Elemente noch die Zusammenstellung Werkscharakter besitzt und damit urheberrechtlich nicht geschützt ist. Hier kommt es ähnlich wie beim Datenbankschutz darauf an, dass eine Investition in die Erstellung erforderlich gewesen ist. Zusätzlich zur Übernahme ist noch ein besonderes, die Unlauterkeit begründendes, Merkmal erforderlich, etwa dass Investitionen des anderen frustriert werden oder dass er mit seinen eigenen Ergebnissen konkurrenziert wird. Da beim Framing keinerlei eigene Leistung vorliegt (es wird bloß ein Link eingetragen), werden an die Unlauterkeit keine großen Ansprüche mehr gestellt. Durch die Einbindung wird der Eindruck einer eigenen Leistung hervorgerufen, was bereits ausreicht. Diesfalls ist daher eine klare und deutliche Kennzeichnung, dass es sich um fremde Inhalte handelt und dass keine besonderen Beziehungen bestehen, erforderlich. Weiters darf natürlich auch keiner der anderen Fälle vorliegen, z.B. Konkurrenzierung[294]. Insbesondere bei Inline-Elementen ist dies eindeutig, da dann nicht einmal eine andere graphische Gestaltung[295] als Hinweis auf Fremdheit dienen kann. Zusammenfassend kann gesagt werden, dass es bei der Leistungsübernahme nicht auf die konkrete technische Gestaltung (das Kopieren auf den eigenen Server und das anschließende Veröffentlichen, direktes Framen etc.) ankommt, sondern auf den Eindruck, der damit beim Betrachter hervorgerufen wird.

Ein anderer Fall für Ausbeutung fremder Leistung könnte in Form von Einsparung eigener Bandbreite bzw. reduzierter Serverbelastung vorkommen, z.B. wenn Standard-Bilder, die urheberrechtlich nicht geschützt sind bzw. für die keine Nutzungsberechtigung beim Ver-

---

[292] Siehe auch die Möglichkeit eines Wettbewerbsverhältnisses "ad hoc": Das Wettbewerbsverhältnis wird erst durch die beanstandete Handlung selbst begründet: Das, z.B. unentgeltliche, Anbieten der fremden Leistung schafft eine Konkurrenz zum originären Anbieter, bei dem diese ev. kostenpflichtig ist.

[293] Siehe OGH 9.11.2004, 4 Ob 185/04s: Sittenwidrige "schmarotzerische Ausbeutung" ist, "... wenn das Arbeitsergebnis eines anderen ohne jede ins Gewicht fallende eigene Leistung ganz oder in erheblichen Teilen glatt übernommen wird und der Übernehmer [....] im Hinblick auf seine Kostenersparnis preisgünstiger anbieten kann, sodass er letztlich dem Mitbewerber mit dessen eigener Leistung Konkurrenz macht (...)." Hier durch Übernahme (wahrscheinlich auch urheberrechtlich geschützter) Webetexte.

[294] Die Übernahme zur Förderung des eigenen Unternehmens wird regelmäßig ausreichen. Wenn (potentielle) Kunden einen Nutzen davon haben, bedeutet dies einen Wettbewerbsvorteil, der aufgrund der fremden Leistung erlangt wird.

[295] Andere Gestaltung alleine reicht auch bei Frames nicht aus: Dies kann auf verschiedenste Gründe zurückzuführen sein und insbesondere beseitigt sie nicht den Eindruck vom Bestehen einer besonderen Beziehung zur echten Quelle.

linkenden besteht, von einem fremden Server geladen werden. Ein Beispiel hierfür sind direkte Links auf Produktfotos, welche der Hersteller Händlern eigentlich nur zum Download zur Verfügung stellt. Hier wird der eigene Server auf Kosten eines anderen entlastet, sodass solches Vorgehen als unlauterer Wettbewerb anzusehen ist, selbst wenn urheberrechtlich nichts zu beanstanden ist.

"Behinderung" fremder Werbung durch das Setzen von Deep-Links an ihr vorbei ist nicht per se wettbewerbswidrig; siehe den Meteodata-Fall: Wer sich des Internets bedient, muss auch dessen Nachteile in Kauf nehmen.

Eine Ausbeutung fremden guten Rufs könnte eventuell dann vorliegen, wenn durch Framing der Eindruck hervorgerufen wird, dass es sich um zwei verbundene Firmen handelt, z.B. wenn es gelingt, den eigenen Frame in eine fremde Webseite einzubauen[296]. Ansonsten dürfte sich dies eher im Bereich des Textinhaltes oder der Verwendung von Firmenlogos abspielen. Derartiges Vorgehen kann auch unter die Spezialregelung gegen den Missbrauch von Unternehmenskennzeichen fallen (§ 9 UWG).

IV.7.4. Zitat als Rechtfertigung

Bei Frames und Einbettungen könnte man versucht sein, die Einbindung als Zitat zu rechtfertigen. Dies geht jedoch vielfach ins Leere: Ein Zitat setzt voraus, dass es sich um kleine Teile handelt. Dies dürfte bei einem ganzen Subframe wohl schon zweifelhaft sein, da dieser vielfach ein Werk ist[297]. Weiters ist das Zitatrecht hauptsächlich für Texte vorgesehen. Obwohl auch Bild-Zitate möglich sind, ist doch die unveränderte Übernahme eines ganzen Bildes damit wohl nur in wenigen Fällen gedeckt. Problematisch ist weiters, dass ein Zitat eine Quellenangabe voraussetzt, um als solches überhaupt erkennbar zu sein. Dies ist durch den bloßen Link sicherlich nicht erfüllt, da dieser für den Benutzer "unsichtbar" ist, sondern es bedarf eines expliziten und ohne besondere Manipulationen direkt sichtbaren Quellen-Hinweises (Titel und Urheberbezeichnung). Weiters benötigt ein aufnehmendes Werk auch eigene Substanz. D.h. eine Zusammenstellung ausschließlich aus Zitaten mit nur nebensächlichem eigenen Inhalt, z.B. nur Überschriften oder Werbebanner, ist nicht erlaubt. Es wird sich daher bei Framing oder Inline-Elementen nur in Ausnahmefällen um Zitate handeln, beispielsweise wenn explizit auf die Quelle hingewiesen wird und die anderen Voraussetzungen ebenfalls erfüllt sind.

IV.8. Literatur

IV.8.1. Allgemein

Anderl, Alex: Die Haftung der Nic.at und Denic EG - Der trügerische Frieden. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): IT in Recht und Staat. Wien: Verlag Österreich 2002, 165-174

[296] Hierfür ist typischerweise ein Bug im Browser oder die Mithilfe des Servers erforderlich.

[297] Dies wird wohl auf die Intention des Urhebers zurückzuführen sein: Ist der Frame ein separates Werk mit äußerer "Dekoration", oder ein unselbständiger Teil eines Werkes, das aus einem Frameset besteht. Im ersteren Fall ist kein (Klein-)Zitat mehr möglich, da es sich nicht mehr um einen Teil handelt, im zweiten Fall ist an eine Störung der Werkintegrität zu denken.

Brenn, Christoph: E-Commerce – Die Richtlinie und das E-Commerce-Gesetz. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): Auf dem Weg zur ePerson. Wien: Verlag Österreich 2001, 313-322

Ebensperger, Stefan: Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132

Filzmoser, Friedrich: Gewerbe- und berufsrechtliche Aspekte des E-Commerce-Gesetzes, RdW 2002/337

Geist, Anton: Rechtlicher Schutz von Layout. http://www.rechtsprobleme.at/doks/geist-layoutschutz.pdf

Haindl, Barbara: Streitschlichtung für Domainstreitigkeiten. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): IT in Recht und Staat. Wien: Verlag Österreich 2002, 157-164

Handig, Christian: Downloads aus dem Internetradio. ecolex 2005, 921

Hasberger, Michael, Semrau-Deutsch, Katharina: Host-Provider als Richter? ecolex 2005, 197

Junkers, Markus: Haftung des Admin-C - Anmerkung zu OLG Stuttgart. http://www.jurpc.de/aufsatz/20040098.htm

Krenn, Jürgen: Die METEO-data-Entscheidung – Hyperlinking/Framing und Urheberrecht. http://www.it-law.at/papers/Die%20METEO-data-Entscheidung%20%20%20Hyperlinking%20Framing%20und%20Urheberrecht.pdf

Mosing, Max W., Otto, Gerald, Proksch, Wolfgang: Internet Governance oder Die (Nicht-) Legitimation zur Domain-Verwaltung. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): IT in Recht und Staat. Wien: Verlag Österreich 2002, 145-156

Ott, Stephan: Urheber- und wettbewerbsrechtliche Probleme von Linking und Framing, Diss. 2004. http://www.linksandlaw.com/ownpublications-zsfgpromotion.htm

Ott, Stephan: Der Herr des Links – Die zwei Frames. http://www.linksandlaw.de/framing-druckversion.htm

Reinstadler, Armin: Browsing und Framing aus urheberrechtlicher Sicht. JurPC Web-Dok. http://www.jurpc.de/aufsatz/20030332.htm

Schmidbauer, Franz: Die Zulässigkeit des Linkens aus urheberrechtlicher und wettbewerbsrechtlicher Sicht. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther, Liebwald, Doris (Hg.): Zwischen Rechtstheorie und e-Government. Wien: Verlag Österreich 2003, 503-510

Schmidbauer, Franz: Hilfe, Gehilfe! http://www.internet4jurists.at/news/aktuell56.htm

Schramböck, Michael: Urheberrechtsschutz von Internet-Web-Sites und anderen Bildschirmdarstellungen von Computerprogrammen. ecolex 2000, 126

Silberbauer, Kristina: Internet und Unlauterer Wettbewerb. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): Auf dem Weg zur ePerson. Wien: Verlag Österreich 2001, 411-416

Smejkal, Vladimir: Unlauterer Wettbewerb im Internet. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther, Liebwald, Doris (Hg.): Zwischen Rechtstheorie und e-Government. Wien: Verlag Österreich 2003, 563-570

Sonntag, Michael: Voluntariness of permissions required for security measures. In: Ralf Steinmetz, Andreas Mauthe (Eds.): Euromicro 2004. Proceedings of the 30th Euromicro Conference. Los Alamitos, IEEE Computer Society 2004, 551-557

Sonntag, Michael: A small product line needing requisitely holistic management. Case study of a call-center application and its legal protection. In: Trappl, Robert (Ed.): Cybernetics and Systems 2006. Wien: Austrian Society for Cybernetic Studies 2006, 454-459

Stadler, Thomas: Die Zulässigkeit von sog. Deep-Links – Eine Anmerkung zur Paperboy-Entscheidung des BGH. JurPC Web-Dok. http://www.jurpc.de/aufsatz/20030283.htm

Stomper, Bettina: Urheberrechtliche Aspekte von Links. ÖBl 2002/44, 212-216

Strasser, Mathias: § 14 ECG - Paradies auf Erden für Napster & Co? ecolex 2002, 241

Thiele, Clemens: Comments on the OGH decision "Telering.at". WBl 2001, 318

Thiele, Clemens: Anmerkungen zu OGH 11.12.2003, 6 Ob 218/03g "Haftung von Online-Archiven" http://www.eurolawyer.at/pdf/OGH_6_Ob_274-03t.pdf

Wass, Clemens: Think Before You Link – Zur Verantwortlichkeit für fremde Inhalte, auf die mittels Hyperlink verwiesen wird. http://www.rechtsprobleme.at/doks/clemens-wass-verantwortlichkeit-links.pdf

Wass, Clemens: Freie Werke (§ 7 UrhG) im Internet. Diplomarbeit Salzburg 2000. http://www.rechtsprobleme.at/doks/clemens-wass-freie-werke.pdf

Wiebe, Andreas: Auskunftsverpflichtung der Access Provider. MR 2005 H 4 Beilage, 1

IV.8.2. Rechtsvorschriften

UrhG: Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (BGBl 1936/111 idF BGBl I 81/2006)

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

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

V. 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[298]. 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.

Werbung muss als solche zu erkennen sein, also entweder eindeutig sein wie z.B. Bannerwerbung, oder vom einem redaktionellen Teil klar getrennt werden[299].

V.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. In den meisten Fällen handelt es sich um einfache Grafiken, welche dynamisch ausgewechselt werden, sodass bei wiederholtem Besuch der Seite jeweils andere Werbung eingeblendet wird. Vielfach wird das Bild von einem anderen Server geladen: Die Datenseite verweist auf den Server eines unabhängigen Werbeanbieters oder einer anderen Firma (Banner-Tausch). Dies ermöglicht eine Verfolgung des Benutzers über mehrere Web-Sites hinweg, was ein Datenschutzproblem erzeugen kann (siehe unten).

Unerwünscht sind Banner hauptsächlich deshalb, da sie sichtbaren Platz am Bildschirm belegen und den Benutzer oft durch ihre Gestaltung ablenken bzw. es zumindest versuchen. Weiters benötigen sie zum Download Bandbreite, um so mehr, je stärker animiert sie sind. Dieser Nachteil verschwindet jedoch praktisch bei Breitbandzugängen. Um den Benutzer zu einer genauen bzw. überhaupt einer Betrachtung 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 ist[300].

---

[298] Daher auch das geflügelte Wort "Wer nicht wirbt, stirbt"!

[299] 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.

[300] Hierfür sind Modifikationen am Webserver nötig. Auch dies dürfte wegen der Breitbandnutzung eher abnehmen.

Im Anschluß wird der Aufbau von Bannern erläutert und welche Elemente verwendet werden, die Click-through-rate[301] zu erhöhen. Nicht jeder dieser Versuche ist jedoch ohne weiteres rechtlich zulässig.

V.1.1. Typen von Bannern

Banner können, je nach ihrer Gestaltung, in mehrere Gruppen eingeteilt werden. Hier werden nur einige wichtige Grundformen dargestellt[302].

- Statische Banner: Hierbei handelt es sich um einfache statische Bilder, ähnlich einem Werbeplakat. 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[303], 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[304].
- Animierte Banner: Sie bestehen aus einer Aneinanderreihung von Einzelbildern, welche mit kurzem Abstand angezeigt werden. Interaktionen über das 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 (x Anzahl der Bilder). Die Kosten sind naturgemäß höher als bei statischen Bannern, da mehr Bilder zu erzeugen 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.
- 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.
- Applikatorische Banner: Derartige Banner können sowohl statisch wie animiert sein, besitzen jedoch ein gemeinsames Element: Sie täuschen eine Anwendung vor. Typischerweise werden dazu Fensterrahmen, Menüs oder Dialogboxen dargestellt (siehe

[301] 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 jetzt von Kunden gemieden.

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

[303] 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.).

[304] Etwa Besonderheiten bei vergleichender Werbung, verbotene Produkte, ...

Abbildung 8 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[305]. 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 Täuschen des Benutzers erfolgen kann und meist auch genau dies beabsichtigt wird. Die Konsequenz kann einerseits Schadenersatz bei konkreten finanziellen Einbußen sein, andererseits aber auch unlauteren Wettbewerb darstellen[306].

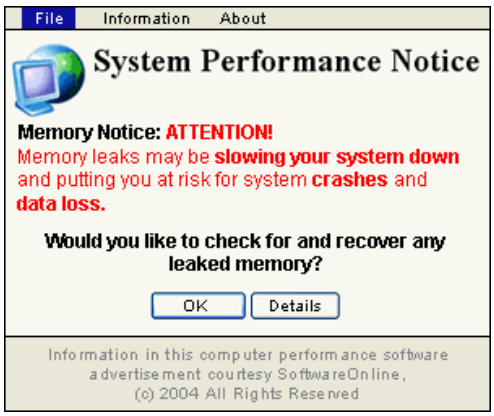


Abbildung 8: Beispiel eines applikatorischen Banners

- Site in the Site: Hierbei handelt es sich um eine voll funktionsfähige "Subseite" im Rahmen eines Bannerplatzes. Dies kann etwa eine Java-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. 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.

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

[306] 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".

V.1.2. Gestaltungselemente

Zur Erhöhung der Klickrate 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 bedeutet 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 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 und diese betrachtet. 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.
- Neues Browserfenster (Pop-up): Eine Möglichkeit besteht darin, für die Werbung ein eigenes Browserfenster zu öffnen. Dies hat den Vorteil, dass die Werbung auch dann sichtbar bleibt, wenn der Benutzer die Seite verlässt. 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 einge-

setzt 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, beim Verlassen der Seite darf jedoch keines mehr geöffnet werden. Hierbei handelt es sich um nicht angeforderte kommerzielle Kommunikation, welche unlauterer Wettbewerb ist[307]. 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[308].

- Vergrößern des Fensters: Beim Öffnen einer Webseite mit Werbung das Fenster auf die maximale Größe zu vergrößern[309], 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 Werbung von anderen, z.B. in dahinter/daneben liegenden Fenstern verdeckt wird.
- Automatische Einblendung: Mittels Javascript, Flash etc. kann eine Werbung an einer bestimmten Stelle des Fensters als Überlagerung des eigentlichen Inhalts angezeigt werden. 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 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 einen weiteren Link[310]. 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 rechtlich unproblematisch.

---

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

[308] Siehe aber die Entscheidungen in Amerika, welche sich meist gegen eine Verletzung aussprechen. Rachman/Kibel, Online Advertising Challenges Tradition, New York Law Journal 1017.10.2005. http://www.dglaw.com/images/OnlinAdvertising19D41C.pdf

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

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

V.1.3. Datenschutz und Bannern von externen Seiten

Werbebanner oder die oben erwähnten Elemente können entweder von der eigentlich besuchten Web-Site stammen oder von einem anderen Server[311]. 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 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 9). Diese Art der Datenübermittlung ist datenschutzrechtlich äußerst bedenklich, da hierzu fast nie eine Zustimmung bestehen wird: Weder ausdrücklich[312] noch konkludent[313]. Eine generelle Zustimmung ("an Anbieter von Werbung") durch Teilnahme am Internet kann weder angenommen werden, noch wäre sie datenschutzrechtlich erlaubt.

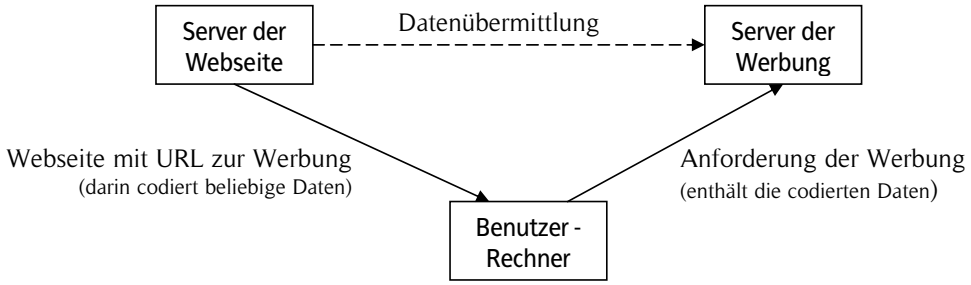


Abbildung 9: Datenweitergabe bei Werbung von Dritt-Servern

Unbedenklich ist deshalb die Einbindung lokaler Bilder und die bloße Einbettung entfernter Bilder ohne Zusatzinformationen, Cookies oder ähnlichem[314]. 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)

---

[311] 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

[312] 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.

[313] 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.

[314] Die Referer-Daten geben zwar auch an, von welcher Webseite aus die Werbung aufgerufen wurde, doch ist dies vom Betreiber der einbettenden Webseite nicht beeinflussbar und liegt vollkommen beim Benutzer, und ist daher irrelevant.

oder nicht (beispielsweise dynamische 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.

V.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 der Webseite noch nichts wissen, bzw. nur Web-Sites besuchen, auf denen das zugehörige Banner nicht eingeblendet wird. Der Nachteil ist jedoch, dass diese Art von Werbung bei den Empfängern meist unerwünscht und daher großteils verboten ist.

V.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, Inhalt sind:

- Gesundheits- / Potenzsteigerungs- und Diätangebot
- Zusatzeinkommen ohne Aufwand und Kosten (Heimarbeitsangebote)
- Kredite / Kreditauskünfte / Verbesserung der Kreditwürdigkeit
- Phishing: Ausspähen von Bank-Passwörter (PIN) und TANs oder Kreditkartendaten
- Anwerben von Zwischenpersonen für illegale Geldtransfers
- Versand von Massen-E-Mails / Anbieten von Anti-Spam-Programmen
- Kettenbriefe; meist mit Unheilsandrohung bei Nicht-Weiterleitung
- Gratisprodukte, z.B. Handys, Urlaub oder Software
- Investitionsgelegenheiten, insbesondere Penny-Stocks
- Angebot gefälschter Produkte, z.B. Rolex Uhren
- Werbung für irgendwelche 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, die sowohl legal als auch korrekt ist und lediglich ohne Anforderung zugeschickt wird, und deshalb auch 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 selber höhere Investitionen tätigen und bereiten ihre Vorschläge daher viel besser

und glaubwürdiger auf, sodass dort die Rate der Hereingefallenen auch viel höher ist. Bei Spam hingegen handelt es sich sehr oft um "Amateure".

In letzter Zeit treten jedoch auch in diesem Bereich vermehrt Profis auf, insbesondere im Bereich Phishing. Die organisierte Kriminalität scheint also nun auch diesen Erwerbszweig entdeckt zu haben.

Will man daher E-Mail-Werbung seriös einsetzen, ist es erforderlich, echte Investitionen in die Erstellung des Inhalts zu tätigen, diese korrekt zu formulieren, sie 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 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[315].

V.2.2. Sammlung von E-Mail-Adressen

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

- 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). Dies ist eine Hauptquelle an Adressen für Spam-Versender. 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 ist jedoch erlaubt, wenn darauf schon bei der Anmeldung explizit hingewiesen wurde[316]. Diesfalls besteht eine Einwilligung analog einem Newsletter. Archive von Mailinglisten entsprechen Newsgruppen.
- 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 dorthin gerichtet werden.
- Kettenbriefe: Werden Kettenbriefe weitergeschickt, so erfolgt dies üblicherweise durch "Forward" und Eintragen einer Vielzahl von Empfängern im TO-Feld. Daraus folgt, dass sich nach einigen Weiterleitungen eine große Anzahl von Mail-Adressen im Inhalt befindet: Alte Empfänger werden beim Weiterleiten in den Inhalt übernommen. Ganz all-

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

[316] Nicht, wenn es sich um unbeteiligte Dritte handelt, die Werbung "einschleusen".

gemein ist der Empfang einer E-Mail von einer Person oder die Erwähnung ihrer Adresse im Text/Header einer E-Mail keine Zustimmung zur Zusendung von Werbung.

- 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 verwendet 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.
- 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 nur mehr Einzelabfragen anzubieten (eine Suche nach dem Namen ergibt die E-Mail-Adresse).
- Domain contact points: Die meisten Domains bzw. Mailserver besitzen allgemein übliche Adressen für festgelegte Zwecke[317]. 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[318]. 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, ist eine Einwilligung unmöglich. Die Teilnahme am E-Mail-Verkehr ist keine Zustimmung zum Werbungsempfang.
- Sonstige Quellen: Finger-Dämon[319], Webbrowser[320], IRC/Chat[321], lokale Benutzer[322]. Diesen ist gemeinsam, dass eine Zustimmung zum Empfang von Werbung alleine durch die Eintragung der E-Mail-Adresse nicht in Frage kommt.

---

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

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

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

[320] 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).

[321] 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).

- 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[323]. Listen mit verpflichtender Eintragung fallen jedoch nicht hierunter. Hier kann ev. davon ausgegangen werden, dass für jeweils spezifisch erstellte und relevante Einzelangebote eine Zustimmung zum Empfang von Werbung besteht. Eine regelmäßige Zusendung von Werbung ist jedoch sicher nicht umfasst[324].
- 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 kann daher festgestellt werden, dass die Sammlung von Adressen zum Versenden von E-Mail-Werbung in fast allen Fällen, ausgenommen dem letzten, illegal ist, da keine Zustimmung zur Verwendung dieser eindeutig personenbezogenen Daten für diesen Zweck vorliegt. Schon die Erhebung selbst ist nach dem Datenschutz illegal, sodass bereits die bloße Sammlung als Vorbereitung für eine spätere Zusendung verboten ist. Für einen rechtlich einwandfreien Erwerb von Adressen bleiben daher übrig:

- Kauf von E-Mail Adressen, z.B. von Adressverlagen: 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.
- 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).

In allen Fällen sind die vielfältigen Vorschriften für die eigentliche Zusendung, z.B. Inhalt und Kennzeichnung, zu beachten.

V.2.3. Auswirkungen von Spam

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

V.2.3.1. 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 bzw.

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

[323] Typischerweise jedoch gegenüber Kunden, um diesen Waren oder Dienstleistungen zu verkaufen. Potentielle Lieferanten sind wohl normalerweise eher nicht von der Intention mitumfasst.

[324] So zumindest auch nach alter Rechtslage in Deutschland. Nach der neuen, die ähnlich der österreichischen ist, wäre dies nicht mehr zulässig.

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, was sehr teuer enden kann, sofern nicht alle Vorschriften eingehalten wurden[325]. International (vom Sender aus gesehen ins Ausland verschickte 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: 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[326], welche zu verschwindend geringen Kosten erreicht wurden!

V.2.3.2. 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. Hierauf beruht insbesondere 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.

V.2.3.3. Im Internet

Durch den Versand von Spam wird eine hohe Bandbreite belegt[327]. 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 Antwort auf dem Rückweg weitere Bandbreite beansprucht. Ebenso kann sich eine signifikante Änderung des Benutzerverhaltens ergeben: Da Newsgruppen die Hauptquelle für die Adressensammlungen sind, verzichten immer mehr Personen dar-

---

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

[326] 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!

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

auf, dort teilzunehmen, obwohl es sich grundsätzlich um eine gute Einrichtung zur Diskussion und dem Wissensaustausch handelt.

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.

V.2.3.4. 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.
- Die Versuchung, Spam zu versenden, ist für Werber sehr groß: Mit minimalem Aufwand kann ein riesiges Zielpublikum erreicht werden.
- 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[328]. 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[329] oder Vorauszahlungsbetrug[330]. Nur ein verschwindend kleiner Teil der Empfänger wird darauf hereinfallen, doch wegen der minimalen bis nicht-existenten Kosten kann ein Gewinn daraus gezogen werden. Hierher gehört auch Phishing, wobei schon einzelne Erfolge sehr hohen Gewinn bedeuten können, z.B. das Abräumen eines Kontos.

---

[328] 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 Versender, sondern die Empfänger.

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

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

V.2.4. 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

V.2.4.1. 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 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.
- 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 sollte nicht das TO sondern das BCC-Feld verwendet werden. Auf diese Weise erfahren die Empfänger nicht die E-Mail Adressen der 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[331], 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.

[331] 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!

- 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 empfangenen 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.

V.2.4.2. 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.

V.2.4.3. 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 weitere Alternative ist die Eintragung in el. Robinsonlisten. Versender von Werbe-E-Mails sollten diese konsultieren, in Österreich müssen sie es, und dort enthaltene Adressen aus ihren Datenbanken entfernen bzw. sperren. Da sich jedoch meist nur die Versender, welche legale und reelle Angebote versenden und daher weniger 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[332].

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.

[332] 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.

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 USA, keine Überprüfung der Identität des Antragstellers erfolgt und teilweise auch anonym Accounts vergeben werden[333].

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[334], 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) 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[335]. 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, die erkannte Spam-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[336]), 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[337], 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.

---

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

[334] Siehe als bekanntes und sehr erfolgreiches Programm SpamAssassin (http://spamassassin.apache.org/). Dieses ist für verschiedenste Betriebssysteme verfügbar und erzielt sehr gute Quoten (Persönliche Erfahrung: ca. 90% Reduktion).

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

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

[337] Beispiele: SPF: Sender Policy Framework (http://www.openspf.org/) und Sender ID (http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx)

- 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. El. Briefmarken wären eine ideale Lösung, sind aber realistischerweise in der Praxis nicht umsetzbar, da die Lösung weltweit und fast ausnahmslos erfolgen müsste. Auch hier wären legitimen Absender vieler E-Mails wieder „Leidtragende“.

V.2.5. Rechtliche Aspekte von Spam

Die Zusendung von unerbetenen Werbe-E-Mails kann auch 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[338]. 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 Brief-Werbung muss von Mitarbeitern 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[339]. Daher ist Spam in der Praxis ein viel größeres Problem als andere Formen der Werbung ohne Aufforderung für die Zusendung. Die Gefahr besteht und ist vielfach real, dass derartige Werbung überhand nimmt und in der Summe die Arbeit unzumutbar behindert.

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.[340]

---

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

[339] 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!

[340] 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 wer-

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).

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 dies 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 EU-Richtlinie, als Grundlage dienen kann.

V.2.5.1. § 107 Telekommunikationsgesetz

Anrufe, inklusive Fax, bedürfen nach dem Telekommunikationsgesetz (TKG) der vorherigen Zustimmung des Empfängers oder einer anderen Person, welche diesen Anschluss benützen darf. 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.

Die Zusendung von E-Mails oder SMS[341] ist verboten, wenn es sich um Werbung handelt[342] oder die Nachricht an mehr als 50 Empfänger geht[343] (=opt-in). Eine Zustimmung ist jedoch nicht erforderlich (=opt-out), 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 der Beantwortung, jedoch nicht[344].
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!

---

den. Hier hilft nur eine Eintragung auf der Robinsonliste. Mit Zustimmung erhaltene Werbung oder Werbung direkt vom Erhebenden kann nur durch Kontakt mit dieser Person/Firma verhindert werden.

[341] 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

[342] 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.

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

[344] 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.

4. Keine Eintragung in die Robinsonliste besteht[345]: 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[346] seine Zustimmung erklärt haben[347] oder es sich um "Nachfass-Kommunikation" zu geleisteten Lieferungen oder Diensten handeln, um ihm el. Werbepost zusenden zu dürfen. 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. Die Ausnahme für Nachfass-Kommunikation bezieht sich nur auf E-Mail und SMS, und gilt nicht für Telefonanrufe[348].

Immer verboten ist die Zusendung el. Post zu Werbezwecken, wenn die Identität des Absenders verschleiert oder verheimlicht wird 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 nicht aus, wenn die Werbung schon in der Überschrift eindeutig als solche gekennzeichnet ist, und eine funktionierende Abmeldemöglichkeit bereitgestellt wird: Dies wäre das Opt-out-Modell[349].

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 vom Ausland aus[350] explizit als der Ort angesehen wird, an dem der Anruf den Teilnehmeranschluss erreicht (=und daher dann in Österreich liegt).

Nach einer Entscheidung des OLG Nürnberg[351] 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 gearbeitet werden. Wie im angesprochenen Urteil entschieden, ist das heimliche Anfügen von zusätzlicher Werbung auf jeden Fall verboten.

---

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

[346] 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

[347] Wohl auch in AGBs möglich, allerdings nur bei besonderer Hervorhebung.

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

[349] 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.

[350] Dies gilt nur für Telefonanrufe und Fax (§ 107 Abs 6 TKG), aber nicht für E-Mail oder SMS, was eine bedauerliche Regelungslücke ist, da gerade bei E-Mails inländischer Versand kaum vorkommt.

[351] OLG Nürnberg, 25 10.2005, 3 U 1084/05 http://www.affiliateundrecht.de/olg-nuernberg-produktempfehlung-mails-wettbewerbwidrig-3-U-1084-05.html Inzwischen anscheinend beim BGH anhängig (siehe http://forum.computerbetrug.de/showthread.php?t=38041 sowie die dortigen Überlegungen zu werbefinanzierten E-Mails). Werbung in E-Mails (z.B. GMX) wird aber wohl erlaubt sein, da dort der Zweck der Zusendung nicht die Werbung, sondern der normale Inhalt ist; analog auch Produktempfehlungen: Erfolgt die Zusendung zur privaten Information oder will auch der Dritte hier werben (für jemand anderen), z.B. zum späteren Erhalt von Prämien?

V.2.5.2. 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.

V.2.5.3. 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[352]; siehe oben.

V.2.5.4. Art. 13 Telekom-Datenschutz-Richtlinie

In dieser derzeit letzten Richtlinie von 2002 wurden die Bestimmungen gegen Spam wieder 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[353]) bis März 2006 Werbung an Nicht-Konsumenten erlaubt. Wegen dieser richtlinienwidrigen Umsetzung wurde dies jedoch geändert und auf alle, natürliche und juristische, Personen erweitert. Daher ist jetzt auch die unverlangte Zusendung von Werbung per E-Mail an Firmen verboten.

---

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

[353] 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.

V.2.5.5. 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[354], 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.
- 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 Kennzeichnung 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[355].

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[356].

V.2.6. Informationspflichten

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

- Kommerzielle Kommunikation muss als solche erkennbar[357] 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:", ...),

---

[354] 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

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

[356] 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

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

weshalb die technische Filterung daher wohl kaum erleichtert wird. "Unabhängige Berichte" oder eine Vermischung mit redaktionellen Artikeln[358] 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 unten.
- Angaben zur Absatzförderung (=Werbeversprechen, Zugaben, Geschenke etc.) müssen als solche erkennbar sein. Weiters muss ein einfacher Zugang zu den Bedingungen für 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 Euro.

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[359] entweder direkt im Newsletter oder auf einer verlinkten Webseite zu erfüllen. Siehe näheres dazu im Kapitel VII.

V.2.7. 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[360] 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, sollte das Verfahren "double-opt-in[361]" verwendet werden.

---

[358] 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!

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

[360] 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.

[361] 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.

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.
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 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.

V.2.8. 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[362] 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[363]. 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[364]. 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

---

[362] 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.

[363] 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.

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

Regelungen des DSG zurückzugreifen, d.h. meist eine Einwilligung erforderlich. Nach der GewO hingegen dürfen nur übermittelt werden:

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

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[365] bei Telefon-/Faxwerbung oder der Zusendung von E-Mails von vornherein ausgeschlossen ist, auch bloß als Quelle für die hierzu verwendeten Daten.

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[366] 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 alten Regelung dürfen nun auch durch Analyseverfahren gewonnene[367], d.h. nicht bei den Betroffenen erhobene, sondern berechnete, Daten verwendet und wei-

---

[365] 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. 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

[366] 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.

[367] "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

tergegeben[368] 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.

V.3. Messenger-Popups

Eine weitere Art der Werbung ist die "Zusendung" von Popup-Mitteilungen. Hierbei wird ungefragt ein Fenster 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: 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[369] 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[370] 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"[371], 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.

V.4. Meta-Tags

Bei Meta-Tags handelt es sich um unsichtbare Informationen auf Webseiten für Suchmaschinen. Diese 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.

Für sich genommen sind derartige Techniken rechtlich kein Problem[372]. 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, ty-

---

[368] 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

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

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

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

[372] Siehe Thiele, Meta-Tags und das österreichische Wettbewerbsrecht. ÖJZ 2001, 168

pischerweise Markennamen. Die Grundprinzipien gelten weiters für ähnliche Werbeformen, von denen nur Word-Stuffing kurz erläutert wird.

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

Derartige Wörter sollen dazu dienen, auch auf (teilweise) "sachfremde" Abfragen 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[373]. Ebenso kann keine Subsumption unter den Begriff der irreführenden Werbung[374] erfolgen, da ebenfalls keine potentiellen Kunden betroffen sind[375]. Praktisch besitzt diese Art der Werbung wohl geringe Bedeutung.

Anders ist die Sachlage zu beurteilen, sollte zumindest ein gewisser Zusammenhang zu den angebotenen Produkten bzw. Dienstleistungen bestehen[376], 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[377]. Selbst wenn durch die Beschreibung auf den ersten Blick erkennbar sein sollte, um welche Produkte es sich handelt, so ist allein schon die Darstellung auf der Suchergebnis-Seite eine Werbung: Die Bekanntmachung des Namens. Hierfür wird ansonsten bezahlte Bannerwerbung verwendet.

V.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 insbesondere Markenrecht, z.B. unberechtigte Verwendung fremder Marken, und Wettbewerbsrecht, etwa Ausbeutung fremder Leistung oder Abfangen von Kunden, schlagend werden[378].

---

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

[374] 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.

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

[376] 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.

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

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

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[379], aber wohl zu bejahen[380]. 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. 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[381].

Das OLG Düsseldorf vertritt hingegen die Meinung, dass die Verwendung einer Marke in Meta-Tags keine kennzeichenmäßige Benützung darstellt[382], 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 ist jedoch eine Mindermeinung und wurde vom BGH zurückgewiesen[383].

Auch die entgegengesetzte Meinung bedeutet jedoch nicht, dass keinerlei Verwendung fremder Marken in Meta-Tags erlaubt ist[384]: 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 oder Bereitstellung von Informationen darüber. Wird also die Marke zusätzlich im Inhaltstext der Seite verwendet und erfolgt dies dort rechtmäßig, so kann sie auch als Meta-Tag verwendet werden[385]. Eine Ausnahme gilt nur dann, wenn die Verhältnismäßigkeit fehlt: Eine flüchtige und unbedeutende Erwähnung am Rande reicht wohl nicht aus, eine Marke in den Meta-Tags anzuführen[386, 387]. Ein Beispiel hierfür ist die Aufnahme von Marken der Konkurrenz.

---

[379] 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.

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

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

[382] 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 383; 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 Deustche Rechtsprechung bringt Terhaag, Lichtblick im Tunnel neuerer Meta-Entscheidungen - München hält den aktuellen Entwicklungen aus Düsseldorf stand http://www.aufrecht.de/3317.html

[383] BGH 18.5.2006, I ZR 183/03 http://www.aufrecht.de/4750.html (Volltext mit Begründung derzeit noch nicht verfügbar, da es sich um ein mündlich verkündetes Versäumnisurteil handelt)

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

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

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

V.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: 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.

V.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 nicht durch die Suchmaschine bzw. nur zwischen mehreren Werbenden für dasselbe Suchwort.

Solange es sich bei den ausgewählten Suchwörtern um allgemeine Gattungs- und Sachbegriffe handelt, stellen sich keine Probleme[388]: Jeder darf damit werben, "Bücher" zu verkaufen. Wird jedoch hierzu ein fremder Markenname 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[389]. Separat zu beurteilen ist jedoch immer die Verwendung fremder Markennamen in der Anzeige selbst.

Außer in besonderen Fällen ist die Verwendung fremder Marken als bloßer Auslöser jedoch kein markenrechtliches Problem: 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[390]. Dadurch liegt zwar eine markenmäßige Verwendung vor, diese ist jedoch mangels Verwechslungsgefahr nicht zu

---

[387] 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.

[388] Jahn/Häussle: Aktuelle Entscheindungspraxis zum Internet im Bereich des gewerblichen Rechtsschutzes (Teil II). GesRZ 2003, 144

[389] 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

[390] 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.

beanstanden[391]: 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. Auch eine Behinderung des Markeninhabers liegt nicht vor, da dieser wie bisher an normaler Stelle im Suchergebnis aufscheint.

Problematisch ist hingegen das Wettbewerbsrecht: Ein sittenwidriges Abfangen von Kunden oder Rufausbeutung können vorliegen. Die bloße und getrennte Anzeige von Werbung ist zwar u.U. noch erlaubt, ebenso wie in einer Zeitung neben einem Artikel über eine Marke Werbung für die Konkurrenz erscheinen darf[392]. Die meisten Entscheidungen und Literaturstellen gehen jedoch von einem Verbot aus, zumindest was Marken bzw. Bezeichnungen der Konkurrenz betrifft[393]. Handelt es sich um Bezeichnungen von verkauften Produkten, wird dies jedoch wohl eher nicht zu beanstanden sein[394].

Besondere Vorsicht ist erforderlich, wenn die Suchworte zu denen 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[395].

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[396]. 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[397].

---

[391] So OLG Wien 14.7.2005, 1 R 134/05s "Glucochondrin", das die Verwechslungsgefahr verneint. 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.

[392] LG Hamburg 21.12.2004, 312 O 950/04. Eine solche Platzierung darf auch explizit verlangt werden. Letzteres scheint jedoch eher eine Mindermeinung zu sein.

[393] 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

[394] 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.

[395] 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 Domainnamen.

[396] 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 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 kein Recht an diesen Wörtern behauptet.

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

V.6. Literatur

V.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/

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

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

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

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

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

V.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

V.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.shtml

VI. Datenschutz

E-Business bietet für Kunden und Firmen viele Vorteile, doch können sich aus der Verwendung von IT und el. Kommunikationsmitteln auch erhebliche Gefahren ergeben. Es ist praktisch unmöglich, aus den normalen (physischen) Einkäufen einer Person zu verschiedenen Zeitpunkten bestimmte Vorlieben oder Gewohnheiten herauszulesen[398] und diese dann z.B. für gezielte Werbung zu nützen. Im Gegensatz dazu ist dies im E-Commerce problemlos möglich: Der Kunde kann beispielsweise auf der eigenen Webseite exakt verfolgt werden. Besondere technische Verfahren, z.B. Werbebanner eines einzigen Unternehmens auf verschiedenen Shops, erlauben es sogar, ein Profil über die Bewegungen eines Kunden übergreifend für eine Vielzahl von Web-Sites herzustellen. Da eine Verfolgung der Aktionen bzw. Käufe aber durchaus auch von Nutzen für die Kunden sein kann, beispielsweise im Hinblick auf so genannte Personalisierungen und Empfehlungen, ist ein völliges Verbot nicht sinnvoll. Es muss vielmehr darauf geachtet werden, welche Verwendung von personenbezogenen Daten wann akzeptabel ist, und welche nicht.

Da in nationalen Datenschutzgesetzen meist Regeln enthalten waren, in welche Länder welche Daten weitergegeben werden durften, um eine Umgehung durch Export und Verarbeitung im Ausland zu verhindern, wurde eine Richtlinie der EU erlassen (Datenschutz-Richtlinie, DSRL). Diese Richtlinie war bis zum 24.10.1998 umzusetzen und Österreich daher bereits säumig. 1999 wurde verstärkt an einer Novellierung des (alten) Datenschutzgesetzes aus 1978 gearbeitet, welches der Richtlinie nicht vollständig entsprach. Das neue Datenschutzgesetz zur Umsetzung der Richtlinie wurde am 29.7.1999 dann als "Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG)" vom Nationalrat beschlossen. Dass der Datenschutz ein wichtiges Anliegen ist, kann man auch daraus ersehen, dass die Generalversammlung der Vereinten Nationen bereits am 14.12.1990 eine "Richtlinie betreffend personenbezogener Daten in automatisierten Dateien" beschlossen hat, welche freilich nur an die Staaten adressiert ist und lediglich eine Empfehlung ist; sie besitzt keine Rechtsverbindlichkeit. Ebenso ist der Datenschutz auch in der "Charta der Grundrechte der Europäischen Union" enthalten[399].

In diesem Abschnitt wird ein wichtiger Teil des Datenschutzes nicht behandelt, da er weniger den Inhalt der Kommunikation, also den E-Business, betrifft, als vielmehr die bloße Übertragung an sich: Das Telekommunikationsgeheimnis. Es ist strafrechtlich geschützt und hat durchaus auch im Internet Bedeutung (Logs von WWW-Proxies oder E-Mail-Server, IP-Adress-Zuteilung, …). Hier wird auf das Telekommunikationsgesetz (Abschnitt 12, §§ 87-95) sowie die Telekom-Datenschutz-RL der EU hingewiesen. Neuerdings wurde das Datenschutzrecht jedoch wieder eingeschränkt, indem die Speicherung gewisser Daten

[398] Abgesehen von der Verwendung so genannter Kundenkarten, welche genau zu diesem Zweck eingeführt werden.

[399] Art. 8: Schutz personenbezogener Daten. (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

auf Vorrat, also unabhängig von einem konkreten Verdacht, verpflichtend bis zum 17. September 2007[400] einzuführen ist[401].

VI.1. Einleitung

Das "Datenschutzgesetz 2000" (DSG) setzt die Datenschutz-Richtlinie der EU um, geht aber in Teilbereichen noch darüber hinaus. So werden z.B. auch die Daten von juristischen Personen[402] geschützt, ein Bereich, der aus der Richtlinie ausgenommen ist. Dieser Schutz bestand schon im alten Datenschutzgesetz und wurde beibehalten. Ein Problem könnte sich aufgrund dieses besonderen Schutzes dadurch ergeben, dass daher nur in den wenigsten Ländern ein angemessenes und damit gleichwertiges, Datenschutzniveau besteht. Um dennoch eine Exportvereinfachung zu erreichen, wofür ein solches erforderlich ist, wurden die Ausnahmen von der Genehmigungspflicht für die Daten natürlicher Personen auch auf solche von juristischen Personen erstreckt. Dahinter steht der Grundsatz, dass Daten natürlicher Personen zumindest gleich schützenswert sind wie solche von juristischen. Wenn also eine Übermittlung keine Geheimhaltungsinteressen natürlicher Personen gefährdet, kann auch davon ausgegangen werden, dass eine solche in Bezug auf juristische Personen ungefährlich ist.

Ein wichtiges Element des Datenschutzes ist das "Datengeheimnis": Auftraggeber einer Verarbeitung, beauftragte Dienstleister oder Mitarbeiter derselben müssen Daten, die ihnen ausschließlich auf Grund ihrer beruflichen Beschäftigung anvertraut oder bekannt wurden, geheim halten und dürfen nur aus einem rechtlich zulässigen Grund eine Übermittlung vornehmen[403]. Diese Verschwiegenheitspflicht ist auch durch eine Verwaltungsstrafe abgesichert (siehe Abschnitt VI.6.6).

Hinzuweisen ist darauf, dass für publizistische Tätigkeit, rein private Verarbeitung sowie wissenschaftliche Forschung und Statistik Ausnahmen bzw. Erleichterungen gelten.

VI.2. Begriffsbestimmungen

In diesem Abschnitt werden die wichtigsten Begriffe erläutert, wie sie im Datenschutzgesetz definiert sind. Bereits am Beispiel "Daten", welche hier ausschließlich als "personenbezogene Daten" verstanden werden, ist zu sehen, dass diese Definitionen nicht im Sinne der Informatik allgemeingültig sind: Sie gelten ausschließlich für dieses Gesetz. Die Definitionen sind im DSG in § 4 und in der DSRL in Art. 2 zu finden, wobei in der Richtlinie jedoch teilweise eine andere Benennung (auch in der Deutschen Fassung) und eine etwas geringere Differenzierung erfolgt.

---

[400] Österreich erklärte, die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail für einen Zeitraum von weiteren 18 Monaten zurückzustellen, d.h. bis zum 17.3.2009.

[401] Richtlinie 2006/24/EG des Europäischen Parlamentes und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher el. Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. Bei der angesprochenen Richtlinie 2002/58/EG handelt es sich um die Datenschutzrichtlinie für el. Kommunikation.

[402] Dies betrifft z.B. Bilanzen. Siehe OGH 13.2.2003, 8 Ob 4/03a. Anders in Deutschland: § 3 Abs 1 BDSG.

[403] Derartige Daten müssen daher selbst gegenüber Arbeitskollegen, der Familie oder Freunden geheimgehalten werden.

VI.2.1. Daten

Unter Daten werden Angaben über natürliche und juristische Personen (=Betroffene) verstanden, wenn die Identität der Person, der sie zugeordnet sind, bestimmt ist oder zumindest bestimmt werden kann. Beispiele für Daten natürlicher Personen sind Name, Geschlecht, Kaufkraft oder die Internet-Surfgewohnheiten. Bezüglich juristischer Personen fallen darunter etwa Rechtsform, Eigentümer oder Ertragsdaten. Es handelt sich daher ausschließlich um personenbezogene Daten. Anonymisierte Informationen, die also von *niemandem* mehr einer Person zugeordnet werden können, sind nicht geschützt. Hierfür kommt ev. ein Schutz als Geschäftsgeheimnis in Frage.

Damit es sich um "personenbezogene" Daten handelt, ist es nicht notwendig, dass der *Verarbeiter* die absolute und eindeutige Identität der Person feststellen kann, z.B. wenn nur die Sozialversicherungsnummer (SVNR) bekannt ist, aber nicht Name oder Wohnort, sondern dass dies zumindest für *irgendeine* andere Person möglich ist. Im Beispiel wären dies die Krankenkassen, welche die Zuordnung SVNR $\Leftrightarrow$ restliche Personendaten vornehmen können, ev. in Verbindung mit dem Melderegister oder anderen Datenbanken. Damit in Verbindung steht die Unterscheidung in "direkt" und nur "indirekt" personenbezogene Daten, welche eine große praktische Bedeutung besitzt. Im zweiten Fall, bei nur indirekt personenbezogene Daten, sind die Vorschriften für die Verarbeitung durch einen bestimmten Verarbeiter, für den sie eben nur indirekt personenbezogen sind, stark erleichtert. Indirekt personenbezogen sind Daten dann, wenn es mit *legalen* Mitteln und *vertretbarem* Aufwand dem *konkreten* Dateninhaber (=Auftraggeber; siehe unten) nicht möglich ist, sie einer einzigen bestimmten Person zuzuordnen. Die Möglichkeit der Verwendung illegaler Mittel, z.B. verbotene Verknüpfung mit anderen Daten oder übermäßigem Aufwand, etwa dem Durchprobieren aller Möglichkeiten, beseitigt daher den nur indirekten Bezug nicht. Zu beachten ist, dass indirekter Personenbezug immer nur im Hinblick auf einen bestimmen Verarbeiter vorliegen kann: Beispielsweise ist für Privatpersonen die SVNR indirekt personenbezogen, für die Krankenkassen hingegen nicht.

Im Gegensatz zum alten Datenschutzgesetz wird nicht mehr gefordert, dass die Daten auf einem Datenträger festgehalten sein müssen. Auch bloß temporäre Daten sowie ausschließlich im Hauptspeicher befindliche Informationen sind geschützt.

Drei grobe Kategorien von direkt personenbezogenen Daten hinsichtlich ihres Inhalt werden vom Gesetz unterschiedlich stark geschützt: Den höchsten Schutz besitzen "sensible Daten" (siehe sogleich), etwas geringeren Daten mit Strafrechtsbezug. Alle anderen (="normalen") Daten unterliegen dem allgemeinen Schutzniveau.

VI.2.2. Sensible Daten

Bei sensiblen Daten handelt es sich um besonders geschützte Informationen, wobei die Unterscheidung zu "normalen" Daten nach dem Inhalt erfolgt. Insbesondere sind die Ausnahme für ihre Verwendung abschließend im Gesetz aufgezählt, was im Gegensatz zu den nicht-sensiblen Daten steht, bei welchen die Liste lediglich beispielhaft ist. Der Katalog ist abschließend in Art. 8 Abs 1 DSRL bzw. § 4 Z 2 DSG angeführt und betrifft ausschließlich natürliche Personen[404].

[404] Da sie inhaltlich für juristische Personen nicht wirklich passen. Dies ist aber explizit festgelegt, da etwa bei politischer Meinung oder Gewerkschaftszugehörigkeit sonst u.U. Zweifel auftauchen könnten.

Sensible Daten sind:

- Rassische und ethnische Herkunft
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Religiöse oder philosophische Überzeugung (z.B. Atheismus)
- Gesundheit
- Sexualleben

VI.2.3. Auftraggeber

Bei einem Auftraggeber handelt es sich um eine natürliche oder juristische Person, Personengemeinschaften oder Organe (="Behörden") einer Gebietskörperschaft ebenso wie deren Geschäftsapparate (="Ämter"), welche die Entscheidung getroffen haben, Daten (=personenbezogene Daten) für einen bestimmten Zweck zu verarbeiten.

Auch wenn für die tatsächliche Verarbeitung Subunternehmen, im DSG „Dienstleister“ genannt, herangezogen werden[405], verbleibt die Auftraggeber-Eigenschaft beim Besteller des Werkes bzw. der Dienstleistung. Nur wenn der Auftragnehmer trotz ausdrücklichen Verbotes oder aufgrund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln eine gesonderte Verarbeitung vornimmt, wird er zum Auftraggeber. Diese Zurechnungsregeln sind sinnvoll, da für den Betroffenen meist nur der Auftraggeber, aber nicht der Dienstleister ersichtlich ist[406]. Weiters besitzt dieser normalerweise das Verfügungsrecht über die Daten, sodass daher nur er eine Löschung, Richtigstellung oder Auskunft durchführen kann und darf.

VI.2.4. Datei

Eine Datei ist eine strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich ist. Eine el. Verarbeitung wird nicht vorausgesetzt. Daher erfüllen selbst Zettelkarteien und einfache Listen diesen Begriff. Daraus ergibt sich auch die Ausweitung des Datenschutzes auf manuell verarbeitete Daten, da auch diese nunmehr unter den Begriff "Datei" fallen.

Diese Definition wurde direkt der Richtlinie entnommen und ist leider etwas missverständlich. Aus den Beratungen zum Gesetzesentwurf ergibt sich, dass eigentlich nicht strukturierte Sammlungen von Daten, sondern Sammlungen strukturierter Daten geschützt werden sollen. Es geht also um eine (zusätzliche) interne Struktur, und nicht um eine rein externe. Eine Korrektur ist eventuell durch Auslegung möglich. Diese Unterscheidung ist deswegen notwendig, da beispielsweise eine Sammlung von Papierakten nicht als Datei gelten soll (und gilt), obwohl sie zweifellos eine strukturierte Sammlung ist (äußerlich nach der Aktenzahl), während eine Datenbank meist nicht strukturiert ist, sondern nur aus

[405] Hierfür bestehen besondere Vorschriften, siehe § 10 DSG.

[406] Beispiel Postwerbung: Die werbende Firma ist eindeutig erkennbar, aber wer die Kuverts tatsächlich mit der Adresse versehen hat, ist praktisch nie feststellbar. Dem entspricht auch, dass die Druckerei in Bezug auf Auskunft, Richtigstellung, Beschwerden etc. nicht der richtige Ansprechpartner wäre.

einer ungeordneten Menge[407] von Datensätzen besteht, welche jedoch in sich stark strukturiert sind. Dennoch sind auch Daten sehr einfacher Strukturierung geschützt: Eine Zuordnung Person → einzelne Eigenschaft reicht bereits aus.

Unter Datei wird daher eine Sammlung von Daten verstanden, welche eine äußere Ordnung besitzt, d.h. aus identifizierbaren Elementen besteht, und welche *inhaltlich* zumindest durch ein einziges Kriterium erleichtert durchsucht werden kann[408]. Von Bedeutung ist diese Definition, da die Rechte auf Auskunft, Widerspruch und Löschung nur für automationsunterstützt verarbeitete Daten, sowie manuell in Dateien niedergelegten Informationen zur Verfügung stehen. Computerverarbeitung führt daher immer zu diesen Rechten, manuelle Verarbeitung hingegen nur, wenn es sich um Dateien handelt[409].

VI.2.5. Datenanwendung

Hierbei handelt es sich um die Summe von logisch verbundenen Verwendungsschritten (siehe Abschnitt VI.2.6) zur Erreichung eines inhaltlich bestimmten Ergebnisses. Diese Verarbeitung muss zumindest teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen. Wichtig ist, dass die Datenverarbeitung eine logische Einheit ist, die zwar aus unterschiedlichen Handlungen wie Verarbeitung, Übermittlung etc. in beliebiger Reihenfolge bestehen kann, aber einem übergeordneten Gesamtzweck dient.

Datenanwendungen sind grundsätzlich dem Datenverarbeitungsregister zu melden. Problematisch kann dabei sein, dass keinerlei Struktur der Verarbeitung notwendig ist, und daher z.B. auch die Benutzung von Adressen zur Adressierung eines Briefes in einer Textverarbeitung darunter fällt: Auch dieser Vorgang ist eine Datenanwendung. Um unnötige Bürokratie zu vermeiden, existieren Standard- und Musteranwendungen für häufige Verarbeitungen, bei welchen eine Meldung dann gar nicht mehr erforderlich, bzw. stark vereinfacht möglich ist (siehe Abschnitt VI.6.1).

VI.2.6. Verwenden von Daten

Im Gegensatz zur DSRL wird im DSG eine feinere Differenzierung getroffen. Das "Verarbeiten" der Richtlinie wird in Österreich als "Verwenden" definiert und anschließend weiter in „Verarbeiten“ und „Übermitteln“ differenziert, sodass bei „Verarbeiten“ jeweils auf die angesprochene Rechtsordnung bedacht zu nehmen ist. Es betrifft jede Art der Handhabung von Daten in einer Datenanwendung: Was auch immer konkret mit Daten erfolgt, es ist eine Verwendung.

---

[407] Und damit nicht äußerlich strukturiert; auch wenn schneller Zugriff oder Sortierungen über z.B. Indizes möglich sind! Dies gilt jedoch genauso für Aktensammlungen, welche nach der Geschäftszahl, aber eben nur nach dieser und nicht nach zumindest einem weiteren inhaltlichen Kriterium, leicht aufzufinden sind, aber nicht darunter fallen. OGH 28.6.2000, 6 Ob 148/00h

[408] Ausführlich dazu auch VwGH Erkenntnis vom 21.10.2004, 2004/06/0086. Derartige Erleichterungen können eine alphabetische oder chronologische Sortierung sein, aber auch automatisierte Erschließungssysteme. Praktisch stellt ein körperliches Aktenarchiv keine Gefahr dar: Es ist nicht möglich, alle Akten aufzufinden, in welchen eine bestimmte Person vorkommt, da kein derartiger Index existiert. Bei el. Aktenarchivierung, also automationsunterstützter Verarbeitung, ist dies hingegen problemlos durchführbar.

[409] Siehe dazu auch OGH 25.6.2002, 1 Ob 109/02i. Die Aussage aus OGH 28.6.2000, 6 Ob 148/00h, dass das Grundrecht an sich nur bei Vorliegen von Dateien, also völlig unabhängig von der Art der Verarbeitung, gilt, mit Hinweis auf die Literatur relativiert wird, ohne jedoch darüber zu entscheiden. Dies betrifft insbesondere den Geheimhaltungsanspruch, der sonst nur bei Dateien gegeben wäre, selbst wenn automatisierte Verarbeitung stattfände. Siehe auch Rosenmayr-Klemenz: Zum Schutz manuell verarbeiteter Daten durch das DSG 2000. ecolex 2001, 639

VI.2.6.1. Übermitteln von Daten

Bei einer Datenübermittlung werden Daten aus einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder Dienstleister weitergeben. Daher ist eine Auskunft von Daten an den davon Betroffenen keine Übermittlung, ebenso wenig wie die Weitergabe an andere zum Zwecke der eigentlichen Verarbeitung (⇒ Überlassung; siehe unten). Sehr wohl eine Übermittlung stellt jedoch eine Veröffentlichung dar. Ein Personenwechsel im Auftraggeber bzw. Verfügungsberechtigten ist für eine Übermittlung nicht notwendig: Eine Übermittlung findet selbst dann statt, wenn Daten bei einem Auftraggeber von einer Datenanwendung zu einer anderen transferiert werden, d.h. lediglich der Zweck geändert wird.

Die Essenz liegt also in einem Wechsel des Verwendungszweckes der Daten, um sie für ein anderes Aufgabengebiet zu nutzen. Darunter kann ein Tätigkeitsfeld verstanden werden, das seinem Umfang und der Verkehrsauffassung nach geeignet ist, für sich allein einen eigenen Geschäftsbereich eines Auftraggebers zu bilden, also eine tatsächlich "andere" Datenanwendung darstellt. In den Erläuterungen wird dieser im privaten Bereich mit dem Umfang einer Gewerbeberechtigung und im öffentlichen Bereich mit einem Kompetenztatbestand (Art. 10 bis 15 B-VG) verglichen[410].

VI.2.6.2. Verarbeiten von Daten

Das Verarbeiten von Daten ist umfassend definiert und besteht aus vielen einzelnen Elementen: Ermitteln, Überlassen, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Sperren, Löschen, Vernichten oder jeder anderer Art der Handhabung. Ausgenommen davon ist lediglich die Übermittlung. Es handelt sich also eigentlich um eine negative Definition: Jede beliebige Verwendung von Daten, die *keine* Übermittlung ist, ist eine Verarbeitung. Jeder Einsatz von Daten ist daher entweder eine Übermittlung oder der Rest (=Verarbeitung); Überschneidungen existieren nicht. Das Übermitteln wurde im DSG deshalb aus der Verarbeitung ausgeschieden, da hierfür besondere abweichende Vorschriften gelten.

Interessant sind insbesondere zwei spezielle Arten der Verarbeitung:

- Ermitteln von Daten: Beim Ermitteln von Daten handelt es sich um das Erheben von personenbezogenen Daten in der Absicht, sie in einer Datenanwendung zu gebrauchen. Entstehen solche Daten zufällig, so findet zwar keine Ermittlung statt, doch sind auch derart entstehende Daten geschützt. Schon das bloße Sammeln oder Einspeichern unterliegt daher den datenschutzrechtlichen Vorschriften.
- Überlassen von Daten: Darunter wird die Weitergabe von Daten von einem Auftraggeber an einen Dienstleister verstanden. Hierbei handelt es sich eben *nicht* um eine *Übermittlung,* sondern um eine Verarbeitung, und ist daher den dafür maßgeblichen Vorschriften unterworfen. Der Unterschied zur Übermittlung liegt darin, dass beim Überlassen eine (natürliche oder juristische) Person beauftragt wird, eine bestimmte Verarbeitung mit beigestellten Daten für den Auftraggeber an dessen Stelle (und daher im Bereich des ursprünglichen Zweckes) durchzuführen. Es handelt sich also um die "Weitergabe" einer rein manipulativen Tätigkeit. Bei einer Übermittlung ändert sich hingegen der Zweck und eine Verbindung zu einer bestimmten Tätigkeit fehlt.

[410] Siehe dazu auch Pomaroli: Das "Aufgabengebiet" im Datenschutz. ÖZW 2006, 13

VI.2.7. Zustimmung

Eine Zustimmung (§ 4 Z 14 DSG) zur Verwendung von Daten liegt dann vor, wenn der Betroffene gültig (d.h. ohne Irrtum), ohne Zwang und in Kenntnis der Sachlage in die konkrete Verwendung seiner Daten einwilligt. Eine solche kann immer nur auf eine bestimmte Verarbeitung bezogen sein, auch wenn diese relativ weit gefasst werden kann. Eine generelle Ermächtigung zu beliebiger Verwendung ist jedoch keine erlaubte bzw. wirksame Zustimmung. Eine Zustimmung ist jederzeit widerrufbar, worauf explizit hinzuweisen ist.

Die Zustimmung muss bei "normalen" Daten nicht unbedingt ausdrücklich erfolgen, sondern kann auch konkludent erteilt werden. Im Gegensatz dazu muss sie bei sensiblen Daten ausdrücklich erfolgen. Schriftlichkeit ist nicht erforderlich[411], kann aber für den Nachweis der Erteilung hilfreich sein.

Die drei konstitutiven Elemente einer Zustimmung sind:

1. Frei: Die Zustimmung muss ohne Zwang erfolgen. Dies bedeutet ganz klar, dass beispielsweise keine Erpressung vorliegen darf. Dies würde jedoch schon allgemein gelten und bedürfte keiner besonderen Erwähnung. Daher ist dieses Erfordernis noch etwas schärfer zu sehen und etwa eine (sonst noch erlaubte) Druckausübung bzw. eine entsprechende "Notsituation" ein Hindernis[412]. Nicht jeder tatsächliche Druck ist jedoch verboten: So kann z.B. ein Vertragsabschluss von der Zustimmung zur Datenverwendung abhängig gemacht werden[413].
2. Konkreter Fall: Eine generelle Erlaubnis ist nicht möglich. "Konkret" bedeutet hier die spezifische Verarbeitung von Daten über die betroffene Person durch einen bestimmten Verantwortlichen[414] für bestimmte Zwecke[415]. Es ist daher insbesondere in einer für den Betroffenen verständlichen Form anzugeben, welche Daten genau verwendet werden und welche Verarbeitungen mit ihnen erfolgen. Bei Übermittlungen sind zusätzlich auch die Empfänger näher zu umschreiben[416].

---

[411] Siehe jedoch § 4a deutsches BDSG!

[412] Siehe etwa Arbeitnehmer gegenüber Arbeitgeber, FN 22 in Damman/Simitis: EG Datenschutzrichtlinie (1997), 108.

[413] Siehe Urteil OLG Brandenburg 11.1.2006, 7 U 52/05 (Vertragsbedingungen bei der eBay-Internet-Auktion), http://www.jurpc.de/rechtspr/20060047.htm Das Koppelungsverbot des deutschen § 3 Abs 4 TDDSG ist kein Hindernis für eine gültige Zustimmung, selbst wenn der konkrete Anbieter einen Marktanteil von 73% hält. Ähnliches könnte für die "Freiheit" der Zustimmung gelten: Ist ein Zugang zu Waren oder Dienstleistungen nicht oder nicht in zumutbarer Weise ohne die Zustimmung möglich, so liegt keine freie Einwilligung vor. Hier sollte jedoch eine zusätzliche Einschränkung erfolgen, da etwa reine Luxusgüter solchen Schutz wohl nicht rechtfertigen, sondern zumindest eine gewisse "Not"-Lage erforderlich sein sollte.

[414] Die Angabe "im Konzern" ist nicht ausreichend, OGH 27.1.1999, 7 Ob 170/98w. Auch wenn diese Entscheidung zum alten DSG erging, wird dies auch heute noch zu ungenau sein. Siehe dazu OGH 15.12.2005, 6 Ob 275/05t: Die "Weitergabe bekannt werdender Daten in banküblicher Form" ist nicht konkret genug. Weder Anlassfall, Daten noch Empfänger werden durch diese Ausführung ausreichend determiniert.

[415] Insbesondere der Zweck der Verwendung muss hinreichend bestimmt sein: "Werbezwecke" alleine reichen nicht aus (OGH 13.9.2001, 6 Ob 16/01y unter Berufung auf OGH 22.3.2001, 4 Ob 28/01y). Dieser Zweck determiniert ja insbesondere, welche Verarbeitungen erlaubt sind, bzw. wann eine Übermittlung eintritt. Eine "abschließende" Definition ist im Gegensatz zu früher wohl nicht mehr erforderlich. Grabenwarter, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, ÖJZ 2000, 861; Damman/Simitis, 115; Kassai: "Location Base Services" im Gefüge des Satenschutzrechts, MR 2004, 433; Rosenmayr-Klemenz, Neue Rechtsgrundlagen für Adressverlage und Direktmarketingunternehmen, RdW 2003/150

[416] LG München I 01.02.2001, 12 O 13009/00: Eine AGB-Klausel, welche die Nutzung erhobener Daten "im Rahmen der jeweils geltenden Datenschutzgesetze" und zu Zwecken der Abwicklung sowie für Werbe- und Marktforschungszwecke erlaubt, ist wegen mangelnder Konkretisierung unwirksam. Umfang, Zweck und Übermittlungsempfänger sind nicht hinreichend bestimmt.

3. Informiert: Der Betroffene muss von der Verarbeitung der Daten über ihn informiert werden[417], sodass dieser Vor- und Nachteile abwägen kann. Insbesondere bei konkludenter Zustimmung ist dies bedeutsam[418]. Inbegriffen sind insbesondere die Informationen, die zur Konkretisierung der geplanten Verarbeitung dienen.

VI.3. Das Grundrecht auf Datenschutz

Ein Grundrecht ist ein verfassungsgesetzlich gewährleistetes subjektives Recht. Das konkrete Grundrecht auf Datenschutz resultiert in einem Anspruch auf Geheimhaltung personenbezogener Daten. Da es jedoch viele Situationen gibt, in denen dieses Recht ohne schwere Folgen nicht unbeschränkt bleiben darf, existieren davon vielfältige Ausnahmen.

VI.3.1. Inhalt

Das Grundrecht auf Datenschutz[419] bezieht sich nur auf personenbezogene Daten, d.h. Daten, die einer bestimmten Person zuordenbar sind. Der Schutz besteht auch nur dann, wenn ein (subjektives) Interesse an der Geheimhaltung besteht und dieses (objektiv[420]) schutzwürdig ist. Voraussetzung ist, dass die Daten geheim gehalten werden können, wozu ausreicht, dass sie nicht allgemein bekannt sind[421]. Deshalb unterliegen allgemein zugängliche Daten, z.B. das Telefonbuch[422], nicht dem Datenschutz, solange sie im Augenblick der Verarbeitung auch tatsächlich frei zugänglich sind. Ein subjektives Geheimhaltungsinteresse wird im Zweifel für alle Daten vermutet[423]. Ob dieses objektiv schutzwürdig ist, muss jeweils nach den Umständen beurteilt werden. Hilfreich sind hierbei die §§ 8 und 9 DSG welche festlegen, wann solche schutzwürdigen Interessen nicht verletzt werden[424]. Der Schutzanspruch besteht nur für die Person selbst, da es sich um ein höchstpersönliches Recht handelt.

Ausnahmen von diesem Grundrecht sind nur in besonderen Fällen möglich, insbesondere bei Zustimmung oder überwiegenden berechtigten Interessen Dritter, und müssen die gelindeste mögliche Form besitzen.

VI.3.1.1. Erhebungsschutz

Aus dem Anspruch auf Geheimhaltung personenbezogener Daten kann das Recht auf den Schutz vor Erhebung abgeleitet werden. Daten dürfen nur dann festgestellt oder gesam-

---

[417] Siehe dazu die Informationspflichten in §§ 24 und 26 DSG; Grabenwarter, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel. ÖJZ 2000, 861

[418] Siehe "Große Haushaltsumfrage": OLG Frankfurt 13.12.2000, 13 U 204/98, CR 2001, 294 = ZVI 9/2003, 462 http://www.rws-verlag.de/zeitsch/zvi/zvi_0903_umb_pdf.pdf Ausführliche Erläuterungen und Beantwortung eines vierseitigen Fragebogens reichen aus, die Zustimmung zu erklären. Das (damals in D noch bestehende, aber mit Ausnahmen versehene) Schriftformerfordernis ist (wettbewerbsrechtlich) nur eine Ordnungsvorschrift und macht die Zustimmung nicht ungültig. OLG: Hier würde auch eine konkludente Einwilligungserklärung für das Datenschutzgesetz ausreichen.

[419] In anderem Zusammenhang dazu: Kunnert: Die abschnittsbezogene Geschwindigkeitsüberwachung (Section Control) aus datenschutzrechtlicher Sicht. ZVR 2006/17

[420] Zur alten Rechtslage: DSK 13. 10. 1993, 120.434, ZfVBDat 1994/5

[421] Ein eingeschränkter Personenkreis, auch wenn groß, bedeutet noch keine Öffentlichkeit.

[422] Siehe dazu ev. den urheberrechtlichen Schutz als bloße Datenbank (Problematisch ist die erforderliche Investition).

[423] Im Zweifel spricht die Vermutung für die Schutzwürdigkeit: OGH 26. 8. 1999, 2 Ob 244/99t

[424] Die angeführten Beispiele (§ 8) bzw. Punkte (§ 9) sind also als schutzwürdig anzusehen, was aber die Verwendung in den konkreten Fällen dennoch nicht hindert.

melt werden, wenn dies den gesetzlichen Vorschriften entspricht, also z.B. eine Zustimmung des Betroffenen vorliegt. Dies betrifft beispielsweise eine automatische Erfassung von Nutzungsdaten beliebiger Internetdienste und gilt auch für indirekt personenbezogene Daten, d.h. WWW Logs bedürfen einer Ausnahme[425]. Nicht nötig ist eine solche jedoch für anonyme Daten, d.h. wenn weder IP-Adresse noch Benutzerkennung gespeichert wird.

VI.3.1.2. Auskunftsrecht

Gemäß § 26 DSG hat jeder Betroffene das Recht darauf, vom Auftraggeber[426] einer Datenverwendung innerhalb von acht Wochen Auskunft darüber zu erhalten, ob, und wenn ja welche, Daten über ihn verarbeitet werden[427]. Dies betrifft ausschließlich "echt" personenbezogene Daten. Nur indirekt personenbezogene Daten unterliegen, da ja die Identität des Betroffenen für den Verarbeiter nicht feststellbar ist, nicht der Auskunftspflicht. Um eine solche zu erhalten, muss ein schriftlicher Antrag gestellt werden und der Betroffene hat seine Identität in geeigneter Form nachzuweisen, was zur Verhinderung der Datensammlung über andere Personen dient; es handelt sich schließlich um ein höchstpersönliches Recht. Folgende Informationen sind dem Betroffenen allgemein verständlich mitzuteilen:

- Welche Daten verarbeitet werden (Kategorie und Inhalt)
- Sofern zutreffend und verfügbar, woher die Daten stammen (Er-/Übermittlung, ...)
- Wenn anwendbar, an welche Empfänger/-kreise die Daten übermittelt wurden
- Der Zweck der Datenverwendung
- Die Rechtsgrundlagen für die Verwendung

Die Auskunft darf nicht erteilt werden, wenn dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist[428], z.B. medizinische Gründe oder beim Strafregisterauszug erschwerte Bewerbungen oder soweit überwiegende berechtigte Interessen des Auftraggebers oder Dritter, z.B. öffentliche Interessen, dem entgegenstehen. Diese Ausnahme ist jedenfalls restriktiv auszulegen.

Um dem Auftraggeber keine zu große Belastung aufzubürden, ist der Antragsteller verpflichtet, über Befragung in zumutbarem Ausmaß mitzuwirken. Dies bedeutet, dass er, sofern ihm bekannt, beispielsweise angeben muss, in welchem Zusammenhang seine Daten vermutlich gespeichert sind (Geschäftszweig, Subunternehmen, ...), oder wie seine Kundennummer lautet, um die Suche nach seinen Daten zu erleichtern.

Betrifft die Anfrage den aktuellen Datenbestand einer Datenanwendung und hat der Betroffene im laufenden Jahr noch kein Auskunftsbegehren an den Auftragsteller zum selben Aufgabengebiet gestellt, so ist die Auskunft unentgeltlich zu erteilen. Andernfalls, d.h. bei mehreren Auskunftsbegehren in einem Jahr oder z.B. Auskunft über einen Datenbestand zu einem bestimmten Zeitpunkt in der Vergangenheit, ist ein pauschalierter Kostenersatz von derzeit € 18,89 vorgesehen, von dem nur wegen tatsächlich höherer Kosten, welche nachzuweisen sind, abgewichen werden darf. Führt die Auskunft zu einer Richtigstellung

---

[425] Jahnel, Spamming, Cookies, Web-Logs, LBS und die Datenschutzrichtlinie für el. Kommunikation. WBl 2003, 108.

[426] Nicht vom Dienstleister, selbst wenn dieser die Verarbeitung tatsächlich durchführt.

[427] Siehe Reichmann: Das Auskunftsrecht nach dem Datenschutzgesetz 2000 - Eine Fallstudie. ZfV 2004/1529 sowie OGH 25.3.1999, 6 Ob 292/98d (zum ähnlichen Auskunftsrecht des § 25 altes DSG)

[428] Hier wird der Betroffene vor sich selbst geschützt, daher müssen die Gründe wirklich sehr schwerwiegend sein!

oder werden die Daten rechtswidrig verwendet, so ist der Kostenersatz in jedem Fall in voller Höhe rückzuerstatten. Der Auftraggeber der Datenanwendung hat in diesen Fällen den notwendigen Aufwand selbst zu tragen.

Wird ein Auskunftsbegehren gestellt, so dürfen die Daten zumindest vier Monate lang, oder bis zum Abschluss einer ev. angestrengten Beschwerde bei der Datenschutzkommission, nicht mehr gelöscht werden!

VI.3.1.3. Richtigstellung oder Löschung

Jeder Auftraggeber ist verpflichtet, von sich aus Daten richtigzustellen bzw. zu löschen, sobald ihm die Unrichtigkeit oder die Unzulässigkeit der Verwendung bekannt wird. Darüber hinaus ist er hierzu auch auf begründeten Antrag des Betroffenen verpflichtet. Diese Pflicht ist auf diejenigen Daten beschränkt, die einer Person zuordenbar sind, d.h. nicht bei nur indirekt personenbezogenen Daten, sowie auf Daten, deren Unrichtigkeit oder Unvollständigkeit für den Zweck der Datenanwendung von Bedeutung ist. Sofern gesetzlich nichts anderes angeordnet ist, hat der *Auftraggeber* die Richtigkeit der Daten nachzuweisen. Dies gilt dann nicht, wenn die Daten ausschließlich durch Angaben des Betroffenen ermittelt wurden und auch genau diesen Angaben entsprechen. Die Richtigstellung/Löschung hat innerhalb von acht Wochen nach Einlangen des Antrags zu erfolgen. Gleichzeitig ist dem Betroffenen Mitteilung zu machen, wie mit seinem Begehren, sofern ein solches vorliegt, verfahren wurde.

Kann eine Richtigstellung oder Löschung aus technischen Gründen nicht erfolgen oder lässt der Dokumentationszweck der Datenanwendung dies nicht zu, wie etwa bei Krankengeschichten, so ist an Stelle einer Korrektur oder Löschung ein entsprechender Vermerk den Daten hinzuzufügen.

Kann die Korrektheit oder Unrichtigkeit von Daten nicht festgestellt werden und wird sie vom Betroffenen bestritten, ist keine Richtigstellung durchzuführen, sondern ein Bestreitungsvermerk anzubringen. Dieser darf nur mit Betroffenen-Zustimmung oder auf Grund einer Entscheidung eines Gerichtes oder der Datenschutzkommission gelöscht werden.

Wurden Daten richtiggestellt oder gelöscht und erfolgte in der Vergangenheit eine Übermittlung dieser Daten, so ist der Auftraggeber verpflichtet, die Empfänger der Daten von der Korrektur in geeigneter Weise zu unterrichten, um auch die entstandenen Kopien zu berichtigen. Dies ist dann nicht erforderlich, wenn die Empfänger nicht mehr feststellbar sind oder wenn dies einen unverhältnismäßigen Aufwand im Hinblick auf das berechtigte Interesse des Betroffenen an der Propagierung der Änderung bedeutet[429]. Umso bedeutender daher das Interesse des Betroffenen an der Richtigstellung oder Löschung ist, desto extensiver müssen die Bemühungen des Auftraggebers ausfallen, um auch alle im Wege der Übermittlung entstandenen Kopien der Daten zu korrigieren.

Auch in besonderen Konstellationen (Ausnahmen wegen besonderer, z.B. staatlicher, Interessen; VI.3.3.5) besteht dieses Recht, doch ist dem Betroffenen dann nur mitzuteilen, dass eine Prüfung durchgeführt wurde. Die Antwort ist immer identisch und unabhängig davon, ob Daten verarbeitet werden, ob diese richtiggestellt oder gelöscht wurden, oder ob dies nicht erfolgte.

---

[429] Adresskorrekturen verpflichten daher wohl normalerweise nicht zu einer Weitergabe, Bonitätsinformationen schon.

VI.3.1.4. Widerspruch

Das Widerspruchrecht (§ 28 DSG) stellt das Recht eines Betroffenen dar, die Verwendung seiner Daten, daher wieder nicht bei nur indirekt personenbezogenen Daten, wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben zu untersagen. Ein Widerspruch ist nicht möglich, wenn die Verwendung gesetzlich vorgesehen ist; diese kann nicht verhindert werden. Der Auftraggeber muss dann die Daten binnen acht Wochen löschen und darf keine weiteren Übermittlungen dieser Daten durchführen. Dies unterscheidet sich vom Recht auf Löschung darin, dass die Daten zwar korrekt waren und auch rechtmäßig verarbeitet wurden, jedoch einzelne Betroffene aufgrund besonderer Umstände, die auch konkret begründet werden müssen, trotzdem die Verwendung ihrer Daten untersagen können. Ein typischer Anwendungsbereich ist die Speicherung von Adressen für Marketingzwecke, z.B. bei legaler Erhebung aus dem Telefonbuch.

Zusätzlich zu diesem allgemeinen Widerspruchsrecht existiert noch ein spezielles: Sollen Daten ohne gesetzliche Anordnung in eine *öffentliche* Datei aufgenommen werden, so kann jederzeit auch *ohne* Begründung Widerspruch eingelegt werden. Die Daten sind dann ebenfalls binnen acht Wochen zu löschen. Dies beruht darauf, dass für die Öffentlichkeit nützliche Verzeichnisse (Bsp.: Telefonbuch[430], E-Mail-Adressen-Verzeichnis, Branchenverzeichnisse etc.) meist nicht gesetzlich vorgesehen sind und in einer Durchschnittsbetrachtung auch keine Verletzung schutzwürdiger Geheimhaltungsinteressen darstellen. Wenn jedoch Personen abweichend von dieser Durchschnittsbetrachtung für sich eine größere Gefahr annehmen, so soll dieses besondere Interesse berücksichtigt werden können.

VI.3.2. Umfang

Der Datenschutz erstreckt sich nicht nur auf automationsunterstützt sondern auch auf manuell verarbeiteten Daten, unabhängig davon, ob in Dateien abgelegt oder nicht[431]. Hieraus resultiert eine bedeutende Ausweitung gegenüber früheren Vorschriften, die lediglich automationsunterstützt verarbeitete Daten schützten. Der Zweck dieser Ausweitung war, Umgehungen zu vermeiden, selbst wenn für Betroffene an sich "gefährliche" Datensammlungen meist ohne Automationsunterstützung mangels Auswertungsmöglichkeiten nicht besonders gefährlich sind. Die Rechte auf Auskunft, Richtigstellung und Löschung gelten jedoch bei manuell verarbeiteten Daten nur, wenn es sich um Dateien handelt.

Wichtig ist zusätzlich, dass manuell verarbeitete Daten nicht Bundesangelegenheit sind, sondern die geltenden Vorschriften in neun Landes-Datenschutzgesetzen festgelegt sind, welche allerdings sehr stark dem Bundes-Datenschutzgesetz ähneln. Bedeutsam ist noch die Gegenausnahme, dass Daten sehr wohl unter das (Bundes-) Gesetz fallen, wenn es sich um Angelegenheiten handelt, in denen der Bund für die Gesetzgebung zuständig ist[432]. Für die Landesgesetze bleibt daher nur mehr ein äußerst geringer Bereich übrig.

Der räumliche Umfang erstreckt sich auf alle Datenverwendungen, welche im Inland stattfinden. Weiters ist österreichisches Recht auch dann anzuwenden, wenn ein österreichi-

---

[430] Siehe hierzu jedoch die Sonderregelungen im TKG in den §§ 18, 28, 69, 96f und 103!

[431] Siehe dazu aber die Ausführungen in VI.2.4

[432] Beispiel: Dateien, die für den Betrieb eines Gewerbes geführt werden (Gewerbeordnung ist Bundeskompetenz). OGH 4.5.2004, 4 Ob 50/04p; Siehe auch Rosenmayr-Klemenz: Zum Schutz manuell verarbeiteter Daten durch das DSG 2000. ecolex 2001, 639. Der Grund dieser Komplexe Regelung liegt in der Kompetenzverteilung zwischen Bund und Ländern.

scher Auftraggeber eine Verwendung in einem anderen EU-Staat vornimmt, ohne dort eine Niederlassung zu besitzen. Spiegelbildlich ist in Österreich fremdes Recht anzuwenden, wenn ein Auftraggeber aus einem anderen EU-Staat Daten im Inland verwenden lässt, ohne hier eine Niederlassung zu besitzen. Eine Niederlassung liegt nur dann vor, wenn die zu verarbeitenden Daten auch mit dieser in materiellem Zusammenhang stehen[433]. Eine Verarbeitung materiell "fremder" Daten[434] unterliegt daher trotz Vorhandensein einer Filiale oder Niederlassung nicht dem lokalen Recht. Für Auftraggeber ohne Sitz innerhalb der EU gilt immer das Recht des Landes, in dem die Verwendung stattfindet.

VI.3.3. Ausnahmen

Im Folgenden werden die viele Ausnahmen vom Recht auf Datenschutz kurz erläutert.

VI.3.3.1. Zustimmung

Die wichtigste Ausnahme ist die Zustimmung des Betroffenen selbst. Zu den genauen Voraussetzungen für eine gültige Zustimmung siehe oben unter VI.2.7. Betroffene sollen darüber entscheiden können, welche Daten über sie für welche Zwecke verwendet werden. Ein Widerruf der Zustimmung ist jederzeit möglich und bewirkt die Unzulässigkeit jeder weiteren Verwendung, sofern keine andere Ausnahme greift. Ein Spezialfall davon ist, dass eine Verwendung auch dann zulässig ist, wenn dies im lebenswichtigen Interesse des Betroffenen selbst liegt, da dann eine Zustimmung meist gegeben werden würde[435].

VI.3.3.2. Private Verarbeitung

Werden die Daten ausschließlich für persönliche oder familiäre Tätigkeiten verarbeitet, so sind sie vom Datenschutz ausgenommen (keine Meldepflicht, kein Auskunftsrecht etc.). Sie müssen jedoch entweder durch eine rechtmäßige Übermittlung erhalten oder dem Verarbeiter, der eine natürliche Person sein muss, direkt vom Betroffenen mitgeteilt worden sein. Zur Verhinderung der Umgehung von Schutzvorschriften ist eine Übermittlung aus diesem Bereich heraus, d.h. um die Daten für andere Zwecke zu verwenden, ausschließlich mit Zustimmung des Betroffenen erlaubt. Der typische Anwendungsfall dieser Bestimmung (§ 45 DSG) sind persönliche Adress- und Telefonverzeichnisse.

VI.3.3.3. Gesetzesvorbehalt

Das Grundrecht steht unter materiellem Gesetzesvorbehalt, daher kann selbst der einfache Gesetzgeber[436] weitere Ausnahmen schaffen, die jedoch besonderen Anforderungen zu genügen haben, wie sie in Art. 8 Abs 2 der Menschenrechtskonvention festgelegt sind:

1. Die Beschränkung muss der Wahrung überwiegender und berechtigter Interessen des Betroffenen selbst oder Dritter dienen. Diese müssen gegenüber dem Geheimhaltungsinteresse des Betroffenen überwiegen.

---

[433] Beispiel: Die Filiale verarbeitet Daten über Kunden des anderen Landes.

[434] Die Filiale verarbeitet daher Daten ohne lokalen Bezug. Diese betreffen nur "Heimatland"-Kunden des Unternehmens.

[435] Hier ist aber keine Ablehnung möglich. Siehe im Gegensatz dazu § 9 Z 7 DSG: Bei sensiblen Daten, hier typischerweise Gesundheitsdaten, reichen die lebenswichtigen Interessen nur, wenn keine Zustimmung eingeholt werden kann (echt vermutete Zustimmung). Ist eine Befragung möglich, so kann der Betroffene die Verarbeitung ablehnen, selbst wenn dies seinen Tod bedeutet.

[436] D.h. es ist kein *Verfassungs*gesetz hierfür erforderlich.

2. Die Ausnahme muss durch ein Gesetz erfolgen und kann daher z.B. nicht durch Verordnungen der Verwaltung eingeführt werden.
3. Der Eingriff muss im Bereich der Gründe des Art. 8 Abs 2 EMRK[437] liegen.
4. Der Eingriff muss notwendig sein und in der gelindesten möglichen Art erfolgen (Notwendigkeit und Verhältnismäßigkeit).
5. Betrifft der Eingriff besonders schutzwürdige, also insbesondere "sensible" nach dem DSG, Daten so muss er zudem aus einem wichtigen öffentlichen Interesse erfolgen und angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen bieten.

VI.3.3.4. Wissenschaftliche Forschung und Statistik

Für Zwecke konkreter wissenschaftlicher Forschung und statistischer Untersuchungen dürfen folgende Kategorien von Daten verwendet werden, sofern keine personenbezogenen Ergebnisse erzielt werden sollen. D.h. die Verarbeitung darf noch personenbezogen sein, die Ergebnisse aber nicht mehr. Konkret sind dies:

- Öffentlich zugängliche Daten
- Daten, die vom Auftraggeber für andere Untersuchungen oder andere Zwecke zulässigerweise ermittelt wurden. Eine interne Zweckänderung, d.h. eine Übermittlung, ist hier ausnahmsweise erlaubt.
- Daten, die für den Auftraggeber nur indirekt personenbezogen sind.

In diesen Fällen ist z.B. keine Zustimmung der Betroffenen zur Übermittlung oder Verarbeitung notwendig. Damit soll die Durchführung von statistischen Erhebungen erleichtert werden, die häufig mit einer großen Anzahl von Betroffenen verbunden ist und deren Verständigung großen Aufwand bedeuten würde.

Sind die Ergebnisse jedoch personenbezogen oder stellen sie kein konkretes Projekt dar, beispielsweise die Führung von Hilfsregistern[438] für zukünftige Projekte, so bestehen strengere Voraussetzungen: Es müssen besondere gesetzliche Vorschriften bestehen (Verpflichtung zur Verarbeitung/Erstellung einer Statistik) oder die Zustimmung der Betroffenen muss vorliegen. Eine solche Zustimmung kann unter bestimmten Voraussetzungen durch eine Genehmigung der Datenschutzkommission ersetzt werden, die für jede derartige Verarbeitung einzuholen ist. Besondere Auflagen und Bedingungen für die Verwendung der Daten können hierbei vorgeschrieben werden.

In jedem Fall ist der direkte Personenbezug so früh wie möglich durch Verschlüsselung zu entfernen, bzw. sind die Daten endgültig zu anonymisieren, sobald die Verarbeitung dies zulässt. Werden die Daten nicht mehr benötigt, so muss entweder der Personenbezug vollständig beseitigt oder die Daten gelöscht werden. Diese Ermächtigung betrifft nur wissenschaftliche Statistik, welche keiner besonderen gesetzlichen Regelung unterliegt[439].

---

[437] Art. 8 EMRK (Konvention zum Schutze der Menschenrechte und Grundfreiheiten): "(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs. (2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft *für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer* notwendig ist.

[438] Um etwa für Befragungen eine repräsentative Auswahl an zu befragenden Personen treffen zu können.

[439] Sonderregelungen bestehen beispielsweise im Bundesstatistikgesetz.

VI.3.3.5. Sonstige Ausnahmen

Von der Meldepflicht (§ 17 Abs 3 DSG), der Informationspflicht des Auftraggebers (§ 24 Abs 4 DSG) und dem Auskunftsrecht (§ 26 Abs 2 DSG) sind Daten bzw. Datenanwendungen ausgenommen, wenn sie zu folgenden Zwecken dienen und die Ausnahme zur Zweckverwirklichung auch notwendig ist:

- Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich
- Sicherstellung der Einsatzbereitschaft des Bundesheeres
- Sicherstellung der Interessen der umfassenden Landesverteidigung
- Schutz wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der EU
- Vorbeugung, Verhinderung oder Verfolgung von Straftaten

Daten aus solchen Datenanwendungen dürfen zusätzlich ohne explizite Genehmigung ins Ausland, sowohl inner- als auch außerhalb der EU, übermittelt oder überlassen werden.

VI.3.4. Drittwirkung

Das Grundrecht auf Datenschutz ist mit Drittwirkung ausgestattet. Dies bedeutet, dass es nicht nur gegenüber dem Staat in dessen Hoheitsfunktion geltend gemacht werden kann, wie sonst fast alle anderen Grundrechte, sondern auch zwischen den Bürgern untereinander zu beachten ist.

VI.4. Grundsätze für die Verwendung von Daten

In der Datenschutzkonvention des Europarates finden sich Grundsätze, die für die Erhebung, Verwendung und Qualität von Daten gelten sollen. Diese Grundsätze wurden auch in die DSRL aufgenommen und finden sich daher nun ebenso im DSG. Neben diesen allgemeinen Grundsätzen wird auch erläutert, welche Geheimhaltungsinteressen vom Gesetz als schutzwürdig eingestuft werden. Dies erfolgt in einer negativen Abgrenzung: Außer in den angeführten Fällen besteht immer ein Schutz. Da auch die Ermittlung von Daten eine Verwendung ist, werden hier auch die Informationspflichten des Auftraggebers erläutert, deren Einhaltung, neben anderen Verpflichtungen, eine Erhebung rechtmäßig macht.

VI.4.1. Allgemeine Grundsätze

Die allgemeinen Grundsätze[440] bedeuten bereits als solche eine Verpflichtung, da insbesondere ein Auftraggeber die Verantwortung dafür trägt, dass bei seinen Verarbeitungen die Grundsätze eingehalten werden. Hierbei haftet er auch für ev. herangezogene Dienstleister. Zusätzlich sind sie zur Auslegung der verschiedenen Bestimmungen anzuwenden.

Allgemein ist bei jeder Datenverwendung besondere Rücksicht auf das Grundrecht zu nehmen und die Verhältnismäßigkeit des Eingriffs gegenüber den Interessen des Betroffenen zu beachten. Nur der gelindeste mögliche ist erlaubt und dieser hat nach den unten angeführten Grundsätzen zu erfolgen.

---

[440] Allgemein und mit Anwendung auf den konkreten Bereich des Artikels: Grabenwarter: Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel. ÖJZ 2000, 861

VI.4.1.1. Verwendung nur nach Treu und Glauben und auf rechtmäßige Weise

Dies beinhaltet, dass der Betroffene über alle Aspekte der Verwendung informiert ist und er nicht irregeführt oder im Unklaren gelassen wird. Insbesondere muss er über seine Rechte und deren Durchsetzungsmöglichkeiten aufgeklärt bzw. darauf hingewiesen werden[441]. Dazu zählen besonders die Informationspflicht des Auftraggebers (VI.4.4), das Auskunftsrecht (VI.3.1.2) und die Anmeldung der Datenanwendung beim Datenverarbeitungsregister (VI.6.1). Dass Daten nur auf rechtmäßige Weise verwendet werden dürfen weist darauf hin, dass eine ausreichende rechtliche Befugnis (Private) bzw. Zuständigkeit (öffentlicher Bereich) erforderlich ist.

VI.4.1.2. Ermittlung nur für festgelegte, eindeutige und rechtmäßige Zwecke, Weiterverwendung nicht in einer mit diesen Zwecken unvereinbaren Weise

Aus diesem Grundsatz ergibt sich das Prinzip der Zweckbeschränkung[442]: Eine Übermittlung von Daten (= jeder Wechsel des Verwendungszweckes) ist nur erlaubt, wenn dafür eine gesetzliche Grundlage vorliegt, beispielsweise die Einwilligung des Betroffenen. Weiters enthält dieser Grundsatz den Erhebungsschutz: Personenbezogene Daten dürfen grundsätzlich nicht ermittelt werden, es sei denn, dass dafür eine explizite Erlaubnis, durch den Betroffenen oder per Gesetz, vorliegt. Eine Sammlung "auf Vorrat" ist damit nicht ohne besondere Ausnahme, z.B. Zustimmung, erlaubt[443]. Eine Genehmigung ist jeweils auf einen bestimmten konkreten Zweck beschränkt, worauf auch das grundsätzliche Übermittlungsverbot beruht.

VI.4.1.3. Verwendung nur insoweit, als für den Zweck der Datenanwendung wesentlich

Hier wird ein Minimalitätsprinzip festgelegt: Nur diejenigen Daten, die unbedingt für die Datenanwendung notwendig sind, dürfen verwendet werden. Alles, was darüber hinausgeht, ist Sammlung auf Vorrat und benötigt damit eine separate Ausnahme. Dadurch soll vermieden werden, dass große Datensammlungen "vorsorglich" angelegt werden.

Da der Zweck einer Datenanwendung jedoch, im Rahmen der Gesetze, relativ frei festgelegt werden kann, hat dieser Grundsatz nur für den Fall der Zwecküberschreitung eine Bedeutung und ist auch dann stark auslegungsbedürftig[444].

VI.4.1.4. Verwendung nur insoweit, als Daten in Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf dem neuesten Stand sind

Das Genauigkeitsprinzip legt fest, dass der Auftraggeber einer Datenanwendung dafür zu sorgen hat, dass die von ihm verwendeten Daten sachlich richtig sind. Es ist jedoch keine absolute, objektive Richtigkeit gefordert, sondern nur relative: Im Hinblick auf den Zweck der Datenverwendung dürfen keine Fehler enthalten sein[445]. Dieses bloß relative Korrekt-

---

[441] Beispiel: Die Eintragung in die Banken-Warnliste bedarf einer vorherigen Information des Betroffenen. Diese kann auch schon im Vorhinein erfolgen. OGH 15.12.2005, 6 Ob 275/05t. Siehe auch OGH 19. 11. 2002, 4 Ob 179/02f.

[442] Siehe Entscheidung der DSK, 16.11.2004, K 120.951/0009-DSK/2004 und dazu Brodil: Zeiterfassung ohne Zeiterfassung? ecolex 2005, 459. Siehe hierzu auch FN 482.

[443] Knyrim/Haidinger: RFID-Chips und Datenschutz. RdW 2005, 2

[444] Was ist für diesen bestimmten Zweck wirklich notwendig/noch nützlich/eigentlich unwichtig?

[445] Beispiel: Ein Verzeichnis "säumiger Kunden" darf nur Kunden enthalten, bei denen die Zahlungsfrist auch tatsächlich abgelaufen ist, jedoch keine Kunden, die zwar sehr spät, aber noch innerhalb der Frist bezahlen. Anders bei einem Verzeichnis von "Kunden, die eventuell säumig werden".

heitsgebot ist jedoch gefährlich: Bei einem Zweckwechsel wie einer Übermittlung wird in der Praxis kaum überprüft werden, ob die Daten auch noch für den neuen Zweck richtig (genug) sind. Dieser Grundsatz ist daher eher streng auszulegen. Aus den Erläuterungen geht auch hervor, dass in bestimmten Fällen daraus eine Pflicht des Auftraggebers abgeleitet werden kann, Daten regelmäßig auf ihre Aktualität zu überprüfen[446] und gegebenenfalls von sich aus richtigzustellen, um ungerechtfertigte Nachteile für Betroffene zu vermeiden.

VI.4.1.5. Aufbewahrung nur so lange in personenbezogener Form, als dies für den Zweck erforderlich ist oder gesetzliche Vorschriften dies erfordern

Daten müssen gelöscht oder anonymisiert werden, sobald sie nicht mehr benötigt werden. Da oft gesetzliche Vorschriften bestehen, dass Daten zu archivieren sind und bei vielen Anwendungen der Zweck auf sehr lange oder unbestimmte Zeit angelegt ist[447], ist auch dieser Grundsatz hauptsächlich bei Verletzungen von Bedeutung. Zu beachten ist, dass auf den Zweck der Ermittlung abgestellt wird: Ein späterer Zweckwechsel, um Daten länger aufbewahren zu können, ist daher eine Übermittlung und muss rechtmäßig erfolgen.

VI.4.1.6. Verhaltensregeln

In Art. 27 der DSRL und § 6 Abs 4 DSG ist vorgesehen, dass "Berufsverbände und andere Vereinigungen[448], die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten" Verhaltensregeln ausarbeiten. Diese sollen näher präzisieren, was eine Datenverwendung nach Treu und Glauben im Einzelnen für den privaten Bereich darstellt. Solche Regeln sind vor der Veröffentlichung dem Bundeskanzler vorzulegen, der ihre Gesetzmäßigkeit zu prüfen hat. Eine derartige für das österreichische Recht äußerst ungewöhnliche Einrichtung wurde durch die genaue Vorgabe in der DSRL notwendig. Obwohl der Bundeskanzler hier eine Vorab-Prüfung durchführt, ist damit keine Aussage über die Gesetzmäßigkeit der Verhaltensregeln verbunden; er gibt lediglich ein unverbindliches Gutachten darüber ab. Weiters haben die Verhaltensregeln keinen bindenden Charakter, sondern dienen lediglich als Richtschnur und können nur für die Auslegung herangezogen werden. Bedeutung könnten sie unter Umständen bei Schadenersatzprozessen erhalten, da ein Verstoß dagegen wohl eine zumindest fahrlässige Verletzung von Sorgfaltspflichten darstellt. Eine Prüfung durch die Datenschutzkommission kommt nicht in Frage, da diese die Regeln in einem (späteren) Beschwerdefall konkret zu prüfen hat und daher keine Vorab-Kontrolle vornehmen kann, ohne die Unvoreingenommenheit zu verlieren (Recht auf "fair trial" nach der EMRK).

---

[446] Dies wird beispielsweise für die Bonitätsdateien der Banken sowie Kreditauskunfteien vertreten. Hier kann die Beifügung eines Datums (=korrekt zu exakt diesem Zeitpunkt) hilfreich sein.

[447] Beispiel Kundendatei: Die Person könnte ev. in vielen Jahren wieder Kunde sein, daher müssen die Daten theoretisch bis zum Tode des Betroffenen aufbewahrt werden.

[448] Z.B. Vereine für bestimmte Branchen. Ein Beispiel könnte die ISPA http://www.ispa.at/ sein, die Vereinigung der Internet Service Provider Österreichs.

VI.4.2. Schutzwürdige Geheimhaltungsinteressen bei "normalen" Daten

Sollen nicht-sensible Daten verwendet werden, so werden schutzwürdige Geheimhaltungsinteressen nur in den folgenden Fällen nicht verletzt, d.h. ansonsten immer:

- Es besteht eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten. Dies gilt insbesondere für den öffentlichen Bereich, hat aber auch für den privaten Bereich Geltung (z.B. Mitarbeiterdaten).
- Der Betroffene hat der Verwendung seiner Daten zugestimmt. Ein Widerruf ist jedoch jederzeit möglich und bewirkt die Unzulässigkeit der weiteren Verwendung der Daten.
- Lebenswichtige Interessen des Betroffenen erfordern die Verwendung.
- Überwiegende und berechtigte Interessen des Auftraggebers oder eines Dritten erfordern die Verwendung. Hierbei handelt es sich um eine Art Generalklausel mittels einer Interessensabwägung[449].

Kann nicht festgestellt werden, ob es sich um normale oder sensible Daten handelt, z.B. bei Proxy-Server-Logfiles bei erlaubter Privatnutzung, so sind jedenfalls die Regelungen für sensible Daten anzuwenden.

VI.4.2.1. Beispiele, in denen keinesfalls eine Verletzung vorliegt

Die folgende Aufzählung bringt nur *Beispiele*, in denen keine Verletzung vorliegt. Alle Fälle sind Spezialisierungen des letzten Punktes der allgemeinen Regelung: Überwiegende berechtigte Interessen des Auftraggebers oder Dritter. Sie besitzen trotzdem eine gewisse Sonderstellung, da hier niemals eine Verletzung vorliegen kann. In anderen Fällen, die aufgrund einer allgemeinen Interessensabwägung ebenso unter die Generalklausel fallen, kann es in Einzelfällen dennoch dazu kommen, dass trotz grundsätzlicher Erlaubtheit (Interessenabwägung) eine Verletzung im besonderen Fall vorliegt (bei dieser Person anders als beim Durchschnitt). Bei den nachfolgend angeführten Beispielen erübrigt sich daher die Prüfung im Einzelfall, sondern es ist lediglich zu untersuchen, ob einer der Fälle vorliegt, um die Gesetzmäßigkeit zu bejahen.

Schutzwürdige Geheimhaltungsinteressen sind jedenfalls dann nicht verletzt, wenn die Verwendung der Daten:

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist. Hiermit soll vermieden werden, dass immer, wenn eine Datenverwendung notwendig ist, ein expliziter gesetzlicher Ermächtigung/Auftrag festzulegen ist. Es muss sich jedoch um eine wesentliche Voraussetzung handeln und es darf daher anders gar nicht oder nur mit großen Schwierigkeiten möglich sein, die Aufgabe zu erfüllen. Eine bloße Tätigkeitserleichterung reicht nicht aus.

[449] Siehe BAG 27.3. 2003, 2 AZR 51/02. Die heimliche Videoüberwachung am Arbeitsplatz führt nicht zu einem Beweisverwertungsverbot, da sie zulässig war: "... ist die heimliche Videoüberwachung eines Arbeitnehmers zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Video-Überwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist.". Anders BAG 29.6.2004, 1 ABR 21/03: Die verdachtsunabhängige Videoüberwachung eines Briefverteilzentrums ist unverhältnismäßig (es kommen Sendungen abhanden, aber es ist nicht einmal klar, ob dies gerade im Verteilzentrum erfolgt).

2. für einen Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe (Art. 22 B-VG) erfolgt. Die Zulässigkeit ist nach der ersuchenden Stelle zu beurteilen und die Amtsverschwiegenheit zu beachten.
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist. Gegenüber einem Menschenleben, auch dem eines Dritten und nicht nur des Betroffenen selbst, tritt der Datenschutz zurück. Beispiel dafür wäre etwa das Durchsuchen einer (fremden) Datenbank nach einem geeigneten Blutspender[450].
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist. Es wird per Gesetz sozusagen festgelegt, dass mit dem Vertragsabschluss auch automatisch eine Einwilligung gegeben wurde. Hiermit soll vermieden werden, dass ansonsten gültige Verträge durch Weglassen einer expliziten Regelung und anschließenden Einspruch beseitigt werden können[451]. Die Verwendung der Daten muss jedoch "erforderlich" sein, d.h. eine Erfüllung wäre ansonsten unmöglich.
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden. Einem Auftraggeber, der Daten rechtmäßig in seinem Besitz hat, kann nicht zugemutet werden, diese nicht verwenden zu dürfen, um ihm zustehende Rechte zu verfolgen. Dasselbe wird auch für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor Gerichten anzunehmen sein, da kein gewichtiger Grund ersichtlich ist, der dies ausschließen würde. Problematisch könnte aber die Öffentlichkeit einer Verhandlung sein.
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat.
7. im Katastrophenfall zur Hilfeleistung für unmittelbar betroffene Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen oder zur Information von Angehörigen notwendig ist.

VI.4.2.2. Geheimhaltungsinteresse bei Daten ohne Geheimhaltungsanspruch

Besteht kein Geheimhaltungsanspruch, so wird in zwei Fällen doch ein Widerspruchsrecht (§ 28 DSG) eingeräumt. Diese Daten dürfen daher solange legal verwendet werden, wie der Betroffene keinen Widerspruch eingelegt hat. Es handelt sich hierbei um zulässigerweise veröffentlichte sowie nur indirekt personenbezogene Daten. Bei ersteren Daten ist jedoch genau zu prüfen, ob tatsächlich alle Elemente veröffentlicht wurden, oder ob Teile davon zwar aus den öffentlichen Daten durch eine Auswertung gewonnen wurden, selbst aber nicht öffentlich sind[452]. In diesem Fall handelt es sich um "normale" Daten, und es sind die oben angeführten Interessen zu prüfen. Der Grund hierfür ist, dass auch aus einer Auswertung veröffentlichter Daten in besonderen Fällen neue Daten gewonnen werden könnten, die schutzwürdige Geheimhaltungsinteressen berühren[453], z.B. durch die Kombi-

[450] Hierbei handelt es sich zwar um medizinische, aber nicht um Gesundheitsdaten (und daher auch nicht um sensible Daten), da die Blutgruppe alleine nichts über den Zustand der Person oder ev. Krankheiten aussagt.

[451] Beispiel: Versandhandelskauf mit anschließendem Verbot der Adressverwendung, sodass das bestellte Produkt nicht zugesandt werden könnte (Paket-Etikettierung und Rechnungserstellung wären dann verbotene Datenverarbeitungen).

[452] Beispiel: Die Kundenliste einer Firma enthält etwa nur öffentliche Daten (Name, Telefonnummer). Die Zugehörigkeit zu dieser Liste ist aber selbst ein Datum, und genau dieses ist nicht öffentlich!

[453] Bekannt hierfür ist die "Herold Marketing-CD private", welche Tiefendaten enthält. Dies sind einzelnen Personen zugeordnete Informationen, z.B. die Bonitätsklasse, welche aber ausschließlich aus statistischen und bekannten Informatio-

nation mehrerer derartiger Quellen. Daher soll auch hier die Möglichkeit bestehen, eine Verwendung zu untersagen.

VI.4.2.3. Sonderregelungen für Straftaten

Zwischen den "normalen" und den sensiblen (siehe nächster Abschnitt) Daten existiert noch eine Zwischenkategorie: Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen, Daten über den Verdacht der Begehung von Straftaten sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen. Werden diese Daten verwendet, so liegt nur dann keine Verletzung des Datenschutzes vor, wenn:

- eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht. Beispiel: Strafregister.
- die Verwendung der Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrung einer ihnen gesetzlich übertragenen Aufgabe ist.
- sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen des Betroffenen gewährleistet. Gegenüber normalen Daten ist hier eine besondere Sorgfalt bei der Verwendung gefordert, um die Interessen des Betroffenen zu wahren. Es ist also eine besondere Aufmerksamkeit hinsichtlich des Schutzes vor unbefugtem Zugriff nötig. Dritte werden hier nicht angesprochen, daher betrifft diese konkrete Ausnahme nur eine direkte Verarbeitung aber nicht Übermittlungen. Die Interessen des Auftraggebers müssen zusätzlich im Verhältnis stärker sein, um die Verwendung strafrechtsbezogener Daten zu rechtfertigen.

VI.4.3. Schutzwürdige Geheimhaltungsinteressen sensibler Daten

Im Gegensatz zu den nicht-sensiblen Daten handelt es sich bei § 9 DSG um eine *abschließende* und nicht eine beispielhafte Aufzählung: Andere Eingriffe sind jedenfalls und immer verboten (siehe dazu auch Art. 8 Abs 2 und 3 der DSRL).

Schutzwürdige Geheimhaltungsinteressen werden daher nur dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat. Wer Daten selbst veröffentlicht, gibt damit zu erkennen, dass er kein besonderes Interesse an deren Geheimhaltung hat. Dies gilt um so mehr, je stärker die Daten sonst geschützt wären.
2. die Daten in nur indirekt personenbezogener Form verwendet werden. Da kein Rückschluss auf eine bestimmte Person möglich ist, besteht kein Geheimhaltungsinteresse.
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen. Dieser Eingriff muss dem Vorbehalt des Grundrechts entsprechen und ist dann erlaubt.
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht (siehe oben: VI.4.2.1).

---

nen, wie etwa der Wohngegend und den Titeln, errechnet werden. Siehe hierzu die Entscheidung des DSK vom 28.11.2003, K 211.507/024-DSK/2003, http://www.dsk.gv.at/ presse_herold1.htm sowie die Produkt-Homepage http://www.herold.at/servlet/hbdsite_menu?sd=AH6_11486357435020106&menu=1_2_2_2

5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben (siehe oben: VI.4.2.1).
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat. Dieser Punkt ist ähnlich dem Tatbestand bei nicht-sensiblen Daten mit dem Unterschied, dass hier explizit eine ausdrückliche Zustimmung erforderlich ist: Eine konkludente Einwilligung reicht für sensible Daten nicht aus.
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann. Auch dies ist ähnlich den allgemeinen Ausnahmen, doch darf eine Verarbeitung nur dann erfolgen, wenn das Einholen einer Zustimmung den Zweck der geplanten Verwendung vereiteln würde. Ist die Einholung (noch) möglich, so ist eine Verwendung ausschließlich auf Grund der Zustimmung erlaubt bzw. sonst eben verboten (Selbstbestimmungsrecht[454]).
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist (siehe oben: VI.4.2.1). Hier ist keine Zustimmung notwendig, zusätzlich wäre eine Verweigerung auch unbeachtlich: Für sich selbst kann man Nachteile zugunsten des Datenschutzes in Kauf nehmen, zu Lasten Dritter jedoch nicht.
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden (siehe oben: VI.4.2.1; wohl auch für Gerichte).
10. die Daten für private Zwecke, zur wissenschaftlichen Forschung oder Statistik, zur Benachrichtigung des Betroffenen oder im Katastrophenfall verwendet werden. Für diese Bereiche bestehen Sonderregelungen in den §§ 45-47 und 48a DSG.
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechtes Rechnung zu tragen[455], und sie nach besonderen Rechtsvorschriften zulässig ist. Dies betrifft insbesondere Gesundheitsdaten und in Österreich die Gewerkschaftszugehörigkeit[456].
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verwendung der Daten durch ärztliches Personal oder sonstige Personen mit einer entsprechenden Geheimhaltungspflicht erfolgt.
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten. Nur Daten von Mitgliedern, Förderern oder sonstigen Personen, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben, dürfen verwendet werden. Sie dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden. Hiermit wird es Vereinen erlaubt, die Daten ihrer eigenen Mitglieder oder eng mit ihnen verbundener Personen zu verarbeiten. Da viele

---

[454] Ähnlich bei ärztlicher Behandlung: Jede Person kann jede Behandlung an sich selbst ablehnen; ist dies nicht erfolgt oder keine Äußerung mehr möglich, so hat der Arzt sie jedoch durchzuführen.

[455] Sehr großzügig hier Brodil: Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis. ZAS 2004/28

[456] Gewerkschaftsbeiträge werden u.a. vom Arbeitgeber einbehalten und an die Gewerkschaft abgeführt, weshalb der AG in diesen Fällen natürlich über die Mitgliedschaft informiert sein muss und diese zu speichern hat.

Organisationen existieren, welche Zwecke im Bereich der sensiblen Daten verfolgen, z.B. politische Parteien oder Kirchen, lassen sich aus ihren Mitgliederlisten naturgemäß sensible Daten extrahieren. Solche Daten dürfen nur mit Zustimmung des Betroffenen weitergegeben werden, wenn die Vereinigung selbst sie auch verwalten und für sich, d.h. die Vereinszwecke, verwenden darf.

VI.4.4. Informationspflicht des Auftraggebers

Bei einer Ermittlung von Daten muss der Betroffene in geeigneter Weise über folgende Sachverhalte informiert werden (§ 24 DSG), falls er diese Informationen nicht bereits hat[457]: Der Zweck der Datenanwendung sowie Name und Adresse des Auftraggebers.

In vielen Fällen werden zusätzliche Informationen weiterzugeben sein, um eine Verwendung nach Treu und Glauben (die allgemeinen Grundsätze aus § 6 DSG; siehe oben) zu gewährleisten. Dies ist insbesondere dann der Fall, wenn der Betroffene ein Widerspruchsrecht (siehe VI.3.1.4) gegen die Verarbeitung oder Übermittlung besitzt, oder es für den Betroffenen aus den Umständen nicht klar ist, ob er zur Beantwortung der Fragen rechtlich verpflichtet ist oder nicht.

Keine Informationspflicht besteht für Datenanwendungen gemäß § 17 Abs 2 und 3 DSG. Hierbei handelt es sich um die nicht meldepflichtigen Datenanwendungen, insbesondere Standardanwendungen entsprechend der VO des Bundeskanzlers und u.a. um Datenanwendungen zum Schutz der Republik Österreich, der Einsatzbereitschaft des Bundesheeres und der Vorbeugung oder Verfolgung von Straftaten.

VI.5. Datenverkehr mit dem Ausland

Der Datenverkehr (Übermittlung oder Überlassung; bloße Durchfuhr ist nicht betroffen) mit dem Ausland ist in zwei große Gruppen zu unterteilen: EU und sonstige Staaten. Befindet sich der Empfänger einer Übermittlung in der Europäischen Union, so gibt es keinerlei Beschränkungen im privatrechtlichen Bereich. Bei Auftraggebern des öffentlichen Bereichs betrifft dies jedoch nur Angelegenheiten, die dem Recht der EU unterliegen.

Im Verkehr mit Drittstaaten (=Nicht-EU) ist grundsätzlich eine Genehmigung der Datenschutzkommission notwendig, die auch Auflagen und Bedingungen festsetzen kann. Alle Übermittlungen setzen voraus, dass die Datenanwendung im Inland rechtmäßig ist. In folgenden Ausnahmen ist keine Genehmigung und keine Anzeige an die DSK notwendig:

- Wenn im Empfängerstaat ein angemessener Datenschutz besteht. Welche Staaten dies sind, wird per Verordnung des Bundeskanzlers[458] bzw. Feststellung der Kommission[459]

---

[457] So geht z.B. bei einer schriftlichen Bestellung auf einem Formular eines Versenders schon aus den Umständen hervor, dass Name, Adresse etc. zum Zweck der Bestellungsbearbeitung verarbeitet werden sollen. Ebenso ist der Auftraggeber bekannt (=der Versender). Hier ist keine gesonderte Information notwendig. Anders jedoch, wenn die Daten auch an zusätzliche Firmen weitergegeben oder auch für andere Zwecke verwendet werden sollen!

[458] Schweiz, Ungarn (inzwischen gegenstandslos): Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV). BGBl. II Nr. 521/1999

[459] Siehe http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm Aktueller Stand: Argentinien, Kanada, Schweiz, USA (Nur Safe Harbor und Fluggastdatensätze; nicht allgemein!), Guernsey, Isle of Man. Das Abkommen über die Weitergabe der Fluggastdatensätze wurde aber vom EuGH gekippt: Der zugehörige Ratsbeschluss und die Kommissionsentscheidung wurden für nichtig erklärt. Das Abkommen ist daher zu kündigen. Urteil des EuGH vom 30.5.2006, C-317/04 (verbunden mit C-318/04)

bestimmt. Ob ein entsprechendes Niveau vorliegt, ist an der Ausgestaltung der allgemeinen Grundsätze (siehe VI.4.1) und der Möglichkeit ihrer Durchsetzung zu messen.

- Wenn die Daten im Inland zulässigerweise veröffentlicht wurden. Dies muss nicht durch den Betroffenen selbst, aber jedenfalls rechtmäßig erfolgt sein.
- Falls die Daten für den Empfänger nur indirekt personenbezogen sind. Wenn sie daher für den Absender direkt personenbezogen sind, der Empfänger jedoch nur einen Teil der Daten erhält oder ihm andere Daten fehlen, sodass sie für ihn nur mehr indirekt personenbezogen sind, besteht durch die Übermittlung keine besondere Gefahr.
- Ist die Übermittlung/Überlassung von Daten ins Ausland in innerstaatlichen Gesetzen (des Quell-Landes) mit direkter Anwendbarkeit vorgeschrieben, so ist dies erlaubt.
- Die Übermittlung erfolgt für private oder publizistische Zwecke.
- Wenn der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat. Es ist zu beachten, dass eine Zustimmung zur Verwendung und Übermittlung normalerweise eine Übermittlung in Drittstaaten nicht mit einschließt. Dafür ist aus den Umständen (konkludent) oder explizit eine gesonderte Zustimmung notwendig.
- Wenn ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann. Beachtenswert ist, dass lediglich "irgendwie" im Interesse des Betroffenen abgeschlossene Verträge nicht zu einer Verwendung der Daten ermächtigen, sondern die Eindeutigkeit dieses Interesses gefordert ist, um Schutzbehauptungen zu vermeiden.
- Erlaubt ist die erforderliche Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden, wenn die Daten rechtmäßig ermittelt wurden.
- Wenn die Übermittlung oder Überlassung in einer Standardverordnung oder Musterverordnung (siehe VI.6.1.1) ausdrücklich angeführt ist. In diesen Verordnungen sind explizit für jedes Datum die Empfängerkreise angeführt sowie ob diese sich auch in Drittländern (d.h. außerhalb der EU) befinden dürfen (dort durch "*" gekennzeichnet).
- Datenverkehr mit österreichischen Dienststellen im Ausland ist nicht betroffen. Die Daten verlassen zwar physikalisch Österreich, befinden sich jedoch immer noch in österreichischem Einflussbereich. Eine Gefährdung ist daher nicht zu befürchten, da auch diese Dienststellen das DSG anzuwenden haben.
- Übermittlungen oder Überlassungen aus Datenanwendungen, die gemäß § 17 Abs 3 DSG von der Meldepflicht ausgenommen sind, können ebenso in Drittstaaten erfolgen. Hierbei handelt es sich um Datenanwendungen zum Schutz des Staates, der Landesverteidigung, wirtschaftlicher und außenpolitischer Interessen Österreichs und der EU und für Vorbeugung, Verhinderung und Verfolgung von Straftaten (siehe VI.3.3.5).
- Wenn zwar eine Genehmigung zur Übermittlung notwendig wäre, diese aber nicht ohne Gefährdung bestimmter Interessen eingeholt werden kann. Ein solches Vorgehen muss jedoch der Datenschutzkommission angezeigt werden; eine Genehmigung ist jedoch dann nicht erforderlich. Nur für folgende Zwecken ist eine Übermittlung erlaubt: Zur Wahrung eines wichtigen öffentlichen Interesses oder zur Wahrung eines lebenswichtigen Interesses einer Person. Die DSK-Kontrolle wird daher von einer Vorab- zu einer Nachkontrolle umgewandelt.

Ein Einstellen in das Internet selbst bedeutet zwar eine automationsunterstützte Datenverarbeitung und eine weltweite Veröffentlichung[460], jedoch *keine* Übermittlung an das Ausland[461]. Dies entspricht auch den technischen Gegebenheiten, wonach der eigentliche Transfer durch den jeweils konkret Abfragenden erfolgt.

VI.6. Rechtsdurchsetzung

Um Betroffenen die Möglichkeit zu geben herauszufinden, welche Datenarten von wem über sie verarbeitet werden, wird bei der Datenschutzkommission ein Register aller Datenanwendungen geführt[462]. Weiters wird in diesem Abschnitt noch die Beschwerde bei der Datenschutzkommission, und der Unterschied zur Anregung einer Kontrolle durch diese, sowie Schadenersatzregelungen erläutert.

VI.6.1. Anmeldung beim Datenverarbeitungsregister

Die Datenschutzkommission (DSK) führt ein Register aller Datenanwendungen in Österreich. Grundsätzlich müssen alle Datenanwendungen vor ihrer Aufnahme dort angemeldet werden, inklusive späterer Änderungen oder Ergänzungen, sofern nicht eine der Ausnahmen vorliegt. Dieses Register ist öffentlich zugänglich. Ist man Betroffener und stehen dem keine schutzwürdigen Interessen des Auftraggebers oder Dritter entgegen, so ist auch Einsicht in den Registrierungsakt einschließlich der darin enthaltenen Bescheide möglich. Eine Meldung für das Register muss auch automationsunterstützt erfolgen können. Leider ist nicht vorgesehen, dass auch die Einsicht auf diese Weise durchzuführen sein muss; sie könnte aber so erfolgen.

Nicht meldepflichtig und daher nicht im Register enthalten sind Datenanwendungen, die

- ausschließlich veröffentlichte Daten enthalten. Da für diese Daten kein Geheimhaltungsanspruch besteht, ist eine besondere Publizität der Anwendung entbehrlich. Wie in Abschnitt VI.4.2.2 erläutert, ist jedoch streng zu prüfen, ob wirklich *ausschließlich* veröffentlichte Daten enthalten sind, oder auch Auswertungen aus veröffentlichten Daten oder "private" Informationen, durch welche sich eine Meldepflicht ergibt.
- von Gesetz wegen eingerichtete öffentliche Register zum Inhalt haben. Die Einsicht muss nicht völlig öffentlich, aber zumindest bei Nachweis eines berechtigten Interesses möglich sein. Ansonsten besteht Meldepflicht. Eine Meldung ist bei öffentlichen Registern nicht nötig, da deren Existenz als bekannt vorauszusetzen ist (es existiert ein Gesetz, auf dem es beruht) und sich jeder durch Abfrage von dem exakten Datenumfang informieren kann: Das Auskunftsrecht ist gleichzeitig mit enthalten.
- einer Standardanwendung entsprechen: Siehe separater Abschnitt unten.
- nur indirekt personenbezogene Daten enthalten. Da kein Geheimhaltungsanspruch besteht, ist auch eine Meldung nicht sinnvoll. Das Datenverarbeitungsregister soll insbesondere das Auskunftsrecht ermöglichen: Dieses ist bei nur indirekt personenbezogenen Daten ausgeschlossen, da ja der Auftraggeber alleine keine Verbindung zu einer be-

[460] "Hausbesorgerdaten im Internet": OLG Innsbruck 27.9.1999, 1 R 143/99k und 28.3.2000, 1 R 30/00x. Mit Anmerkungen von Thiele, http://www.eurolawyer.at/pdf/OLG_Innsbruck_1_R_30-00x.pdf

[461] "Bodil Lindqvist": EuGH 6.11.2003, Rs C-101/01 http://www.jurpc.de/rechtspr/20040030.htm Siehe dazu auch Hörlsberger: Veröffentlichung personenbezogener Daten im Internet. ÖJZ 2004/45

[462] Trotzdem heißt es aus historischen Gründen "Datenverarbeitungsregister" und nicht "Datenanwendungsregister".

stimmten Person herstellen und damit auch dieser keine Auskunft erteilen kann. Eine Registrierung wäre deshalb sinnlos und ist nicht notwendig.

Laut § 17 Abs 3 DSG sind zusätzlich Datenanwendungen für folgende Zwecke von der Meldepflicht ausgenommen, wenn dies zu ihrer Zweckverwirklichung notwendig ist: Schutz der Republik Österreich, der Einsatzbereitschaft des Bundesheeres und der Vorbeugung und Verfolgung von Straftaten (siehe zu sonstigen Ausnahmen unter VI.3.3.5)

Bestimmte Anwendungen werden als gefährlicher angesehen und dürfen erst nach erfolgreicher Prüfung durch die DSK gestartet werden. Dazu zählen Datenanwendungen mit sensiblen oder strafrechtlich relevanten Daten, Auskunftserteilung über die Kreditwürdigkeit sowie Informationsverbundsysteme. Sofort mit derartige Datenanwendungen begonnen werden darf doch, wenn sie einer Musteranwendung entsprechen, innere Angelegenheiten einer Religionsgemeinschaft betreffen oder im Katastrophenfall eingesetzt werden.

Nach der ersten Anmeldung beim Datenverarbeitungsregister[463] erhält jeder Auftraggeber eine Datenverarbeitungsregister-Nummer (DVR-Nummer; sieben Stellen, führende Nullen sind signifikant). Diese muss bei Übermittlungen an Betroffene angegeben werden, also z.B. auf Rechnungen, E-Mails etc.

VI.6.1.1. Inhalt der Meldung

Die Meldung einer Anwendung an die DSK muss folgende Elemente enthalten:

- Name und Anschrift des Auftraggebers. Besitzt der Auftraggeber bereits eine Registernummer, so ist diese zur Vereinfachung anzuführen.
- Nachweis der gesetzlichen Zuständigkeit (öffentlicher Bereich) oder der rechtlichen Befugnis (privater Bereich; meist Gewerbeberechtigung) für die erlaubte Ausübung der Tätigkeit des Auftraggebers. Dies ist nur notwendig, wenn eine solche Befugnis erforderlich ist.
- Der Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit diese sich nicht bereits aus der Befugnis ergeben. Der Zweck ist genau anzugeben, da er für die Beurteilung, ob später eine Übermittlung vorliegt oder nicht bzw. eine konkret durchzuführende Verarbeitung erlaubt ist, ausschlaggebend ist.
- Die Kreise der von der Datenanwendung Betroffenen, d.h. wessen Daten verarbeitet werden. Klarerweise ist nur eine ungefähre Umschreibung erforderlich, z.B. "Kunden".
- Die verarbeiteten Datenarten. Typischerweise die einzelnen Felder, die in der geplanten Datenbank enthalten sein sollen, mit ihrer genauen Inhaltsbeschreibung.
- Handelt es sich um die Meldung einer Übermittlung ist anzugeben, welche Betroffenenkreise enthalten sein sollen, die zugehörigen Empfängerkreise einschließlich allfälliger ausländischer Empfangsstaaten sowie die Rechtsgrundlagen der Übermittlungen.
- Ist eine Genehmigung der Datenschutzkommission notwendig, so ist die Geschäftszahl der Genehmigung anzuführen.
- Allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen, die eine Beurteilung der Angemessenheit erlauben. Im Gegensatz zu den vorherigen Punkten sind diese Angaben im Register jedoch nicht öffentlich einsehbar.

[463] Keine DVR-Nummer besitzt daher derjenige, der *ausschließlich* Standardanwendungen durchführt!

VI.6.1.2. Musteranwendungen

Der Bundeskanzler kann per Verordnung Musteranwendungen[464] definieren, welche eine Anmeldung vereinfachen. Hier handelt es sich um anmeldungspflichtige Datenanwendungen, die oft in identischer Form vorkommen. Darin liegt lediglich eine Vereinfachung des Verfahrens, denn materiell sind alle Bestimmungen über eine Anmeldung anzuwenden. Man kann dies als eine Art "vorausgefülltes Anmeldungsformular" ansehen.

Eine Anmeldung entsprechend einer Musteranwendung darf nur dann erfolgen, wenn nicht mehr als die darin enthaltenen Daten, Verwendungen und Übermittlungen vorgesehen sind, also eine (echte) Teilmenge. Zu dieser genügt dann die Bezeichnung gemäß der Musteranwendung, Name und Anschrift des Auftraggebers, der Nachweis seiner Befugnis zur Verarbeitung, falls erforderlich, und ev. die Registernummer des Auftraggebers.

VI.6.1.3. Standardanwendungen

Für jene Fälle, in welchen Datenanwendungen mit demselben Inhalt oder Übermittlungen aus diesen von vielen Auftraggebern in gleicher Weise und routinemäßig durchgeführt werden sowie gleichzeitig inhaltlich die schutzwürdigen Geheimhaltungsinteressen voraussichtlich nicht gefährdet werden, kann der Bundeskanzler per Verordnung eine Standardanwendung schaffen, wodurch die Meldepflicht entfällt. Es werden darin sowohl die Kreise der Betroffenen, bei Übermittlungen inklusive möglicher Empfänger, als auch die zulässigen Datenarten und die Höchstdauer der Aufbewahrung festgelegt. Eine Registrierung im Datenverarbeitungsregister ist nicht mehr notwendig, da die Durchführung solcher Anwendungen jeder in einer bestimmten Situation voraussetzen muss. Ein Beispiel hierfür ist die Führung einer automationsunterstützten Buchhaltung. Es ist deshalb nicht notwendig, die Betroffenen durch eine explizite Meldung beim Datenverarbeitungsregister darauf hinzuweisen. Um aber das Auskunftsrecht auch hier sicher zu gewährleisten ist jeder Auftraggeber verpflichtet, jedermann, d.h. nicht nur Betroffenen, mitzuteilen, welche Standardanwendungen tatsächlich durchgeführt werden. Diese Auskunft ist also unabhängig von der Eigenschaft als Betroffener: Bei der Anfrage kann man noch nicht wissen, ob man ein solcher ist oder nicht, da dies von den konkret durchgeführten Anwendungen abhängt.

VI.6.2. Gerichtliche Geltendmachung

Ein Betroffener hat Anspruch auf Unterlassung und Beseitigung eines dem Datenschutzgesetz widersprechenden Zustandes, u.a. durch Richtigstellung, Löschung und Schadenersatz. Ist der Verursacher ein Auftraggeber des privaten Bereichs, so sind diese Ansprüche vor den ordentlichen Gerichten durchzusetzen.

Zuständig ist in erster Instanz das Landesgericht, in dessen Sprengel der gewöhnliche Aufenthalt des Betroffenen, bzw. bei juristischen Personen der Sitz, liegt. Der Betroffene kann jedoch auch die Möglichkeit wählen, Klage bei dem Gericht zu erheben, in dessen Sprengel der Auftraggeber oder Dienstleister seinen gewöhnlichen Aufenthalt/Sitz hat.

Die Datenschutzkommission muss einem Verfahren als Nebenintervenient beizutreten, wenn der Betroffene dies verlangt und es zur Wahrung der Interessen einer größeren Zahl von Betroffenen geboten ist. Hierbei ist vor allem an Musterprozesse oder Prozesse gegen

[464] Praktisch bedeutsam dürfte die Musteranwendung MA 002 sein: Zutrittskontrollsysteme. http://www.dsk.gv.at/ma002.htm Dies betrifft physische Sicherheit. Passwörter und Ähnliches fallen unter die Standardanwendung SA 007 (Verwaltung von Benutzerkennzeichen) http://www.dsk.gv.at/sa007.htm

große Auftraggeber mit entsprechend besseren Möglichkeiten der Datenschutzkommission, z.B. Privatgutachten bzw. Expertise, zu denken.

VI.6.3. Beschwerde bei der Datenschutzkommission

Es ist zwischen einer Beschwerde an die Datenschutzkommission (§ 31 DSG) und der Anregung einer Kontrolle (§ 30 DSG; siehe Abschnitt VI.7.2) zu unterscheiden: Im ersten Fall hat sie eine quasi-richterliche Entscheidungsfunktion, während bei einer Kontrolle lediglich eine amtswegige Überprüfung ohne Anspruch auf Durchführung oder ein bestimmtes Ergebnis vorgeschlagen wird.

Die Zuständigkeit der Datenschutzkommission umfasst Verletzungen des Auskunftsrechts, auch durch Auftraggeber des privaten Bereichs, sowie alle Verletzungen durch Auftraggeber des öffentlichen Bereichs. Handelt es sich um Handlungen, die nach funktionalen Gesichtspunkten entweder der Gerichtsbarkeit oder der Gesetzgebung[465] zuzurechnen sind, so ist die DSK unzuständig. Es verbleibt daher nur mehr die Verwaltung, allerdings inklusive der obersten Organe[466]. Die Datenschutzkommission kann auch einstweilige Verfügungen mit dem Inhalt treffen, dass eine weitere Verwendung der Daten untersagt wird oder ein Bestreitungsvermerk anzubringen ist. Erfolgt eine Beschwerde wegen Daten, die nicht dem Auskunftsrecht unterliegen[467], so ist während des Verfahrens die Geheimhaltung nur gegenüber dem Betroffenen zu wahren: Gegenüber der DSK besteht kein Recht auf eine solche. Ist die Beschwerde im Ergebnis nicht gerechtfertigt, so ist eine Offenlegung per Bescheid (Beschwerde an den VwGH ist möglich) anzuordnen. Erfolgt diese nicht binnen acht Wochen, so wird die Auskunft der Daten, bzw. welche Berichtigung oder Löschung erfolgte, von der Datenschutzkommission selbst vorgenommen. Ist die Geheimhaltung gerechtfertigt, so erfolgt lediglich die Auskunft, dass eine Überprüfung und ev. Berichtigung vorgenommen wurde.

VI.6.4. Schadenersatzregelung

Grundsätzlich gelten die allgemeinen Bestimmungen über Schadenersatz bzw. Amtshaftung[468]. Dies bedeutet, dass nur bei Verschulden eine Haftung eintritt. In besonderen Fällen wird jedoch auch (normalerweise nicht ersatzfähiger!) immaterieller Schaden[469] ersetzt: Handelt es sich um die öffentlich zugängliche Verwendung von sensiblen, strafrechtlich relevanten oder die Kreditwürdigkeit betreffenden Daten[470] und wird dadurch eine Bloßstellung im Sinne des Mediengesetzes (§ 7 Abs 1 MedienG) verwirklicht, so fällt die dort nötige Veröffentlichung in einem Medium als Tatbestandsmerkmal weg. Sowohl rechtsmissbräuchliche wie auch fehlerhafte Datenverwendung kann diese Folge auslösen.

---

[465] Siehe Bericht des Verfassungsausschusses, welche Teile der Parlamentsverwaltung der Kontrolle der Datenschutzkommission unterstehen sollen. Diese Aufzählung hat freilich keinen verbindlichen Charakter. Zur Gesetzgebung gehört z.B. auch der Rechnungshof. Dies entsprich der Richtlinie, da diese im Bereich der Gesetzgebung und der Gerichtsbarkeit nicht anwendbar ist: Dies ist einzelstaatlicher Bereich und nicht Angelegenheit der EU.

[466] D.h. selbst Minister werden von der DSK geprüft. Deren Entscheidungen (Verordnungen, Bescheide, ...) sind ansonsten innerhalb der Verwaltung, zu der auch die DSK gehört, nicht mehr überprüfbar. Hiergegen steht nur mehr die Gerichtsbarkeit zur Verfügung (VwGH, VfGH).

[467] Schutz der Republik etc.

[468] Siehe auch Lukas: Schadenersatz bei Verletzung der Privatsphäre. RZ 2004, 33

[469] Gemäß § 6 und 7 MedienG: Derzeit maximal € 20.000

[470] Siehe OGH 15.12.2005, 6 Ob 275/05t mit Anmerkungen von Knyrim, MR 2006, 83

Zugunsten des Betroffenen wurde eine Beweislastumkehr geschaffen und die Haftung beim Auftraggeber bzw. Dienstleister konzentriert: Sie haften auch für das Verhalten ihrer Gehilfen und Angestellten, welche sie mit der Verarbeitung beauftragt haben. Der Auftraggeber kann sich von der Haftung befreien indem er nachweist, dass der Umstand, der den Schaden verursachte, nicht ihm bzw. seinen Mitarbeitern zur Last gelegt werden kann. Gleiches gilt für Dienstleister. Zuständig ist das gleiche Gericht wie für Klagen gegen private Auftraggeber wegen Verletzung der Rechte des Betroffenen.

VI.6.5. Gerichtliche Strafbestimmung

Gegenüber dem alten Datenschutzgesetz aus 1980 wurden die gerichtlichen Strafbestimmungen stark ausgedünnt, da sich zeigte, dass sie einerseits fast nicht zu verwirklichen waren, bzw. zu einer Kriminalisierung des Großteils aller Datenverarbeiter führen könnten. Dafür wurden Verwaltungsstrafen eingeführt, die diesen Ausfall ersetzen bzw. ergänzen.

Gerichtlich strafbar mit Freiheitsstrafe bis zu einem Jahr bleibt lediglich die rechtswidrige Verwendung von personenbezogenen Daten in besonders verwerflicher Absicht[471]: Um sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Schaden[472] zuzufügen. Voraussetzung dabei ist, dass es sich um personenbezogene Daten handelt, an denen der Betroffene ein schutzwürdiges Geheimhaltungsinteresse (§ 8, 9 DSG) besitzt. Diese Daten müssen dem Täter ausschließlich durch seine berufliche Tätigkeit anvertraut oder bekannt geworden sein bzw. er hat sich diese widerrechtlich verschafft. Die Tathandlung besteht darin, Daten zu "benützen" (ohne nähere Definition im Gesetz), sie insbesondere anderen zugänglich zu machen oder zu veröffentlichen. Es handelt sich um ein Ermächtigungsdelikt, der Täter darf daher nur mit Zustimmung des Verletzten verfolgt werden.

Zu beachten ist, dass kein Bezug auf *automatisierte* Verarbeitung erfolgt. Das Delikt kann daher mit jeder Art personenbezogener Daten begangen werden, unabhängig davon, wie sie verarbeitet werden (Computer, Kartei), oder ob sie überhaupt gespeichert werden.

Eine Verletzung des Datenschutzes, weder hinsichtlich einer gerichtlich strafbaren Handlung noch einer Verwaltungsstrafe, führt nicht zu einem Beweisverwertungsverbot[473], was in vielen praktischen Fällen von Bedeutung sein kann.

VI.6.6. Verwaltungsstrafen

Die Verwaltungsstrafbestimmungen sind in zwei Gruppen eingeteilt: Tatbestände, bei denen eine tatsächliche Verletzung stattgefunden hat und solche, bei denen zwar noch keine Verletzung vorliegt, aber zumindest die Gefahr dafür, oder für eine Behinderung der Durchsetzbarkeit der Betroffenen-Rechte, besteht. Bei allen Taten ist der Versuch strafbar.

---

[471] Siehe LG Linz 7. 12. 1999, 27 E Vr 591/99, 27 Hv 123/99, ARD 5120/27/2000: Das Kopieren von Kunden- und Lieferantendaten durch einen ausscheidenden Arbeitnehmer würde dieser Bestimmung unterfallen. Im konkreten Fall war sie nicht anzuwenden, da zum Tatzeitpunkt das neue DSG noch nicht in Kraft war (keine Rückwirkung bei strafrechtlichen Bestimmungen!).

[472] Ein Vorteil muss das Vermögen betreffen, Schäden sind jedoch ganz allgemein zu betrachten, sodass auch immaterielle Schäden hiervon erfasst sind.

[473] Führt aber zu einer Strafbarkeit nach dem Datenschutzgesetz, was auch Schadenersatz beinhalten kann! U.U. ist die Verletzung des Datenschutzes sogar sanktionslos, falls die Verletzung aus Notwehr erfolgte, d.h. dies die einzige Möglichkeit ist, das eigene Recht zu beweisen.

Für die Verfolgung ist die Bezirksverwaltungsbehörde des Bezirks zuständig, in dem der Auftraggeber der Datenverarbeitung seinen gewöhnlichen Aufenthalt bzw. Sitz hat. Es kommt also nicht darauf an, wo die Daten verarbeitet wurden, noch wo die geschädigte bzw. die potentiell in ihren Rechten gefährdeten Person(en) ihren Sitz haben. Letzteres deshalb, da in vielen Fällen die Anzahl der Verletzten oder Gefährdeten sehr groß ist und das Verwaltungsstrafverfahren ohnehin amtswegig durchgeführt wird: Partei ist nur der Beschuldigte, nicht die Betroffenen. Zusätzlich zur Geldstrafe kann der Verfall von Datenträgern und Programmen ausgesprochen werden, die im Zusammenhang mit der strafbaren Handlung stehen. Dies soll dazu dienen, die widerrechtlich erlangten/erstellten personenbezogenen Daten bzw. deren Auswertungen dem Täter sicher zu entziehen, ebenso wie die dafür verwendeten Programme. Die Datenverarbeitungsanlagen selbst (=Computer) können jedoch nicht für verfallen erklärt werden: Höchstens Festplatten könnten als Datenträger entfernt werden[474].

VI.6.6.1. Konkrete Verletzungen

Diese Straftaten sind subsidiär zu strengeren Verwaltungsstrafen sowie gerichtlichen Straftaten. Die Strafdrohung ist mit Geldstrafe bis € 18.890 relativ hoch. Strafbar ist:

- wer sich vorsätzlich und widerrechtlich Zugang zu einer Datenanwendung verschafft. Dies entspricht dem klassischen "Hacken" von Rechnern. Es ist hierbei unerheblich, ob auch tatsächlich personenbezogene Daten ausspioniert wurden. Lediglich relevant ist, dass jemand sich die Möglichkeit dazu verschaffte. Aufgrund der Definition von "Daten" in § 4 Abs 1 DSG müssen jedoch in der Anwendung personenbezogene Daten verarbeitet werden. "Zeitdiebstahl" ist daher auch hier nicht erfasst. Nur wer vorsätzlich versucht, in personenbezogene Daten Einsicht zu nehmen, ist strafbar.
- wer einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält. Darunter fällt beispielsweise das Arbeiten an einem Terminal, auf dem personenbezogene Daten verarbeitet werden, was ermöglicht wurde, indem der vorherige Benutzer sich nicht ausloggte. Wenn daher jemand erkennt, dass Zugang zu personenbezogenen Daten besteht, obwohl dieser nicht offen sein dürfte, so ist man verpflichtet, ihn zu schließen oder schließen zu lassen, und währenddessen keine Kenntnis von den Daten oder irgendeinen Einfluss auf die Verarbeitung zu nehmen. Arbeitsrechtlich besteht hier eine aktive Hinweispflicht an den Arbeitgeber.
- wer Daten vorsätzlich in Verletzung des Datengeheimnisses übermittelt. Hierzu reicht es bereits aus, wenn die Daten eines einzigen Betroffenen übermittelt werden. Es ist zu beachten, dass bereits die Verwendung von Daten für einen anderen Zweck eine Übermittlung darstellt und daher strafbar ist. Sowohl Indiskretionen als auch kommerzieller Verkauf verletzen das Datengeheimnis und fallen unter diese Bestimmung.
- wer Daten trotz rechtskräftigem Urteil oder Bescheid verwendet, keine Auskunft dazu erteilt, nicht richtig stellt oder die Löschung unterlässt. Hierbei handelt es sich um eine zusätzliche Maßnahme, die rasche und vollständige Erfüllung von festgestellten Pflichten zu erzwingen. Dies ersetzt nicht die normale Durchsetzung von Urteilen oder Bescheiden, sondern ist u.U. eine zusätzliche Strafe.
- wer Daten vorsätzlich löscht, obwohl er bereits Kenntnis von einem Auskunftsverlangen oder der Erhebung einer Beschwerde bei der Datenschutzkommission hat. Dies soll die Vernichtung von Beweismitteln verhindern. Es stellt sich jedoch wie bei allen el. Be-

[474] Hierbei stellt sich ev. ein Problem mit darauf enthaltenen rechtmäßigen Daten.

weismitteln insbesondere die Frage, wie sich nachweisen lässt, dass sie zu einem früheren Zeitpunkt existierten und zu einem bestimmten späteren Zeitpunkt gelöscht wurden. Eine solche Möglichkeit bieten z.B. Backups oder Logs.

- wer sich unter Vortäuschung falscher Tatsachen Daten verschafft, die im Katastrophenfall erleichtert weitergegeben bzw. übermittelt werden dürfen.

VI.6.6.2. Gefährdungen von Rechten oder deren Durchsetzbarkeit

Diese Straftaten sind wieder subsidiär zu gerichtlichen Straftaten, aber zusätzlich zu anderen Verwaltungsstraftaten. Die Sanktion ist eine Geldstrafe bis € 9.445. Strafbar ist:

- die Ermittlung, Verarbeitung oder Übermittlung von Daten, ohne dass die Meldepflicht erfüllt wurde. Ist eine solche gegeben (Ausnahmen siehe Abschnitt VI.6.1), so darf in den meisten Fällen unmittelbar nach dieser Meldung der Betrieb aufgenommen werden. Erfolgt jedoch keine oder darf der Betrieb erst nach einer Genehmigung starten (§ 18 Abs 2 DSG) und wird dennoch sofort begonnen, so ist dieser Tatbestand verwirklicht. Auch eine Überschreitung der Meldung fällt hierunter.
- die Übermittlung von Daten ins Ausland, obwohl dafür eine Genehmigung der Datenschutzkommission notwendig gewesen wäre und diese nicht eingeholt wurde. Hiermit soll sichergestellt werden, dass Übermittlungen nur dann erfolgen, wenn diese auch tatsächlich geprüft und genehmigt wurden. Nur wenn die Übermittlung voll genehmigungsfähig ist, gilt dieses Delikt, ansonsten ist die oben erläuterte schärfere Bestimmung anzuwenden (tatsächliche Verletzung; hier: bloße Gefährdung).
- die Verletzung der Offenlegungsvorschriften. Darunter fallen die Auskunft über vorgenommene Standardanwendungen an Benutzer und nicht-meldepflichtiger Anwendungen gegenüber der Datenschutzkommission (§ 23 DSG), Verletzungen der Informationspflicht des Auftraggebers gegenüber den Betroffenen (§ 24 DSG) und die Offenlegung der Identität des Auftraggebers (§ 25 DSG). In diesem Tatbestand sind Verletzungen der Vorschriften enthalten, welche die Durchsetzbarkeit der Rechte der Betroffenen schmälern: Wenn man nicht weiß, wer genau welche Daten über einen besitzt oder verarbeitet, kann man dies auch nicht auf Rechtmäßigkeit untersuchen oder per Beschwerde überprüfen lassen.
- die gröbliche Außerachtlassung der erforderlichen Sicherheitsmaßnahmen. Hiermit soll verhindert werden, dass durch schwere Verletzungen der Sorgfalt beim Umgang mit Daten ein unbefugter Zugriff viel leichter möglich ist. Das Delikt ist daher bereits dann verwirklicht, wenn aufgrund mangelnden Schutzes die Gefahr für eine unrechtmäßige Verarbeitung sehr groß ist, aber (noch) keine solche tatsächlich erfolgte. Dies bestraft daher mangelnde technische oder organisatorische Sicherheitsvorkehrungen.

VI.7. Die Datenschutzkommission

Im Vergleich zum lediglich beratend tätigen Datenschutzrat spielt die Datenschutzkommission eine wichtige Rolle im Gefüge des Datenschutzes. Sie ist zur Wahrung der Rechte aufgrund des DSG berufen und besitzt echte Kontroll- und Entscheidungsbefugnisse.

Im Gegensatz zu den normalen Grundsätzen der Bundesverfassung ist sie auch zur Kontrolle der obersten Organe der Vollziehung ermächtigt, daher ist dies auch eine Verfassungsbestimmung. Die Besonderheit liegt darin, dass Bundespräsident, Bundesminister

und Mitglieder der Landesregierung ihrer Kontrolle unterliegen, was sonst bei derartigen *obersten* Organen begrifflich ausgeschlossen ist (die sie sonst nicht wären).

In Ausübung ihres Amtes sind die Mitglieder der Datenschutzkommission weisungsfrei. Dies ist eine Verfassungsbestimmung wegen der ihr eingeräumten Kontrollbefugnisse. Für ihre Entscheidungen würde sich die Weisungsfreiheit zusätzlich aus Art. 20 Abs 2 B-VG ergeben. Administrativ ist sie jedoch dem Bundeskanzleramt zu- und untergeordnet.

VI.7.1. Zusammensetzung

Die Datenschutzkommission besteht aus sechs Mitgliedern, welche für die Dauer von fünf Jahren vom Bundespräsidenten auf Vorschlag der Bundesregierung bestellt werden. Dabei bestehen folgende Vorschlagsrechte:

- Dreiervorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied, das den Vorsitz führt
- Vorschlag der Länder für zwei Mitglieder
- Dreiervorschlag der Arbeiterkammer für ein Mitglied
- Dreiervorschlag der Wirtschaftskammer für ein Mitglied
- Ein Mitglied muss dem Kreis der rechtskundigen Bundesbeamten angehören

Zusätzlich ist für jedes Mitglied ein Ersatzmitglied zu bestellen, welches bei Verhinderung dessen Stelle einnimmt. Seine Funktionsperiode entspricht der des vertretenen Mitgliedes. Ein Ausschluss eines Mitgliedes aus schwerwiegenden Gründen oder wegen wiederholtem unentschuldigtem Fernbleiben ist nur durch Beschluss der Kommission selbst möglich. Die Mitglieder (Ersatzmitglieder nur bei Vertretung) haben Anspruch auf Abgeltung der Reisekosten und einer dem Arbeitsaufwand entsprechenden Vergütung, die vom Bundeskanzler per VO festgelegt wird. Die Kommission gibt sich ihre Geschäftsordnung selbst.

Beschlüsse erfolgen mit einfacher Mehrheit, wobei bei Stimmengleichheit die Stimme des Vorsitzenden den Ausschlag gibt. Eine Stimmenthaltung ist unzulässig. Im Gegensatz zum Datenschutzrat ist die Beifügung von Minderheitenvoten nicht möglich.

VI.7.2. Kontrollbefugnisse

Die Datenschutzkommission kann in zwei Fällen eine Kontrolle der Datenverarbeitung vornehmen: Wenn eine Person eine Verletzung ihrer Rechte oder die Verletzung sie betreffender Pflichten eines Datenverarbeiters behauptet sowie in bestimmten Fällen[475] auch ohne Verdacht. Wird auf Anzeige einer Person hin untersucht oder eine solche Untersuchung abgelehnt, so ist die betroffene Person über das Ergebnis bzw. den Grund der nicht erfolgten Kontrolle zu informieren.

Im Fall des begründeten Verdachtes der Verletzung der Rechte einer Person kann (hier wohl im Sinn von "muss" gebraucht) die Datenschutzkommission die Datenanwendung überprüfen. Dazu kann sie alle notwendigen Aufklärungen vom Verarbeiter verlangen, selbst Einschau nehmen und sogar Verarbeitungen durchführen. Um dies zu ermöglichen,

[475] Bei Anwendungen, die der Vorabkontrolle gem. § 18 Abs 2 DSG unterliegen: Keine Musteranwendung und u.a. Verarbeitung sensibler oder strafrechtlicher Daten oder Daten, welche die Kreditwürdigkeit betreffen. In diesen Fällen darf der Betrieb erst nach der Prüfung aufgenommen werden; ansonsten unmittelbar nach Abgabe der Meldung.

ist es ihr gestattet, die Räume, in denen die Datenverwendung stattfindet, nach Verständigung des Inhabers zu betreten und auch Kopien von Datenträgern herzustellen. Letzteres jedoch nur in dem Umfang, wie es zur Kontrolle des konkreten Vorfalles bzw. etwaiger sich aus dem Laufe der bisherigen Durchführung der Kontrolle ergebenden weiteren Anhaltspunkte erforderlich ist. Diese Kontrolle ist unter größtmöglicher Schonung der Rechte des Auftraggebers, z.B. nur innerhalb der Betriebszeiten, und Dritter, etwa der Behinderung der Verarbeitung von deren Daten durch Beanspruchung der Rechenanlagen wegen der Kontrolle, durchzuführen.

Bezüglich der bei einer Kontrolle gewonnenen Informationen, welche nicht die Anzeige bzw. den Verdacht oder sonstige datenschutzrechtliche Vorschriften betreffen, besteht eine strenge Verschwiegenheitspflicht, sowohl gegenüber Gerichten wie auch Verwaltungsbehörden[476]. Es ist jedoch zu beachten, dass bei Verletzung dieser Vorschrift die Information dennoch verwendet werden darf (kein Verwertungsverbot!). Folgende Ausnahmen von dem Verwertungsverbot solcherart erlangter Informationen bestehen:

- Eine gerichtlich oder verwaltungsbehördlich strafbare Handlung gegen das DSG wird aufgedeckt oder es ergeben sich Hinweise darauf (§§ 51 und 52 DSG; siehe oben).
- Es kommen Anhaltspunkte für eine strafbare Handlung zutage, welche mit mehr als 5 Jahren Freiheitsstrafe bedroht ist.
- Indizien für ein Verbrechen nach § 278a StGB (Kriminelle Organisation) kommen bei der Überprüfung hervor[477].

Tritt ein Verdacht für eine dieser Handlungen während der Kontrolle auf, so ist Anzeige zu erstatten und entsprechende Auskunftsbegehren von Gerichten zu beantworten.

Falls bei der Kontrolle sonstige Unregelmäßigkeiten oder Verstöße hervorkommen, so kann die Datenschutzkommission eine Empfehlung aussprechen, wie diese Missstände behoben werden können. Solche Mitteilungen sind mit einer angemessenen Frist auszustatten. Wird ihr nicht oder nicht rechtzeitig entsprochen, so stehen der Datenschutzkommission die folgenden Möglichkeiten offen:

- Ein Verfahren zur amtswegigen Berichtigung des Datenverarbeitungsregisters kann eingeleitet werden: fehlende/unrichtige Angaben werden ergänzt/korrigiert/gestrichen.
- Es kann Strafanzeige erstattet werden; entweder bei Gericht (§ 51 DSG; siehe Abschnitt VI.6.5) oder der Bezirksverwaltungsbehörde (§ 52 DSG; siehe Abschnitt VI.6.6).
- Handelt es sich um einen schwerwiegenden Verstoß, der sonst vom Verletzten selbst vor Gericht zu verfolgen wäre (Auftraggeber entstammt dem privaten Bereich), so kann[478] die Datenschutzkommission anstatt des Verletzten Feststellungsklage erheben. Der Betroffene erhält damit, ohne das zugehörige Prozessrisiko tragen zu müssen, eine sichere Rechtsbasis für darauf folgende Unterlassungs- oder Schadenersatzansprüche.

---

[476] Explizit angeführt sind die Abgabenbehörden; d.h. steuerrelevante Erkenntnisse dürfen nicht weitergegeben werden!

[477] Freiheitsstrafe von 6 Monaten bis 5 Jahren: Da die Strafdrohung nicht über 5 Jahre, sondern genau an der Grenze liegt, musste dieses Delikt separat aufgeführt werden.

[478] Nach den Erläuterungen zur Regierungsvorlage "kann", also nach Ermessen der Datenschutzkommission. Nach § 32 Abs 5 DSG ("hat") muss eine Feststellungsklage jedoch erfolgen, wenn ein begründeter Verdacht auf eine schwerwiegende Datenschutzverletzung besteht. Es kann nicht darauf ankommen, wie die DSK von dem Missstand erfährt. Bei schwerwiegenden Verstößen *ist* eben die Klage zu erheben.

- Handelt es sich beim Auftraggeber der Verarbeitung um eine Gebietskörperschaft, so kann die DSK das zuständige oberste Organ befassen (Minister, Landesregierung/-rat, Gemeinderat). Innerhalb angemessener Frist (max. 12 Wochen), muss der entsprechende Zustand hergestellt werden oder es ist der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Um auch hier gewisse Sanktionen setzen zu können, kann die Kommission die Öffentlichkeit über die Begründung in geeigneter Weise in Kenntnis setzen, d.h. insbesondere über die Presse, sofern es die Amtsverschwiegenheit erlaubt.

VI.7.3. Rechtszug und besondere Bescheidwirkungen

Erlässt ein einzelnes Mitglied der Kommission einen Bescheid[479], so kann Vorstellung, eine Art Einspruch, an die Kommission erhoben werden, die dann endgültig entscheidet. In allen anderen Fällen entscheidet die gesamte Kommission als erste Instanz und gleichzeitig letztinstanzlich, d.h. ohne Möglichkeit einer weiteren Überprüfung. In diesem Fall ist nur mehr die Anrufung des Verwaltungs- oder Verfassungsgerichtshofes möglich.

Bescheide betreffend die Genehmigung der Übermittlung von Daten ins Ausland sind gegenüber "normalen" Bescheiden von geringerer Bestandskraft. Wird von der Europäischen Kommission per Verordnung festgestellt, dass die Voraussetzungen für Übermittlungen in dieses Land nicht vorliegen, also entgegen der Beurteilung durch die Datenschutzkommission, so sind die Bescheide zu widerrufen[480]. Dies ist auch dann möglich, wenn durch Änderung der Sach- oder Rechtslage die Voraussetzungen nicht mehr gegeben sind.

VI.8. Besondere Aspekte

In diesem Abschnitt sollen abschließend noch einige Punkte betrachtet werden: Um die gesetzlich vorgeschriebene Geheimhaltung von Daten auch zu gewährleisten, müssen entsprechende Maßnahmen gesetzt werden. Weiters hat oft auch der Betroffene ein Interesse an der Weiterexistenz der Daten, sodass auch die Sicherung gegen Verlust ein Teil davon ist. Eine spezielle Gefahr für einzelne Personen besteht dann, wenn sie einer ausschließlich automatisierten Entscheidung unterworfen werden sollen, z.B. einer Beurteilung ihrer Kreditwürdigkeit. Auch im Bereich der Direktwerbung spielt der Datenschutz eine wichtige Rolle, da die Werbungsversender großes Interesse daran besitzen, ihre Werbung möglichst zielgerichtet zu verteilen. Dieser Aspekt ist zwar in der DSRL enthalten, in Österreich aber in der Gewerbeordnung umgesetzt. Aufgrund des engen Zusammenhangs mit Werbung wird dieser Aspekt im Kapitel "Werbung im Internet" behandelt. Abschließend wird kurz der wenig bedeutsame Datenschutzrat erläutert.

VI.8.1. Datensicherheitsmaßnahmen

Je nach Art der verwendeten Daten sowie nach Umfang und Zweck der Verwendung ist sicherzustellen, dass Daten vor zufälliger oder unrechtmäßiger Zerstörung oder Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt, und dass Unbefugte keinen Zugang dazu erlangen. Beim Ausmaß des Schutzes ist auf den Stand der technischen

[479] Geschäftsführendes Mitglied: Vorläufige Untersagung der Datenanwendung gem. § 20 Abs 2 DSG und amtswegige Änderungen und Streichungen im Datenverarbeitungsregister nach § 22 Abs 3 DSG.

[480] Eine Besonderheit, da Bescheide sonst nur aus sehr wenigen Gründen widerrufen werden können. Praktisch jedoch wohl von zu vernachlässigender Bedeutung.

Möglichkeiten und die wirtschaftliche Vertretbarkeit der Maßnahmen Bedacht zu nehmen. Es muss ein bestimmtes Schutzniveau gewährleistet werden, wobei die von der Verwendung und der Art der zu schützenden Daten ausgehenden Risiken den aufgrund der Durchführung der Maßnahmen entstehenden Kosten angemessen sind[481]. Erforderlich sind z.B. die folgenden Maßnahmen, jeweils von angemessenem Niveau entsprechend den Risiken bzw. der Daten:

- Die Aufgabenverteilung bei der Datenverwendung ist zwischen den Organisationseinheiten und den Mitarbeitern ausdrücklich festzulegen.
- Die Datenverwendung muss an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter gebunden sein.
- Jeder Mitarbeiter ist über seine Pflichten nach dem DSG und nach innerbetrieblichen Datenschutz- und Datensicherheitsvorschriften zu belehren.
- Die Zutrittsberechtigung zu den Räumlichkeiten ist zu regeln.
- Zugriffsberechtigungen auf Daten und Programme sind vorzusehen.
- Datenträger sind vor Einsicht und Verwendung durch Unbefugte zu sichern. Dies schließt die Sicherung vor Löschung/Entfernung mit ein.
- Berechtigungen zum Betrieb von Datenverarbeitungsgeräten sind festzulegen und Geräte durch Hard-/Software-Vorkehrungen gegen unbefugte Inbetriebnahme zu sichern.
- Protokolle müssen geführt werden, damit tatsächlich durchgeführte Verwendungsvorgänge, insbesondere Änderungen, Abfragen und Übermittlungen, auf ihre Zulässigkeit im notwendigen Ausmaß überprüft werden können.
- Es ist eine Dokumentation über alle Datensicherheitsmaßnahmen zu führen, um eine Kontrolle und Beweissicherung zu erleichtern.

Protokoll- und Dokumentationsdaten dürfen ausschließlich für den Zweck ihrer Ermittlung verwendet werden: Die Kontrolle der Zulässigkeit der Verwendung des Datenbestandes. Nicht erlaubt ist insbesondere die Verwendung zur Kontrolle der Personen, deren Daten im Datenbestand enthalten sind[482]. Weiters dürfen sie nicht zu einer anderen Kontrolle der auf den Datenbestand zugreifenden Personen dienen, als deren Zugriffsberechtigung zu prüfen, z.B. der Erstellung von Zugriffsprofilen oder einer Arbeitskontrolle. Eine Ausnahme von diesem Verbot besteht, wenn es sich um die Verfolgung oder Verhinderung eines Verbrechens handelt, welches mit mehr als fünfjähriger Freiheitsstrafe bedroht ist oder wenn es sich um eine kriminelle Organisation handelt (§ 278a StGB). Protokoll- und Dokumentationsdaten sind drei Jahre lang aufzubewahren. Abweichungen sind nur zulässig bzw. verpflichtend, insoweit die davon betroffenen Daten kürzer oder länger existieren.

VI.8.2. Automatisierte Einzelentscheidungen

Gemäß § 49 DSG darf niemand einer Entscheidung zum Zweck der Bewertung einzelner Aspekte seiner Person unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Datenverarbeitung getroffen wurde, wenn dies für ihn rechtliche Folgen

[481] Gesundheitsdaten sind daher besser und aufwendiger zu sichern als bloße Adressen von Interessenten.

[482] Das Eingabeprotokoll, d.h. wann eine Eingabe erfolgte, eines Arbeitszeiterfassungssystems darf nicht zur Verifikation der Eintragungen selbst verwendet werden. Kritisch dazu: Brodil: Zeiterfassung ohne Zeiterfassung? ecolex 2005, 459 zur Entscheidung DSK 16. 11. 2004, K 120.951/0009-DSK/2004

nach sich zieht oder ihn erheblich beeinträchtigt. Als Beispiele werden die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit sowie das Verhalten angeführt.

Da jedoch vielfach ein starkes praktisches Bedürfnis nach solchen Entscheidungen besteht, insbesondere im staatlichen Bereich (Beihilfeverfahren, Steuerbescheide etc.), wurden einige Ausnahmen geschaffen, welche das Verbot sehr stark einschränken:

- Ist die automatisierte Einzelentscheidung gesetzlich vorgesehen, so ist dies erlaubt.
- Ergeht die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages und wurde dem Ersuchen des Betroffenen auf Abschluss oder Erfüllung des Vertrages entsprochen. Beispiel: Die (positiv verlaufende) automatische Überprüfung der Kreditwürdigkeit vor Vertragsabschluss. Wird diese jedoch verneint, so muss eine persönliche Nachkontrolle stattfinden, sofern nicht die nächste Ausnahme greift!
- Wenn die berechtigten Interessen des Betroffenen durch geeignete Maßnahmen garantiert werden. Da als Beispiel die Möglichkeit angeführt wird, dass der Betroffene seinen Standpunkt geltend machen kann, erlaubt dieser Punkt sehr weitgehende Einschränkungen bzw. automatische Verarbeitungen: Es muss lediglich eine Art "Beschwerdestelle" existieren.

Auf Antrag des Betroffenen ist der Ablauf der automatisierten Entscheidung in allgemein verständlicher Form vom Auftraggeber darzulegen. Einschränkungen dieses Rechts ergeben sich jedoch u.a. aus dem Urheberrecht und dem Geschäftsgeheimnis. Diesbezüglich ist eine Verhältnismäßigkeitsprüfung durchzuführen.

VI.8.3. Informationsverbundsysteme

Bei einem Informationsverbundsystem schließen sich mehrere Auftraggeber zusammen, um Daten in einen gemeinsamen Pool einzubringen. Speziell hierbei ist, dass jeder Teilnehmer Zugriff auf *alle* Daten besitzt, also auch die, welche von anderen Teilnehmern am System stammen. Hier ist daher eine (unbeschränkte) Übermittlung an alle weiteren Informationsverbundsystemteilnehmer implizit enthalten. Ein Beispiel ist die Kredit-Warnliste: Alle Banken stellen Informationen zur Verfügung, und jede weitere Teilnehmerbank kann nicht nur ihre eigenen, sondern auch die der anderen Banken abrufen.

Für Informationsverbundsysteme ist eine Vorabkontrolle durch die DSK erforderlich. Mit der Verarbeitung darf also erst nach der Genehmigung begonnen werden.

Für ein Informationsverbundsystem ist ein Betreiber zu bestellen, wobei es sich um einen der Teilnehmer oder einen Dritten handeln kann. Dieser dient als "Ansprechpartner" für Dritte und hat Auskunft zu erteilen, wer genau der Auftraggeber für die über ihn im Informationsverbundsystem gespeicherten Daten ist. Der Betreiber ist auch für die Datensicherheitsmaßnahmen im System verantwortlich.

VI.8.4. Vorratsdatenspeicherung

Nach der Telekom-Datenschutz-RL können Rechte und Verpflichtungen aus der DSRL aus Gründen der demokratischen Gesellschaft, der Staatssicherheit, der Verteidigung, der öffentlichen Sicherheit und der Vermeidung, Untersuchung, Erkennung und Verfolgung von Straftaten eingeschränkt werden. Dies hat sich auf das erforderliche Ausmaß zu beschränken und muss angemessen und zu dem Grund, aus dem die Einschränkung erfolgt, pro-

portional sein. Zu diesem Zweck kann u.a. die Vorratsdatenspeicherung für eine beschränkte Zeitspanne vorgeschrieben werden. Eine solche verdachtsunabhängige[483] Speicherung wurde mit der Vorratsdatenspeicherungs-RL[484] eingeführt. Verpflichtet dazu sind Betreiber öffentlicher Kommunikationsnetze oder öffentlich zugänglicher el. Kommunikationsdienste. Dies betrifft daher ISPs, nicht jedoch normale Firmen, da diese Dienste nur für ihre eigenen Mitarbeiter, aber nicht für die Öffentlichkeit, bereitstellen.

Folgende Daten[485] sind zu speichern, sofern sie vom Betreiber erzeugt oder verarbeitet werden, wobei aber keinesfalls Inhaltsdaten gespeichert werden dürfen[486]:

- Daten zur Rückverfolgung und Identifizierung der Quelle einer Nachricht bei Internet-Zugang, Internet-E-Mail und Internet-Telefonie: Die zugewiesene Benutzerkennung, die Rufnummer im öffentlichen Telefonnetz sowie Name und Anschrift des Teilnehmers bzw. des registrierten Benutzers, dem eine IP-Adresse, Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war.
- Daten zur Identifizierung des Adressaten einer Nachricht bei Internet-E-Mail und Internet-Telefonie (also nicht bei bloßem Zugang!): Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Internet-Telefonats, Namen und Anschriften der Teilnehmer oder registrierte Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht.
- Daten zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung bei Internet-Zugang, Internet-E-Mail und Internet-Telefonie: Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst zusammen mit der (dynamischen bzw. statischen) IP-Adresse, der Benutzerkennung des Teilnehmers oder des registrierten Benutzers.
- Daten zur Bestimmung der Art der Nachrichtenübermittlung bei Internet-E-Mail und Internet-Telefonie (also nicht bei bloßem Zugang!): Der in Anspruch genommene Internetdienst[487].
- Daten zur Bestimmung der (vorgeblichen) Endeinrichtung von Benutzern bei Internet-Zugang, Internet-E-Mail und Internet-Telefonie: Die Rufnummer des anrufenden Anschlusses bei Wählanschluss (wohl: Einwahl über Modem über eine Wählleitung), der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorganges.

Erhobene Daten dürfen nur in bestimmten Fällen und gemäß dem jeweiligen Recht an die zuständigen nationalen Behörden weitergegeben werden, was aber unverzüglich erfolgen muss[488]. Die Speicherdauer hat mindestens sechs Monate zu umfassen und darf maximal

---

[483] Bei konkretem Verdacht konnte ein Richter unter bestimmten Bedingungen schon bisher eine Überwachung im Einzelfall anordnen, sowohl hinsichtlich Telefonüberwachung, Wanzen, aber auch Internet-Aufzeichnung.

[484] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher el. Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF Die Umsetzung in nationales Recht hat bis September 2007 zu erfolgen.

[485] Neben anderen, welche Telefonfestnetz und Mobilfunk betreffen.

[486] Dies könnte sich bei E-Mail als schwierig erweisen: Eine Mail an "drugabuse@helpme.com" lässt schon durch die E-Mail Adresse einiges über den Inhalt vermuten.

[487] Hierbei könnte es sich um das Protokoll handeln: Skype, ICQ, H.323, ...

[488] Auslagerung auf extern verwahrte Backups ist daher wohl nicht möglich.

zwei Jahre dauern. Hinsichtlich der Sicherheit sind die gleichen Methoden und Vorkehrungen zu verwenden wie sie für die Grunddaten bestehen. Weiters sind geeignete technische und organisatorische Maßnahmen gegen zufällige oder unrechtmäßige Zerstörung, Verlust oder Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu ergreifen. Darüber hinaus ist sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen möglich ist.

Eine staatliche Ersatzpflicht für die bei den ISP zusätzlich entstehenden Aufwendungen wurde zwar diskutiert, aber nicht in die RL eingebaut. Es bleibt daher den Einzelstaaten überlassen, ob sie eine solche einführen möchten.

VI.8.5. Der Datenschutzrat

Der Datenschutzrat ist in den § 41-44 DSG geregelt. Er hat keine Aufgaben bei der Durchführung oder Durchsetzung des DSG zu erfüllen, sondern besitzt lediglich beratende Funktion. Er soll sowohl Bundes- wie auch Landesregierungen, bei letzteren aus kompetenzrechtlichen Gründen nur auf deren Ersuchen hin, in rechtspolitischen Fragen des Datenschutzes beraten und hierzu Stellungnahmen zu Gesetzesvorhaben abgeben. Weiters kann er Kommentare zu Vorhaben im öffentlichen Bereich abgeben, die datenschutzrechtlich von Bedeutung sind. In diesem Zusammenhang kann er von Auftraggebern des öffentlichen Bereichs Auskünfte, Berichte und Unterlageneinsicht verlangen, wenn dies für die Beurteilung eines Vorhabens in datenschutzrechtlicher Hinsicht notwendig ist[489].

Der Datenschutzrat ist folgendermaßen zusammengesetzt: Vertreter der Nationalratsparteien entsprechend ihrer Stärke, je ein Vertreter der Arbeiterkammer und der Wirtschaftskammer, zwei Ländervertreter, je ein Vertreter des Gemeinde- und des Städtebundes sowie ein Vertreter des Bundes. Diese Mitglieder sind auf unbestimmte Zeit ernannt und scheiden nur durch Nominierung eines anderen Mitgliedes oder Zurücklegung des Amtes aus. Die Beratungen sind vertraulich und werden nach Bedarf abgehalten. Die Einberufung erfolgt durch den Vorsitzenden oder auf Verlangen eines Mitgliedes. Die Tätigkeit ist ehrenamtlich, es besteht lediglich Anspruch auf Reisekostenersatz.

VI.9. Literatur

VI.9.1. Allgemein

Bizer, Johann: Die dienstliche Telekommunikation unter dem Schutz des Fernmeldegeheimnisses, DuD 2001, 619

Brandl, Ernst O., Mayer-Schönberger, Viktor: CPU-IDs, Cookies und Internet-Datenschutz, ecolex 1999, 367

Brenn, Christoph: Das Signaturgesetz. In: Schweighofer, Erich, Menzel, Thomas (Hg.): E-Commerce und E-Government. Wien: Verlag Österreich 2000, 43-50

Brodil, Wolfgang: Zeiterfassung ohne Zeiterfassung? ecolex 2005, 459

Brodil, Wolfgang: Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis. ZAS 2004/28

[489] Eine Ausnahme besteht für die inneren Angelegenheiten von anerkannten Religionsgemeinschaften.

Büllesbach, Alfred: Datenschutz bei Data Warehouses und Data Mining. CR 1/2000, 11

Buxel, Holger: Die sieben Kernprobleme des Online-Profiling aus Nutzerperspektive. DuD 25 (2001) 10, 582

Cavoukian. Ann, Gurski, Michael, Mulligan, Deirdre, Schwartz, Ari: P3P und Datenschutz. Ein Update für die Datenschutzgemeinde. DuD 24 (2000) 8, 475

Österreichische Datenschutzkommission: http://www.dsk.gv.at/

Damman, Ulrich, Simitis, Spiros: EG Daten-. Schutzrichtlinie Baden-Baden 1997, 115;

DuD: Datenschutz und Datensicherheit http://www.dud.de/

Ehmann, Eugen, Helfrich, Marcus: EG Datenschutzrichtlinie (1999)

Eidgenössischer Datenschutzbeauftragte, Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz, 33 http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html

Ermer, Dieter: Systemdatenschutz und Chipkarte. CR 2/2000, 126

Golembiewski, Claudia: Das Recht auf Anonymität im Internet, DuD 2003, 129

Grabenwarter, Christoph: Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, ÖJZ 2000, 861

Grimm, Rüdiger, Roßnagl, Alexander: Datenschutz für das Internet in den USA. DuD 24 (2000) 8, 446

Hillenbrand-Beck, Renate, Greß, Sebastian: Datengewinnung im Internet. DuD 25 (2001) 7, 390f

Hohl, Michael: Private e-mails am Arbeitsplatz, http://www.ak-it-recht.de/hohl_email.html

Hörlsberger, Felix: Veröffentlichung personenbezogener Daten im Internet. ÖJZ 2004/45

Ihde, Rainer: Cookies: Datenschutz als Rahmenbedingung der Internetökonomie. CR 7/2000, 417

Imhof, Ralf: One-to-One-Marketing im Internet, CR 2/2000, 110

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

Jahnel, Dietmar: Datenschutz im Internet – am Beispiel des Speicherns von Cookies. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther: Auf dem Weg zur ePerson: aktuelle Fragestellungen der Rechtsinformatik. Wien: Verlag Österreich 2001

Jahnel, Dietmar: Spamming, Cookies, Web-Logs, LBS und die Datenschutzrichtlinie für el. Kommunikation. WBl 2003, 108

Kassai, Klaus: "Location Base Services" im Gefüge des Satenschutzrechts, MR 2004, 433

Knyrim, Rainer: Anmerkungen zu OGH 15.12.2005, 6 Ob 275/05t, MR 2006, 83

Knyrim, Rainer, Haidinger, Viktoria: RFID-Chips und Datenschutz. RdW 2005, 2 http://www.preslmayr.at/puplikationen/ArtikelKnyrim_Haidinger_Datenschutz_und_RFID.pdf

Köhntopp, Marit, Köhntopp, Kristian: Datenspuren im Internet. CR 4/2000, 253

Krauß, Claudia: Internet am Arbeitsplatz. JurPC Web-Dok 14/2004, http://www.jurpc.de/aufsatz/20040014.htm

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

Kunnert, Gerhard: Die abschnittsbezogene Geschwindigkeitsüberwachung (Section Control) aus datenschutzrechtlicher Sicht. ZVR 2006/17

Lohse, Christina, Janetzko, Dietmar: Technische und juristische Regulationsmodelle des Datenschutzes am Beispiel von P3P. CR 1/2001, 55

Lukas, Meinhard: Schadenersatz bei Verletzung der Privatsphäre. RZ 2004, 33

Menzel, Thomas: Haftung von Zertifizierungsdiensteanbietern. In: Schweighofer, Erich, Menzel, Thomas (Hg.): E-Commerce und E-Government. Wien: Verlag Österreich 2000, 55-64

Peters, Falk, Kersten, Heinrich: Technisches Organisationsrecht im Datenschutz – Bedarf und Möglichkeiten. CR 9/2001, 576

Pomaroli, Nicolaus: Das "Aufgabengebiet" im Datenschutz. ÖZW 2006, 13

Rasmussen, Heike: Die el. Einwilligung im TDDG, DuD 2002, 406

Rasmussen, Heike: Datenschutz im Internet. Gesetzgeberische Maßnahmen zur Verhinderung der Erstellung ungewollter Nutzerprofile im Web – Zur Neufassung des TDDSG. CR 1/2002, 36

Reichmann, Gerhard: Das Auskunftsrecht nach dem Datenschutzgesetz 2000 - Eine Fallstudie. ZfV 2004/1529

Rosenmayr-Klemenz, Claudia: Zum Schutz manuell verarbeiteter Daten durch das DSG 2000. ecolex 2001, 639

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

Rosenthal, David: Internet-Überwachung und –Kontrolle am Arbeitsplatz, http://www.btnet.de/pdf/kontrolle.pdf

Schaar, Peter: Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung. DuD 24 (2000) 5, 276

Schaar, Peter: Persönlichkeitsprofile im Internet. DuD 25 (2001) 7, 383

Schaumüller-Bichl, Ingrid: Datenschutz und Informationsrecht. Vorlesung SS 99. Universität Linz 1999

Schrader, H.-H.: Selbstdatenschutz mit Wahlmöglichkeiten, DuD 1998, 128

Simitis, Spiros: Der Transfer von Daten in Drittländer – ein Streit ohne Ende? CR 7/2000, 472

Sonntag, Michael: Webbugs – Wanzen im Internet. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): IT in Recht und Staat. Wien: Verlag Österreich 2002, 355ff

Sonntag, Michael: Engineering for Privacy. Reducing personal information and complying to privacy laws. In: Hofer Christian, Chroust Gerhard (Eds.): IDIMT-2002. 10th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2002

Sonntag, Michael, Wimmer, Maria: Datenschutzaspekte von e-Government mit besonderem Bezug auf das eGOV-Projekt. In: Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt. Informatik 2002 - 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI). Bonn: Gesellschaft für Informatik 2002, 462-468

Sonntag, Michael: Rechtsprobleme von Online Lernplattformen. Logging, Prüfung und Filterung von Inhalten. In: Schweighofer, Erich, Liebwald, Doris, Kreuzbauer, Günther, Menzel, Thomas (Hrsg.): Informationstechnik in der juristischen Realität. Aktuelle Fragen der Rechtsinformatik 2004. Wien: Verlag Österreich 2004, 407-414

Sonntag, Michael: Datenschutz im Fernunterricht. In: Oliver Plöckinger, Dieter Duursma, Michael Mayrhofer (Hrsg.): Internet-Recht. Wien: Neuer Wissenschaftlicher Verlag 2004, 455-474

Streitberger, Thomas: Privacy am Rechnerarbeitsplatz, Master Thesis, http://rechtsprobleme.at/doks/privacy_arbeitsplatz-streitberger.pdf

Thiele, Clemens: Anmerkungen zu OLG Innsbruck, 27.9.1999, 1 R 143/99k und 28.3.2000, 1 R 30/00x, "Hausbesorgerdaten im Internet" http://www.eurolawyer.at/pdf/OLG_Innsbruck_1_R_30-00x.pdf

Tinnefeld, Marie-Therese, Ehmann, Eugen: Einführung in das Datenschutzrecht[3] (1998)

Wedde, Peter: Internetnutzung und Kontrollmöglichkeiten, http://www.onlinerechte-fuer-beschaeftigte.de/service/dates/download/bigbrother_wedde.pdf

Warren, Samuel D., Brandeis, Louis D.: The right to privacy, Harvard Law Review Volume IV 1890, 193 http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html

VI.9.2. Rechtsvorschriften

DSG: Datenschutzgesetz 2000 - DSG 2000, BGBl. I Nr. 165/1999, idF. BGBl. I Nr. 13/2005

Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl. II Nr. 312/2004. http://www.dsk.gv.at/verord.htm

Erläuterungen zur Regierungsvorlage (1613 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP) http://www.parlinkom.gv.at/pls/portal/docs/page/PG/DE/XX/I/I_01613/FNAMEORIG_000000.HTML

Bericht des Verfassungsausschusses (2028 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP) http://www.parlinkom.gv.at/pls/portal/docs/page/PG/DE/XX/I/I_02028/FNAMEORIG_000000.HTML

Richtlinien betreffend personenbezogenen Daten in automatisierten Dateien (UN Generalversammlungsbeschluss vom 14.12.1990) http://www.datenschutz-berlin.de/recht/int/uno/gl_pbdde.htm

Charta der Grundrechte der Europäischen Union http://www.europarl.europa.eu/charter/default_de.htm

Datenschutz-Richtlinie: Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl. L 281/31 vom

23.11.1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML

Rahmenrichtlinie (Framework Directive): Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie). ABl. L 108/33 vom 24.4.2002 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021: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 elektronischen 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

Vorratsdatenspeicherungs-RL der EU: Richtlinie 2006/24/EG des Europäischen Parlamentes und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG ABl. L 105 vom 13.4.2006 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:DE:HTML

VII. Vertragsabschluss und Konsumentenschutz im Fernabsatz

Einer der Hauptpunkte von E-Business ist der Abschluss von Kaufverträgen mittels elektronischer Kommunikation. Hier stellen sich nicht nur rechtliche Fragen sondern auch Probleme der Beweissicherung, der Durchsetzung und der konkreten Anwendung der Vorschriften. So kommt ein Vertrag durch Übereinstimmung von Angebot und Annahme zustande. Aber was ist im Internet ein Angebot: Eine Webseite, ein Warenkorb mit Lieferauskunft oder etwa eine persönliche E-Mail? Zusätzlich wurden noch Vorschriften für den Verbraucherschutz eingeführt, welche besonders auf das Internet abzielen, aber auch für den normalen Versandhandel von Bedeutung sind (allgemein für alle Distanzgeschäfte).

VII.1. Einleitung

Dieser Abschnitt behandelt einige wenige Sonderprobleme bei el. Abschluss von Verträgen. Es wird jedoch vorausgesetzt, dass der Vertragsschluss und seine Probleme bereits bekannt oder nicht relevant sind.

VII.1.1. Vertragsabschluss allgemein

Sowohl Angebot wie auch Annahme sind empfangsbedürftige Willenserklärungen. Dies bedeutet, dass ein Angebot im Rechtssinn erst dann vorliegt, wenn es dem Empfänger zugegangen ist. Das Übertragungsrisiko liegt daher beim Sender (Beweislast für vollständigen/rechtzeitigen Empfang; § 862a ABGB). Dies ist besonders bei E-Mails ein Problem, da technisch keine Rückmeldung vorgesehen ist, wann bzw. ob eine Mail beim Endempfänger in der Mailbox angekommen ist, an dessen Rechner ausgeliefert oder tatsächlich angezeigt wurde[490]. Im Zustellgesetz existieren dazu, allerdings hier nicht anzuwendende, Sonderregelungen[491], da es dort um die Zustellung amtlicher Schriftstücke geht.

Im E-Business stellt sich oft das Problem, dass manche Erklärungen des Verkäufers, sofern es sich tatsächlich um Erklärungen im Rechtssinne handelt, nicht unbedingt von einer natürlichen Person stammen. Stattdessen werden diese Antworten automatisch erzeugt, z.B. durch einen Webserver. Hier ist laut österreichischer Lehre[492] der Mangel des Erklärungsbewusstseins irrelevant, wenn die Handlung, die als solche gesetzt wird, zumindest fahrlässig von der Person, der sie zugerechnet werden soll, verursacht wurde. In der Bereitstellung eines Rechners mit dem zugehörigen Programm und den Webseiten ist jedenfalls ei-

[490] Es bestehen verschiedene Protokolle, die dies unterstützen. Ihnen ist jedoch gemeinsam, dass sie keine verbindlichen Regelungen und sichere Benachrichtigungen spezifizieren. So erfolgt die Rückmeldung z.B. meist als E-Mail, welche natürlich ebenfalls verloren gehen kann! Geschlossene Systeme bieten typischerweise mehr und zuverlässigere Funktionen.

[491] Zustellung mit Nachweise: zweimalige el. Verständigung, dann Mitteilung auf Papier, dass ein el. Dokument zu Abholung bereitgestellt wurde. Bei technischen Problemen, z.B. die E-Mail ist unzustellbar, erfolgt die Papier-Benachrichtigung sofort.

[492] Siehe dazu näher Koziol/Welser, Grundriß des bürgerlichen Rechts. Band I: Allgemeiner Teil und Schuldrecht. Wien: Manz 1995, 94. Für Deutschland: LG Köln 16.04.2003, 9 S 289/02 http://www.jurpc.de/rechtspr/20030138.htm

ne solche Handlung zu sehen[493]. Durfte der Empfänger daher eine automatische Mitteilung vom Inhalt her als Erklärung werten, und hat er dies auch tatsächlich getan, so wird sie dem Absender selbst dann zugerechnet, wenn dieser kein Aktualwissen davon hatte.

VII.1.2. Anwendbares Recht

Grundsätzlich steht es Vertragspartnern frei, den von ihnen abgeschlossenen Vertrag einem (fast) beliebigen Recht zu unterwerfen. Diese Rechtsordnung braucht keinerlei Beziehung zum Gegenstand des Vertrages oder den Parteien zu besitzen. Regelmäßig wird jedoch das Recht des Ortes eines der beiden Partner vereinbart werden. Eine Einschränkung dieses Grundsatzes ergibt sich durch Schutzvorschriften für Endverbraucher (=Konsumenten), welche teilweise durch Vereinbarung nicht abgeändert werden können und daher trotz abweichender Rechtswahl bestehen bleiben (siehe unten). Von der Rechtswahl zu unterscheiden ist der Fall, dass keine bestimmte Rechtsordnung vereinbart wurde. In diesem Fall gilt nach internationalem Privatrecht (siehe IPRG[494] und EVÜ[495]) das Recht, zu dem die stärkste Beziehung besteht. Dies ist allgemein das Recht des Staates der Partei, welche die charakteristische Leistung (=nicht aus Geld bestehende, d.h. die Ware) erbringt. Bei einem Kaufvertrag handelt es sich dabei um den Staat, in dem der Verkäufer seinen gewöhnlichen Aufenthalt bzw. bei juristischen Personen den Sitz der Hauptverwaltung hat. Zusätzlich ist noch das UN-Kaufrecht zu beachten[496].

Allgemein ist zum anwendbaren Recht zu sagen, dass eine höchst komplexe Rechtslage besteht. Eine ausdrückliche Rechtswahl ist daher dringend zu empfehlen; siehe dazu auch die Festlegungen in den AGBs der meisten Online-Shops. Doch selbst wenn eine eindeutige Aussage möglich ist, insbesondere im B2B E-Commerce[497], wo freie Rechtswahl ohne Einschränkungen wie bei Verbrauchergeschäften existiert, besteht oft das Problem der tatsächlichen Rechtsdurchsetzung. Ein gewonnenes Verfahren vor österreichischen Gerichten hat wenig Sinn, wenn das Urteil nicht vollstreckt werden kann, weil das betroffene Unternehmen seinen Sitz im (Nicht-EU-) Ausland hat und keine Tätigkeit in Österreich entfaltet. Die Alternative, im Ausland zu klagen, ist meist sehr kostspielig und wegen mangelnder Rechtskenntnis riskant. International sollte daher als Endverbraucher besonderes Augenmerk auf die Wahl des Verkäufers gelegt werden, um im Fall von Problemen auf Kulanzregelungen oder vorab vereinbarte Verfahren, z.B. ein garantiertes Rückgaberecht, vertrauen zu können. Im Bereich der EU ist hierfür die EuGVVO[498] bedeutend, welche die Anerkennung und Exekution von Gerichtsentscheidungen betrifft. Als Verkäufer sollte spiegelbildlich darauf geachtet werden, nur an Konsumenten in Länder zu verkaufen, wo

---

[493] "Übermittlungsfehler": OLG Frankfurt/Main 20.11.2002, 9 U 94/02 http://www.aufrecht.de/1369.html

[494] Bundesgesetz vom 15. Juni 1978 über das internationale Privatrecht (IPR-Gesetz). Dieses Gesetz regelt, welche Rechtsordnung auf bestimmte Sachverhaltskategorien anzuwenden ist.

[495] EG-Römer Übereinkommen vom 19. Juni 1980 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (EVÜ) ABl. L 266/1 vom 9.10.1980

[496] Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf - UN-Kaufrecht. BGBl. Nr. 96/1988 http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG.html

[497] Achtung auf den Anwendungsbereich (EVÜ inkludiert etwa auch Finanzierungsgeschäfte) und die Definition von "Verbraucher": Nach dem EuGH ist (EVÜ-)Verbraucher nur, wer den Vertrag zur Deckung des eigenen privaten Verbrauchs abschließt, und dies auch für den Vertragspartner aus konkreten Umständen erkennbar ist (EuGH 3.7.1997, Rs C-269/95). Das KSchG setzt jedoch keinerlei Erkennbarkeit voraus, sondern stellt nur darauf ab, dass ein Geschäft für den Konsumenten nicht zu einem Unternehmensbetrieb gehört. Der Unterschied könnte etwa bei (halb-privaten) Firmenfeiern schlagend werden. Diese gehören nicht zum Unternehmensbetrieb, dienen jedoch auch nicht privatem Verbrauch.

[498] Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (EuGVVO) ABl. L 12/01 vom 16.1.2001

auch eine entsprechende Rechtssicherheit für die Kaufpreiserlangung besteht. Hierfür ist, siehe unten, eine explizite Einschränkung der Zielländer empfehlenswert.

Vom anwendbaren Recht zu unterscheiden ist der Gerichtsstand, welcher für die EU ebenfalls im EuGVVO geregelt wird: Es kann in einem Vertrag die Anwendung deutschen Rechts vereinbart werden und ein Prozess dann doch in Österreich stattfinden. In der Praxis tritt dies insbesondere bei Konsumenten auf: Anwendbares Recht ist das Recht des ausländischen Verkäufers, Gerichtsstand aufgrund von Konsumentenschutzbestimmungen jedoch das Inland[499]. Hierfür reicht aus (Art 15 EuGVVO), wenn die Webseite auf den Wohnsitzstaat des Verbrauchers ausgerichtet ist und in diesem Bereich ein Vertrag abgeschlossen wird[500]. Hinzu kommt, dass gewisse Konsumentenschutzbestimmungen zwingend sind. Es gilt also für den Vertrag nicht ausschließlich fremdes Recht, sondern im Prozess ist dann eine Mischung von beiden Rechtsordnungen anzuwenden.

VII.2. Konsumentenschutz bei Distanzgeschäften

Konsumenten sind gegenüber Unternehmern meist in einer praktisch deutlich schwächeren Position, auch wenn sie rechtlich gleichgestellt sind. So wäre zwar in Supermärkten beispielsweise ein Verhandeln über den Preis rechtlich problemlos möglich, wird aber praktisch nie erfolgreich sein. Um Konsumenten vor faktischer Übermacht zu schützen, wurden Bestimmungen eingeführt, welche besondere Rechte, wie beispielsweise eine begründungsfreie und kostenlose Rückgabe, ermöglichen, oder typische Gefahren wie benachteiligende Geschäftsbedingungen verhindern sollen. Schutzvorschriften bestehen einerseits allgemein für Konsumenten, aber auch im speziellen für Distanzgeschäfte, bei denen der Kunde keine Möglichkeit hat, sich ein persönliches Bild von der Ware zu machen.

VII.2.1. Verbraucherverträge/Konsumentenschutzgesetz allgemein

Nach dem Europäischen Vertragsstatutübereinkommen (Art. 5 EVÜ) besteht bei Verbraucherverträgen zwar eine freie Rechtswahl, doch sind Bestimmungen, welche dem Verbraucher den Schutz im Staat seines gewöhnlichen Aufenthalts entziehen, unter einigen zusätzlichen Bedingungen, unwirksam. Eine ähnliche Bestimmung findet sich auch im Konsumentenschutzgesetz (KSchG) in § 13a Abs 2. Für E-Commerce ist hier die Klausel wichtig, dass dies gilt, wenn dem Vertragsabschluss ein ausdrückliches Angebot oder eine Werbung in diesem Staat vorausgegangen ist und der Verbraucher[501] dort die zum Abschluss des Vertrages notwendigen Rechtshandlungen vorgenommenen hat. Der letzte Punkt ist einfach zu beurteilen, aber ev. schwer nachzuweisen: Der Konsument muss seine Erklärung in Österreich abgegeben[502], d.h. das Bestellformular auf der Webseite ausgefüllt oder die E-Mail abgeschickt haben[503]. Der erste Punkt ist schwieriger zu beurteilen. Eine

---

[499] Siehe OLG Wien 22.3.2006, 13 R 257/05t. Ein Deutscher bot auf eBay einen Ferrari zur Miete an, der österreichische Käufer ging jedoch von einem Kauf aus. Zuständig war ein österreichisches Gericht (Sitz des Käufers), da es sich um ein Verbrauchergeschäft handelt.

[500] Ein Gerichtsstand kann daher für Web-Anbieter in der gesamten EU vorliegen. Die einzige Abhilfe sind ausdrückliche oder konkludente Ausschlüsse, an welche man sich auch tatsächlich hält. LG Feldkirch 20.10.2003, 3 R 259/03s

[501] Schon teilweise geschäftliche Nutzung beseitigt dieses Privileg: OGH 19.5.2005, 6 Ob 19/05w

[502] Wo der Server steht ist unerheblich: Auch bei Briefen kommt es auf das Absenden und nicht die Ankunft an. Für den Empfänger ist das hier im Gegensatz nicht ersichtlich: Österreichische E-Mail Adressen können vor der ganzen Welt aus verwendet werden. Andererseits sind Poststempel oft nur äußerst schwer lesbar.

[503] Bezüglich des Gerichtsstandes sind die Regelungen des EuGVVO "weicher". Dort reicht es schon aus, wenn die Tätigkeit auf den Wohnsitz des Verbrauchers hin "ausgerichtet" wird. Es ist also *keine* Handlung im Heimatstaat mehr er-

Webseite allein wird, nur weil sie im Inland abgerufen werden kann, noch nicht unbedingt als Werbung im Inland zu qualifizieren sein[504]. Demgegenüber sind Bestellseiten auf Deutsch[505] oder die explizite Möglichkeit, z.B. über eine Listbox, nicht aber die Option, ein Empfangsland in ein Textfeld einzutragen, nach Österreich zu liefern ein Hinweis auf eine Betätigung im Inland. Gleiches wird bei Zahlung über österreichische Konten, nicht aber allgemein bei Kreditkartenzahlung, gelten. Wird hingegen ein österreichischer Domain Name ("*.at") verwendet oder kann eine länderspezifische Darstellung gewählt werden, beispielsweise mittels Landesflaggen, so liegt mit Sicherheit eine Betätigung im bzw. mit Ausrichtung auf das Inland vor, was den Schutz zur Folge hat[506].

Für Endverbraucher legt das österreichische Konsumentenschutzgesetz besondere Schutzvorschriften fest, die auf diese Weise, trotz sonst geltendem ausländischem Recht, gültig bleiben und anzuwenden sind. Um ein "Verbrauchergeschäft" im Sinne des KSchG handelt es sich, wenn jemand, für den das Geschäft zum Betrieb seines Unternehmens gehört, ein Rechtsgeschäft mit jemandem abschließt, für den dieses Geschäft eben nicht zum Betrieb eines Unternehmens gehört[507]. Wichtigster Punkt ist, dass viele Bestimmungen dieses Gesetzes zwingender Natur sind, also entgegenstehende Vereinbarungen zum Nachteil des Verbrauchers nichtig sind.

Derartige Ausschlüsse sind insbesondere (§ 6 Abs 1 KSchG):

- Bindungswirkung des Angebots (Z1): Der Unternehmer darf sich keine unangemessen lange oder unbestimmte Frist für die Annahme des Angebotes festlegen. Im E-Commerce wird die Frist wegen der schnellen Kommunikation und starken EDV-Unterstützung regelmäßig sehr kurz sein. Hier gibt das E-Commerce Gesetz einen Hinweis, da dort 30 Tage als Höchstgrenze vorgesehen sind (siehe dazu später im Detail).
- Haftungsausschlüsse (Z9): Der Unternehmer kann den Ersatz von Personenschäden nicht einschränken und auch sonst seine Haftung für Vorsatz und grobe Fahrlässigkeit nicht ausschließen, was besonders beim Softwareverkauf relevant sein dürfte. So ist der Ausschluss der Haftung beim Versand von virenverseuchter Software unmöglich, da das Unterlassen der Prüfung jedenfalls heutzutage grobe Fahrlässigkeit darstellt.
- Zusätzliche Beweislast (Z11): Dem Verbraucher darf keine andere als die gesetzliche Beweislast auferlegt werden.

---

forderlich und es muss auch *keine besondere Tätigkeit* mehr entfaltet werden: Internet ⇒ Gerichtsstand beim Verbraucher, außer dieser Staat wird als Ziel explizit ausgeschlossen und man hält sich auch normalerweise an diesen Ausschluss. Siehe LG Feldkirch 20.10.2003, 3 R 259/03s sowie LG Salzburg 28.1.2004, 53 R 13/04z

[504] Siehe auch: Fallenböck/Haberler: Rechtsfragen bei Verbrauchergeschäften im Internet (Online-Retailing), RdW 1999, 505. Obwohl der Anbieter mit den positiven Effekten des Internets auch die negativen akzeptieren muss, darf dieses Kriterium nicht völlig leer laufen. Als Beispiele zum Ausschluss der an sich weltweiten Wirkung werden ein Disclaimer sowie das insgesamte Erscheinungsbild angeführt.

[505] Eine Versteigerung auf eBay.de wurde problemlos als auch nach Österreich gerichtet betrachtet: OLG Wien 22.3.2006, 13 R 257/05t Das Ausfüllen des Bestellformulars erfolgte unbestrittenerweise in Österreich. Daher war österreichisches (Konsumentenschutz-) Recht anzuwenden. Die Verwendung von Englisch bedeutet aber aufgrund ihrer Internationalität nicht grundsätzlich einen Ausschluss.

[506] Eine genaue Darstellung erfolgt in Mochar/Seidl: Internationales Verbraucherschutzrecht und e-commerce. ÖJZ 2003/13, die eine universelle Ausrichtung jedes Internet-Auftritts annehmen. Dem Verkäufer bleibt dann nur mehr die Möglichkeit, Verträge entweder abzulehnen oder das "fremde" Recht zu akzeptieren.

[507] Geschäfte zwischen Endverbrauchern sind daher nicht erfasst! Beispiele hierfür wären Tauschbörsen oder Flohmärkte, selbst wenn sie im Internet von einer Firma organisiert werden, da der Verkauf/Kauf regelmäßig nicht mit der Firma zustande kommen wird, die hier nur die Rolle eines Vermittlers übernimmt. Praktisch bedeutsam z.B. bei eBay.

- Überhöhte Verzugszinsen (Z13): Kommt der Verbraucher mit seiner Zahlung in Verzug, so dürfen die hierfür verlangten Zinsen höchstens fünf Prozent über den Zinsen bei vertragsgemäßer Zahlung betragen. Von den Zinsen sind Betreibungs- und Einbringungskosten zu unterscheiden, die sehr wohl verlangt werden können[508].
- Irrtumsausschluss (Z14): Unterliegt der Verbraucher bei Abgabe seiner Erklärung (Angebot/Annahme) einem relevanten Irrtum, so kann dieser immer, natürlich nur entsprechend den sonstigen normalen Voraussetzungen, geltend gemacht werden; ein Ausschluss der Irrtumsanfechtung ist nicht möglich. Auch sind Klauseln des Inhalts, dass bestimmte Zusagen des Unternehmers über Produkteigenschaften keine wesentliche Beschaffenheit oder Hauptsache betreffen, unzulässig. Dies würde dazu führen, dass eine Anfechtung wegen Fehlen oder Wegfall der Geschäftsgrundlage nicht mehr möglich ist. Wesentliche angepriesene Eigenschaften müssen daher auch tatsächlich vorliegen. Ansonsten kann der Verbraucher den Vertrag anfechten.

VII.2.2. Distanzgeschäfte/Fernabsatz- und E-Commerce-Richtlinie

Die Vorschriften der EU-Fernabsatzrichtlinie wurden in das Konsumentenschutzgesetz, hauptsächlich in den §§ 5a-i KSchG, integriert. Danach treffen den Unternehmer zwei getrennte Informationspflichten und der Konsument erhält ein besonderes Rücktrittsrecht. Weiters bestehen noch Sonderregeln für die Lieferfrist und beim Missbrauch von Zahlungskarten, was zwar nicht unbedingt zum Thema Konsumentenschutz gehört, aber wichtige psychologische Faktoren im E-Commerce darstellen. Hinsichtlich dieser Schutzbestimmungen ist die Rechtswahl eines nicht EWR-Staates unbeachtlich, wenn ansonsten ein solches Recht anzuwenden wäre (§ 13a Abs 1 KSchG).

VII.2.2.1. Anwendbarkeit

Diese Sonderbestimmungen kommen immer dann zur Anwendung, wenn ein Verbraucher mit einem Unternehmer einen Vertrag abschließt, wobei ausschließlich Fernkommunikationsmittel verwendet werden. Ein einziges persönliches Treffen genügt daher bereits für einen Ausschluss dieser Regeln. Hiervon sind nicht nur E-Commerce, sondern auch Teleshopping und der gesamte Versandhandel (Kataloge + Telefon, Bestellkarten etc.) betroffen. Weitere Voraussetzung ist, dass es sich um ein organisiertes Distanz-Geschäft handelt; d.h. ein einmaliger Verkauf ausschließlich über Fernkommunikationsmittel bei sonst persönlichen Geschäftsverkehr reicht nicht aus. Dies ist wohl eher streng zu beurteilen.

Nicht darunter fällt daher z.B. ein Kauf auf eBay von Privatpersonen, da hier beiderseits Konsumenten auftreten. Ob jedoch ein Verkäufer tatsächlich ein Privater ist und nicht etwa gewerblich tätig ist, kann in vielen Fällen nur sehr schwer abzuschätzen sein. Als Richtwert kann die Anzahl der Geschäftsabschlüsse dienen. So werden die meisten "Powerseller" geschäftlich tätig sein, worunter eine Tätigkeit in der Absicht, sich ein kontinuierliches Einkommen zu verschaffen, zu verstehen ist. Ob eine Gewerbeberechtigung/-anmeldung vorliegt, ist unerheblich! Relevant ist ausschließlich die konkrete Tätigkeit.

Es bestehen einige Ausnahmen, wobei für einen Teil davon gesonderte Regelungen bestehen. Keine Anwendung finden die Bestimmungen beispielsweise Bank- und Wertpapier-

[508] Siehe hierzu jedoch Z 15 desselben Paragraphen, wonach nur zweckentsprechende und notwendige Kosten verlangt werden dürfen und diese gesondert aufgeschlüsselt werden müssen.

dienstleistungen sowie Versicherungsgeschäfte[509], Verträge über Immobilien (sehr wohl anwendbar hingegen in Bezug auf Mietverträge), Warenautomaten und Versteigerungen[510].

VII.2.2.2. Informationsbereitstellung

Bevor der Konsument seine Vertragserklärung abgibt, müssen ihm einige Informationen zur Verfügung gestellt werden. Dies hat *vor* seinem Angebot zu erfolgen, bei einer Werbung des Unternehmers, welche der Konsument nur mehr annehmen muss (rechtlich echtes Angebot), daher schon in der "Werbung". Alle Vertragsbestimmungen müssen dem Kunden so zur Verfügung stehen, dass er sie speichern und reproduzieren kann. Die bereitzustellenden Informationen, welche der Fernabsatz-RL entstammen, sind im Einzelnen:

1. Name und geographische Anschrift des Unternehmers: Ein Postfach reicht nicht aus; es muss sich um eine ladungsfähige Anschrift[511] handeln (d.h. Name, Straße, PLZ, Ort). Für juristische Personen bedeutet dies, dass auch ein für die Person Vertretungsberechtigter genannt werden muss, z.B. Geschäftsführer oder Vorstand.
2. Wesentliche Eigenschaften der Ware oder Dienstleistung: Wichtig für den Rücktritt; erfordert auch die Vollständigkeit der Beschreibung hinsichtlich wichtiger Elemente.
3. Preis inklusive aller Steuern: Dies beinhaltet auch die Umsatzsteuer, da für B2B das Gesetz ja nicht anwendbar ist.
4. Lieferkosten: Porto, Verpackung, Versand, Versicherung, zusätzliche Gebühren[512] etc.
5. Einzelheiten zu Zahlung und Lieferung: Wann und wie diese erfolgt, z.B. versichert oder nicht, durch Paketdienst oder die Post etc.
6. Bestehen des Rücktrittsrechts, sofern es nicht durch das Gesetz ausgeschlossen ist: Eine Belehrung über die zustehenden Rechte (erfolgt meistens in den AGBs) ist nötig.
7. Kommunikationskosten über den Grundtarif: Bei Mehrwertnummern. Kosten des Internetzugangs selbst zählen hier nicht; diese sind "Grundtarif".
8. Bindungsdauer für Angebot und Preis: Die Geltungsdauer ist explizit festzulegen, sofern es sich rechtlich gesehen überhaupt um ein Angebot handelt. Derartige Regelungen sind meist ebenfalls in den AGBs enthalten, etwa in folgender Form: Kein Angebot sondern Werbung, Preis freibleibend, unverbindlich, ...
9. Mindestlaufzeit bei Dauerschuldverhältnissen: Handy-Bindungsfrist, Mindest-Abonnement-Zeitraum etc.

Bei diesen Informationen handelt es sich um keine schwierig zu erfüllenden oder geheimhaltungswürdigen Elemente und jeder seriöse Anbieter sollte damit keine Probleme haben.

---

[509] Siehe dazu die Richtlinie 2002/65/EG des Europäischen Parlamentes und des Rates vom 23. September 2002 über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 90/619/EWG des Rates und der Richtlinien 97/7/EG und 98/27/EG

[510] Achtung: Auktionen wie bei eBay sind keine Versteigerungen im Rechtssinne, daher *gelten* die folgenden Vorschriften! Siehe dazu Schummer/Weinberger: Zum Rücktrittsrecht bei "Online-Auktionen": JBl 2005, 765; Besenböck/Bitriol: Zum Ersten, zum Zweiten – Rücktritt! ecolex 2005, 104; sowie OLG Oldenburg 28.7.2005, 8 U 93/05 und BGH 3.11. 2004, VIII ZR 375/03. Dagegen jedoch Anderl: Versteigerung bleibt Versteigerung - Kein Rücktrittsrecht bei Online-Auktionen. RdW 2005, 440 http://www.dbj.at/publ299.pdf

[511] Siehe "3 Pagen" OGH 23.0.2003, 4 Ob 175/03v: Die Angabe eines Postfachs erfüllt die Vorschrift nicht und ist auch wettbewerbswidrig, da Konsumenten die Rechtsdurchsetzung erschwert wird (Beim Einbringen einer Klage ist eine ladungsfähige Anschrift des Beklagten anzugeben).

[512] Etwa Provisionen an Dritte; beispielsweise eBay Gebühren oder Gebühren bestimmter Zahlungsarten wie Nachnahme.

Praktische Schwierigkeiten können höchstens der Gesamtpreis inkl. Steuern sowie die Versandkosten bereiten, sofern international verkauft wird. In dieser Hinsicht ist daher, neben der Bedeutung für die generelle Anwendbarkeit, eine genaue Definition der Kunden-Nationalität, also wohin verkauft wird, wiederum von großer Bedeutung.

Folgende Punkte entstammen der E-Commerce RL (siehe § 9 ECG) und sind zusätzlich erforderlich, falls nicht der gesamte Vertrag ausschließlich durch den Austausch von E-Mail oder vergleichbarer individueller Kommunikation erfolgt:

10. Die einzelnen technischen Schritte, die zu einem Vertragsabschluss führen: D.h. Hilfe-Seiten, welche den Bestellvorgang erläutern, sind notwendig.
11. Angaben, ob der Vertragstext nach Vertragsabschluss vom Anbieter gespeichert wird und ob er zugänglich sein wird (künftige Möglichkeit zur Einsichtnahme): Damit der Konsument sich die Seite notfalls ausdruckt, abspeichert etc.
12. Technische Mittel zur Erkennung/Korrektur von Eingabefehlern vor Bestellungsabgabe: Für den potentiellen Kunden hat vor dem endgültigen Abschluss der Bestellung noch einmal die Möglichkeit zur Korrektur seiner Eingaben zu bestehen.
13. Für den Vertragsabschluss zur Verfügung stehende Sprachen: Damit der Konsument sich diejenige aussuchen kann, welche er am besten versteht.
14. Freiwillige Verhaltenskodizes denen sich der Verkäufer unterwirft samt elektronischem Zugang zu diesen; sofern anwendbar.

Durch die E-Commerce RL, in § 5 ECG umgesetzt, kommen noch folgende Zusatzinformationen hinzu, welche leicht, unmittelbar und ständig verfügbar sein müssen, also schon in etwaiger Werbung, d.h. unabhängig von jedwedem zukünftigen Vertragsabschluss. Besonderheiten bestehen weiters für reglementierte Berufe wie Ärzte, Rechtsanwälte, Ziviltechniker etc. Zu beachten ist, dass diese folgenden Anforderungen *nicht* konsumentenschutzbezogen sind, sondern auch im B2B Verkehr einzuhalten sind (vergleiche dazu besonders Punkte 20 und 3)!

15. Angaben, die es ermöglichen, schnell mit dem Diensteanbieter Kontakt aufzunehmen (Telefon, Fax, ...) und unmittelbar und effizient mit ihm zu kommunizieren, einschließlich seiner E-Mail-Adresse[513]: Verpflichtung[514] zur Verwendung von E-Mail!
16. Handelsregister- oder gleichwertige Nummer, sofern eine solche Eintragung vorgeschrieben ist: In Österreich ist daher die Firmenbuchnummer zusammen mit dem zuständigen Firmenbuchgericht anzugeben.
17. Wenn eine Zulassung/behördliche Aufsicht für die Tätigkeit nötig ist, Angaben zur Aufsichtsbehörde: Beispielsweise die Bankenaufsicht. Ev. fällt hierunter auch die Gewerbebehörde, da diese die Gewerbeausübung untersagen kann[515].

---

[513] Die E-Mail muss daher direkt angegeben werden. Ein E-Mail Link ist nicht erforderlich. Die Angabe als Grafik, d.h. durch Markieren und Kopieren nicht zu übernehmen, sondern händisch abzutippen, wird wohl noch als schnell und effizient gelten: E-Mail-Adressen sind nicht so lang und komplex, dass dies unzumutbar oder besonders hinderlich wäre.

[514] Für "Diensteanbieter" gemäß Richtlinie 98/48/EG und 98/34/EG ("Richtlinie des Europäischen Parlaments und des Rates über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft"): d.h. Anbieter von el. im Fernabsatz angebotenen Dienstleistungen gegen Entgelt auf individuellen Abruf eines Empfängers.

[515] In Deutschland wird dies anscheinend angenommen (Zuständigkeit der Gemeindeverwaltung für die dGewO): OLG Koblenz 25.04.2006, 4 U 1587/04

18. Bei Unterliegen von Gewerbe- oder berufsrechtlichen Vorschriften sind diese anzugeben (Kammer/Berufsverband/..., Berufsbezeichnung und Mitgliedsstaat, in dem diese verliehen wurde, sonstige Vorschriften und Zugang zu ihnen[516]). Meistens wird hier die Gewerbeordnung zutreffen. Zusätzlich bestehen für bestimmte Berufe Sondergesetze.
19. Wenn die Tätigkeit der Mehrwertsteuer unterliegt, die Identifikationsnummer (wichtig für Firmenkunden): In Österreich die Umsatzsteueridentifikationsnummer (UID-Nr.), welche aus "ATU" gefolgt von acht Ziffern besteht.
20. Sofern Preise angegeben werden, müssen diese klar und eindeutig ausgewiesen werden und insbesondere ist anzugeben, ob Steuern und Versandkosten darin enthalten sind, bzw. welche nicht: Siehe aber die Sonderregelungen für Konsumentengeschäfte oben, die eine Angabe inklusive Mehrwertsteuer erfordern!

Bei Hauslieferungen und Freizeitdienstleistungen, siehe Abschnitt VII.2.2.5, entfallen einzelne dieser Pflichten (Punkte 1-9).

Für E-Commerce bedeutet dies, dass diese Angaben, neben etwaigen AGBs, siehe VII.6.3, einfach abrufbar sein müssen. Es sollten diese Informationen daher auf der Bestellseite wiederholt werden oder ein deutlicher (hervorgehobener) Link zu ihnen platziert werden.

Handelt es sich um Konsumenten, denn zwischen anderen Parteien sind abweichende Vereinbarungen möglich, so ist jeder Bestellungseingang unverzüglich auf el. Wege zu bestätigen, d.h. in der Regel per Rück-E-Mail. Dies ist nicht notwendig, falls der gesamte Vorgang *ausschließlich* per E-Mail oder über andere individuelle Kommunikation erfolgte. Hierbei kann, aber muss es sich nicht um eine Annahme- oder Ablehnungserklärung handeln: Es ist lediglich der Eingang der Kommunikation zu bestätigen! Die exakte Formulierung ist hier besonders wichtig, um nicht unbeabsichtigt das Vertragsangebot des Kunden anzunehmen und ev. später als Verkäufer nicht mehr zurücktreten zu können[517].

VII.2.2.3. Informationserteilung

Während der Erfüllung, jedoch spätestens mit Warenlieferung[518], müssen dem Konsumenten die obigen Informationen (ausgenommen die Punkte 7-9; siehe § 5d Abs 1 KSchG) zugesandt werden, und zwar schriftlich oder auf dauerhaftem Datenträger[519]. Auch diese Pflicht entfällt bei Hauslieferungen und Freizeitdienstleistungen.

Weiters sind folgende zusätzliche Informationen mitzuteilen:

1. Erläuterungen über die Bedingungen und Einzelheiten der Ausübung des Rücktrittsrechts: Damit der Kunde weiß, was er genau tun muss, wenn er vom Vertrag zurücktreten möchte[520].

---

[516] Ein Verweis auf das Rechtsinformationssystem RIS genügt hier.

[517] Siehe "Willenserklärung durch Auto-Reply-E-Mail": LG Köln 16.4.2003, 9 S 289/02

[518] Eine Ausnahme besteht für Mehrwertnummern: Von den Informationen muss nur die geographische Anschrift für Beanstandungen in Erfahrung gebracht werden können. Eine explizite Ansage ist also wohl nicht nötig.

[519] Hierfür werden die Anforderungen sehr niedrig angesetzt: Ist ein Ausdruck möglich (z.B. E-Mail), so ist dies bereits ausreichend: E-Mail, Disketten, CD-ROMs etc. Auch zählt hierzu etwa die Festplatte des Konsumenten. Nicht dauerhaft ist die Webseite als solche alleine. Eine genauere Definition ist allerdings erst in der Finanzdienstleistungs-Fernabsatz-RL enthalten. Diese Information ist nicht mehr nötig, wenn sie bereits vorher derart verfügbar war, z.B. im Katalog.

[520] In Deutschland existiert hierzu ein offizielles Muster in Anlage 3 des BGB-InfoV, die weiters in § 14 Abs 1 festlegt, dass diese jedenfalls ausreicht. Problematisch an ihr ist, dass sie Fehler enthält; siehe Richard/Schmidt, Offizielle Mus-

2. Die Anschrift des Unternehmers, bei der Reklamationen vorgenommen werden können: Dies kann dieselbe Anschrift wie oben sein, jedoch auch eine andere. Auch hier ist ein Postfach nicht erlaubt, da der Kunde dort persönlich vorsprechen können soll.
3. Informationen über Kundendienst und Garantiebedingungen: Sofern vorhanden.
4. Kündigungsbedingungen bei Dauerschuldverhältnissen (nicht bei Dauer unter einem Jahr): Die Angabe ist nötig, damit der Konsument später einfach herausfinden kann, wie der Vertrag beenden werden kann. Bei kurzer Laufzeit wird offenbar angenommen, dass er sich diese merkt.

VII.2.2.4. Rücktrittsrecht

Bei einem im Fernabsatz geschlossenen Vertrag kann der Verbraucher innerhalb von sieben Werktagen[521] zurücktreten, wobei die rechtzeitige Absendung der Rücktrittserklärung ausreicht. Die bloße Rücksendung der Ware alleine[522] reicht nicht. Eine besondere Form, z.B. Schriftform, wie sonst teilweise im KSchG gefordert, ist jedoch nicht notwendig. Ein Rücktritt kann daher auch mündlich bzw. per E-Mail erfolgen. Hat der Unternehmer seine Pflicht zur Informationserteilung, und damit auch zur Informationsbereitstellung, nicht erfüllt, so verlängert sich diese Frist auf *drei Monate*. Werden innerhalb dieses Zeitraums die Informationen übermittelt, so beginnen die sieben Tage mit Empfang der (nachgereichten) Informationen durch den Konsumenten zu laufen. Diese Frist beginnt mit dem Eingang der Ware beim Empfänger, d.h. nicht bei der Postaufgabe, der Rechnungserstellung etc.: Der Kunde soll die Ware prüfen können, was deren Empfang voraussetzt. Bei Dienstleistungen beginnt die Rücktrittsfrist mit dem Tag des Vertragsabschlusses. Fehlerhafte Informationserteilung oder –bereitstellung hat ansonsten normalerweise keinen Einfluss auf die Gültigkeit des Rechtsgeschäftes[523].

Nach einer Rücktrittserklärung ist das gesamte Geschäft rückabzuwickeln. Der Verbraucher erhält geleistete Zahlungen ohne Abzug zurück[524] und der Unternehmer die Ware sowie gegebenenfalls Benützungs- und Wertminderungsersatz[525]. Die Tatsache, dass die Ware nicht mehr im Erstbesitz ist, gilt explizit nicht als Wertminderung. Für den Konsumenten dürfen außer den Kosten der Rücksendung, und diese auch nur bei expliziter Vereinbarung, keine zusätzlichen Kosten auferlegt werden (z.B. Bearbeitungsgebühren).

---

terwiderrufsbelehrung unwirksam? http://www.internetrecht-rostock.de/lg-halle-widerrufsbelehrung.htm Siehe dazu auch LG Halle 13. 5. 2005, 1 S 28/05. In Österreich existiert keine derartige Vorschrift.

[521] Samstag ist hierfür abweichend von der normalen österreichischen Regelung *kein* Werktag! Längere Fristen sind (freiwillig) möglich. In Deutschland ist die Mindestfrist generell, über die Richtlinie hinaus, 14 Tage lang. Da bei Verkauf an Deutsche Verbraucher auch Deutscher Konsumentenschutz gilt, ist in diesem Fall auch von österreichischen Verkäufern die längere Frist anzuwenden!

[522] Ev. schon, falls daraus der Rücktrittswille *eindeutig* ablesbar ist, z.B. durch eine kurze Bemerkung auf der mit zurückgeschickten Rechnung: "Storno", "Rücktritt", ... Ansonsten könnte es sich auch um eine Reklamation handeln. Die bloße Nicht-Annahme der Ware ist jedoch keinesfalls ausreichend; dann beginnt auch die Rücktrittsfrist nicht zu laufen.

[523] Siehe LG Feldkirch 21.6.2005, 2 R 154/05w: Fehlerhafte erfüllte Informationspflichten führen nicht zur Nichtigkeit eines Vertrages über Telefon-Mehrwertdienstleistungen. Diese unterliegen den Regeln für Fernabsatz (OGH 29.4.2003, 4 Ob 92/03p) und das Fehlen von Informationen kann wettbewerbswidrig sein (OGH 18.11.2003, 4 Ob 219/03i), aber nur Irrtümer über Ware und Preis führen im Allgemeinen dazu, dass ein Kaufvertrag erst gar nicht zustande kommt.

[524] So bald wie möglich, jedoch auf jeden Fall binnen 30 Tagen.

[525] Siehe HG Wien 2.12.2004, 50 R 95/04h: Die Benutzung eines Computermonitors für zehn Tage (43 Stunden Betriebsdauer) trotz Ausübens des Rückgaberechts führte zu einem Nutzungsentgelt von 15 % des Kaufpreises. Die Wertminderung durch zwischenzeitliches Erscheinen eines Nachfolgemodells wurde explizit nicht miteinberechnet, da sie nicht auf die Nutzung zurückzuführen ist. Siehe dazu auch Maderbacher/Otto: Fernabsatz: Vertragsrücktritt nur gegen Entgelt? ecolex 2006/117

Für Finanzierungskredite in wirtschaftlicher Einheit mit dem Vertrag bestehen Sonderregelungen, welche den gleichzeitigen entschädigungsfreien Rücktritt vom Kreditvertrag ermöglichen. Dies dient dazu, dass nicht der Kredit, welcher für den Kauf der Ware aufgenommen wurde, weiter besteht, während der Kauf selbst aufgrund des Rücktritts wegfällt. Voraussetzung ist jedoch ein enger Zusammenhang mit dem Kauf, z.B. die Vermittlung des Kredits durch den Verkäufer.

In folgenden Fällen ist das Rücktrittsrecht ausgeschlossen:

- Dienstleistungen, deren Ausführungen vereinbarungsgemäß innerhalb von sieben Werktagen nach Vertragsabschluss beginnen[526]: Hintergrund ist, dass meist kein Ersatz-Geschäft für den Unternehmer mehr möglich ist.
- Waren und Dienstleistungen, deren Preis von der Entwicklung der Finanzmärkte abhängt, auf die der Unternehmer keinen Einfluss hat: Kein Rücktritt bei Fehlspekulationen. Bloßer Wertverlust durch die Zeit[527] zählt jedoch nicht als Ausschlussgrund. Dies dürfte kaum Bedeutung besitzen, da entsprechende Produkte wohl nicht unter diese Richtlinie fallen, sondern unter die Finanz-Fernabsatz-Richtlinie (Relikt aus dem früheren gemeinsamen Entwurf). Ev. könnte dies auf Käufe von Produkten übertragen werden, welche an Warenbörsen gehandelt werden (z.B. Metalle); dies besitzt jedoch wiederum (Konsumenten!) wohl kaum eine Bedeutung.
- Sonderanfertigungen nach Kundenspezifikationen[528]: Diese kann der Händler nicht mehr weiterverkaufen. Wichtig ist, dass das Konzept der "Sonderanfertigung" nicht zu weit gesehen werden darf: So wurde ein nach Kundenwünschen zusammengestellter PC nicht als Sonderanfertigung angesehen, da er ohne großen Aufwand und ohne Beschädigung wieder in seine Einzelteile zerlegt werden kann, welche ihren Wert unverändert beibehalten[529].
- Verderbliche oder zur Rücksendung ungeeignete Waren sowie Waren mit überschrittenem Verfalldatum: Frische Lebensmittel oder Ähnliches. Was genau "zur Rücksendung ungeeignet" ist, ist sehr umstritten und unklar. Angeführte Beispiele sind Handys mit bekannter Super-PIN, getragene Unterwäsche, alle Arten von Lieferungen per Download[530] (Musik, Programme etc.), oder Heizöl[531].

---

[526] Entgegen anderer Meinungen handelt es sich bei Software-Download nicht um eine Dienstleistung: Es wird als Hauptpunkt des Vertrages nicht für die Bereitstellung zum Download bezahlt (ev. Hunderte von Euro!), sondern für die Einräumung der Benutzungsbewilligung. Hier ist kein Unterschied zum normalen "Verkauf" auf CDs oder anderen Datenträgern zu erkennen, der eindeutig als Warenkauf und nicht als Dienstleistung zu qualifizieren ist. Auch dort muss die Ware im Versandhandel verschickt werden, was nur durch die Vornahme bestimmter Tätigkeiten erfolgen kann (Verpacken, Transport zur Post etc.), was aber dennoch nicht zur Annahme einer Dienstleistung führt!

[527] Etwa durch stetig fallende Preise (im Urteil wurde als "nicht zur Rücksendung geeignet" untersucht): OLG Dresden 23.8.2001, 8 U 1035/01

[528] Bestellung von Standardsoftware speziell für einen besonderen Kunden ist keine Sonderanfertigung nach Kundenspezifikationen, da nichts "verändert" wird: Die Software wird so verkauft, wie sie ist. LG Memmingen 10.12.2003, 1 H O 2319/03 Anders aber, wenn die Software tatsächlich für den Kunden speziell umprogrammiert wird.

[529] Dies ist sicherlich ein Grenzfall: So ist etwa eine CPU mit aufgeklebtem Kühlkörper nicht mehr so einfach zu "zerlegen", genauso wie das Zerlegen einen erheblichen Aufwand (Arbeit, Rückbuchung, Einlagern, ...) verursachen kann. Siehe BGH 19.3.2003, VIII ZR 295/01

[530] Meiner Meinung nach nicht; siehe Sonntag: Das Rücktrittsrecht nach dem Fernabsatzgesetz beim Online-Musikkauf. In: Schweighofer/Liebwald/Augeneder/Menzel (Hrsg.): Effizienz von e-Lösungen in Staat und Gesellschaft. Düsseldorf: Boorberg 2005, 419. Ein Verzicht des Verkäufers auf eine Versiegelung, welche auch bei Download technisch möglich ist (DRM), darf den Konsumenten nicht belasten.

[531] Dieses dürfte jedoch unter "Hauslieferung" fallen und dadurch ohnehin ausgenommen sein. Bei der sonst angeführten Vermischung mit altem Öl ist hingegen an den Untergang der Sache durch Konfusion zu denken.

- Entsiegelte Audio-, Video- oder Software-Datenträger: Es ist anzunehmen, dass eine Kopie hergestellt wurde, wenn auch verbotenerweise, was im Keim erstickt werden soll. Ein anderer Aspekt ist etwa, dass z.B. ein Film dann bereits "konsumiert" worden sein kann.
- Zeitungen, Zeitschriften und Illustrierte (nur bei Einzelexemplaren): Diese sind nicht mehr aktuell und daher unverkäuflich. Abonnements für derartige Waren unterliegen dem Rücktrittsrecht sehr wohl. Es kommt daher zu einer Kompensationspflicht des Konsumenten für bereits erhaltene Exemplare.
- Wett- und Lotteriedienstleistungen: Bei Verlust der Wette soll kein Rücktritt möglich sein (Beispiel: Lottozahlen werden nicht gezogen).
- Hauslieferungen und Freizeitdienstleistungen: Siehe sogleich näher!

VII.2.2.5. Ausnahme: Hauslieferungen und Freizeitdienstleistungen

Informationsbereitstellung, Informationserteilung und Rücktrittsrecht sind bei so genannten "Hauslieferungen und Freizeitdienstleistungen" nicht erforderlich bzw. möglich.

Unter Hauslieferungen versteht man die Lieferung von Lebensmitteln, Getränken und sonstigen Haushaltsgegenständen des täglichen Bedarfs, sofern sie an den Wohnsitz, den Aufenthaltsort oder den Arbeitsplatz des Verbrauchers im Rahmen regelmäßiger Fahrten geliefert werden (z.B. Pizza-Zustellung). Die Informationspflichten wären zu aufwendig und ein, für den Konsumenten kostenloser, Rücktritt ist aus verständlichen Gründen nicht möglich. Da es sich nicht um eine Dienstleistung handelt, trifft die Ausnahme "Beginn binnen sieben Tagen" nicht zu.

Freizeitdienstleistungen sind Dienstleistungen in den Bereichen Unterbringung und Beförderung (Hotel-, Taxi-Bestellung) sowie Lieferung von Speisen und Getränken sowie Freizeitgestaltung, wenn sie zu einem bestimmten Zeitpunkt oder in einem exakt bestimmten Zeitraum zu erbringen sind (=Buffet-Service). Der Grund ist hier, dass eine spätere Ersatz-Belegung des Termins meist nicht möglich sein wird und so der Verkäufer unverhältnismäßig benachteiligt würde.

VII.2.2.6. Leistungsfrist

Ist nichts anderes vereinbart, so hat der Unternehmer die Leistung binnen 30 Tagen nach der Bestellung des Kunden auszuführen, sofern er das Angebot annimmt[532]. Dies gilt wiederum nicht für Hauslieferungen und Freizeitdienstleistungen. Kann er die Bestellung innerhalb dieser Zeit nicht ausführen oder will er das Angebot überhaupt nicht annehmen, so hat er den Verbraucher davon *unverzüglich* zu verständigen und etwaige geleistete Zahlungen zurückzuerstatten. Erfolgt dies nicht oder nicht rechtzeitig, wird er eventuell schadenersatzpflichtig, aber es kommt dennoch kein Vertrag zustande. Diese Pflicht besteht unabhängig von der Bestätigung des Eingangs der Bestellung per E-Mail.

VII.2.2.7. Missbrauch von Zahlungskarten

Wenn im Fernabsatz eine Zahlungskarte, worunter hauptsächlich Kreditkarten fallen, oder deren Daten (=Kreditkartennummer, Ablaufdatum, Name) missbräuchlich verwendet wird,

[532] Anders in Deutschland: Sofern keine Lieferfrist vereinbart oder auf eine solche hingewiesen wurde, hat die Lieferung *sofort* zu erfolgen, da Lieferfristen jederzeit problemlos aktualisiert werden könnten. BGH 7.4.2005, I ZR 314/02

so kann der Inhaber Rückerstattung verlangen. Die Besonderheit liegt darin, dass er die Rückzahlung vom Aussteller der Karte verlangen kann (=der Kreditkartengesellschaft; nach der RL nur allgemein festgelegt, sodass dies im Ausland auch der Geschäftsinhaber sein könnte), und zwar unabhängig davon, ob den Aussteller ein Verschulden trifft. Die Regelung gilt sowohl für Unternehmer wie für Konsumenten, doch können Unternehmer sie vertraglich abbedingen, während sie gegenüber Konsumenten zwingend ist. Zu beachten ist, dass ein Recht auf Rückerstattung nur bei sorgfältigem Umgang besteht, d.h. wenn den Inhaber der Karte kein Verschulden trifft[533].

VII.3. Zugang von Erklärungen

Auch auf elektronischem Wege müssen Erklärungen dem Empfänger zugehen (siehe dazu § 862 ABGB), bevor Rechtsfolgen ausgelöst werden. Hier stellen sich Probleme, die zwar auch bei gewöhnlichen Käufen auftreten können, jedoch selten sind, wie etwa die automatische Entgegennahme von Erklärungen durch Maschinen. Wann bei verschiedenen Kommunikationsformen nun der maßgebliche Zeitpunkt für den Zugang der Erklärung vorliegt, wird im Einzelnen aufgezeigt.

VII.3.1. E-Mail

E-Mail ist eine Kommunikation unter Abwesenden, also ein asynchrones Kommunikationsmedium. Ein Vergleich mit konventionellen Briefen ist möglich. Diese gelten jedenfalls dann als zugegangen, sobald sie der Empfänger tatsächlich in Händen hält. Zusätzlich gilt als Zugang auch die üblichere Form des Einwurfs in einen Postkasten bzw. allgemeiner: wenn die Mitteilung in den Machtbereich des Empfängers gelangt sind. Hier sind jedoch einige zeitliche Besonderheiten zu beachten: Ein Zugang liegt nur dann vor, wenn der Empfänger die Möglichkeit der Kenntnisnahme hat und dies nach der Verkehrsauffassung auch zu erwarten ist. Bei Geschäftspostkästen kann daher nur an Werktagen und während der normalen Geschäftszeit ein Zugang erfolgen. Ein Einwurf außerhalb dieser Zeiten bewirkt den Zugang erst zu dem nächsten innerhalb dieser Zeiten liegenden Moment. Im Gegensatz dazu ist bei Privatpersonen ein Zugang normalerweise einmal täglich tagsüber bzw. am Abend anzunehmen, am Wochenende jedoch nur bedingt.

Bei E-Mails liegt im Gegensatz dazu ein Zugang nur dann vor, wenn der Empfänger auch tatsächlich davon Kenntnis nehmen kann. So auch die E-Commerce RL (Art. 11 Abs 1), die bei Bestellungen und Empfangsbestätigungen für den Zugang auf die Abrufmöglichkeit abstellt, also nicht das Einlangen am Mailserver[534]. Maßgeblich ist daher, wann die Mail auf dem Mailserver des Endempfängers einlangt[535] und abrufbar ist. Die Nicht-

---

[533] Als Verschulden wird z.B. bereits angesehen, wenn die Kreditkartennummer irgendwann einmal über eine unverschlüsselte Internet-Verbindung übertragen wird. In diesem Fall kann zwar die Rückerstattung verlangt werden, gleichzeitig besitzt das Kreditkartenunternehmen jedoch einen gegenläufigen Schadenersatzanspruch.

[534] Die Umsetzung im E-Commerce Gesetz legt in § 12 fest, dass der Zugang erfolgt, wenn der Empfänger sie "unter gewöhnlichen Umständen abrufen kann". Hierbei sind die technischen Möglichkeiten maßgeblich, nicht die Verfügbarkeit der Personen (Erläuterungen zur Regierungsvorlage). Die Stellungnahme des Vereins für Konsumenteninformation tritt dieser Interpretation entgegen und stellt dagegen auf die Geschäftszeiten ab.

[535] Siehe dazu auch § 26a ZustellG in der früheren Fassung, wonach eine Zustellung vorlag, wenn die Sendung "in den el. Verfügungsbereich des Empfängers gelangt" war. Hier war nur die Abwesenheit von der Abgabestelle als aufschiebendes Hindernis angeführt, sodass dem eine Unmöglichkeit der Abfrage gleichzuhalten war. Die neue Fassung in § 34 Abs 1 ZustellG legt demgegenüber fest, dass es für die Rechtsfolgen auf den "Zeitpunkt der erstmaligen Versendung einer Verständigung" ankommt. Dies beruht darauf, dass nach zwei erfolglosen el. Benachrichtigungen eine posta-

Erreichbarkeit dieses Rechners für den Benutzer verhindert den Zugang solange, als dieses Hindernis besteht. Hier besteht das Problem, dass der Absender dies nicht weiß und auch nicht zu erwarten braucht. Diese Schwierigkeit liegt auch im Machtbereich des Empfängers, da dieser seinen eigenen Provider selbst bestimmt. Für den genauen Zeitpunkt ist wohl weiter analog zu Briefen bei Unternehmen die Geschäftszeiten (praktisch sofort: heute kann kontinuierliche Überwachung des E-Mail-Eingangs erwartet werden) bzw. einmal täglich bei Privatpersonen maßgeblich.

VII.3.2. Webseiten und -Formulare

Beim Ausfüllen von Formularen im WWW bzw. dem zur Verfügung stellen von Webseiten taucht die Frage auf, ob es sich erstens um synchrone oder asynchrone Kommunikation handelt und zweitens, ob eine solche Erklärung rechtlich gesehen überhaupt zugehen kann, da in vielen Fällen keine natürliche Person diese wahrnimmt. Der zweite Fall ist von dem oben (VII.1.1) erläuterten der unbewussten Erklärungsabgabe zu unterscheiden: Hier geht es um den entgegengesetzten Akt, die Entgegennahme der Erklärung und nicht deren Abgabe. Es kommt wieder der allgemeine Grundsatz zur Anwendung, dass es genügt, wenn eine Erklärung in den Machtbereich des Empfängers gelangt. Eine tatsächliche Kenntnisnahme ist nicht unbedingt erforderlich. Wird ein technisches Gerät zur Entgegennahme von Erklärungen eingerichtet, so trägt dessen Verwender die damit verbundenen Gefahren. Erklärungen mittels Eingaben in Web-Formulare gehen daher dem Inhaber der Webseiten sofort mit dem Empfang der Daten auf dem Webserver zu, selbst wenn er einen externen Betreiber für den Server verwendet, da dieser zu seiner Sphäre zählt.

Meiner Meinung nach handelt es sich bei Eingaben auf statisch bereitgestellten Webseiten um Erklärungen unter Abwesenden (=asynchrone Kommunikation), da eine solche Webseite nicht an einzelne Personen adressiert werden kann und daher ein Zugang zu einem bestimmten Zeitpunkt vom Erklärenden nicht erwartet werden kann und wird. Der Zugang tritt daher unmittelbar mit dem Abruf ein. Diese Unterscheidung ist von Bedeutung für eine eventuelle Bindungsfrist des Angebots: Da Webseiten jedoch meist nur Werbung darstellen, besitzt dies geringe praktische Bedeutung.

Ähnliches gilt bei dynamisch generierten Webseiten, die auf Anforderung eines Benutzers hin erstellt werden. Ob dieser Benutzer namentlich bekannt ist oder nicht, ist unerheblich. Hierbei dürfte es sich ebenso um Erklärungen unter Abwesenden handeln. Im Gegensatz zu Chat (siehe unten) wird im WWW eine sofortige Antwort nicht erwartet, ganz im Gegenteil, es handelt sich um ein zustandsloses Protokoll, bei dem davon ausgegangen wird, dass eine beliebige, und oft lange, Zeit bis zur nächsten Anforderung vergeht. Die Verwendung entspricht im Verkehrsgebrauch eher dem des Briefverkehrs: Antworten (z.B. in Formularen) werden längere Zeit überlegt und geändert, bis sie dann schließlich abgeschickt werden, oder eben auch nicht. Der Zugang von Erklärungen erfolgt daher mit dem tatsächlichen Eingang in den Machtbereich des Empfängers (Server-/Benutzerrechner). Ob eine Bestätigung erhalten wird, z.B. Antwortseite oder Fehlermeldung[536], obwohl die Daten korrekt gespeichert wurden, ist ohne Bedeutung für Zeitpunkt und Tatsache des Zugangs.

---

lische durchgeführt wird. Letztere erfolgt sofort, falls eine E-Mail (technisch) nicht abgeliefert werden kann, z.B. aufgrund einer Fehlermeldung. Diese Regeln gelten nur für behördliche Zustellungen, nicht den normalen Geschäftsverkehr.

[536] Etwa bei der Generierung der Antwortseite nach der erfolgreichen Übernahme der Eingabe.

Anderes könnte bei der Verwendung von Ajax[537] gelten, da hierbei eine sofortige Übermittlung, und ev. auch Antwort des Servers, erfolgt. Weiters können Push-Dienste durch kontinuierliches und regelmäßiges Polling simuliert werden[538]. Für den Benutzer ist jedoch vielfach nicht erkennbar, ob die Reaktion lokal berechnet oder vom Server zurückgeschickt wurde. Im Zweifel wird eher von einer Erklärung unter Abwesenden auszugehen sein, da Benutzer die Webseiten entsprechend dem gewohnten Umgang mit einem Browser beurteilen werden und nicht nach einer besonderen technischen Realisierung.

Da Server rund um die Uhr arbeiten, liegt ein sofortiger Zugang dann vor, wenn eine automatische Verarbeitung erwartet werden kann (der Server ist Adressat). Ergibt sich aus der Erklärung oder den Umständen jedoch, dass eine natürliche Person diese bearbeiten soll, so ist der Zugang erst mit Wiederbeginn der Geschäftszeiten anzunehmen. Hier ist der Server nur ein Kommunikationsmittel ähnlich einem Briefkasten. Dabei können sich Probleme stellen, wenn dieses Unterscheidungsmerkmal (gedachter Empfänger: Rechner oder Mensch?) für den die Erklärung Abgebenden nicht klar ersichtlich ist[539]. Im Zweifelsfall wird bei strukturierten Eingaben (Auswahl von Produkten aus Listen) eine automatische Verarbeitung anzunehmen sein, bei freier Texteingabe (Produktname wird in Textfeld geschrieben) jedoch manuelle Bearbeitung. Ob die Erklärung tatsächlich verarbeitet bzw. angezeigt wird, ist unerheblich. Da es sich um Kommunikation unter Abwesenden handelt, hat eine Antwort aber auch nicht sofort zu erfolgen. Eine angemessene Überlegungs- bzw. Verarbeitungszeit und die Transferzeit für eine Antwort sind zu berücksichtigen.

VII.3.3. Chat

Bei dieser, wenn auch synchronen, Kommunikationsform existieren doch Unterschiede zu einem Telefon. Es könnte sich hier durchaus um schriftliche Kommunikation unter Abwesenden handeln, bei welcher der Transport der Erklärungen eben sehr schnell erfolgt[540]. Meiner Meinung nach handelt es sich jedoch um einen Austausch unter Anwesenden:

- Dass an einem Chat mehrere Personen teilnehmen, ist zwar ein Unterschied zum Telefon, hier aber bedeutungslos. Es besteht etwa auch die Möglichkeit zu Telefonkonferenzen mit mehreren Teilnehmern, welche gleich einem Gespräch unter Anwesenden behandelt werden. Auch in einem persönlichen Gespräch mit mehreren Personen gleichzeitig können rechtsgeschäftliche Erklärungen stattfinden, ohne dass Differenzierungen erfolgen.
- Sollte eine Erklärung übersehen werden, da gleichzeitig viele Meldungen eingehen, so entspricht dies exakt dem Überhören, wenn mehrere Personen gleichzeitig reden.
- Auch das Problem, dass ein Computer abstürzt und dadurch eine eingegangene Meldung nicht mehr angezeigt wird und dies für den Absender der Erklärung auch nicht erkennbar ist, kann von einem Telefonat nicht unterschieden werden. Hier kann es ebenso zu einseitigen technischen Störungen wie einem Wackelkontakt im Apparat kommen, welche für den Sender nicht erkennbar sind.

---

[537] Per JavaScript werden lokal Daten zusammengestellt und an den Server geschickt. Dessen Antwort wird per JavaScript wieder in die Webseiten eingebaut. Der Vorteil liegt darin, dass nicht die gesamte Seite übertragen werden muss, sowie dass kein Seitenwechsel erfolgt. Die Webseite im Browser ähnelt daher stärker einer normalen Applikation.

[538] Ein Beispiel für diese Technik ist die Realisierung eines Chats ohne Plugin, Applet etc. und ohne Seiten-Reload.

[539] Zeitzone, Arbeitszeiten, wo ist der Rechner physikalisch, wo werden die Daten von Menschen verarbeitet, …

[540] Siehe dafür Wendel, Dominik A.: Wer hat Recht im Internet? Aachen: Shaker Verlag 1997

- Auch die einfache Abwesenheit vom Computer beim Chat entspricht direkt dem Telefon, wenn der Hörer beiseite gelegt wird. Beides kann der Sender nicht erkennen.
- Ein Chat dient als Art Internet-Ersatz für das Telefon und wird auch auf die selbe Weise verwendet. Die Verkehrsauffassung entspricht daher viel stärker einer synchronen Kommunikation unter Anwesenden.
- Letztlich kann noch technisch eingewendet werden, dass auch bei einem Telefon bei der heutigen Technik keine direkte Verbindung mehr vorhanden ist. Die Töne werden digitalisiert und nach mehrfacher Zwischenspeicherung und Weiterleitung schließlich am anderen Ende wiederhergestellt. Ein qualitativer Unterschied zu einem Chat, bei dem der Text eingetippt, über mehrere Rechner weitergeleitet, und am anderen Ende wieder angezeigt wird, ist nicht erkennbar. Insbesondere werden Texte bei Chat auch nicht einmal kurz zwischengespeichert, z.B. für bessere Netzwerkauslastung, sondern unverzüglich weitergeleitet.

Eine Erklärung über Chat ist daher sofort zugegangen, d.h. erfolgt unter Anwesenden, und muss, wenn nichts anderes vereinbart wurde, auch sofort beantwortet werden.

VII.3.4. SMS

Erklärungen über SMS, z.B. im M-Commerce[541], sind genauso möglich. Hier handelt es sich, trotz der Schnelligkeit des Mediums, um Kommunikation unter Abwesenden, da diese Briefen ähnlicher sind als Telefonaten. Im Gegensatz zu Chats wird eben nicht erwartet, dass der Empfänger die SMS sofort liest und reagiert (d.h. online ist), insbesondere da ja keine Anmeldung oder ein Start wie bei einem Chat erfolgt, sondern ein Handy rund um die Uhr für SMS empfangsbereit ist. Daher ist eine Erklärung zwar sofort zugegangen, sofern sie am Handy eingelangt ist und nicht noch im Messaging-Center liegt (siehe hierzu die Möglichkeit der Rückmeldung!), jedoch erst nach einer angemessenen Überlegungsfrist zu beantworten.

VII.4. Angebot und Annahme bei E-Commerce

Dieser Abschnitt stellt im Überblick dar, wie bestimmte Formen des Auftretens im E-Business rechtlich zu bewerten sind: Was ist jeweils das Angebot, was die Annahme? Insbesondere ein rechtlich bindendes Angebot, wenn eigentlich nur Werbung geplant war, kann für Unternehmen besonders unangenehm sein.

VII.4.1. Webseiten: Werbung oder Angebot?

Das Angebot von Waren auf Webseiten entspricht fast immer dem Katalog eines Versandhauses. Rechtlich bedeutet dies, dass der Verkäufer zur Stellung von Angeboten einladen, sich aber nicht in Bezug auf jeden möglichen Interessenten fest binden will. Es ist regelmäßig davon auszugehen, dass angebotene Waren nicht in unbegrenzter Stückzahl vorhanden sind und ein fester Bindungswille fehlt. Webseiten sind daher fast ausschließlich unverbindliche Anpreisungen, d.h. Werbung. Dies gilt selbst dann, wenn beliebig vervielfältigbare Produkte wie Software mit el. Auslieferung oder Musik-Downloads angeboten werden: Auch hier wird der Verkäufer zuerst die Kreditwürdigkeit prüfen und daher noch

[541] Beispielsweise der Kauf von Handy-Logos, Handy-Spielen oder Klingeltönen.

keine feste Bindung eingehen wollen. Ausnahmen könnten ev. bei Abonnements oder Vorauszahlung[542] bestehen, da hier der Verkäufer praktisch keinerlei Risiko mehr trägt.

Wählt daher ein Kunde einige Waren aus und legt sie in seinen Warenkorb, schreitet zum "Check-out" und wählt Zahlungs- und Versandart, so wird hiermit ein ausführliches und bindendes Angebot erstellt, dem der Anbieter zustimmen kann oder nicht. Dies ist insbesondere deshalb wichtig, da Webseiten international zugänglich sind und es der Verkäufer sich oft vorbehält, nur in bestimmte Länder zu liefern. Gründe dafür können gesetzliche Gebote sein, bestimmte Waren in manche Länder nicht[543] oder nur unter besonderen Bedingungen zu liefern.

Die Annahme durch den Verkäufer kann auf verschiedene Arten erfolgen: Einerseits kann die Rückmeldung auf der Webseite oder in der Bestätigungs-E-Mail eine bloße Empfangsbestätigung sein (etwa "Vielen Dank für Ihre Bestellung"), andererseits aber auch eine explizite Annahme (beispielsweise "Wir danken für Ihren Auftrag. Ihre Bestellung wird am 25. Juni ausgeliefert werden."). Im fast ausschließlich[544] in der Praxis vorkommenden ersteren Fall erfolgt die Annahme später entweder ausdrücklich, z.B. per E-Mail, oder durch tatsächliche Entsprechung, also den Versand der Ware. Fast immer (siehe die bei Konsumenten verpflichtende Benachrichtigung über den Eingang der Bestellung; § 10 Abs 2 ECG) wird zusätzlich zur Rückmeldung direkt auf den Webseiten eine E-Mail versandt, welche wiederum eine der beiden Formen, Bestätigung oder Annahme, darstellen kann.

Bei der Entscheidung, ob eine Mitteilung eine Annahme oder lediglich eine Empfangsbestätigung darstellt, ist zu berücksichtigen, wie ein redlicher Empfänger der Mitteilung diese unter Berücksichtigung aller Umstände verstehen darf. Ein guter Hinweis für eine Annahme ist etwa, wenn ein fixer Liefertermin genannt oder die Lieferung fest zugesagt wird. Wendungen der Art "Ihre Bestellung wird in Kürze bearbeitet werden" deuten hingegen auf eine bloße Empfangsbestätigung hin. Die Formulierung der Antworten auf Webseite und E-Mail sind rechtlich schwierig und sollten von Spezialisten, z.B. Rechtsanwälten, vorgegeben werden, um exakt die gewünschten rechtlichen Konsequenzen sicherzustellen.

VII.4.2. "Persönliche Warenkörbe"

Unter einem "persönlichen Warenkorb" wird hier ein el. Warenkorb verstanden, der für eine ganz bestimmte Person zusammengestellt wird, d.h. *nach* einer Anmeldung, und bereits *exakte* Auskünfte über die Lieferzeit und/oder Verfügbarkeit enthält. Hierbei wird viel eher von einem Angebot auszugehen sein, da Kreditwürdigkeit, Ort des Empfängers etc. bereits feststehen und vom Verkäufer bzw. dessen Computersystem bereits beurteilt werden konnten. Auch kann bei einem modernen Warenwirtschaftssystem davon ausgegangen werden, dass es sich um einen Lagerbestand handelt, der zumindest täglich oder laufend aktualisiert wird. Es kann daher eine Bindungswirkung angenommen werden, da, im Gegensatz etwa zu einem Versandkatalog, der Verkäufer nicht befürchten muss, über sei-

---

[542] Beispiel: Versand von SMS über Web-Formulare, wobei vorher ein Guthaben aufzuladen ist. Auf AGBs ist jedoch zu achten, da hier beispielsweise der tatsächliche Versand durch Dritte erfolgt, sodass der Vertragsschluss eventuell erst durch Übergabe an diesen (tatsächliche Erfüllung) zustande kommen könnte.

[543] Ein österreichisches Beispiel sind Arzneimittel: Versandhandels-Vertrieb ist verboten (§ 59 Abs 9 ArzneimittelG).

[544] Siehe LG Köln, 16.4.2003, 9 S 289/02 für einen Fall, wo die unglückliche Formulierung ("baldige Ausführung") der E-Mail-Bestätigung zu einer, allerdings nicht gewünschten, Annahme führte. Aber auch mehrfache E-Mails müssen, bei entsprechender Gestaltung, nicht eine Annahme herbeiführen: LG Essen 13.2.2003, 16 O 416/02

ne Liefermöglichkeiten hinaus verpflichtet zu werden. Weil dies jedoch meist unerwünscht ist, sollte bei der Formulierung auf entsprechende "Unverbindlichkeit" geachtet werden.

Der persönliche Warenkorb kann analog zum Automatenverkauf gesehen werden, bei dem das Angebot an die Allgemeinheit unter der Voraussetzung "solange der Vorrat reicht" gerichtet wird. Auch hier ist beim tatsächlichen Vertragsabschluss keine Person mehr involviert, wie es auch bei E-Commerce, der meist vollkommen automatisch abläuft, der Fall ist. Das Angebot (=Aufstellung des Automaten) entspricht dem Zugänglichmachen der Webseiten, während der Vorrat im Automaten mit der aktuellen Lieferauskunft und der dahinterstehenden Programmlogik, die entweder eine längere Lieferfrist für Produktion/Bestellung festlegt oder das Produkt als "ausverkauft" markiert, verglichen werden kann. Problematisch kann bei E-Commerce sein, dass im Gegensatz zu einem Automaten für den Käufer die Aktualität der Lieferauskunft nicht (klar) erkennbar ist. Bei Unklarheiten der Formulierung ist wieder darauf abzustellen, wie ein redlicher Empfänger sie verstehen darf: Als allgemeine und ungefähre Angabe der durchschnittlichen Lieferzeit[545] oder als Auskunft über die Möglichkeit und den konkreten Zeitpunkt der Lieferung. In der Praxis kommen verbindliche Warenkörbe praktisch nicht, zumindest nicht absichtlich, vor.

VII.4.3. E-Mail-Werbung

Bei einer persönlich adressierten E-Mail wird es sich viel eher um ein Angebot handeln als um reine Werbung. Wird eine Person direkt angesprochen und ihr ein genügend konkreter Vorschlag unterbreitet, so ist von einem verbindlichen Angebot auszugehen. Auch hier ist freilich zu berücksichtigen, ob sich aus dem Inhalt nicht anderes ergibt ("Angebot freibleibend", "So lange der Vorrat reicht", ...; analog zu einem schriftlichen Angebot bzw. der Aufforderung, ein solches zu stellen). Handelt es sich hingegen um eine Massenaussendung mit unpersönlichem Inhalt oder ist die Nachricht an eine Mailingliste, also an eine sehr große oder unbestimmte Anzahl von Adressaten, gerichtet, so liegt kein Angebot vor, da von einem Bindungswillen des Absenders nicht auszugehen ist. Hier handelt es sich daher um reine Werbung, und oftmals nur um Spam.

Schwierig ist die Abgrenzung bei personalisierter E-Mail. Hat man sich beispielsweise auf einer Webseite angemeldet und dort bestimmte Vorlieben angegeben, um ein besser abgestimmtes Service zu erhalten, so kann automatisch eine passende E-Mail mit persönlicher Anrede und anderen konkreten Angaben, z.B. bereits teilweise vorausgefülltes Bestellformular, erstellt werden, die anschließend einzeln und persönlich adressiert verschickt wird. Hier muss vom Anbieter jedenfalls explizit klargestellt werden, ob es sich um Werbung oder ein Angebot handelt. Ist trotz der persönlichen Anpassung aus dem Text ersichtlich, dass es sich um eine mehrfach verschickte E-Mail handelt oder wird eine große Anzahl von Produkten angeboten, so ist dies ein Hinweis, dass es sich um unverbindliche Werbung handelt.

Allgemein kann zusammengefasst werden, dass es sich in der Praxis bei E-Mails nur selten um echte Angebote handeln wird. Es werden fast ausschließlich händisch und individuell abgefasste und auf Anfrage hin erstellte Vorschläge rechtlich gesehen Angebote sein, während unverlangt zugesandte E-Mails fast immer als Werbung anzusehen sind. Probleme bei der Erkennung durch Kunden können und müssen durch entsprechende Formulierung des Mail-Textes verhindert werden.

---

[545] Siehe Amazon.com http://www.amazon.at/: "*Gewöhnlich* versandfertig bei Amazon in 24 Stunden"

VII.5. Erfüllung

Bei E-Commerce ist es nicht nur möglich, Verträge el. abzuschließen, sondern je nach Art des Kaufgegenstandes kann auch die Erfüllung auf diese Art sofort und direkt erfolgen. Ebenso kann u.U. die Bezahlung online abgewickelt werden. Hier ist jedoch zu untersuchen, wann tatsächlich die Verpflichtung erfüllt wird, da nicht jede Art von Lieferung bzw. Zahlung sofortige Erfüllung (=Leistung des Geschuldeten) bewirkt. Im Hinblick auf die Gefahrtragung ist es weiters wichtig festzustellen, wo die Leistungen zu erbringen sind.

VII.5.1. Erfüllungsort

Der Erfüllungsort ist der Ort, an dem die Leistung erbracht werden muss. Dies ist im E-Business deshalb bedeutsam, da sich danach regelmäßig die Maßeinheiten (heute weniger wichtig) und Währungen bestimmen sowie den Zeitpunkt, an dem die Schuld erfüllt ist. Ist also der Erfüllungsort bei einem grenzüberschreitenden Kauf am Sitz des Verkäufers, so ist der geschuldete Betrag in der dortigen Währung zu bezahlen, die zu liefernde Menge nach dortigen Maßen[546] zu berechnen[547] und die Schuld erst mit dem Einlangen des Geldes am Ziel bezahlt. Der Erfüllungsort kann im Vertrag selbst frei festgelegt werden. Nach dem Gesetz liegt grundsätzlich eine Holschuld vor, d.h. der Gläubiger muss die Leistung am Wohnsitz des Schuldners abholen. Bei einem Versendungskauf, wie er bei E-Commerce regelmäßig vorliegen wird, besteht bezüglich der Ware eine Schickschuld[548]. Dies bedeutet, dass der Leistungsort der Wohnsitz des Schuldners bleibt, diesen aber die Verpflichtung trifft, den Schuldinhalt an den Gläubiger abzusenden. Letzterer hat daher dann, im Gegensatz zu einer Bringschuld mit Erfüllung am Wohnsitz des Empfängers, auch die Transportgefahr zu tragen. Geldschulden sind in der Regel qualifizierte Schickschulden, wobei der Schuldner auch Kosten und Gefahr der Versendung tragen muss.

Für E-Commerce ergeben sich daraus folgende Punkte: Der Versender (=Verkäufer) muss die Ware an den Käufer abschicken. Der Käufer trägt die Kosten und Gefahren des Versands. Der Konsument (=Käufer) muss weiters das Geld zum Verkäufer schicken, wobei er auch hier Kosten und Gefahr des Transports, z.B. Nicht-Durchführung einer Überweisung durch die Bank, trägt. Die Menge ist nach Maßeinheiten des Versenders zu berechnen, während die Währung durch den Wohnort/Sitz des Käufers festgelegt wird. Sowohl für Maßeinheiten wie Währung bestehen jedoch praktisch immer explizite Vereinbarungen.

Beim Versand der Ware in el. Form, z.B. als E-Mail-Anhang, trägt daher der Käufer die Gefahr des Verlusts der Mail. Wird die Mail etwa wegen voller Mailbox von seinem Mail-Provider nicht angenommen, so hat der Versender seine Leistung bereits erfüllt. Dies ist weniger bedeutsam bezüglich Verlust der Leistung, da E-Mails jederzeit neu geschickt werden können, ohne dass großer Aufwand anfällt, als vielmehr für Fristen bzw. deren Versäumnis. Wurde vereinbart, dass der Käufer die Daten per FTP oder Web-Download von einem Rechner des Verkäufers abholt, so ist mit der Bereitstellung (=Gültigkeit von

---

[546] Wichtig etwa für Rechtsgeschäfte mit den USA oder England, wo noch immer nicht-metrische Maßsysteme vorgeschrieben bzw. in Verwendung sind!

[547] Hierbei ist jedoch zu beachten, dass der Erfüllungsort bei einem Kauf auch auseinander fallen kann: Erfüllung bezüglich der Lieferung der Ware am Wohnsitz des Konsumenten, aber Erfüllung der Geldschuld am Sitz des Verkäufers.

[548] Siehe etwa folgendes Beispiel in den USA, wo der Versand von Bier über Bundesstaatsgrenzen besondere Probleme aufwirft (es handelte sich um die Bestellung eines Minderjährigen): Die Klage wurde wegen Unzuständigkeit zurückgewiesen, da der Verkaufsort ein anderer Bundesstaat war. Butler v. Beer Across America, No. CV99-H-2050-S, 2000 LW 156005 (http://cyber.law.harvard.edu/ilaw/Jurisdiction/Butler_sum.html; Urteilstext: http://euro.ecom.cmu.edu/program/courses/tcr840/2003/ButlerBeer.htm).

Name und Passwort) und der Erreichbarkeit des Rechners vom Internet aus die Leistung bewirkt. Verbindungsprobleme oder Schwierigkeiten beim Download treffen daher auch hier den Käufer. Eine Bringschuld wird bei el. Lieferung (=Speicherung der Daten auf einem Käuferrechner) nur höchst selten vorkommen. Diesfalls trifft die Gefahr von Verbindungsproblemen den Verkäufer, doch muss der Käufer für die Zugriffsmöglichkeit sorgen.

VII.5.2. Leistungsinhalt bei Geldschulden

Bei einer Geldschuld ist grundsätzlich das gesetzliche Zahlungsmittel zur Begleichung zu verwenden (Geldscheine und Münzen). Dies bedeutet bei einem Versendungskauf, dass echte Geldscheine mit der Post verschickt werden müssten. Da dies unpraktisch und mit großer Gefahr verbunden ist, wird meist eine andere Zahlungsart vereinbart. Alternativ kann heute davon ausgegangen werden, dass der Gläubiger bei Stundung (=Lieferung auf Rechnung) mit Zahlung durch Überweisung einverstanden ist, wodurch die Leistung mit Gutschrift (und Verfügbarkeit!) auf dem Empfänger-Konto[549] eintritt.

Von besonderer Bedeutung ist bei E-Commerce die Bezahlung per Kreditkarte. Hier wird die Leistung an den Verkäufer erst bei dessen Abrechnung mit der Kreditkartenfirma erbracht[550]. Der Verkäufer muss daher explizit mit einer Zahlung per Kreditkarte einverstanden sein, da er durch diese zusätzliche Kosten zu tragen hat (Gebühr der Kreditkartenfirma[551]) und den Kaufpreis erst später erhält. Rechtlich gesehen wird hier die Schuld nicht durch den Käufer erfüllt, sondern über eine Anweisung an die Kreditkartenfirma, welche an den Händler (bevor der Letztkunde an sie bezahlt hat, daher "Kredit"karte) bezahlt und diesen Betrag dann später vom Kunden erstattet erhält.

VII.6. Allgemeine Geschäftsbedingungen

Bei allgemeinen Geschäftsbedingungen (AGB) handelt es sich um vorformulierte Vertragsbedingungen und Klauseln, die für eine Vielzahl von Verträgen verwendet werden. Typischerweise schließt ein Großteil aller Unternehmer nur entsprechend ihren AGBs Geschäfte ab. Dies dient der Rationalisierung und Vereinheitlichung der Geschäfte, kann aber auch verwendet werden, für den Vertragspartner nachteilige Bestandteile "heimlich" zu integrieren. Ein Problem ergibt sich daraus, dass Konsumenten praktisch immer nur die eine Wahl haben, die AGBs entweder zu akzeptieren oder keinen Vertrag abschließen zu können. Von AGBs sind Vertragsformblätter zu unterscheiden, bei denen bis auf einige Bestandteile der komplette Vertrag fertig vorgedruckt ist. Rechtlich sind sie jedoch wie AGBs zu behandeln. Besondere Probleme hinsichtlich AGBs stellen sich im B2B Bereich, wenn beide Parteien solche verwenden und darin inkompatible Bestimmungen enthalten sind.

In Hinsicht auf Vollständigkeit der Informationspflichten und Gesetzeskonformität von AGBs wird auf die Checklisten der Wirtschaftskammer[552] verwiesen, welche für die österreichische Rechtslage sehr hilfreich sind.

---

[549] Es muss sich um das richtige Konto handeln: Die Gefahr von Falschüberweisungen trägt der Käufer, da qualifizierte Schickschulden vorliegen; siehe oben.

[550] Und steht ev. unter dem Vorbehalt, dass der Käufer die Schuld bei der Kreditkartenfirma tatsächlich begleicht.

[551] Europay Austria (Mastercard): Disagio vom Kaufpreis (z.B. 2,7 %; Pressemitteilung vom 24.2.2005) + Buchungsentgelt pro Transaktion.

[552] http://portal.wko.at/wk/format_detail.wk?AngID=3&StID=216698 Login mit Mitgliedsnummer und PIN für diese und viele weitere Informationen erforderlich, daher großteils nur für WK-Mitglieder zugänglich und gratis.

VII.6.1. Wirksamkeit

Da der Unternehmer keine Möglichkeit hat, von sich aus verbindliche Regeln für den Kunden aufzustellen, liegt der Rechtsgrund für die Wirksamkeit von AGBs ausschließlich in einer beiderseitigen Vereinbarung. Dies bedeutet jedoch auch, dass der Kunde explizit darauf hingewiesen werden muss, dass der Unternehmer nur unter seinen AGBs abschließen will und auch tatsächlich eine Einsichtnahme möglich ist[553]. Die oft geübte Praxis, AGBs auf die Rückseite der Rechnung oder von Lieferscheinen aufzudrucken, hat daher rechtlich keine Wirkung. Der Vertrag kommt zuerst zustande und anschließend wird eine Rechnung ausgestellt, weshalb die AGBs nicht Bestandteil des Vertrags werden[554].

VII.6.2. Ungültige Klauseln

Aufgrund der oft starken faktischen Benachteiligung von Konsumenten durch AGBs bestehen besondere Vorschriften, wonach einzelne Bestandteile ungültig sein können. Hier ist zu beachten, dass die normale Wirkung, dass der Vertrag anfechtbar oder anpassbar wird, nicht eintritt, sondern lediglich die verbotene Bestimmung automatisch als nichtig angesehen wird[555]. Es kommt zu Restgültigkeit, d.h. alle anderen Vertragsbestimmungen bleiben aufrecht, da eine Vertragsauflösung erst recht wieder gegen die Konsumenteninteressen wäre.

Wichtige derartige Vorschriften bezüglich AGBs sind:

- § 864a ABGB: Nach diesem Paragraph sind AGB-Bestimmungen ungewöhnlichen Inhalts, die den anderen Vertragspartner benachteiligen, unwirksam, wenn er nicht aufgrund der Umstände mit ihnen rechnen musste. Sie können dennoch gültig vereinbart sein, wenn besonders auf sie hingewiesen wird oder sie optisch hervorgehoben sind, z.B. durch Fettdruck, Farbdruck oder Umrandung. In langen Texten "verborgene" Bestimmungen sind deshalb unwirksam, wobei besonders auf die optische Gestaltung ("äußeres Erscheinungsbild") abgestellt wird. Auch in el. Form ist daher auf gute Lesbarkeit zu achten, d.h. lange AGBs/Webseiten zu vermeiden, und "gefährliche" Bestimmungen optisch besonders hervorzuheben.
- § 879 Abs 3 ABGB: In AGBs enthaltene Bestimmungen sind jedenfalls nichtig, wenn sie unter Berücksichtigung aller Umstände einen Teil gröblich benachteiligen[556] und nicht die Hauptleistungen (Kaufvertrag: Ware und Preis) betreffen. Eine solche Benachteiligung liegt vor, wenn ein grobes Missverhältnis der gegenseitigen Leistungen besteht. Bei einem besonders unterschiedlichen Wert kommt auch die laesio enormis, § 934 ABGB[557], in Frage, welche aber hier nicht erreicht werden muss. Im Unterschied zum KSchG sind die Hauptpunkte des Vertrages ausgeschlossen und daher gültig, das beinhaltet auch Zahlungsort oder Währung beim Kauf, da diese einen der Hauptpunkte betreffen. Bedeutung besitzt die Bestimmung daher nur für Nebenaspekte.

---

[553] Siehe dazu § 73 Abs 1 GewO: AGBs müssen in den Geschäftsräumen ausgehängt werden.

[554] Eine Ausnahme besteht bei regelmäßiger Geschäftsbeziehung. Hier wird nach längerer Praxis aufgrund der früheren Rechnungen die Wirksamkeit für spätere Geschäfte bejaht.

[555] Die gesamte Klausel fällt dann weg und wird nicht etwa auf das gerade noch erlaubt Maß reduziert. Eine solche geltungserhaltende Reduktion wird vom OGH im B2B Bereich vertreten, jedoch *nicht* gegenüber Konsumenten. Ihnen gegenüber muss also eine besondere Transparenz eingehalten werden, ansonsten fällt die gesamte Klausel weg.

[556] Zum ähnlichen § 9 Abs 1 des deutschen AGB-Gesetzes: LG München I 01.02.2001, 12 O 13009/00. Eine AGB-Klausel die auch Telefonwerbung erlaubt, ist nicht rechtswirksam.

[557] Verkürzung über die Hälfte: Ein Teil erhält nicht einmal die Hälfte an Wert wie seine Gegenleistung Wert ist.

- § 915 ABGB legt eine Regel für Unklarheiten fest: Bedient sich eine Seite einer unklaren Formulierung, so wird sie zu ihren Ungunsten ausgelegt. Dies wird insbesondere bei AGBs sehr streng beurteilt, sodass für AGBs immer jene Auslegung gilt, welche für die sie verwendende Person am schlechtesten ist.
- § 6 Abs 3 KSchG: Unklare oder unverständliche Bestimmungen in AGBs oder Vertragsformblättern sind unwirksam. Diese Vorschrift betrifft nur Verbraucherverträge, während die obigen Bestimmungen grundsätzlich gelten.
- Zusätzlich sind natürlich alle Vorschriften in AGBs ungültig, welche explizit gesetzlichen Anforderungen widersprechen. Beispiele hierfür sind insbesondere zwingende Konsumentenschutzvorschriften[558].

Nicht speziell AGBs betreffend, aber darüber hinaus von Bedeutung für Konsumenten ist, dass sich auf § 934 ABGB (laesio enormis) nicht berufen kann, für wen es ein Handelsgeschäft ist. Dies bedeutet, dass sich ein Konsument gegenüber dem Händler gegen eine Übervorteilung wehren kann, umgekehrt aber nicht[559].

VII.6.3. Anwendbarkeit bei E-Commerce

Sollen AGBs im E-Commerce wirksam verwendet werden, so ist es notwendig, explizit und bereits vor Vertragsabschluss auf sie hinzuweisen. Dies bedeutet, dass der Kunde vor Abgabe seiner Erklärung darauf aufmerksam zu machen ist, dass AGBs Anwendung finden sollen und andernfalls kein Vertrag möglich ist. Weiters muss ihm eine Einsichtnahme ermöglicht werden, z.B. durch einen Link. Solche Hinweise müssen zusätzlich klar erfolgen, es darf daher der Link nicht etwa in Kleindruck in einer Fußzeile versteckt werden. Nach der E-Commerce RL muss der Kunde die Möglichkeit haben, die Vertragsbedingungen zu speichern und zu reproduzieren, was bei Webseiten[560] immer gegeben ist. Es ist jedoch nicht notwendig, dass der Benutzer sich "durchklicken" *muss*, um die Bestellung abschicken zu können[561]. Ein expliziter Hinweis auf der letzten Webseite in der Nähe der "finalen" Schaltfläche[562], mit welcher die Erklärung endgültig abgeschickt wird, ist ausreichend. Auch im Internet sind ungewöhnliche Bestandteile optisch hervorzuheben, um sie gültig zu vereinbaren.

In Bezug auf die verwendete Sprache ist wichtig, dass fremdsprachige AGBs nicht grundsätzlich "unverständlich" und damit ungültig sind. Es wird vielmehr vom Verständnis eines dieser Sprache Mächtigen auszugehen sein[563]. Insbesondere wird Englisch z.B. in Hard- oder Software Fachgeschäften etwa für Wiederverkäufer akzeptabel sein, nicht aber ge-

---

[558] Siehe LG Waldshut-Tiengen 7.7.2003, 3 O 22/03 KfH für eine ganze Kollektion unerlaubter AGB-Klauseln, großteils bezüglich des Rückgaberechts: nicht originalverpackt, preisreduziert, Rückgabefrist beginnt mit Rechnungsdatum, ...

[559] Bei Kaufleuten geht man davon aus, dass sie über den tatsächlichen Wert der ge-/verkauften Waren informiert sind.

[560] Wohl auch bei (druckbaren) PDFs. Word-Dateien dürften zweifelhaft sein, da es sich um ein kommerzielles Programm handelt. Es ist zwar ein kostenloser „Viewer“ verfügbar, dieser ist aber eher unbekannt. Noch exotischere Dateiformate sind wohl von vornherein unzureichend.

[561] Siehe dazu Wendel, Wer hat Recht im Internet? Aachen: Shaker Verlag 1997: Im Internet hat der Kunde die Möglichkeit, die AGBs in Ruhe zu studieren, ohne zur Unterschrift gedrängt zu werden. Es sollte daher keine Verschärfung im Gegensatz zu Papier-Verträgen stattfinden.

[562] Darüber; bei Platzierung darunter besteht in Einzelfällen die Gefahr, dass sie erst durch Scrollen sichtbar würde, was zu ihrer Unwirksamkeit führen könnte. Siehe auch LG Essen 13.2.2003, 16 O 416/02

[563] Ist die Webseite nur für Inländer gedacht, wird eine Beherrschung gleich der Muttersprache zur Auslegung zu verwenden sein. Bei Bestimmung für internationalen Gebrauch werden gute Fremdsprachen-Kenntnisse anzunehmen sein.

genüber "normalen" Verbrauchern. Es ist jedoch auf eine klare und einfache Abfassung zu achten. So genanntes "Legalese" kann dazu führen, dass eine sonst zumutbare Fremdsprache, aber selbst Deutsch bei verhältnismäßig stärkerer Ausprägung, zu einer Unwirksamkeit der AGBs führt.

VII.7. Literatur

VII.7.1. Allgemein

Anderl, Axel: Versteigerung bleibt Versteigerung - Kein Rücktrittsrecht bei Online-Auktionen. RdW 2005, 440 http://www.dbj.at/publ299.pdf

Besenböck, Alexander, Bitriol, Michael: Zum Ersten, zum Zweiten – Rücktritt! ecolex 2005, 104

Fallenböck, Markus, Haberler, Michael: Rechtsfragen bei Verbrauchergeschäften im Internet (Online-Retailing), RdW 1999, 505

Kilches, Ralph: Electronic Commerce Richtlinie. Medien und Recht 1/99 (17. Jahrgang) 3ff

Koziol, Helmut, Welser, Rudolf: Grundriß des bürgerlichen Rechts. Band I: Allgemeiner Teil und Schuldrecht. 10. Auflage. Wien: Manz 1995

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

Ledolter, Gunther: Die Allgemeinen Geschäftsbedingungen im E-Commerce. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther, Liebwald, Doris (Hg.): Zwischen Rechtstheorie und e-Government. Wien: Verlag Österreich 2003, 571-587

Maderbacher, Gregor, Otto, Gerald: Fernabsatz: Vertragsrücktritt nur gegen Entgelt? ecolex 2006/117

Mochar, Veronika, Seidl, Simone: Internationales Verbraucherschutzrecht und e-commerce. ÖJZ 2003/13

Mohr, Martina: KSchG-Novelle 1999 - Verbraucherschutz im Fernabsatz. ecolex 1999, 755

Mohr, Martina: El. Verkauf - Verbraucherschutz im Fernabsatz. ecolex 1999, 47

Schummer, Gerhard, Weinberger, Markus: Zum Rücktrittsrecht bei "Online-Auktionen": JBl 2005, 765

Sonntag, Michael: Das Rücktrittsrecht nach dem Fernabsatzgesetz beim Online-Musikkauf. In: Schweighofer/Liebwald/Augeneder/Menzel (Hrsg.): Effizienz von e-Lösungen in Staat und Gesellschaft. Düsseldorf: Boorberg 2005, 419

Stöger, Theresa: Die Gerichtszuständigkeit für Streitigkeiten aus Vertragsabschlüssen und Wettbewerbsverstössen via Internet. Dissertation Uni Wien 2002. http://www.e-xam.at/update/literatur/pdf/gerichtszustandigkeit.PDF

Wendel, Dominik A.: Wer hat Recht im Internet? Aachen: Shaker Verlag 1997

VII.7.2. Rechtsvorschriften

ABGB: Allgemeines bürgerliches Gesetzbuch (ABGB) vom 1. Juni 1811 JGS 946

Konsumentenschutzgesetz: Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG), BGBl 1979/140 idF BGBl I 92/2006

UN-Kaufrecht: Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf, BGBl 1988/96

IPRG: Bundesgesetz vom 15. Juni 1978 über das internationale Privatrecht (IPR-Gesetz), BGBl 1978/304 idF BGBl I 58/2004

EVÜ: Europäisches Vertragsstatutübereinkommen. Übereinkommen über das auf vertragliche Schuldverhältnisse anzuwendende Recht BGBl III 1998/208; EG-Römer Übereinkommen vom 19. Juni 1980 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (EVÜ) ABl. L 266/1 vom 9.10.1980 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41980A0934:DE:HTML

EuGVVO: Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (EuGVVO) ABl. L 12/1 vom 16.1.2001 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:DE:HTML

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

Richtlinie 2002/65/EG des Europäischen Parlamentes und des Rates vom 23. September 2002 über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 90/619/EWG des Rates und der Richtlinien 97/7/EG und 98/27/EG ABl. L 271/16 vom 9.10.2002 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065: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 vom 17.7.2000 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:DE:HTML

VIII. Elektronische Signaturen

Elektronische Signaturen dienen dazu, die traditionell handschriftliche Unterschrift durch eine elektronische Form zu ersetzen. In diesem Abschnitt wird das österreichische Signaturgesetz (SigG), welches in Durchführung der Signatur-Richtlinie (SigRL) der Europäischen Union beschlossen wurde, behandelt. Neben den verschiedenen rechtlichen Aspekten wird einerseits besprochen, worauf sich diese Vorschriften genau beziehen, andererseits, welche Rechtsfolgen sich aus sicheren el. Signaturen ergeben. Augenmerk wird weiters auf die Akkreditierung gelegt, mit der ein Anbieter von Zertifizierungsdiensten (ZDA) eine besonders überprüfte Qualität nachweisen kann. Zum Abschluss wird kurz der Electronic Signatures Act aus den USA besprochen.

Die rechtliche Anerkennung von Signaturen ist im E-Business deshalb wichtig, da nur dann die sichere Beweisbarkeit von Forderungen, beispielsweise aus Kaufverträgen, gegeben ist[564]. Weiters ermöglichen sie die sichere Erkennung des Geschäftsinhabers über dessen Zertifikat, was dazu beiträgt, das Vertrauen der Konsumenten zu erhöhen und damit den el. Handel fördert. Dies ist insbesondere ein Anliegen der Europäischen Union, da auf diese Weise der freie Waren- und Dienstleistungsverkehr verstärkt wird. Aus diesem Grund wurde auch eine Signatur-Richtlinie geschaffen, sodass in der gesamten EU einheitliche Regelungen bestehen, Signaturen gegenseitig anerkannt werden, und grenzüberschreitende Transaktionen mit ihnen problemlos möglich sind.

Zwei weitere Aspekte sind zwar allgemein von großer Bedeutung, werden hier aber nicht besprochen: Die el. Rechnung, welche in bestimmten Fällen ebenfalls el. Signaturen voraussetzt, sowie der Einsatz von Signaturen im Verwaltungsbereich. Letzterer betrifft sowohl den el. Rechtsverkehr als auch interne Verwaltungsvorgänge sowie den Zugang von Personen zu Verwaltungsprozessen[565].

VIII.1. Einleitung

Elektronische Signaturen sollen es ermöglichen, dass Dokumente nicht nur in physischer Form, sondern auch elektronisch unterschrieben (=signiert) werden können. Dadurch ist es möglich, sowohl die Beweisbarkeit von Rechtsgeschäften zu verbessern wie auch den Anwendungsbereich von E-Commerce zu vergrößern, insbesondere im Hinblick auf Geschäfte mit hohem Transaktionswert und damit hohem Sicherheitsbedürfnis. Grundsätzlich kann nach der SigRL jedes Rechtsgeschäft, welches die einfache Schriftform (=Unterschrift) erfordert, nun auch el. abgeschlossen werden. Solche Formvorschriften sind jedoch zumindest in Österreich selten. Meist ist die Unterschrift eine freiwillige Form der "Bekräftigung" mit dem einzigen Zweck der Beweiserleichterung, da mündliche Verträge zwar fast überall möglich und gültig sind, aber nur schwer bewiesen werden können.

---

[564] Der Beweiswert von E-Mails oder Logs von WWW-Formularen ist äußerst gering. Dies sollte jedoch nicht darüber hinwegtäuschen, dass in der Praxis anscheinend nur sehr wenige Probleme durch diesen "Mangel" auftreten!

[565] Etwa die el. Abgabe der Steuererklärung nach der Identifizierung mit der Bürgerkarte oder auch den Datenverkehr von Unternehmen mit der Krankenversicherung.

Höherwertige Formen (notarielle Beurkundung, Notariatsakt, gerichtliche Beglaubigung, ...) sind bisher nicht erfasst und können nur in Zusammenwirkung mit/vor der entsprechenden Stelle durch physische Unterschrift auf Papier erfolgen. Dies wird sich mit 1.1.2007 ändern, wenn u.a. der "elektronischer Notariatsakt" eingeführt wird, für den zusätzlich zur Signatur des Unterzeichnenden der Notar seine Signatur anbringen muss. Damit soll insbesondere auch die Einrichtung eines Daten-Urkunden-Archivs ermöglicht werden.

El. Signaturen ähneln sehr stark physischen Unterschriften, doch existiert ein besonderer Unterschied: Sie besitzen ein "Ablaufdatum". Durch den technischen Fortschritt ist eine Signatur, die heute noch unfälschbar ist, in einigen Jahren wahrscheinlich ohne großen Aufwand zu brechen und damit fälschbar. Als Konsequenz ist zwar der dadurch beurkundete Rechtsakt weiterhin gültig, doch der Beweis hierüber geht verloren. Da Unterschriften mit rechtlicher Bedeutung aber oft sehr lange gültig sein müssen (3-40 Jahre Verjährungsfrist!), kann es notwendig sein, später eine erneute (Nach-)Signierung durchzuführen. Dies hat aber natürlich nur dann einen Sinn, wenn mit der Nachsignierung ein Zeitstempel einer unabhängigen Instanz, meist eines Zertifizierungsdiensteanbieters (ZDA), verbunden ist, der den tatsächlichen Zeitpunkt der Nachsignierung bestätigt. Die Nachsignierung und damit der Nachweis der Existenz und Korrektheit zu einem bestimmten Zeitpunkt muss natürlich innerhalb des Gültigkeitszeitraums der ursprünglichen Signatur liegen.

In geschlossenen Gruppen, z.B. firmenintern oder bei dauernder Geschäftsverbindung, können weiterhin beliebige Signaturen und Verfahren verwendet werden. Diese werden auch rechtlich anerkannt, sofern sie die entsprechenden Eigenschaften erfüllen und besitzen dann Beweiswert vor Gericht. Dessen Ausmaß ist jedoch an Hand der Technik, der Sicherheitsvorkehrungen etc. individuell zu beurteilen. Es kann daher im gegenseitigen Übereinkommen jederzeit eine andere Signatur vereinbart und verwendet werden.

Wichtig ist zu bemerken, dass durch das Signaturgesetz *nicht* die allgemeine Zulässigkeit el. Kommunikation mit irgendjemandem, insbesondere nicht mit Behörden, festgelegt wird. In diesem Bereich ergeben sich durch eine Signatur keinerlei Änderungen. Wenn allerdings el. Kommunikation bzw. Einbringung von Anträgen akzeptiert wird, dann ermöglichen Signaturen eine besondere *Qualität* der Eingaben und daher ev. einen größeren Anwendungsbereich. Im Gegenzug ist es aber so, dass ohne Signaturen el. Kommunikation immer eine unsichere und daher seltene Ausnahme bleiben könnte. Praktisch werden von Behörden derzeit jedoch vielfach elektronische Eingaben ohne jegliche Unterschrift/Signatur akzeptiert, z.B. per Fax oder E-Mail. Nur wenn Fragen der Gültigkeit auftauchen ist eine schriftliche Version im Nachhinein vorzulegen, auf Papier oder el. signiert. Grundsätzlich wird davon ausgegangen, dass qualifizierte Signaturen, soweit die el. Kommunikation vorgesehen ist, auch für den Verkehr mit Behörden sicher genug sind. In besonders zu begründenden Fällen könnten jedoch auch besondere Vorkehrungen gefordert werden, so etwa nur Signaturen, die auf Chipkarten mit Fingerabdruck zur Autorisierung basieren und keine "rein" el. Signaturen. Zur Zeit sind jedoch keine solchen Zusatzerfordernisse vorgesehen, sondern es werden, wie angeführt, eher Reduktionen der Anforderungen eingebaut.

In der SigRL ist explizit festgelegt, dass die Aufnahme des Betriebes eines Zertifizierungsdiensteanbieters nicht von einer Genehmigung abhängig gemacht werden darf, es sich also nicht um ein Konzessionssystem handeln darf. Werden die Vorschriften erfüllt, was im Laufe der Zeit und wiederholt überprüft wird, so kann sofort mit der Tätigkeit begonnen werden. Hierdurch wird eine Mindestqualität garantiert, die jedoch bei Betriebsbeginn

noch nicht unbedingt tatsächlich gegeben sein muss, auch wenn sie es rechtlich gesehen sein müsste. Um daher das Vertrauen der Konsumenten zu erhöhen, steht es einem Anbieter frei, sich einer besonderen Prüfung, genannt Akkreditierung, zu unterziehen, wodurch von staatlicher Seite aus eine *besondere* Qualität bestätigt wird. Inhaltlich ist diese Qualität jedoch nichts Außergewöhnliches, da es sich *ausschließlich* um die ohnehin gesetzlich für alle vorgeschriebene handelt! Dies darf jedoch nicht verpflichtend vorgesehen sein und auch zu keiner Wettbewerbsverzerrung führen.

VIII.1.1. Anforderungen an eine elektronische Unterschrift

Handschriftliche Unterschriften entsprechen in den meisten Fällen den folgenden Anforderungen. Eine äquivalente Unterschrift auf elektronischem Wege muss, bzw. soll, alle diese Punkte erfüllen. In vielen Fällen der Praxis ist jedoch ein el. Unterschrift sogar sicherer als eine konventionelle[566]! Eine „Unterschrift" muss folgende Punkte erfüllen:

- *Personenabhängigkeit:* Die Unterschrift ist eindeutig mit einer bestimmten Person verbunden, welcher der Inhalt deshalb zugerechnet wird (=Zuordnung zu einem bestimmten Namen). Die Unterschrift ist also "lesbar", wodurch der, allerdings auf Papier nicht unbedingt eindeutige[567], Name herausgefunden werden kann.
- *Dokumentenabhängigkeit:* Die Unterschrift ist untrennbar mit dem Dokument verbunden und kann nicht auf ein anderes übertragen werden (=kein Ausschneiden und Aufkleben bzw. kopieren; Computerfaxe!). Vergleiche hierzu früher verwendete Siegel[568]!
- *Überprüfbarkeit:* Die Unterschrift kann durch jeden überprüft werden, insbesondere, ob sie von einer bestimmten Person stammt oder nicht. Diese Eigenschaft ist handschriftlich sehr selten: Wer hat schon Referenzunterschriften und kann gut verstellte Unterschriften erkennen! El. ist dies über das Zertifikat und Widerrufslisten relativ einfach.
- *Fälschungssicherheit:* Die Unterschrift kann nur durch eine einzige Person erzeugt werden. Fälschungen sind daher unmöglich, genauso wie der echte Unterzeichner nicht abstreiten kann, selbst unterschrieben zu haben (=auf Papier nur durch Experten möglich). El. kann dies durch Geheimhalten der Signaturerstellungsdaten[569] realisiert werden.
- *Dokumentenechtheit:* Das Dokument kann nach der Unterschrift nicht mehr verändert werden. Die Unterschrift bildet einen Abschluss des Dokumentes. Auf Papier sind hierzu besondere Formatierungsrichtlinien einzuhalten; siehe das besondere Aussehen von Notariatsurkunden. Elektronisch ist die Dokumentenechtheit ein automatisches Nebenprodukt der Signatur; beachte jedoch die Kollisionsproblematik bei Hashfunktionen.

VIII.2. Begriffsbestimmungen

In diesem Abschnitt werden die im Folgenden verwendeten Begriffe definiert, und zwar wie sie nach der SigRL bzw. dem SigG zu verstehen sind. Diese Definitionen können sich von technischen Definitionen unterscheiden und dienen einer einheitlichen Auslegung.

---

[566] Siehe etwa die Überprüfbarkeit: Welches Unternehmen besitzt etwa Referenzunterschriften von Erstkunden?

[567] Beispiel: Es unterschreibt "Johann Müller". In Wien existieren 28, österreichweit ca. 250 Personen dieses Namens.

[568] "Offizielles" Beispiel: Das Privilegium Maius, bei welchem das kaiserliche Siegel von einer älteren Urkunde (Privilegium Minus) entfernt und an dieser Fälschung angebracht wurde. Thomas, C.: Privilegium maius (1358/1359) als Erweiterung des Privilegium minus, 1156 September 17 http://www.uni-klu.ac.at/kultdoku/kataloge/20/html/1818.htm

[569] In der Praxis: Des Passwortes oder PIN-Codes dien den Zugang zum privaten Schlüssel ermöglichen.

Zusätzlich zu den hier besprochenen einfachen, fortgeschrittenen und sicheren Signaturen existieren noch weitere Varianten. Die Verwaltungssignatur[570] wird von Bürgern im Verkehr mit Behörden, sowie ev. umgekehrt, verwendet und darf nur mehr bis Ende 2007 eingesetzt werden. Wieder davon zu unterscheiden ist die Amtssignatur[571], welche eine einfache, eine sichere oder eine Verwaltungssignatur sein kann. Es handelt sich daher hierbei nicht um eine technische sondern eine organisatorische Bezeichnung. Amtssignaturen werden für Bescheide/Erledigungen verwendet, um kenntlich zu machen, dass es sich um amtliche Schriftstücke in el. Form handelt.

VIII.2.1. Elektronische Signatur

Eine Definition ist in § 2 Z 1 SigG und in Art 2 Z 1 SigRL enthalten.

Eine elektronische Signatur sind elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen.

Die Beschränkung auf elektronische Daten hat den Grund, dass ein Ausdruck auf Papier unter Umständen nicht mehr unverändert in die Originaldaten zurückgewandelt werden kann: Nicht-druckbare Zeichen, Zeilenumbrüche, Elemente der Codierung, redundante Elemente in den Daten, die beim Ausdruck wegfallen etc. Dies würde dazu führen, dass original-signierte Daten ohne Veränderung des Inhalts als unecht entlarvt werden könnten. Selbst wenn eine unverwechselbare Codierung vorliegt, z.B. durch Ausdruck als Byte-Codes, kann nicht mehr von einer "elektronischen" Signatur gesprochen werden, obwohl dann eine solche wiederhergestellt werden kann. Diese Bedingung ist hier noch nicht besonders wichtig, wenn auch für den Geltungsbereich des Gesetzes sinnvoll. Bei sicheren Signaturen ist sie jedoch eine unbedingt notwendige Voraussetzung.

Die "Beifügung" entspricht einer externen Signierung (=Verlängerung des Textes), während die "logische Verknüpfung" auf eine Signierung ohne Verlängerung hinweist (interne Signatur). Bei der zweiten Variante werden die gesamten Daten mit dem privaten Teil des Schlüssels verschlüsselt. Der Nachteil dieses Verfahrens ist, dass immer eine Entschlüsselung nötig ist, um den (Klar-) Text zu erhalten. Bei externer Signierung kann die Prüfung auf Zweifelsfälle beschränkt werden.

Da die Daten der Identifizierung des Signators (siehe VIII.2.2) dienen, ist es mit einer (technischen) Signatur alleine nicht getan: Es muss u.U. auch ein Zertifikat beigefügt werden, aus welchem dann die Identität feststellbar ist, wenn auch nicht unbedingt der Name, so etwa bei Pseudonymen. Dieses Zertifikat ermöglicht weiters die Prüfung der Signatur bzw. die Entschlüsselung des Textes. Alternativ würde dem Gesetzestext ein eindeutiger Hinweis entsprechen, welches Zertifikat zu verwenden ist. Dieser Vermerk hat jedoch allgemein verständlich zu sein, sodass potentiell jeder dieses Zertifikat ausheben kann. Achtung: Qualifizierte Zertifikate sind nur mit Zustimmung des Inhabers öffentlich abrufbar: § 7 Abs 2 SigG. Bei "geheimen" Zertifikaten ist daher eine Einbettung erforderlich, um

---

[570] Siehe § 25 E-Government-Gesetz: Hinsichtlich der Sicherheit etwas "verminderte" sichere Signaturen, z.B. nicht auf einem qualifizierten Zertifikat beruhend. Siehe Forgó: Königsweg Verwaltungssignatur? RFG 2004/29

[571] § 19 E-Government-Gesetz. Das Zertifikat enthält ein besonderes Attribut. Eine durchgeführte Signatur enthält nicht nur die mathematischen Daten, sondern auch eine Bildmarke, die meist einem Rundstempel nachgebildet ist. Die Signatur kann selbst bei ausgedruckten Dokumenten noch überprüft werden, sodass derartige Ausdrucke dann ebenfalls voll gültig sind (§ 20 E-Government-Gesetz).

dem Empfänger die Prüfung zu ermöglichen. Fehlt das Zertifikat ist die Signatur dennoch gültig, auch wenn sie für Empfänger nicht überprüfbar ist und diese sie daher ablehnen können. Gerichte und Behörden können diese Veröffentlichungs-Einschränkung umgehen und sind immer in der Lage, das notwendige Zertifikat zu erlangen: § 22 Abs 2, 3 SigG.

Es muss sich bei einer einfachen el. Signatur nicht unbedingt um Kryptographie und Zertifikate handeln, sondern auch eine rein textuelle Angabe des Namens des Signators erfüllt die Anforderungen an eine *einfache* el. Signatur, natürlich dann nur mit äußerst geringer Sicherheit und keinen besonderen Rechtsfolgen. So treffen auf derartige Signaturen die in Abschnitt VIII.3 angeführten Rechtsfolgen nicht zu.

VIII.2.2. Sichere elektronische Signatur

Eine Definition ist in § 2 Z 3 SigG enthalten:

Eine sichere el. Signatur ist eine el. Signatur, die
a) ausschließlich dem Signator zugeordnet ist,
b) die Identifizierung des Signators ermöglicht,
c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie
e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird.

Eine sichere el. Signatur ist gegenüber einer normalen Signatur um einige Punkte erweitert. So wird vorausgesetzt, dass der Signator die Mittel zur Erstellung unter seiner alleinigen Kontrolle halten kann[572]. Dies ist notwendig, da sonst keine Rechtsfolgen an eine sichere Signatur geknüpft werden könnten: Jeder könnte behaupten, dass er nicht in der Lage ist, eine Fälschung zu verhindern und daher die Signatur ihm nicht zugerechnet werden darf. Sie könnte genauso von jemandem anderen stammen. Dies bedeutet jedoch keinen Ausschluss dieser Möglichkeit: Wurde das Sicherungsmittel, z.B. die Smartcard und der PIN-Code, tatsächlich von einem Dritten verwendet, so kann darüber ein Beweis geführt und die Rechtswirkungen abgewendet werden.

Jegliche nachträgliche Veränderung der Daten muss erkennbar sein, um die Dokumentenechtheit zu gewährleisten. Dies erfolgt bei externen Signaturen dadurch, dass sich bei der Überprüfung ein anderer Hashwert ergibt als der Signatur entspricht, während bei internen Signaturen eine (sinnvolle) Entschlüsselung nicht mehr möglich ist.

Dass ein qualifiziertes Zertifikat (siehe VIII.2.6) verwendet werden muss, ist nur im SigG, aber nicht in der SigRL enthalten; siehe dazu auch die "fortgeschrittene" Signatur. Dies ist jedoch kein Widerspruch, da die Richtlinie sich nirgends auf eine fortgeschrittene Signatur alleine ohne qualifiziertes Zertifikat bezieht. Für sichere elektronische Signaturen kommen daher derzeit nur Public-Key-Systeme in Frage, wobei die Verknüpfung einer Person mit einem öffentlichen Schlüssel durch qualifizierte Zertifikate erfolgt.

[572] Trifft etwa bei einer rein textuellen Unterschrift, siehe oben, nicht zu: Jeder kann einen beliebigen Namen an das Ende einer E-Mail schreiben.

VIII.2.3. Fortgeschrittene elektronische Signatur

Eine Definition ist in Art 2 Z 2 SigRL enthalten, jedoch nicht im SigG[573]. Sie unterscheidet sich von der sicheren el. Signatur dadurch, dass kein qualifiziertes Zertifikat[574] erforderlich ist und auch andere technische Verfahren und Komponenten verwendet werden können. Rechtlich gesehen handelt es sich daher um eine "normale" bzw. einfache Signatur.

Bedeutung erlangte sie durch die el. Rechnung[575], für welche eine fortgeschrittene el. Signatur ausreicht und nicht unbedingt eine sichere elektronische Signatur erforderlich ist. Daher ist hiermit eine automatische Massensignierung von Rechnungen möglich.

VIII.2.4. Unterzeichner/Signator

Eine Definition ist in § 2 Z 2 SigG und in Art 2 Z 3 SigRL enthalten.

Ein Signator ist eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet.

Unter "Signaturerstellungsdaten" ist der private Schlüssel zu verstehen, während "Signaturprüfdaten" den öffentlichen Schlüssel bezeichnet. Diese Benennung wurde gewählt, um eine Technik-indifferente Fassung zu ermöglichen, sodass auch etwaige andere Systeme darunter subsumiert werden können, wenn auch derzeit keine anderen spezifiziert sind[576].

Ein Signator kann sowohl im eigenen Namen als auch unter fremdem Namen handeln (Vollmacht, Auftrag, Geschäftsführung, ...), ebenso wie bei händischen Unterschriften. Die tatsächliche Signierung kann jedoch immer nur selbst erfolgen.

Im Gegensatz zur SigRL spricht das SigG ausdrücklich nur von natürlichen Personen (siehe dazu Kapitel VIII.8: Widerspruch zwischen SigRL und SigG). Juristische Personen können deshalb keine Signatoren sein. Von diesem Grundsatz wird eine Ausnahme gemacht: Zertifizierungsdiensteanbieter können als Person im Zertifikat ihre Firma führen, besitzen also ein Zertifikat für die juristische Person und nicht für eine/mehrere Mitarbeiter. Dies hat den Grund, dass sonst bei jedem Wechsel des für die Ausstellung von Zertifikaten zuständigen Mitarbeiters alle von diesem signierten Zertifikate unter dem neuen Wurzelzertifikat, das ja auf den neuen Mitarbeiter ausgestellt werden müsste, ungültig wären[577]. Dies würde dazu führen, dass alle Benutzer bei einem solchen Personenwechsel ein neues Zertifikat der Zertifizierungsstelle installieren müssten, um sowohl alte wie neue Zertifikate als gültig zu erkennen. Weiters müssten *alle* Kunden dieses Anbieters *alle* Zertifikate neu ausstellen lassen, d.h. mit der Signatur des neuen Verantwortlichen signieren lassen.

---

[573] Siehe dazu auch das Positionspapier der Aufsichtsstelle zu § 2 Z 3 lit. a bis d SigG ("fortgeschrittene elektronische Signatur"). http://www.signatur.rtr.at/de/repository/rtr-advancedsignature-10-20040413.html

[574] Daher ist auch nur eine verminderte Überprüfung des Antragstellers erforderlich: Es muss nicht unbedingt ein amtlicher Lichtbildausweis sein.

[575] Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf el. Weg übermittelte Rechnung bestimmt werden, BGBl. II Nr. 583/2003. Dort wird jedoch nur auf § 2 Z 3 lit. a bis d SigG verwiesen (lit e kommt nicht vor); der Begriff "fortgeschrittene Signatur" kommt nicht vor.

[576] Elektronische Signaturen sind damit derzeit nur in Form von digitalen Signaturen möglich.

[577] Genau dieses Problem kann bei Server-basierten fortgeschrittenen Signaturen für elektronische Rechnungen auftreten. Diese müssen zwar nicht manuell ausgelöst werden, sind aber immer noch einer einzigen Person zugeordnet, welche für die Firma die Rechnungen unterschreiben können muss (technisch) und darf (organisatorisch bzw. rechtlich).

VIII.2.5. Zertifikat

Eine Definition ist in § 2 Z 8 SigG und in Art 2 Z 9 SigRL enthalten.

Ein Zertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird.

Diese rechtliche Definition entspricht der technischen: Es wird eine Verbindung zwischen einem öffentlichen Schlüssel und einer konkreten Person hergestellt. Die Personenidentifizierung erfolgt über einen Namen, welcher ihr eindeutig zugeordnet sein muss. Pseudonyme sind zwar im Zertifikat möglich, doch der ZDA muss die wahre Identität kennen.

Im Gegensatz zu den Bestimmungen beim Signator können Zertifikate für alle Personen ausgestellt werden, insbesondere auch für juristische Personen. Diese können daher auch als Unterzeichner auftreten, lösen jedoch eben nicht die Rechtswirkungen aus, die mit dem Begriff eines "Signators" verbunden sind, da sie keine sichere, sondern nur einfache elektronische Signaturen erstellen können[578].

"Wurzel"-Zertifikate der ZDA sind entweder selbst-signiert oder werden mit einem Zertifikat der Aufsichtsstelle (TKK) signiert, sodass im zweiten Fall das Wurzel-Zertifikat der TKK automatisch die Wurzel aller derartigen österreichischen Zertifikate darstellt[579]. Daraus könnte sich theoretisch ein Sicherheitsproblem ergeben, gleichzeitig wird jedoch eine Prüfung der Gültigkeit von Zertifikaten stark erleichtert.

VIII.2.6. Qualifiziertes Zertifikat

Eine Definition ist in § 2 Z 9 SigG iVm § 5, 7 SigG und in Art 2 Z 10 SigRL iVm Anhang I, II SigRL enthalten.

Ein Zertifikat, das zumindest die folgenden Angaben enthält und von einem Zertifizierungsdiensteanbieter für qualifizierte Zertifikate ausgestellt wird und mit der sicheren elektronischen. Signatur des Zertifizierungsdiensteanbieters versehen ist:

a) den Hinweis darauf, dass es sich um ein qualifiziertes Zertifikat handelt,
b) den unverwechselbaren Namen des Zertifizierungsdiensteanbieters und den Staat seiner Niederlassung,
c) den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muss,
d) gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht, eine andere rechtlich erhebliche Eigenschaft des Signators oder weitere rechtlich erhebliche Angaben,
e) die dem Signator zugeordneten Signaturprüfdaten,
f) Beginn und Ende der Gültigkeit des Zertifikates,
g) die eindeutige Kennung des Zertifikates,
h) gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats und
i) gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist.

---

[578] Technisch die gleiche Sicherheit, jedoch rechtlich eine andere Behandlung.

[579] Sicherheits- und Zertifizierungskonzept (Certification Practice Statement) der TKK http://www.signatur.rtr.at/de/repository/tkk-cps-14-20060612.html

Dem Zertifikat muss einerseits zu entnehmen sein, dass es sich um ein qualifiziertes Zertifikat handelt[580], und andererseits von welchem Zertifizierungsdiensteanbieter es ausgestellt wurde. Dadurch soll es dem Empfänger ermöglicht werden zu entscheiden, welches Vertrauen er in das Zertifikat setzt. Hierzu ist eine genaue Identifikation des Ausstellers notwendig. Die Angabe des Staates der Niederlassung des ZDA hat den Sinn, die tatsächliche Überprüfung zu ermöglichen, da in der EU keine Land ein vollständiges Verzeichnis für alle Länder führen muss und dies auch nicht für eine separate EU-Instanz vorgesehen ist. In Österreich ist zwar eine zentrale Stelle vorgesehen, bei der alle Zertifikate der inländischen ZDA hinterlegt werden müssen, doch sind auch hier ausländische Zertifikate nur auf Antrag aufzunehmen, also freiwillig (§ 13 Abs 3 SigG).

Auch Pseudonyme sind als Inhalt von Zertifikaten zulässig, dürfen jedoch weder anstößig sein noch offensichtlich Verwechslungen mit Namen oder Kennzeichen hervorrufen (§ 8 Abs 4 SigG). Dies bedeutet keine vollständige Anonymität: dem ZDA muss die tatsächliche Identität immer bekannt sein, selbst wenn sie nicht im Zertifikat aufscheint.

Angaben über eine Vertretungsmacht betreffen insbesondere die Befugnis zur Außenvertretung von Gesellschaften: Prokura, Handlungsvollmacht, Eigenschaft als Notar/Rechtsanwalt etc. Diese Eigenschaften müssen dem Zertifizierungsdiensteanbieter nachgewiesen werden, bevor ein entsprechendes Zertifikat ausgestellt werden darf.

Weiters können Einschränkungen des Anwendungsbereichs vorgesehen werden. Denkbar sind diese beispielsweise in Bezug auf bestimmte Rechtsgeschäfte, wie etwa Kaufverträge über bewegliche Sachen (Ausschluss von Kaufverträgen über Grundstücke, Darlehensgewährung, bestimmte Gebiete etc.). Optional kann auch eine Beschränkung des Transaktionswertes erfolgen, der mit dem Zertifikat möglich ist. Dies hat zwar keine Auswirkung auf die Zulässigkeit der Verwendung bei höherwertigen Verträgen, welche dadurch nicht ungültig sind, doch wird hiermit die Haftung des ZDA eingeschränkt. Besonders geeignet sind derartige Zusatzmerkmale für Personen, deren Ausgaben eingeschränkt werden sollen (Kinder, Unmündige, ...). Wer ein solches Zertifikat akzeptiert, kann sich später nicht darauf berufen, dass er von der Beschränkung nichts gewusst hat.

VIII.3. Rechtswirkungen elektronischer Signaturen

Aus der Verwendung el. statt handschriftlicher Unterschriften ergeben sich großteils idente Rechtswirkungen: Sie sind gleichgestellt und dürfen nicht diskriminiert werden.

VIII.3.1. Erfüllung der Schriftform

Eine sichere el. Signatur, d.h. auf einem qualifizierten elektronischen Zertifikat beruhend, erfüllt die Anforderung einer eigenhändigen Unterschrift und damit das Erfordernis der Schriftlichkeit gemäß § 886 ABGB[581]. Besondere Formen der Schriftlichkeit, wie etwa Notariatsakt, notarielle Beurkundung etc. sind davon (noch) nicht betroffen und können daher derzeit nicht el. erfolgen; ebenso die (raren) Rechtsgeschäfte des Familien- oder Erbrechts mit Schriftformerfordernis. Siehe hierzu jedoch die Änderungen im Signaturgesetz und der Notariats- bzw. Rechtsanwaltsordnung durch das Berufsrechts-Änderungsgesetz 2006.

---

[580] Diese Anmerkung darf auch *nur* bei diesen eingebaut werden.

[581] Im Gegensatz zu Deutschland erfordert "Schriftlichkeit" *nicht* das Vorliegen einer Urkunde, was in Österreich mangels physischer Festlegung bei elektronische Daten auch nicht möglich ist (siehe dazu analog im Kapitel Strafrecht).

In Zukunft sind daher folgende Bereiche von einer el. Unterschrift ausgenommen (siehe dazu auch E-Commerce RL Art. 9):

- Rechtsgeschäfte des Familien- oder Erbrechts mindestens mit Schriftformerfordernis. Diese Einschränkung kann ab dem Jahr 2007 umgangen werden, wenn zusätzlich ein Notar oder Rechtsanwalt mit seiner Signatur bestätigt, dass er den Signator über die Rechtsfolgen aufgeklärt hat. Hiermit soll der besonderen Übereilungsschutz einer physischen Unterschrift im el. Bereich substituiert werden. Weiters sind diese Bereiche besonders sensibel, da sie häufig vermögensrechtliche Belange besonders schutzbedürftiger Personen betreffen (z.B. Minderjährige). Auch in Zukunft sind letztwillige Anordnungen jedoch el. nicht möglich, nicht einmal zusammen mit einer Notarsignatur. Ein Testament in el. Form ist daher unwirksam.
- Bürgschaftserklärungen[582] durch Nicht-Kaufleute[583]. Hierfür ist gemäß § 1346 Abs 2 ABGB explizit die Schriftform gefordert. Diese Ausnahme existiert, um die besondere Warnfunktion der eigenhändigen handschriftlichen Unterschrift nicht zu entwerten. Analog dem vorigen Punkt ist hier eine elektronische Form möglich, wenn zusätzlich ein Notar oder Rechtsanwalt mit seiner Signatur bestätigt, den Bürgen über die Rechtsfolgen der Verpflichtung aufgeklärt zu haben.
- Willenserklärungen oder Rechtsgeschäfte, die einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsaktes für ihre Wirksamkeit oder für eine Eintragung in ein öffentliches Register[584] bedürfen. Auch diese Ausnahme wird mit 2007 praktisch beseitigt, da der jeweilige Akt dann auch elektronisch erfolgen kann[585].

Absolute Ausnahme ist daher lediglich die letztwillige Verfügung, typischerweise ein Testament. Alle anderen Rechtsgeschäfte können el. durchgeführt werden, wobei in manchen Fällen jedoch besondere Zusatzvorkehrungen erforderlich sind.

Die Nichteinhaltung zivilrechtlicher Schriftformerfordernisse führt zu einer Naturalobligation, welche zwar erfüllbar, aber nicht einklagbar ist. Dies hat zur Folge, dass eine tatsächliche Leistung den Formmangel heilt. Eine Rückabwicklung formmangelhafter Verträge ist damit ausgeschlossen (§ 1432 ABGB). Gleiches gilt für Signaturen, die nicht allen Anforderungen für sichere Signaturen entsprechen: Ihre Verwendung führt zwar nicht zu einem Vertrag, aber zu einer Naturalobligation.

Wichtig ist festzustellen, dass hierdurch keine Formvorschriften berührt werden: Rechtsgeschäfte, die Schriftlichkeit erfordern, benötigen diese weiterhin. Sie kann nun eben zusätzlich anders als nur handschriftlich erfüllt werden. Nicht formgebundene Geschäfte bleiben auch weiterhin formfrei.

---

[582] Dies findet analoge Anwendung auf Garantieerklärungen. Ein Fax, selbst mit Original-Unterschrift, reicht nicht aus, da das "Aus-der-Hand-geben" ein wichtiges Element der Warnfunktion ist.

[583] Kaufleute können Bürgschaftserklärungen auch mündlich wirksam abgeben, sodass sich bei ihnen die Frage gar nicht stellt. Aus Beweiszwecken ist jedoch eine Unterschrift wohl zweckmäßig und kann auch elektronisch erfolgen.

[584] Insbesondere Grund- und Firmenbuch.

[585] D.h. ein Notariatsakt bedarf in Zukunft entweder einer physischen Unterschrift vor dem Notar oder einer elektronischen Signatur vor einem Notar zusammen mit einer elektronischen Signatur des Notars. Eine elektronische Signatur vor einem Notar, welche dieser handschriftlich beglaubigt, z.B. auf einem Ausdruck, reicht nicht aus.

VIII.3.2. Vermutung der Echtheit

Der Unterschrift kommt auch im Beweisrecht eine wichtige Bedeutung zu. Für unterschriebene Privaturkunden gelangt die besondere zivilprozessuale Beweisregel des § 294 ZPO zur Anwendung. Ist eine Unterschrift unbestritten oder nachgewiesenermaßen echt, so erbringt eine Privaturkunde vollen Beweis dafür, dass der Inhalt vom Aussteller, also vom Namensträger der Unterschrift, stammt. Dabei handelt es sich um eine qualifizierte Echtheitsvermutung für den Erklärungsinhalt, die eine Zuordnung der in einer Urkunde enthaltenen Erklärung zum Unterzeichner bewirkt[586]. Der Beweis des Gegenteils ist zulässig, dann jedoch vom Gegner zu führen. Dies bedeutet, dass die Beweislast für die Unechtheit des Inhalts der Urkunde den Gegner des Beweisführers trifft, d.h. denjenigen, der unterschrieben hat. Diese Umkehr bezieht sich aber nur auf den Urkundeninhalt, hinsichtlich der Echtheit der Unterschrift (=el. Signatur) gelangen die normalen Beweislastregeln zur Anwendung. Die Richtigkeit der Signatur hat also der zu beweisen, der die Datei als Beweis verwenden möchte.

Diese Rechtswirkungen treten nicht ein, wenn nachgewiesen wird, dass die Sicherheitsanforderungen durch den ZDA nicht eingehalten oder die Signaturerstellungsdaten kompromittiert wurden, also z.B. der private Schlüssel jemandem anderen bekannt ist. Wenn dies auch unwahrscheinlich ist, können sich dadurch Personen doch von ihrer Haftung befreien, sofern sie ihren Sorgfaltspflicht bei der Schlüssel-Geheimhaltung entsprachen!

VIII.3.3. Zulässigkeit als Beweismittel vor Gericht

Sichere el. Signaturen müssen vor Gericht als Beweismittel zugelassen werden. Dies ist in Österreich kein besonderes Problem, da fast keine Beweisverbote existieren. Nach derzeitigem Beweisrecht stellt ein el. Dokument im visualisiertem Zustand ein Augenscheinsobjekt dar. Wird ein el. Dokument ausgedruckt, so liegt eine – jedoch nicht unterschriebene – Urkunde vor.

Aber auch nicht-sichere (juristisch, nicht technisch gesehen!) Signaturen, also solche, die nicht auf einem qualifizierten Zertifikat beruhen oder bei denen sonstige Punkte fehlen, müssen vor Gericht beachtlich sein. Weder dass sie nur in el. Form vorliegen, nicht auf einem qualifizierten Zertifikat beruhen, nicht von einem akkreditierten Zertifizierungsdiensteanbieter stammen oder nicht mit einer sicheren Signaturerstellungseinheit erzeugt wurden, darf einen grundsätzlichen Ausschluss bedeuten. Ihr Beweiswert ist jedoch weiterhin der freien Beweiswürdigung unterworfen und wird daher in der Praxis geringer sein als bei sicheren Signaturen. Er darf jedoch nicht ohne Begründung einfach ausgeschlossen werden[587]. Dies gilt nur für Gerichte; Verwaltungsbehörden müssen solchen Signaturen keinen Wert beilegen[588] und können z.B. einen Verbesserungsauftrag erteilen.

---

[586] Damit wird nicht die Wahrheit/Tatsächlichkeit des Inhalts bewiesen, sondern nur, dass der Unterzeichner genau diesen Inhalt erklärte. Es verbleibt dann kein Platz mehr für ein Abstreiten.

[587] In der Praxis wird wohl ein Gutachten über den Sicherheitsgrad und die Schwierigkeit einer Fälschung über den konkreten Beweiswert entscheiden.

[588] Achtung: Der europäische Begriff "Gericht" umfasst mehr als in der österreichischen Rechtssprache, z.B. auch die unabhängigen Verwaltungssenate (UVS), welche in Österreich zur Verwaltung zählen.

VIII.3.4. Haftung der Zertifizierungsdiensteanbieter

Ein Zertifizierungsdiensteanbieter haftet gegenüber dritten Personen gemäß § 23 SigG, sofern diese auf das qualifizierte Zertifikat vertrauten, für folgende Punkte:

- Alle Angaben im Zertifikat sind zum Zeitpunkt der Ausstellung richtig.
- Der Empfänger ist zum Ausstellungszeitpunkt im Besitz der Signaturerstellungsdaten.
- Die Signaturerstellungs- und die Signaturprüfdaten entsprechen einander komplementär, wenn von ihm empfohlene/bereitgestellte Produkte/Verfahren verwendet werden.
- Ein Widerruf erfolgt sofort nach Bekannt werden der Erfüllung der dafür notwendigen Voraussetzungen.
- Die Widerrufsdienste sind verfügbar.
- Die Einhaltung der Sicherheitsvorschriften in seinem Unternehmen.

Alle diese Punkte sind unverzichtbar. Es kann daher nur *nach* Entstehen des Anspruchs darauf verzichtet werden. Ein Ausschluss oder Verzicht im vorhinein ist unwirksam.

Diese Haftung unterliegt jedoch auch Einschränkungen: Der ZDA haftet nicht, wenn er nachweist, dass ihn kein Verschulden trifft. Für Handlungen seiner Gehilfen muss er jedoch sehr wohl einstehen. Darin enthalten ist eine Haftung bis hinab zu leichter Fahrlässigkeit. Ausnahmsweise fällt diese weg, wenn das Zertifikat entgegen darin enthaltenen Beschränkungen verwendet wurde. Es trifft ihn gar keine Haftung, wenn das Zertifikat für ein nicht in den Einschränkungen enthaltenes Rechtsgeschäft verwendet wurde bzw. nur in Höhe der Beschränkung des Transaktionswertes bei einer Überschreitung desselben.

Um einem Benutzer von Zertifikaten in einem Prozess den Beweis zu erleichtern, genügt es, wenn dieser *wahrscheinlich* macht, dass die Kompromittierung in der Sphäre des ZDA erfolgte. Daraus resultiert jedoch keine Umkehr der Beweislast, da der ZDA sein Haftung dadurch abwenden kann, dass er gleichfalls nur wahrscheinlich macht, dass die Kompromittierung in der Sphäre des Signators liegt: Hiermit wird der Anscheinsbeweises des Signators außer Kraft gesetzt.

Gemäß der SigVO ist ein Zertifizierungsdiensteanbieter in dieser Hinsicht verpflichtet, eine Haftpflichtversicherung in Höhe von € 700.000 pro Versicherungsfall für mindestens drei Fälle pro Jahr abzuschließen, bevor er seine Tätigkeit aufnehmen darf.

VIII.4. Widerruf von Zertifikaten

Manchmal ist es nötig, Zertifikate zu widerrufen, bevor ihr Geltungszeitraum abgelaufen ist. Mit ansteigender Wahrscheinlichkeit sind dies folgende Fälle:

- Es wurde zufällig ein gleiches Schlüsselpaar erzeugt,
- der private Schlüssel der Zertifizierungsinstanz wurde bekannt,
- der private Schlüssel des Signators wurde bekannt,
- der Signator ist tot oder nicht mehr im Besitz des privaten Schlüssels oder
- die Angaben im Zertifikat sind nicht mehr gültig (Namensänderung, Änderung der Vertretungsmacht etc.)

Es ist zwischen "Sperren" und "Widerrufen" von Zertifikaten zu unterscheiden: Eine Sperre bedeutet nur eine temporäre Ungültigkeit von maximal zehn Werktagen, während ein Widerruf die Gültigkeit eines Zertifikates endgültig beseitigt. Eine Sperre erfolgt dann, wenn es anscheinend Gründe gibt, das Zertifikat zu widerrufen, aber noch genauere Ermittlungen notwendig sind, ob diese tatsächlich vorliegen. Ab einer Sperre erfolgt daher die Akzeptierung des Zertifikates auf eigene Gefahr: Wird es widerrufen, so wirkt der Widerruf rückwirkend mit dem Zeitpunkt der Sperre. Stellen sich die Gründe jedoch als falsch heraus, so war das Zertifikat während der gesamten Zeit gültig (=rückwirkende Aufhebung der Sperre) und bleibt es auch weiterhin.

Sowohl Sperre als auch Widerruf müssen mit einem sicheren Zeitstempel versehen sein, um ihren genauen Zeitpunkt feststellen zu können. Sperren und Widerrufe mit einem Zeitpunkt in der Vergangenheit zu erstellen, ist unzulässig. Um diese den Benutzern auch zur Kenntnis zu bringen, muss jeder Zertifizierungsdiensteanbieter entsprechende Verzeichnisse el. und frei zugänglich führen. Deren Abfrage hat gratis und ohne Identifizierung des Abfragenden möglich zu sein. Unterbrechungen, wie etwa Systemzeiten, sind nicht erlaubt. Für diese Fälle ist ein Ersatzsystem vorzusehen. Daher ist jede länger als 30 Minuten dauernde Unterbrechung als Störfall zu protokollieren. Ein Widerruf, der auch schriftlich möglich ist, muss nach der SigVO während der Geschäftszeiten[589] spätestens drei Stunden nach Bekannt werden des Widerrufsgrundes erfolgen und veröffentlicht sein.

Für die Praxis ist wichtig, dass eine Prüfung des Widerrufs des Zertifikates immer dann notwendig ist, wenn der Transaktionswert eine bestimmte Höhe erreicht, die von der eigenen Risikobereitschaft abhängt. Da Sperr- und Widerrufsverzeichnisse el. und unentgeltlich zur Verfügung stehen müssen, ist aber auch eine grundsätzliche Prüfung in allen Fällen möglich. Damit später ein Beweis möglich ist, muss in einen Vertrag ein gesicherter Zeitstempel aufgenommen werden: Ansonsten ist es nicht möglich zu beweisen, wann exakt die Signierung durchgeführt worden war. Ohne diesen Stempel kann nicht festgestellt werden, ob die Signatur noch vor dem Widerruf erfolgte und damit gültig ist, oder danach, wobei auf eine Überprüfung wegen etwaigen Widerrufs verzichtet wurde, und somit ungültig ist.

VIII.5. Zertifizierungsstellen

An Anbieter von Zertifizierungsdiensten (Engl.: "Certificate Authority", CA) werden hohe Anforderungen gestellt. Dies ist auch notwendig, da an eine Signatur unter Umständen erhebliche rechtliche und finanzielle Folgen geknüpft sind. Es ist daher ein Missbrauch so weit wie nur irgend möglich auszuschließen. Dies soll auch das Vertrauen der Benutzer fördern, da ansonsten keine weite Verbreitung und die damit verbundenen Vorteile wie einfachere und schnellere Erledigung, mehr Möglichkeiten für Kontakte mit der Verwaltung etc. zu erwarten sind.

VIII.5.1. Datenschutz

Zertifikate besitzen nicht nur Vorteile: Durch ihre Verwendung wird jede Anonymität beseitigt. Die einzige Möglichkeit dagegen ist, entweder keine Zertifikate zu verwenden, was eher ungünstig ist, oder solche mit einem Pseudonym einzusetzen. Zusätzliche Zertifikate bedeuten jedoch auch zusätzliche Kosten und mehr Organisationsaufwand. Um die Gefahr

[589] Mindestumfang: Werktage 9-17 Uhr, Samstag 9-12 Uhr

des "gläsernen Menschen" nicht zu groß werden zu lassen, werden an den Datenschutz in Bezug auf Zertifikate besonders hohe Anforderungen gestellt:

- Zertifizierungsdiensteanbieter dürfen nur diejenigen personenbezogenen Daten verwenden, welche für die Durchführung der Dienste notwendig sind (§ 22 SigG). Insbesondere dürfen keine Aufzeichnungen und Auswertungen von Anfragen bezüglich eines etwaigen Widerrufs durchgeführt werden, da sich dadurch eine Datenspur ergibt und Gewohnheiten des Zertifikatsinhabers (besuchte Webseiten, bevorzugte Internet-Geschäfte, ...) festgestellt werden könnten.
- Alle notwendigen Daten für die Überprüfung der Ausstellung inklusive Angaben über besondere Eigenschaften, etwa die Vertretungsmacht, dürfen ausschließlich beim Antragsteller erhoben werden. Mit seiner *ausdrücklichen* Zustimmung ist auch eine Erhebung bei Dritten möglich. Werden keine Nachweise erbracht, so sind weitere Prüfungen verboten: In diesem Fall darf eben kein Zertifikat ausgestellt werden.
- Wird ein Pseudonym verwendet, so hat der ZDA die Identität des Signators auch Dritten zu übermitteln, sofern diese überwiegendes berechtigtes Interesse glaubhaft machen. Solche Auskünfte sind exakt zu dokumentieren.

VIII.5.2. Private Zertifizierungsstellen

Grundsätzlich kann jede Person eine Zertifizierungsstelle betreiben. Von einem Anbieter, der keine qualifizierten Zertifikate ausstellt, werden auch keine besonderen Maßnahmen verlangt: Er muss lediglich ein Sicherheits- und ein Zertifizierungskonzept an die Aufsichtsstelle melden und dieses dann einhalten. Dieses Konzept ist in el. Form[590] zu übersenden und muss signiert sein. Dafür gelten keine besonderen Vorschriften, es ist daher auch keine hohe Qualität notwendig und die Gebühren sind sehr niedrig (SigVO: € 100; Zertifizierungsdiensteanbieter für qualifizierte Zertifikate hingegen: € 6.000). Weiters sind einfache Anbieter auch nicht verpflichtet, Verzeichnis- und Widerrufsdienste zu führen.

Werden Schlüsselpaare von der Zertifizierungsstelle und nicht vom Zertifikatsantragsteller erzeugt, so muss dafür ein besonderer Zufallszahlengenerator[591] verwendet werden und die erzeugten Schlüssel sind auf ihre Zufälligkeit und Eignung zu prüfen. Diese Generatoren sind auch regelmäßig auf ihre Qualität zu überprüfen bzw. neu zu initialisieren.

VIII.5.3. Anforderungen an ZDA für qualifizierte Zertifikate

Gegenüber "normalen" Zertifizierungsdiensteanbietern bestehen für die Anbieter qualifizierter Zertifikate zusätzliche Anforderungen. So müssen etwa die Personalien anhand eines gültigen amtlichen Lichtbildausweises überprüft und diese auch archiviert werden, beispielsweise durch eine Ablichtung (§ 11 Abs 1 SigVO). Bei einer Verlängerung eines bestehenden Zertifikates, d.h. nur während der Gültigkeitsdauer der Signatur, ist es ausreichend, wenn ein solcher Antrag mit der (noch) gültigen Signatur versehen ist, ansonsten ist eine handschriftliche Unterschrift nötig. Im ersten Fall ist deshalb persönliches Erscheinen nicht mehr erforderlich. Diese Option ist nur bis zum Ablauf der Gültigkeit des ver-

[590] Erlaubte Formate nach SigVO: "XML mit Darstellungsfunktion" (wohl ein Stylesheet), PDF, ASCII, Postscript

[591] Früher: Physikalischer Zufallszahlengenerator. Jetzt sind nach der SigVO auch Pseudozufallszahlengeneratoren erlaubt. Der Grund ist nicht ganz einsichtig, da physikalische Generatoren auch nicht übermäßig komplex oder teuer sind und nur ein einziges Exemplar benötigt wird! Nach den Ausführungen in der SigVO könnte der Grund darin liegen, dass physische Generatoren (im Vergleich zu Pseudozufallszahlengeneratoren) sehr langsam arbeiten und damit die rasche Ausstellung einer großen Zahl an Zertifikaten problematisch wäre.

wendeten Algorithmus bzw. der Schlüssellänge möglich. Gemäß § 8 Abs 2 SigG kann die Identitätsprüfung des Antragstellers auch von einer beauftragten Stelle erfolgen. Dieser Passus wurde vermutlich für die Post vorgesehen (Prüfung in jedem Postamt), doch könnten auch andere Firmen mit breitem Filialnetz davon Gebrauch machen, z.B. Banken.

An besonderen Anforderungen ist in § 7 SigG für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, u.a. folgendes festgelegt:

- Er muss die erforderliche Zuverlässigkeit aufweisen
- Ein schneller und sicherer Verzeichnisdienst sowie ein sicherer und unverzüglicher Widerrufsdienst muss gewährleistet werden.
- Qualifizierte Zeitstempel müssen verwendet werden, insbesondere für die Zeitpunkte des Ausstellens und Widerrufens von qualifizierten Zertifikaten.
- Zuverlässiges Personal mit den erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen muss beschäftigt werden.
- Genügend Finanzmittel für Betrieb und insbes. Haftung müssen vorhanden sein[592].
- Alle maßgeblichen Umstände über ein qualifiziertes Zertifikat sind aufzuzeichnen, um später die Zertifizierung nachweisen zu können, insbesondere in Gerichtsverfahren.
- Vorkehrungen sind zu treffen, damit Signaturerstellungsdaten weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.
- Technische Einrichtungen zur Erbringung von Signatur- und Zertifizierungsdiensten sind sowohl im Normalbetrieb wie auch bei Störfällen von anderen Funktionen und Anwendungen zu trennen.
- Die Einrichtungen sind gegen unbefugten Zutritt zu sichern.
- Eingesetzte Systeme und Produkte sind genau zu dokumentieren. Zusätzliche Systemelemente, selbst wenn nicht sicherheitsrelevant oder sicherheitsrelevantes Abweichen von der Dokumentation gilt als Kompromittierung der Sicherheit, auch wenn diese Elemente nicht für die Erbringung der Signatur- oder Zertifizierungsdienste notwendig sind und keine tatsächliche Kompromittierung nachgewiesen wurde.

Grob gesagt ist ein sicheres Rechenzentrum mit besonderer Hard- und Software, speziellen Vorkehrungen, und ein gleichartiges Ersatzrechenzentrum gefordert. Aus diesem Grund kann davon ausgegangen werden, dass qualifizierte Zertifikate in der Praxis nur von relativ wenigen Anbietern ausgegeben werden.

Interessant ist, dass nach der SigVO (§ 9 Abs 3) technische Komponenten und Verfahren in bestimmten Fällen durch oganisatorische substituiert werden können, wenn qualifiziertes und vertrauenswürdiges Personal eingesetzt wird. Dies gilt allerdings nur für kontrollierte Umgebungen, d.h. innerhalb eines Rechenzentrums. Verfahren, die von Signatoren verwendet werden, sind also nicht betroffen.

---

[592] Die SigVO legt hierzu fest, dass ein Mindestkapital von € 300.000 erforderlich ist. Davon sind jedoch der Bund, die Länder, Gemeindeverbände, Gemeinden mit mehr als 50.000 Einwohnern sowie Sozialversicherungsträger befreit. Der Grund liegt wohl darin, dass z.B. der Bund kein "Grundkapital" besitzt und die angeführten Organisationen nicht, oder nur sehr unwahrscheinlich, in Konkurs gehen (können).

VIII.5.4. Aufsichtsstelle

Im SigG ist als Aufsichtsstelle die Telekom-Control-Kommission (TKK) vorgesehen[593]. Diese agiert als eine oberste Zertifizierungsstelle (Root-CA), signiert also die Zertifikate der einzelnen ZDA. Alternativ können diese auch selbst-signiert sein und werden dann in eine Liste aufgenommen, welche von der Aufsichtsstelle signiert ist. Sie ist dafür verantwortlich, dass jederzeit ein el. und frei zugängliches Verzeichnis[594] der gültigen, gesperrten und widerrufenen Zertifikate der österreichischen, auf Antrag unter Einschluss der ausländischen, ZDA geführt wird. Diese Verzeichnisse sind mit ihrer eigenen el. Signatur zu versehen. Das zugehörige Zertifikat wird im Amtsblatt zur Wiener Zeitung veröffentlicht.

Da in der TKK weder die notwendige detaillierte Fachkenntnis noch die personelle Ausstattung vorhanden ist, um diese Aufgaben zu erfüllen, bedient sie sich einer oder mehrerer "Bestätigungsstellen". Zusätzlich kann die Telekom-Control-GmbH mit der Durchführung der von der Kommission vorzunehmenden Aufsicht beauftragt werden. Sowohl Bestätigungsstellen wie Telekom-Control-GmbH werden dann als beliehene Unternehmen tätig und üben behördliche Funktionen aus. Ihre Entscheidungen erfolgen daher in solchen Fällen in der Form eines Bescheides. Bestätigungsstellen werden vom Bundeskanzler und dem Justizminister im Einvernehmen per Verordnung ernannt[595]. Als Bestätigungsstelle ist derzeit ein einziger Verein vorgesehen: "Zentrum für sichere Informationstechnologie – Austria (A-SIT)". Als Mitglieder fungieren das Bundesministerium für Finanzen, die Oesterreichische Nationalbank sowie die Technische Universität Graz. Dies ist einer der Kritikpunkte an dem Gesetz, da hiermit ein weiterer privater Verein mit behördlichen Aufgaben betraut wird. Als Alternative wurde beispielsweise der TÜV (Technischer Überwachungsverein) vorgeschlagen, der bereits umfangreiche Technikprüfungen durchführt.

VIII.6. Akkreditierung

Die Akkreditierung eines Zertifizierungsdiensteanbieters bringt keine zusätzlichen Qualitätsmerkmale mit sich: Es handelt sich nur um eine Bestätigung, dass die ohnedies einzuhaltenden Bestimmungen besonders im Vorhinein überprüft wurden und ihnen entsprochen wird. Die erfolgreiche Akkreditierung berechtigt, das Bundeswappen zu führen und sich als "Akkreditierter Zertifizierungsdiensteanbieter" zu bezeichnen, was hauptsächlich Werbezwecken dient. Für diese ZDA ist bei der Aufsichtsstelle ein eigenes Verzeichnis zu führen bzw. werden sie im allgemeinen Verzeichnis besonders gekennzeichnet.

Dass ein Zertifikat von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellt wurde, ist in das Zertifikat aufzunehmen, sodass ein Empfänger deswegen (eventuell) ein höheres Vertrauen darin setzen kann. In Zertifikate nicht akkreditierter Anbieter darf diese Bezeichnung nicht eingebaut werden. Rechtlich sind sichere Signaturen mit qualifizierten Zertifikaten von "normalen" und "akkreditieren" ZDA jedoch absolut gleichgestellt.

Nach der SigRL ist eine Beschränkung der Anzahl der akkreditierten Anbieter nicht zulässig. Es hat daher jeder Anbieter die Möglichkeit, eine Akkreditierung zu erhalten, sofern er

---

[593] Siehe dazu § 116 TKG; dies ist ein unabhängiges und weisungsfreies Kollegialorgan mit richterlichem Einschlag gemäß Art 133 Z 4 B-VG, das in erster und oberster Instanz entscheidet. Die Anrufung des Verwaltungsgerichtshofes als außerordentliches Rechtsmittel ist explizit gestattet.

[594] http://www.signatur.rtr.at/de/providers/providers.html Die sichere Version ist jedoch nur über LDAP/SSL erreichbar.

[595] Derzeit die einzige: Feststellung der Eignung des Vereins "Zentrum für sichere Informationstechnologie – Austria (A-SIT)" als Bestätigungsstelle, BGBl II 31/2000 vom 2.2.2000

qualifizierte Zertifikate ausstellt. Anbieter "einfacher" Zertifikate können sich nicht akkreditieren lassen. Da Zulassungsbeschränkungen explizit in der SigRL verboten sind, wurde diese Hintertür für eine Vorab-Prüfung geschaffen: Ein ZDA, der akkreditiert werden will, darf erst dann den Betrieb aufnehmen, wenn die Überprüfung und anschließende Akkreditierung angeschlossen ist. Eine Akkreditierung im Nachhinein ist nach § 17 Abs 1 SigG nicht möglich.

VIII.7. Rechte und Pflichten: ZDA und Signator

Der Signator hat die Pflicht, seine Signaturerstellungsdaten sicher zu verwahren und sie nicht weiterzugeben. Verliert er die Erstellungsdaten oder vermutet er, dass sie bekannt wurden, so hat er selbst den Widerruf des Zertifikates zu veranlassen. Ebenso ist er verpflichtet, das Zertifikat widerrufen zu lassen, wenn die Angaben im Zertifikat nicht mehr richtig sind. Er darf nur die vom ZDA bereitgestellten oder empfohlenen Hash- und Signatur-Verfahren verwenden, wenn eine sichere Signatur erstellt werden soll[596].

Im Gegensatz dazu ist der Zertifizierungsdiensteanbieter verpflichtet, den Zertifikatswerber umfassend, klar und allgemein verständlich zu unterrichten. Dies muss vor der Vertragsschließung erfolgen und hat entweder schriftlich oder auf einem dauerhaften Datenträger zu erfolgen (d.h. CD-ROM, aber wohl nicht E-Mail[597]). Der Zertifikatswerber ist vor Vertragsschluss bzw. bei der Zertifikatsausstellung über folgende Punkte aufzuklären:

- Inhalt des Sicherheits- und Zertifizierungskonzeptes des ZDA
- Bedingungen der Verwendung des Zertifikates (Anwendungsbereichs- oder Transaktionswertsbeschränkungen), wenn zwangsweise vorgesehen oder gewünscht
- Erfolgte Akkreditierung des Zertifizierungsdiensteanbieters, sofern zutreffend
- Besondere Streitbeilegungsverfahren, sofern festgelegt
- Geeignete technische Komponenten und Verfahren für das verwendete Signaturverfahren bzw. auch sonstige mögliche Maßnahmen und Anforderungen für die Erzeugung und Prüfung sicherer Signaturen
- Mögliche Rechtswirkungen des verwendeten Signaturverfahrens
- Pflichten eines Signators (siehe oben)
- Haftung des Zertifizierungsdiensteanbieters
- Wann und wie eine Nachsignierung zu erfolgen hat

VIII.8. Widerspruch zwischen SigRL und SigG

Zwischen der Signaturrichtlinie der EU und dem österreichischen Signaturgesetz besteht aufgrund mehrerer Novellen inzwischen nur mehr ein Unterschied, welcher durch eine spätere Novelle beseitigt werden muss, sollen nicht die üblichen Folgen derartiger Verstöße eintreten: Das österreichische SigG ist nicht anzuwenden und Benutzer können sich direkt auf die RL berufen.

---

[596] Andernfalls ist die Signatur ev. rechtlich nicht gültig (siehe § 2 Abs 3 lit e SigG) bzw. die Haftung des ZDA fällt weg.

[597] Siehe dazu auch die Diskussion über "dauerhafte Datenträger" nach Fernabsatz und E-Commerce RL (VII.2.2.3).

VIII.8.1. Zertifikate nur für natürliche Personen

Die SigRL definiert in Art 2 Z 3 einen "Unterzeichner" allgemein als eine Person (streitig!), während das SigG in § 2 Z 2 einen Signator ausschließlich als natürliche Person, mit Ausnahme von Zertifizierungsdiensteanbietern, festlegt.

Der dahinterstehende Sinn ist, dass juristische Personen nie handlungsfähig sind, sondern zur Vornahme einer physischen Unterschrift immer eines Organs oder Vertreters bedürfen, der in ihrem Auftrag handelt. Dies sollte hiermit nachgebildet werden, da insbesondere in Zertifikaten auch Angaben über die Vertretungsmacht enthalten sein können. Damit soll sichergestellt werden, dass eine Signatur immer einer natürlichen Person zugeordnet werden kann, welche den Signierungsvorgang auslöst. Bei juristischen Personen würde sonst oft der Fall eintreten, dass mehrere Person dazu berechtigt und in der Lage sind, eine Firmensignatur anzubringen, ohne dass sich später aus der Signatur feststellen ließe, welche der Personen dafür konkret im Einzelfall verantwortlich war. Es ist jedoch zu beachten, dass dieses Ziel auch auf einem anderen Wege erreichbar wäre: Mit der Richtlinie vereinbar wäre es, z.B. eine Doppelsignatur[598] durch die juristische Person und diejenige natürliche Person, welche die Signierung auslöste, zu verlangen. Auch sind die Zertifizierungsstellen selbst hiervon ausgenommen, was zwar gute Gründe hat (siehe oben), aber als Beispiel für die grundsätzliche Möglichkeit von Firmensignaturen dienen kann.

VIII.9. Verwaltungsstrafbestimmungen

In § 26 des SigG sind einige Verwaltungsstrafbestimmungen festgelegt, welche aber nur dann zur Anwendung kommen, falls die Tat nicht nach anderen Gesetzen strenger zu bestrafen ist oder in die Zuständigkeit der Gerichte fällt (Subsidiarität).

Für den Benutzer ist nur relevant, dass eine Verwaltungsübertretung begeht, wer fremde Signaturerstellungsdaten ohne Wissen und Willen des Signators missbräuchlich verwendet (Strafrahmen bis € 4.000). Wichtig zu beachten ist, dass auch eine Benutzung ohne Wissen des Berechtigten straflos ist, wenn sie in dessen Interesse erfolgt, also kein Missbrauch vorliegt, sowie wenn sie mit dessen Wissen und Willen erfolgt, z.B. zur Schädigung Dritter[599]. Fahrlässiger Missbrauch ist nicht strafbar.

Für ZDA sind die Strafen zahlreicher und mit einem höheren Strafrahmen ausgestattet: Eine Verwaltungsübertretung mit Geldstrafe bis € 8.000 begeht, wer die Widerrufspflicht oder die Dokumentationspflicht verletzt oder den Zertifikatswerber nicht ordnungsgemäß unterrichtet. In allen diesen Fällen reicht schon die Verletzung in Beziehung auf einen einzelnen Benutzer aus. Mit bis zu € 16.000 werden ZDA bestraft, wenn sie verschiedene der Vorschriften verletzen, welche die Sicherheit in ihrem Betrieb oder die der Zertifikate gewährleisten sollen.

Weiters können Gegenstände, mit denen die strafbare Handlung begangen wurde, für verfallen erklärt werden. Dies betrifft insbesondere Computer oder Geräte, mit denen Schlüssel berechnet wurden oder die zur Duplizierung von Erstellungsdaten dienen.

---

[598] Sonntag: Electronic Signatures for Legal Persons. In: Hofer/Beneder (Hrsg.): IDIMT'00. 8th Interdisciplinary Information Management Talks. Linz: Trauner 2000, 233-256

[599] Hier ist dann jedoch an (Computer-)Betrug zu denken.

VIII.10. Derzeitige Parameter nach der SigVO

Einige wichtige Elemente der Signaturverordnung, welche die möglichen kryptographischen Verfahren, die Schlüssellängen und die Dauer deren Zulässigkeit beschreiben, sind:

- Gültigkeitsdauer von qualifizierten Zertifikaten: Maximal fünf Jahre (früher: drei Jahre)
- Signaturerstellungsdaten sind mit physikalischen oder Pesudo-Zufallszahlengeneratoren zu erzeugen. Letztere sind jedoch mit echten Zufallszahlen zu initialisieren. Es dürfen dann maximal 100 Pseudo-Zufallszahlen erstellt werden. Größere Mengen sind zulässig, wenn kontinuierlich zumindest einige tatsächlich zufällige Bits integriert werden.
- Eine Signatur darf nur nach einer Autorisierung ausgeführt werden, z.B. Eingabe eines PIN oder Scannen des Fingerabdrucks. Zum Auslösungszeitpunkt muss bekannt sein, wie viele Signaturen erzeugt werden[600]. Eingabeerleichterungen sind explizit verboten.
- Signaturerstellungsdaten für sichere Zertifikate (privater Schlüssel[601]):
    - RSA, zumindest 1020 Bit Schlüssellänge
    - DSA, zumindest 1024/160 Bit Schlüssellänge
    - DSA-Varianten auf Basis elliptischer Kurven, zumindest 160/10/200 Bit
    - Zulässige Hashverfahren: RIPEMD-160, SHA-1
    - Zulässige Padding-Verfahren: EMSA-PKCS 1 (Version 1.5); EMSA-PSS

VIII.11. US Electronic Signatures Act

Bei diesem Bundesgesetz (USSigAct[602]) handelt es sich um eine breitere Regelung als bei der EU Signatur-Richtlinie, da auch el. Urkunden und Inhaberpapiere geregelt werden. Es betrifft jedoch ausschließlich den Handelsverkehr zwischen einzelnen Bundesstaaten sowie mit dem Ausland, nicht jedoch innerstaatlichen Handel.

VIII.11.1. Elektronische Urkunden und elektronische Signaturen

Eine el. Signatur wird als Geräusch, Symbol oder Prozess definiert, der zu einer el. Urkunde hinzugefügt oder logisch mit ihr verknüpft ist und von einer Person mit der Absicht zu unterzeichnen erzeugt wurde. Es handelt sich daher um eine sehr breite Definition, die insbesondere vollkommen unabhängig von der verwendeten Technologie ist. Auch eine el. Urkunde wird sehr breit definiert: Ein Vertrag oder eine Urkunde, die mit elektronischen Mitteln erzeugt, generiert, gesendet, übermittelt, empfangen, oder gespeichert wird. Hierbei ist "elektronisch" extrem weit reichend zu verstehen: Auch optische und elektromagnetische Technologien oder solche mit ähnlichen Eigenschaften sind enthalten.

El. Signaturen oder Urkunden dürfen gegenüber handschriftlichen nicht diskriminiert werden, analog der EU-RL, sowohl als Beweismittel als auch beim Abschluss von Verträgen.

---

[600] Es können also mehrere Signaturen auf einmal erstellt werden. Speichern des PIN bis zum Entfernen der Karte und dauerndes signieren währenddessen ist jedoch nicht erlaubt.

[601] Ohne führende Nullen: Ein Schlüssel der Länge 1024 Bit beginnt nicht notwendigerweise mit "1". Sind jedoch zu viele führende Nullen vorhanden, im Extremfall 1023, so ist der Schlüssel nicht mehr sicher.

[602] Abgedruckt in DuD 24 (2000), 1 Electronic Signatures in Global and National Commerce Act http://www.dud.de/dud/ documents/usesignact0608.pdf

Demgegenüber besteht jedoch ebenso keine Verpflichtung, sich dieser Möglichkeiten zu bedienen, ausgenommen für Behörden, welche entsprechende Anträge akzeptieren müssen, sofern es sich nicht um privatrechtliche Verträge mit ihnen handelt.

Weiters sind detaillierte Regelungen enthalten, in welchen Fällen eine el. Mitteilung an einen Konsumenten ausreichend und rechtsgültig ist (vorherige Zustimmung, jederzeitige Widerrufsmöglichkeit, Information über Hard- und Software-Anforderungen etc.).

Auch Aufbewahrungsvorschriften können durch el. Urkunden erfüllt werden. Die enthaltene Information ist exakt zu repräsentieren und hat für alle beteiligten Personen zugänglich zu sein. Dies ist wohl besonders im Hinblick auf die Aufbewahrungsvorschriften für Belege sinnvoll.

Von Bedeutung ist weiters, dass auch höherwertige Formen durch el. Signaturen erfüllt werden können: Notarielle Beurkundungen oder besondere Beglaubigungen können durch el. Urkunden ersetzt werden, wenn sie mit der el. Signatur sowie ev. zusätzlichen erforderlichen Daten dessen versehen sind, der sie sonst handschriftlich beglaubigen müsste. Eine Notarsunterschrift kann daher, (noch) im Kontrast zum SigG, voll rechtsgültig durch die el. Signatur des Notars ersetzt werden.

Eine besondere Vorschrift sieht vor, dass el. Agenten im Geschäftsverkehr nicht diskriminiert werden dürfen. Erfolgt daher ein Teil eines Vertragsabschlusses automatisch (Hard-/Software), ist er dennoch rechtsgültig. Die el. Signatur eines Agenten ist daher rechtserheblich, auch wenn sie ohne direkte Beeinflussung oder ohne Aufsicht durch den Besitzer des Agenten erfolgte. Dies stellt in Österreich normalerweise kein Problem dar und gilt auch so: Wer sich eines Werkzeuges bedient, hat die damit verbundenen Folgen zu tragen.

VIII.11.2. Ausnahmen

Einige Bereiche sind, analog zur SigRL/SigG, vom Geltungsbereich ausgenommen:

- Rechtsgeschäfte des Erbrechts
- Adoption, Scheidung und andere familienrechtliche Angelegenheiten
- Alle handelsrechtlichen Angelegenheiten außer Kauf, Miete, schriftliche Verzichtserklärungen und unterschriebene Kaufverträge (UCC[603] 1 107, 1 206, Art. 2, 2A)

Folgende Dokumente müssen auch weiterhin in physikalischer Form ausgestellt werden und sind einer elektronischen Signatur nicht zugänglich:

- Gerichtsdokumente (Urteile, schriftliche Anträge etc.)
- Beendigung von Infrastrukturleistungen (Wasser, Strom, Heizung, …)
- Bestimmte Mitteilungen (z.B. Kündigung) im Zusammenhang mit Mietverträgen oder Kreditverträgen für den Hauptwohnsitz einer Person
- Beendigung einer Kranken- oder Lebensversicherung sowie von Leistungen daraus
- Rückruf von Produkten oder Mitteilung über Produktfehler, welche Gesundheit oder Sicherheit beeinträchtigen können
- Begleitdokumente für Gefahrenguttransporte

[603] Uniform Commercial Code http://www.law.cornell.edu/ucc/ucc.table.html

VIII.11.3. Inhaberpapiere

Unter Inhaberpapieren versteht man Urkunden, bei denen der Rechtsbesitz schon durch den Besitz der Urkunde bewiesen wird, z.B. Schecks mit "Zahlung an den Überbringer", d.h. analog zu Geldscheinen. Dies ist natürlich bei el. Abbildung ein besonderes Problem, da jederzeit absolut identische Kopien hergestellt werden können. Mittels Kryptographie kann jedoch Ähnliches realisiert werden, doch ist dann keine Anonymität mehr gegeben.

Voraussetzung für die rechtliche Anerkennung sind:

- Eine einzige "Autoritative Kopie" muss existieren, die einmalig und identifizierbar ist.
- Sie muss den Besitzer bzw. auch den Nachbesitzer angeben.
- Der Besitzer oder dessen Beauftragter muss die tatsächliche Kontrolle besitzen.
- Änderungen des Originals können nur mit Zustimmung des Besitzers durchgeführt werden. Unberechtigte Änderungen müssen erkannt werden können.
- Jede Kopie, sowohl des Originals wie auch von weiteren Kopien, ist eindeutig als solche zu identifizieren.

Weiters muss ein Besitzer nachweisen können, dass er Inhaber der autoritativen Kopie ist, d.h. Änderungen vornehmen und damit das Papier weiter übertragen kann.

VIII.12. Literatur

VIII.12.1. Allgemein

A-SIT: http://www.a-sit.at/

Baum, Michael: Die el. Identität? Der Name als Zertifikatsbestandteil - ein Interpretationsvorschlag, DuD 1999, 511ff

Bizer, Johann: Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD 1992, 169 ff

Bertsch, Andreas, Pordesch, Ulrich: Zur Problematik von Prozeßlaufzeiten bei der Sperrung von Zertifikaten. DuD 23, 9/1999, 514ff

Brenn, Christoph: Verbürgung durch mouse-click?, ecolex 1999, 243ff

Brenn, Christoph: Signaturgesetz, Wien: Manz 1999

Brenn, Christoph, Posch, Reinhard: Signaturverordnung, Wien: Manz 2000

Brisch, Klaus: Gemeinsame Rahmenbedingungen für el. Signaturen. Richtlinienvorschlag der Europäischen Kommission, CR 1998, 492ff

Dobbertin, Hans: Digitale Fingerabdrücke. Sichere Hashfunktionen für digitale Signaturen, DuD 1997, 82 ff

Erber-Faller, Sigrun: Notarielle Funktionen im el. Rechtsverkehr, DuD 1994, 680ff

Fallenböck, Markus, Schwab, Guido: Zu der Charakteristik und den Rechtswirkungen el. Signaturen: Regelungsmodelle in den USA und Europa, MR 1999, 370

Fischer, Peter; Köck, Heribert: Europarecht. 3. Auflage, Wien: Linde 1997

Forgó, Nikolaus: Was sind und wozu dienen digitale Signaturen?, ecolex 1999, 235ff

Forgó, Nikolaus: Sicher ist Sicher? - Das Signaturgesetz, ecolex 1999, 607ff

Fox, Dirk: Fälschungssicherheit digitaler Signaturen, DuD 1997, 69ff

Fox, Dirk: Zu einem prinzipiellen Problem digitaler Signaturen, DuD 1998, 386ff

Hammer, Volker: Signaturprüfungen nach SigI, DuD 2000, 96ff

Hein, Werner, Rieder, Markus: Digitale Signatur in den USA. Stand der Gesetzgebung und Praxis, DuD. Datenschutz und Datensicherheit 8/1997, 469

Jud, Waldemar, Högler-Pracher, Renate: Die Gleichsetzung el. Signaturen mit der eigenhändigen Unterschrift, ecolex 1999, 610ff

Kilches, Ralph: Electronic Commerce Richtlinie, MR 1999, 3ff

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

Kuner, Chris, Barcelo, Rosa, Baker, Stewart, Greenwald, Eric: An Analysis of International Electronic and Digital Signature Implementation Initiatives. http://www.ilpf.org/groups/analysis_IEDSII.htm

Lenstra, Arten, Verheul, Eric: Selecting Cryptographic Key Sizes, DuD 2000, 166

Mack, HolgeR: Sperren von Zertifikaten in der Praxis – ein Fallanalyse, DuD 2001, 464f

Mayer-Schönberger, Viktor: Bedauerlich: Signatur-Dienstleister nach der SigV, ecolex 2000, 130f

Mayer-Schönberger, Viktor, Pilz, Michael, Reiser, Christian, Schmölzer, Gabriele: Signaturgesetz. Praxiskommentar, Orac: Wien 1999

Menzel, Thomas, Schweighofer, Erich: Das österreichische Signaturgesetz. Umsetzung des EG-Richtlinienvorschlages in einem österreichischen Signaturgesetz. DuD 23, 9/1999, 503ff

Menzel, Thomas: El. Signaturen, Wien: Verlag Österreich, 2000

Miedbrodt, Anja: Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung, DuD. Datenschutz und Datensicherheit 7/1998, 389

Nöcker, Gregor: Urkunden und EDI-Dokumente, CR 2000, 176ff

Öhlberger, Veith: Die el. Signatur im österreichischen Recht: Ein Überblick. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): Auf dem Weg zur ePerson. Wien: Verlag Österreich 2001

Pordesch, Ulrich: Risiken el. Signaturverfahren, DuD 1993, 561ff

Schumacher, Stephan: Digitale Signaturen in Deutschland, Europa und den U.S.A. Ein Problem, zwei Kontinente, drei Lösungen?, Computer und Recht 12/1998, 758

Sonntag, Michael: Electronic Signatures for Legal Persons. In: Hofer Susaane, Beneder Manfred (Ed.): IDIMT-2000. 8th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2000, 233ff

Sontag, Michael: El. Signaturen. Rechtswirkungen, Haftung von ZDA sowie Sonderprobleme. In: Plöckinger, Duursma, Helm (Hrsg.): Aktuelle Entwicklungen im Internet-Recht. Wien: NWV 2002

Sterbenz, Andreas: Digitale Signaturen - Eine Einführung. Institut für Angewandte Informationsverarbeitung und Kommunikationstechnik, TU Graz. http://akitsicherheit. iaik.tu-graz.ac.at/DiGSig-prinzip.htm (16.3.2000; nicht mehr online)

Telekom Control Kommission: Aufsichtsstelle für el. Signaturen http://www.signatur.rtr.at/de/index.html

Telekom Control Kommission: Sicherheits- und Zertifizierungskonzept (Certification Practice Statement) http://www.signatur.rtr.at/de/repository/tkk-cps-14-20060612.html

Telekom Control Kommission: Positionspapier der Aufsichtsstelle zu § 2 Z 3 lit.a bis d SigG ("fortgeschrittene el. Signatur") http://www.signatur.rtr.at/de/repository/rtr-advancedsignature-10-20040413.html

Timm, Birte: Signaturgesetz und Haftungsrecht, DuD 1997, 525ff

Zieschang, Thilo: Sicherheitsrisiken bei der Schlüsselzertifizierung, DuD 1997, 341ff

VIII.12.2. Rechtsvorschriften

SigRL: Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für el. Signaturen, ABl. 19.1.2000 L 13/12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:DE:HTML

EC-RL: Richtlinie 2000/31/EG des Europäischen Parlamentes 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. 17.7.2000 L 178/1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:DE:HTML

SigG: Bundesgesetz über el. Signaturen (Signaturgesetz - SigG), BgBL I 190/1999 idF BGBl. I 164/2005

SigVO: Verordnung des Bundeskanzlers über el. Signaturen (Signaturverordnung - SigV) vom 2.2.2000, BGBl II 30/2000 idF BGBl II 527/2004

Bericht des Justizausschusses über die Regierungsvorlage (1999 der Beilagen): Bundesgesetz über el. Signaturen (Signaturgesetz – SigG) JAB 2065 BlgNR XX. GP http://www.parlinkom.gv.at/pls/portal/docs/page/PG/DE/XX/I/I_02065/FNAMEORIG_000000.HTML

Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf el. Weg übermittelte Rechnung bestimmt werden, BGBl. II Nr. 583/2003

Electronic Signatures in Global and National Commerce Act, DuD 24 (2000), 1 http://www.dud.de/dud/documents/usesignact0608.pdf

Uniform Commercial Code http://www.law.cornell.edu/ucc/ucc.table.html

IX. Internet - Strafrecht

Bei der Informatik, dem E-Business und besonders dem Internet handelt es sich keineswegs um rechtsfreien Raum, sondern alle Gesetze sind ebenso darauf anzuwenden wie Offline. Das beinhaltet auch das Strafrecht. Hier besteht jedoch das spezielle Problem, dass bei diesem stärksten Sanktionsmittel die Durchsetzung international am schwierigsten ist.

Neben einigen allgemeinen Überlegungen werden die Delikte dargestellt, die eine spezifische Beziehung zur Informatik besitzen. Seit dem Jahr 2001 existiert auf diesem Gebiet auch eine internationale Rechtsangleichung in Form der Budapester Konvention über Computerkriminalität (Seit 1.7.2004 in Kraft; von Österreich unterzeichnet, aber noch nicht ratifiziert[604]). Diese wurde von Österreich großteils bereits in nationales Recht umgesetzt, wodurch die Anzahl der expliziten Computerstraftatbestände stark angestiegen ist.

Für E-Business ist dieses Thema deshalb bedeutsam, da einerseits dadurch Betriebsgeheimnisse gesichert werden, andererseits aber besondere Anforderungen erfüllt werden müssen (z.B. "spezifische Sicherheitsvorkehrungen"). Auch ist zu beachten, dass eine entsprechende Überwachung bzw. Schulung der Mitarbeiter zu erfolgen hat, da sonst für Manager ev. eine Haftung als Beitragstäter, oder für die Firma im Rahmen des Verbandsverantwortlichkeitsgesetzes, in Frage kommen kann, sollten diese derartige Taten begehen.

IX.1. Einleitung

In diesem Abschnitt werden grundlegende Konzepte und Definitionen erläutert, die von Bedeutung sind. Weiters wird ein Sonderfall untersucht, der in Bezug auf die Datenverarbeitung im österreichischen Recht von besonderer Bedeutung ist: der Urkundenbegriff.

IX.1.1. Umfang der Betrachtungen

Hier werden hauptsächlich Delikte betrachtet, welche im österreichischen Strafgesetzbuch (StGB) festgelegt sind. Zusätzlich werden wegen der dauernden Aktualität noch Delikte aus dem Verbotsgesetz und dem Pornographiegesetz untersucht. Einzelne strafrechtliche Delikte aus anderen Gebieten in Sondergesetzen, z.B. Datenschutz, werden bei diesen diskutiert. Ausgeklammert bleibt jedoch der gesamte Bereich des Verwaltungsstrafrechts.

IX.1.2. Deliktsarten

Für die hier angestellten Betrachtungen ist von mehreren verschiedenen Möglichkeiten der Einteilung der Delikte bloß eine von besonderer Bedeutung: Je nachdem, wie bzw. von wem aus die Verfolgung durchgeführt wird.

[604] Siehe http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=4/25/2006&CL=ENG

Es existieren vier Gruppen[605]:

1. Offizialdelikte: Dies ist der normale Fall. Die Einleitung des Strafverfahrens erfolgt von Amts wegen durch die Staatsanwaltschaft. Einzige Voraussetzung dafür ist, dass Polizei oder Staatsanwaltschaft auf *irgendeine* Weise von einem (möglichen) Delikt erfahren. Der Verletzte (=Opfer) hat keinen Einfluss auf das Verfahren und kann es weder verhindern noch erzwingen. Beispiele: Körperverletzung, Sachbeschädigung.
2. Ermächtigungsdelikte: Diese Delikte werden vom Staatsanwalt verfolgt und die Einleitung des Verfahrens erfolgt von Amts wegen. Eine Hauptverhandlung und damit eine Verurteilung findet jedoch nur dann statt, wenn der Verletzte seine ausdrückliche Einwilligung erteilt. Diese Zustimmung muss sowohl Tat wie auch Beschuldigten explizit bezeichnen. Eine Anzeige der Tat bei der Polizei alleine reicht nicht aus. Der Staatsanwalt ist verpflichtet, Anklage zu erheben und muss diese Ermächtigung einholen. Beispiele: Delikte gegen die Ehre bei besonderen Personen (Bundespräsident, ...), Verletzung des Fernmeldegeheimnisses, missbräuchliches Abfangen von Daten.
3. Antragsdelikte: Antragsdelikte werden zwar von Staatsanwalt verfolgt, aber nur dann, wenn der Verletzte dies verlangt. D.h. ohne Aktivität des Opfers wird keine Untersuchung durchgeführt, selbst wenn Staatsanwaltschaft/Polizei von der Tat erfahren. Beispiele: Kindesentziehung sowie Privatanklagedelikte mit jugendlichen Beschuldigten.
4. Privatanklagedelikte: Diese Delikte sind vom Verletzten selbst zu verfolgen, er schlüpft in diesem Fall in die Rolle des Staatsanwalts. Er trägt daher auch das volle Prozessrisiko (Kostenersatz: Gerichtskosten, Verteidigerkosten etc.!). Beispiele: Delikte gegen die Ehre, Verletzung des Briefgeheimnisses.

IX.1.3. Daten als Beweise

Nachdem Daten nicht als eigenes Beweismittel erwähnt werden und die Klassifizierung von Beweismitteln in der Zivilprozessordnung als abschließend gilt[606], stellt sich die Frage, ob sie in einem Verfahren überhaupt vorgebracht werden können und wenn ja, wie.

In Bezug auf die Informatik kommen nur zwei Beweismittelkategorien in Frage: Augenschein (u.U. unter Beiziehung eines Sachverständigen; § 118 StPO[607]) und Erstellung eines Gutachtens durch einen Sachverständigen. Ein Augenschein ist in den meisten Fällen jedoch nicht zielführend, da durch das Betrachten eines Datenverarbeitungsvorgangs oder eines Programms durch einen Laien kaum relevante Schlussfolgerungen gezogen werden können. Allenfalls kommt die Beobachtung einer bestimmten Bedienung/Manipulation in Frage, welche so untersucht werden könnte. In den meisten Fällen wird daher die Einholung eines Gutachtens von einem Sachverständigen erforderlich sein, der den Ablauf des Programms, eventuelle Manipulationen daran oder die Wahrscheinlichkeit eines zufälligen Fehlers zu untersuchen und daraus seine Schlüsse zu ziehen hat. Auf diese Weise kann daher auch jedweder Vorgang in einer Computeranlage zu einem Beweis gemacht und in einem Verfahren verwertet werden.

---

[605] Bertel, Grundriß des österreichischen Strafprozeßrechts. 5. Auflage, Wien: Manz 1997 RS 35ff

[606] ZPO: Beschuldigtenvernehmung, Zeugen, Sachverständige, Urkunden und Augenschein. Der Abschluss ist freilich kein Problem: Ausnahmslos alles, was nicht in eine andere Kategorie passt, fällt unter Augenschein. Dies betrifft auch Dinge, die nicht mit den Augen, sondern mit anderen Sinnen untersucht werden.

[607] Strafprozeßordnung 1975 (StPO)

Nach dem Grundsatz der freien Beweiswürdigung (§ 258 Abs 2 StPO), haben Daten, selbst dann, wenn sie mit einer (elektronischen) Signatur versehen sind, keinen festen Beweiswert, insbesondere auch keinen höheren als irgendwelche anderen Beweismittel. Es bleibt dem Gericht überlassen, in freier Beweiswürdigung darüber zu befinden, welche Beweise ihm glaubwürdiger erscheinen und dies anschließend zu begründen. Dies bildet aber kein Hindernis für informelle Regeln, sodass z.B. Daten mit (technisch) sicherer Signatur in der Praxis wohl fast immer höher als unsignierte bewertet würden. Im Einzelfall kann jedoch auch anders entschieden werden. So wird etwa E-Mails generell eher geringer Beweiswert beigemessen, da deren Fälschung sehr einfach ist. Für einen höheren Wert müssen zusätzliche Elemente hinzukommen, wie z.B. Ausdruck mit vertrauenswürdigem Datumsvermerk, Empfang auch durch unbeteiligte Dritte, Mailserver-Log-Dateien etc.

IX.1.4. Qualifizierung von Daten, Urkundendelikte

Für die Informatik ist wichtig, welche rechtliche Qualifizierung die verarbeiteten Informationen besitzen:

- Was sind "Daten" im rechtlichen Sinn? Diese Frage wird sogleich unten behandelt, da eine explizite Definition existiert.
- Welche Kategorien von Daten gibt es? In Österreich sind grundsätzlich zwei Kategorien rechtlich existent: Allgemeine Daten und personenbezogene Daten, welche besonders geschützt sind; siehe zu letzteren den Abschnitt zum Datenschutzgesetz.
- Gibt es "bevorzugte" Daten, z.B. einen el. "amtlichen Lichtbildausweis"? Im österreichischen Strafrecht ist davon auszugehen, dass Daten keine Urkunden sein können, egal wie gut sie gegen Änderung gesichert sind, etwa durch Signaturen, Prüfcodes oder besondere Speicherung. Dafür spricht auch die explizite Einführung des Deliktes der "Datenfälschung" (§ 225a StGB), analog der "Urkundenfälschung" (§ 223 StGB).

Der letzte Punkt soll hier näher untersucht werden. Für den österreichischen Urkundenbegriff ist in § 74 Z 7 StGB festgelegt, dass eine Urkunde eine Schrift sein muss; die weiteren dort vorausgesetzten Merkmale sind in diesem Zusammenhang unerheblich. Im Strafprozess gilt dagegen alles als Urkunde, was vorgelesen werden kann. Schriftlichkeit setzt voraus, dass es sich um mit freiem Auge lesbare Schriftzeichen handelt, welche auf Dauer festgehalten sind und eine allgemein anerkannte Bedeutung besitzen.

All diese Voraussetzungen sind jedoch mit Vorsicht zu betrachten: So ist etwa auch ein Mikrofilm eine Urkunde, obwohl die Zeichen nur mit technischer Hilfe lesbar sind. Ebenso werden an die Dauer keine besonderen Anforderungen gestellt: Auch relativ kurzlebige Aufzeichnungen können eine Urkunde darstellen. Allgemein anerkannte Bedeutung besitzen auch Texte, die in einer völlig ungebräuchlichen Schrift und/oder Sprache abgefasst sind (z.B. Thailändisch), jedoch von einem Fachmann eindeutig "gelesen" werden können. Demgegenüber erzeugt eine private Geheimschrift keine Urkunde, da sie keine *allgemeine* Bedeutung besitzt, selbst wenn sie eventuell entschlüsselt werden kann.

Wenn Daten jedoch nur in el. Form vorliegen, können sie niemals das Erfordernis der Schriftlichkeit erfüllen. Sie sind zwar körperlich (= Elektronen/magnetisierte Partikel in einem räumlich begrenzten Bereich), doch nicht mit freiem Auge sichtbar. Das Festhalten auf einem Datenträger schafft auch keine Urkunde, da wiederum keine freie Lesbarkeit vorliegt. Ein Ausdruck jedoch unterscheidet sich nicht von einer "normalen" Urkunde und gilt daher problemlos als solche, sofern er den sonstigen Anforderungen genügt (Beispiel:

Ausdruck einer E-Mail). Es bestand und besteht von jeher keine rechtliche Differenzierung dadurch, wie eine Urkunde entstand: Handschrift, Buchdruck oder Ausdruck werden gleich behandelt.

Deshalb ist in Österreich die Verwirklichung eines Urkundendeliktes allein durch Datenmanipulation nicht möglich, sondern höchstens eine Unterstützung: z.B. sind Formulare per Laserdrucker einfacher zu fälschen als durch konventionellen Druck. Als „Ersatz“ dient das Delikt der Datenfälschung, welches der Urkundenfälschung nachgebildet ist.

Achtung: In manchen Fällen sind auch el. Daten direkt rechtserheblich[608], z.B. bei der automationsunterstützten Zustellung von Bescheiden[609]. Dies betrifft jedoch das Verwaltungsrecht und wird hier nicht behandelt.

IX.1.5. Definitionen "Computersystem" und "Daten"

Unter einem Computersystem werden (§ 74 Abs 1 Z 8 StGB; nur für das Strafrecht gültig!) sowohl einzelne als auch verbundene Vorrichtungen verstanden, welche der automationsunterstützten Datenverarbeitung dienen. Dies ist sehr weit zu verstehen, sodass auch Netzwerkskomponenten darunter fallen[610]. Wie die Abgrenzung genau erfolgen wird, ist derzeit noch nicht absehbar. Ein möglicher Ansatz liegt darin, dass es sich um Teile handelt, die tatsächlich Daten verarbeiten, diese transportieren oder unerlässliches Zubehör dazu sind. Praktisch könnte dies durch eine räumliche Trennung unterschieden werden: "Fest" verbundene Teile gehören dazu, sonstige Elemente, die nur der Unterstützung dienen, wie etwa Klimaanlage oder Stromversorgung aber nicht.

Unter Daten (§ 74 Abs 2 StGB) sind sowohl personenbezogene als auch nicht personenbezogene Daten sowie Programme zu verstehen. Die Definition ist jedoch nicht sehr glücklich formuliert oder hilfreich, da zirkulär. Es sind wohl alle Elemente umfasst, die ohne weitere Umwandlung direkt in einem Computersystem verarbeitet werden können.

IX.2. Örtliche Geltung des österreichischen Strafrechts

Im Internet stellt sich die Frage, wo eine Tat begangen wurde. Dies ist deshalb wichtig, da, mit einigen Ausnahmen, in Österreich nur Taten strafbar sind, welche im Inland (=österreichisches Staatsgebiet) begangen wurden (§ 62 StGB). Eine Einteilung kann nach der Art des Delikts erfolgen[611], wobei leider die Zuordnung manchmal streitig ist[612]:

- Schlichte Tätigkeitsdelikte: Hier wird lediglich auf die Vornahme einer Handlung abgestellt, ohne dass ein bestimmter Erfolg eintreten muss. Es kommt hier für die Strafbarkeit auf den Ort an, an dem die Handlung durchgeführt wurde. Beispiel: Falsche Be-

---

[608] Siehe dazu insbesondere das Signaturgesetz!

[609] § 1 Abs 2 Zustellgesetz: "... Erledigungen auch ..... im Wege automationsunterstützer Datenübertragung oder in jeder anderen technisch möglichen Weise übermittelt werden können, gelten solche Übermittlungen als Zustellung." Aus *gelten* lässt sich ableiten, dass dadurch lediglich eine rechtliche Fiktion geschaffen wird. Besondere Regelungen finden sich in § 17a ZustellG (El. Bereithaltung) sowie § 26a ZustellG. Siehe ebenso das Verwaltungsverfahrensgesetz (VVG).

[610] Auch per WLAN verbundene Geräte gehören daher wohl zu einem Computersystem.

[611] Anders in der StPO bezüglich der Abwicklung des Verfahrens: Gerichtsstand ist im Gegensatz zum materiellen Recht der Tatort (=Ort der Handlung). Aber manchmal auch bzw. oder, wo der Erfolg eingetreten ist (z.B. Üble Nachrede § 111!). Hier stellen sich Probleme bei Auslandstaten.

[612] Vergleiche dazu Kienapfel, AT· RZ 14

weisaussage vor Gericht. Durch die Aussage wird das Delikt vollendet. Ob die Falschheit entdeckt wird oder nicht, oder ob sie einen Einfluss auf das Urteil hat ist unerheblich. Derartige Delikte sind selten.

- Erfolgsdelikte: Hier ist eine Handlung nur strafbar, wenn ein genau bestimmter Erfolg eintritt. Maßgebender Ort für die Strafbarkeit ist, wo der Täter gehandelt hat, hätte handeln sollen bzw. wo der Erfolg eintrat (§ 67 Abs 2 StGB). Für Delikte mit Auslandsbezug bedeutet dies, dass Handlungen im Ausland mit Erfolg in Österreich sowohl im Ausland, nach den dortigen Gesetzen aufgrund der Handlung, als auch in Österreich wegen des Erfolgseintritts strafbar sein können. Die meisten Delikte fallen hierunter.

Gemäß § 64 StGB sind auch bestimmte bezeichnete Auslandstaten strafbar, egal ob sie von Österreichern begangen wurden oder nicht. Diese Straftaten sind daher grundsätzlich strafbar, egal über welche Distanz sie begangen werden. Beispielsweise wird das Delikt des § 124 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands; siehe dazu den ähnlichen § 123 unter Punkt IX.4.4) immer dann begangen, wenn es sich um ein österreichisches Geheimnis handelt, egal von wo aus und durch wen der Angriff erfolgt. Dass sich hier natürlich oft das Problem der Durchsetzung stellt (Nachforschungen, Auslieferung), hat auf die grundsätzliche Strafbarkeit keinen Einfluss. Wichtig ist noch § 64 Z 8 HS 1 StGB, wonach eine Beteiligung an einer Inlandstat vom Ausland aus ebenfalls strafbar ist[613].

IX.3. Computerstraftaten im engeren Sinn

In Österreich existierten früher nur zwei eigentliche Computerstraftaten. Beide wurden mit der Novelle 1987 in das StGB eingefügt (BGBl 1987/605). Durch das Strafrechtsänderungsgesetz 2002 wurden weitere sechs Delikte, großteils zur Umsetzung der Cybercrime-Konvention, eingeführt. Die Delikte sind Technik-indifferent abgefasst (siehe Definition "Computersystem"). Es wird auch keine bestimmte Vorgangsweise benötigt, sondern nur allgemein von der Verarbeitung von Daten gesprochen.

IX.3.1. Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)

1. *Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.*
2. *Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.*

Mit diesem Delikt besteht bereits eine Strafbarkeit noch bevor ein tatsächlicher Schaden eintritt. Die Überschrift ist jedoch irreführend, da nicht der eigentliche „Zugriff", sondern bereits das Verschaffen eines Zugangs strafbar ist.

[613] Bestimmung (=Anstiftung) einer im Inland begangenen Tag vom Ausland aus, z.B. über E-Mail oder Chat.

Verboten ist, sich Zugang zu einem Computersystem zu verschaffen, sofern ein komplexer erweiterter Vorsatz in Absichtsform vorliegt. Dieser umfasst die Verschaffung der Kenntnis von Daten aus dem System für einen hierzu nicht Berechtigten, die Benützung, Zugänglichmachung oder Veröffentlichung dieser Daten, und einen sich hieraus ergebenden Vermögensvorteil bzw. eine daraus folgende Schädigung[614]. Keine Strafbarkeit liegt vor, wenn Alleinverfügungsberechtigung über das System besteht[615]. Der wichtigste Teil des Deliktes ist jedoch, dass dieser Zugriff unter Verletzung spezifischer Sicherheitsvorkehrungen im Computersystem erfolgt.

Bei diesem Delikt stellen sich jedoch manche Fragen. Es ist explizit strafbar, sich zu einem Computersystem (CS) als auch einem Teil eines CS Zugriff zu verschaffen. Diese Wendung besitzt bei wörtlicher Auslegung nur dann eine Bedeutung, wenn Teile von CS existieren, die selbst keine CS sind, diese Teile aber dennoch von Sicherheitsvorkehrungen im übergeordneten System geschützt werden, und bei denen ein Zugriff darauf zur Datenpreisgabe führen könnte[616]. Im Gegensatz dazu ist in der Konvention die Rede von Zugriff auf "the whole or any part" eines CS, was Zugriff auf "das *gesamte* oder irgendeinen Teil" des CS bedeutet und beides notwendig ist. Da bei wörtlicher Auslegung wohl kein Anwendungsgebiet für den zweiten Teil im StGB verbleibt, muss diese im Sinne der Konvention erfolgen: Das erste "Computersystem" ist als Gesamtsystem zu verstehen.

Nach den Erläuterungen zur Richtlinie soll das bloße Senden einer E-Mail oder einer Datei an ein System diesen Tatbestand nicht verwirklichen. Doch schon daraus lassen sich viele Informationen gewinnen[617]. Auch ist die Unterscheidung zwischen dem Senden von Benutzername und Passwort und Warten auf Erfolgs- oder Fehlermeldung unmöglich. In jedem Fall werden Daten aus dem System, z.B. die Existenz dieses Benutzers mit diesem Passwort oder dieser E-Mail-Adresse, bekannt. Hierbei liegt zwar ein "Zugriff" (Überschrift) auf das System vor und es werden Daten erhoben, es wird aber kein Zugang zum CS erreicht. „Zugang verschaffen“ ist also wohl so zu verstehen, dass gewisse Informationen entnommen werden sowie, wenn auch nur sehr eingeschränkt, Aktionen innerhalb des Systems ausgelöst werden können. Vollständige Kontrolle über den Computer (Administrator-Rechte) ist nicht erforderlich, aber die bloße Informationsabfrage ohne Möglichkeit zu Veränderungen im System reicht nicht.

Die wichtigste Frage ist jedoch, was unter einer "Verletzung spezifischer Sicherheitsvorkehrungen im CS" zu verstehen ist. Im Entwurf[618] war noch von "überwinden" die Rede, was kritisiert wurde, da es keine Umgehung beinhaltet. Worauf die Änderung konkret zurückzuführen ist, kann nicht genau festgestellt werden, doch deuten diese Umstände aufgrund der erfolgten Stellungnahmen darauf hin, dass auch letzteres einbezogen werden soll. Dennoch bleibt die exakte Abgrenzung schwer: Ein Programmierfehler, der in einem

---

[614] Welche nicht notwendigerweise beim Besitzer des Computersystems eintreten muss, sondern auch Dritte, z.B. Kunden, betreffen kann.

[615] Der Besitzer des Systems kann daher dieses Delikt nie begehen, selbst wenn fremde Daten gespeichert werden (z.B. Webhosting-Provider). Es bleiben die normalen Inhaltsdelikte (Datenbeschädigung, Datenschutzverletzungen etc.) übrig.

[616] So ist etwa die Kühlung (Hardware selbst; eine Steuerung, sofern nicht rein analog, ist meist ein CS!) wohl Teil des CS, aber selbst keines. Allerdings ist nur schwer ein Zugriff darauf denkbar, der Sicherheitsvorkehrungen *im CS* verletzt.

[617] Offene Ports, verwendetes Betriebssystem, installierte Mailer-Software inklusive Versionsnummer, Computername, Existenz der Mailadresse, Liste von möglichen Mailadressen etc. Diese Informationen sind im System gespeichert und für sich alleine wertvoll bzw. schädlich wenn sie bekannt werden.

[618] Erläuternde Bemerkungen zum Ministerialentwurf des Strafrechtsänderungsgesetz 2002: http://www.parlinkom.gv.at/portal/page?_pageid=908,309721&_dad=portal&_schema=PORTAL

ganz speziellen Fall Zugriff ohne Passwort erlaubt, ist damit zwar vor einer Ausnützung geschützt, doch was ist mit einem standardmäßig aktivierten Account ohne Passwort? So besteht zwar eine allgemeine Passwortprüfung, welche damit umgangen wird, doch wird hier genau der vorgesehene Zweck realisiert, einen Zugang für Benutzer ohne eigenen Account zu ermöglichen.

Spezifische Sicherheitsvorkehrungen sind solche, die zumindest auch einen Zugriff durch unbefugte Personen verhindern sollen. D.h. Vorkehrungen, die der Erhaltung der Daten, z.B. Markierung als read-only; Verriegelungen gegen selbsttätiges Lösen von Wechselfestplatten oder der Verhinderung, Erkennung oder Nachverfolgung der Weitergabe/Verletzungen wie beispielsweise Wasserzeichen oder Logs, dienen, fallen heraus. Zusammengefasst handelt es sich um das Erreichen von normalerweise nicht zustehenden Rechten. Welche Rechte jemandem normalerweise zustehen ist danach zu beurteilen, wie dies ein maßstabsgerechter Dritter beurteilen würde[619]. Im Beispiel des bloßen Sendens von E-Mails wäre dies eine Überprüfung, ob der Absender berechtigt ist, diesen Rechner als Relay zu benützen. Dies erfolgt üblicherweise über Passwörter oder Zertifikate. Eine Umgehung dieser Prüfung ist dann als Verletzung einer spezifischen Sicherheitsvorkehrung zu beurteilen[620]. Hacken für bloßes Relaying ist dadurch aber nicht strafbar, da keine Absicht vorliegt, an Daten des Systems heranzukommen.

Weiters muss es sich um Sicherheitsvorkehrungen im CS handeln. Aufgrund der nicht sehr ausführlichen Definition ist dies auch nicht immer klar. Laut den Erläuterungen soll etwa das Versperren des Raumes mit dem CS nicht darunter fallen. Im Gegensatz dazu wird jedoch beispielsweise bei el. Zugangskontrolle, welche selbst ein CS ist, dies u.U. doch erfüllt sein: Ist diese Kontrolle Teil des Systems, in welches dann eingebrochen wird, so ist das Tatbild erfüllt. Handelt es sich jedoch um ein eigenständiges System, so wäre dies straffrei! Die Strafbarkeit hängt daher lediglich von der Existenz einer (Daten-)Verbindung zwischen der Zugangskontrolle und dem CS ab, wobei ein bloßer Anschluss an dasselbe Netzwerk ohne echte Kommunikation aber wohl noch nicht genügt.

Besonders im letzteren Fall ist zu untersuchen, was den "Zugang" zum System darstellt. Hier wird auf die tatsächliche und unmittelbare, d.h. ohne Überwindung weiterer Sicherheitsvorkehrungen, Möglichkeit der Vornahme von Aktionen zum Informationsabruf abzustellen sein. Erst die Überwindung oder Umgehung der letzten Schranke vollendet das Delikt, vorhergehende Teile sind nur als Versuch zu werten. Ein tatsächlicher Datenabruf ist jedoch nicht mehr nötig[621].

Zum Abschluss werden einige mögliche Angriffe hinsichtlich dieses Delikts untersucht:

- Installieren von Backdoors per E-Mail: Das Absenden ist der Versuch und die erfolgte Installation die Deliktsvollendung. Die Hintertür ermöglicht sofortigen ungehinderten Zugriff, wobei die Sicherheitsvorkehrung der Passwortanfrage umgangen wird. Doch schon bei der Installation werden Sicherheitsvorkehrungen verletzt, indem Anti-Virenprogramme umgangen bzw. unerlaubt Attachments automatisch ausgeführt werden.

---

[619] Gast-Account ohne Passwort ist damit wohl keine spezifische Sicherheitsvorkehrung.

[620] Fehlen solche Sicherungsmaßnahmen, ist das Senden einer E-Mail an ein CS tatsächlich nicht erfasst.

[621] Dies ist besonders in Beweishinsicht günstig: Sind die Berechtigungen erst erlangt, können die Spuren sehr gut verwischt werden. Die bloße Tatsache des Eindringens ist aber oft noch nachvollziehbar.

- Das Hacken von Passwörtern ist der klassische Fall dieses Delikts. Der Schutz gegen unerlaubten Zugriff wird ausgehebelt, indem solange Passwörter ausprobiert werden, bis ein gültiges gefunden wird. Doch auch die Verwendung gestohlener oder herausgelockter ("social engineering") Passwörter oder die Ausnutzung von Programmfehlern bei der Prüfung fällt darunter.
- Auslesen von Cookies: Nach den Erläuterungen zur Konvention ist das Auslesen von Cookies erlaubt, da der Besitzer des CS dies nicht verhindert hat. Die Unterlassung der Verhinderung kann aber niemals als Zustimmung gewertet werden. Dies ändert nichts am Ergebnis: Die Installation des Programms (=Webbrowser) mit der als bekannt anzunehmenden Möglichkeit des Auslesens von Cookies ist eine konkludente Zustimmung. Weiters werden keine Sicherheitsvorkehrungen verletzt, da dies ja laut der technischen Standards genau der geplante und korrekte Vorgang ist.
- Datenweitergabe durch Mitarbeiter mit Zugriffsrechten: Hier werden keine Sicherheitsvorkehrungen verletzt und der Zugriff erfolgt durch einen hierzu Befugten. Daher sind solche Indiskretionen nach diesem Delikt[622] nicht strafbar. Handelt es sich um personenbezogene Daten, kommt insbesondere § 51 Datenschutzgesetz in Frage. Weiters kann es sich um § 148a StGB, betrügerischer Datenverarbeitungsmissbrauch, handeln.
- "Gutartiges" Hacken eines Systems und Veröffentlichung der Schwachstelle: Wird in ein CS eingebrochen, lediglich um zu zeigen, dass dies möglich ist, also nicht im Rahmen eines Auftrags zur Sicherheitsprüfung, so wird hierdurch dennoch Kenntnis von Daten aus dem CS (=Art und Existenz des "Lochs"; auch Programme sind Daten!) erlangt. Durch die Veröffentlichung liegt in der Regel zumindest dolus eventualis für eine Schädigungsabsicht vor. Da aber volle Absicht Voraussetzung für die Begehung des Delikts ist, wird es nicht erfüllt. Eine solche Art der Suche nach Sicherheitslücken, welche durchaus öfter vorkommt, ist daher nach diesem Paragraphen weiter zulässig.

IX.3.2. Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)

1. *Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation (§ 3 Z 13 TKG) oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.*
2. *Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.*

Bei diesem Delikt handelt es sich um eine analoge Bestimmung zum Briefgeheimnis. Die tatsächliche Verwendung einer Abhöranlage wird unter Strafe gestellt, wobei sowohl Computersysteme als auch Telekommunikationsanlagen[623] betroffen sind. Siehe dazu auch das Verbot in § 93 Abs 3 Telekommunikationsgesetz. Im Gegensatz zu früher ist jetzt jedoch das Anbringen selbst nicht mehr strafbar und auch für einen Versuch zu weit von der Tatbegehung entfernt. Erst die tatsächliche Benützung ist strafbar. Unter Nachricht sind Telefongespräche, Briefe, E-Mails und Ähnliches, also Kommunikation durch Gedankeninhalte von Mensch zu Mensch zu verstehen.

---

[622] Siehe hierfür das Verbot in § 51 Datenschutzgesetz!

[623] Die Erwähnung ist nur insoweit notwendig, als es sich um alte Anlagen handelt, welche noch nicht als Computersysteme ausgeführt sind.

Für die Praxis bedeutet dies, dass das Verwenden eines Netzwerk-Sniffers verboten ist, sofern sich auch andere Benutzer im Netzwerk befinden. Dies ist nur dann erlaubt, wenn vorher die Erlaubnis *aller* Teilnehmer eingeholt wurde (= nun "befugt"), was insbesondere auch alle Personen betrifft, die von außen her Kommunikationsverbindungen starten[624].

Ein nahe verwandtes Delikt hierzu ist § 120 Abs 2a StGB, bei dem es um die Aufzeichnung, Zugänglichmachung oder Veröffentlichung von Nachrichten geht. Dort sind jedoch nur Telekommunikationsanlagen betroffen. Im Gegensatz zu dem hier untersuchten Delikt ist bereits das normale Mithören ohne besondere Vorrichtungen strafbar, wenn auch mit geringerem Strafmaß bedroht.

Eine Vorrichtung ist nicht notwendigerweise ein physisches Gerät. Auch ein installiertes Programm auf einem Computer kann diese Voraussetzung erfüllen. Es muss sich lediglich um ein technisches Hilfsmittel handeln.

IX.3.3. Missbräuchliches Abfangen von Daten (§ 119a StGB)

1. *Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.*
2. *Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.*

Dieses Delikt besitzt große Ähnlichkeiten zu § 119 StGB. Der wichtigste Unterschied zu diesem besteht darin, dass hier auf „Daten“ und nicht auf „Nachrichten“ abgestellt wird. Daher ist auch das Abhören des Transfers eines Programms hierunter zu subsumieren. Im Gegensatz zu oben ist zusätzlich ein erweiterter Vorsatz nötig: Schädigung oder Bereicherung durch Benutzung oder Veröffentlichung durch einen Unbefugten. Die besondere Erwähnung der elektromagnetischen Abstrahlung dürfte keine besondere Bedeutung besitzen, da dies auch eine "sonstige empfangsbereite Vorrichtung" ist.

IX.3.4. Datenbeschädigung (§ 126a StGB)

1. *Wer einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht, oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.*
2. *Wer durch die Tat an den Daten einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer einen 50 000 Euro übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.*

[624] Befindet sich ein Webserver auf dem abgehörten Segment, so ist dies in der Praxis unmöglich. Es müsste daher der Zugang von außen (bzw. auch alle internen Benutzer) vorher getrennt werden, was vielfach wohl den Zweck vereitelt.

Da im österreichischen Recht eine "Sache" als "körperlicher Gegenstand" verstanden wird, ist der § 125 StGB (Sachbeschädigung) nicht auf Daten anwendbar. Aus diesem Grund wurde ein ähnliches Delikt geschaffen, welches dem Schutz des Berechtigten an der Existenz und der Verfügbarkeit der Daten dient. Zu beachten ist, dass der Schutz der Datenträger selbst weiterhin durch die § 125ff StGB erfolgt. Diese sind aber als solche meist praktisch wertlos, z.B. ein CD-Rohling, eine Diskette oder eine Festplatte, insbesondere im Vergleich zu den darauf enthaltenen Daten.

Es handelt sich hier um ein reines Vorsatzdelikt, sodass Fahrlässigkeit, egal welcher Ausprägung, nicht zur Strafbarkeit führt.

Zu den einzelnen Elementen:

- Daten: Was Daten sind, ist im Gesetz nur ungenau definiert; siehe oben. Es wird jedoch ausdrücklich darauf hingewiesen, dass sowohl personenbezogene[625] wie auch personenunabhängige Daten erfasst sind. Weiters sind auch die Programme selbst Daten und nicht nur die Objekte (=Ein-/Ausgabedaten) des Programmablaufs. Daten im Sinne des Strafgesetzbuches können daher auch als analoge oder digitale physische Einheiten definiert werden, die einen bestimmten Wert über eine bestimmte Zeitspanne annehmen. Geschützt werden nur automationsunterstützt verarbeitete, übermittelte oder überlassene, d.h. an jemand anderen zur Verarbeitung weitergegebene, Daten.
- Verändern, löschen, unbrauchbarmachen oder unterdrücken: Allen diesen Begehungsarten ist gemeinsam, dass der Berechtigte keinen Zugriff auf den (richtigen) Dateninhalt mehr hat. Voraussetzung ist beim Löschen, dass der Dateninhalt unwiederbringlich verloren gegangen ist. Daher liegt kein Löschen vor, solange noch Backups existieren. Dann ist jedoch an Unbrauchbarmachen und ev. Unterdrücken zu denken, je nach der für die Wiederherstellung benötigten Dauer. Existieren mehrere Exemplare, z.B. zum Verkauf bestimmte CDs, so bewirkt schon das Zerstören einer CD die Löschung. Dies steht im Gegensatz zu Backups: Ein Backup ist kein zweites Exemplar, sondern eine zusätzliche Inkarnation der Originaldaten und daher diesen zuzurechnen. Sicherungskopien stellen keinen eigenständigen Wert dar, anders als Verkaufsgegenstände. Beim Unbrauchbarmachen ist darauf zu achten, dass nur die Verhinderung des Zugriffs auf die Daten selbst unter § 126a fällt, nicht jedoch eine Zerstörung der Computer-Hardware (⇒ § 125ff StGB). Es kommt also hauptsächlich Verschlüsselung in Betracht: Die Daten müssen wiederherstellbar sein, sonst würde dies unter "Löschen" fallen. Das Unterdrücken beschränkt sich darauf, die Daten der Verwendung des Berechtigten zu entziehen, z.B. durch Entfernen des Datenträgers oder Sperren des Zugriffs darauf, beispielsweise durch die Änderung des Zugangspasswortes[626].
- Alleinverfügungsberechtigung: Wenn auch nur eine einzige andere Person über die Daten mitverfügungsberechtigt ist, kann das Delikt begangen werden. Die Verfügungsbe-

---

[625] Im Datenschutzgesetz (alte Fassung) wurden Daten (unter Außerachtlassung der dort geforderten Personenbezogenheit) als "auf einem Datenträger festgehaltene Angaben" definiert (§ 3 Z 1 DSG aF). Dies entspricht nicht ganz der obigen Definition in Bezug auf das Strafgesetzbuch, da das Festhalten zwar einer Zeitspanne entspricht, aber unter einem Datenträger nur eine dauerhaftere Speicherung zu verstehen ist. Dies entspringt der Intention des Gesetzes, den "gläsernen Menschen" durch Ansammlung einer großen Datenmenge zu verhindern. Rein temporäre Daten sind in dieser Hinsicht ungefährlich und wären daher dort früher nicht betroffen gewesen, hier im StGB bzw. dem neuen DSG schon.

[626] Im physischen Bereich können folgende Analogien zur Verdeutlichung dienen: Das Anzünden eines Autos entspricht der Löschung von Daten: Es ist endgültig und unwiederbringlich vernichtet. Wird es für eine Spritztour „ausgeborgt“, so handelt es sich um Unterdrückung: Das Auto ist weiterhin existent, unverändert und später wieder unter der Kontrolle des Eigentümers, aber im Augenblick nicht verfügbar. Wird hingegen die Luft aus den Reifen gelassen, so wurde es unbrauchbar gemacht: Es ist vorhanden und unter der Kontrolle des Besitzer, kann aber nicht sofort verwendet werden.

rechtigung entsteht aus der Erstellung, der Eingabe oder dem Erwerb der Daten (Träger der Herstellungskosten) und nicht aus der Verfügungsberechtigung über den Datenträger oder der Betroffenheit[627] von den Daten.

- Schaden: Durch die Löschung etc. der Daten muss ein tatsächlicher Schaden entstanden sein. Da es sich um ein Vermögensdelikt handelt, ist der Schaden als Vermögensschaden zu berechnen. Dieser ist definiert als die Verminderung der Summe wirtschaftlicher Werte: Die Differenz zwischen dem Gesamtvermögen vor- und nachher. Die bloße Gefährdung von Vermögen ist nicht einzurechnen. Typischerweise handelt es sich hier um die Kosten der Wiederbeschaffung der Daten. Diese müssen über einer Erheblichkeitsschwelle liegen, um das Delikt zu verwirklichen. Wenn daher statt der vernichteten Daten einfach eine Sicherungskopie verwendet werden kann, liegt kein Schaden vor[628]. Heutzutage ist jedoch wahrscheinlich auch das Einspielen von Backups als Schaden zu qualifizieren: Es kann mehrere Stunden dauern (=Arbeitskosten). Die verlorene Zeit (=Geschäftsentgang) zählt jedoch nicht (siehe unten). Können die Daten z.B. von einer darauf spezialisierten Firma von einem zerstörten Datenträger wiederhergestellt werden, so liegt keine Löschung vor, sondern allenfalls eine Unterdrückung, deren Dauer von wirtschaftlicher Bedeutung sein muss, was hier praktisch immer gegeben ist. Folgeschäden aus der Zerstörung der Daten sind jedoch *nicht* inbegriffen, analog zur Sachbeschädigung[629]. Dies ist dort ein kleines Problem, hier ein größeres[630]! Wichtig ist, dass bei Schadenersatzprozessen diese Einschränkung der Schadensberechnung *nicht* gilt.

Praktische Beispiele für dieses Delikt:

- Unterbrechung der Kommunikationsverbindung (denial-of-service attack; DOS): Wenn dadurch die Daten auf einem entfernten Rechner für längere Zeit nicht zugänglich sind (Störung der Kommunikation mit Filialen), so ist an Datenunterdrückung zu denken.
- Verfälschung einer Kommunikation: Hier liegt eine klassische Veränderung vor. Dies ist besonders interessant während der Übertragung von wertvollen Daten, z.B. einer Kontotransaktion oder wichtigen Plänen.
- Einbruch in einen Server und Ersetzen/Verändern von Webseiten: Diese immer wieder vorkommenden und Aufsehen erregenden Tätigkeiten setzen zwangsläufig eine Veränderung von zumindest einigen Daten voraus. Zweifelhaft kann höchstens der Schaden sein, da dieser ja im Wert der Daten selbst bestehen muss. Ein Imageschaden, sofern bezifferbar, ist kein ersetzbarer Folgeschaden.
- Löschen von Daten, Ändern von Passwörtern, Einbau von Viren: Dies sind üblicherweise Taten ehemaliger oder im Kündigungsstadium befindlicher Mitarbeiter.
- Viren/Würmer: Diese werden absichtlich erstellt und freigesetzt. Wenn sie Zerstörungen anrichten ist das Delikt erfüllt. Doch auch ein Systemstillstand wegen Überlastung oder zur Entfernung ohne tatsächlicher Datenveränderung[631] fällt hierunter: Unterdrückung. Dass der Autor in der Praxis nicht weiß, wessen Daten er schädigt, ist unerheblich.

---

[627] Wessen Daten es sind, wenn es sich um personenbezogene Daten handelt.

[628] Seiler, Kritische Anmerkungen zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JBl 1989, 746

[629] Siehe Zagler, Strafrecht. Besonderer Teil. Wien: LAST&CO Verlag 2000 http://www.rechtsverlag.at/Verlagsprogramm/Bucher/Strafrecht/strafrbt.pdf, 128

[630] Imageschäden und entgangener Gewinn sind wohl solche nicht zu ersetzende Folgeschäden; Schmölzer, Das neue Computer-Strafrecht (Strafrechtsänderungsgesetz 1987). EDVuR 1988 H 1, 20

[631] Z.B. Verzeichniseinträge werden zwar auch dann verändert, doch dies ist kein (relevanter/bezifferbarer) Schaden.

- Mail-Flut: In Verbindung mit Spam kann es manchmal zu "Vergeltungsaktionen" kommen: Dem Absender werden riesige Dateien, bis zu mehreren hundert Megabyte, per E-Mail zugeschickt. Durch diese Vorgehensweise kann es zu einer Überlastung des Mailservers des Empfängers kommen, wodurch dieser entweder abstürzt oder andere E-Mails löscht. Auf diese Weise kann leicht ein Vermögensschaden entstehen und daher dieses Delikt verwirklicht werden. Beim Vorsatz ist hier in zwei Fälle zu unterscheiden: Werden absichtlich große Dateien verschickt, so liegt Vorsatz vor. Senden jedoch eine große Anzahl von Personen kurze Protest-Mails, so kann dies zwar zum selben Erfolg führen, es fehlt dann jedoch der Vorsatz.

IX.3.5. Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)

Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Hier wird die schwere Störung der Funktionsfähigkeit eines Computersystems unter Strafe gestellt, wobei als Tatbegehungsweise nur Eingabe[632] und Übermitteln von Nachrichten in Frage kommen. Besitzt der "Täter" Alleinverfügungsberechtigung[633] über das System, so kann das Delikt nicht begangen werden. Die Störung selbst ist bereits strafbar, nicht erst Folgen daraus, wie Schädigungen. Es handelt sich aber dennoch um ein Erfolgsdelikt.

Dieses Delikt ist explizit subsidiär zu § 126a StGB (Datenbeschädigung). Nun sind jedoch nur wenige Fälle denkbar, bei denen die Funktionsfähigkeit des Systems gestört wird, ohne dass technisch eine Datenveränderung vorliegt. Auch wenn nur Daten eingegeben oder übermittelt werden, müssen irgendwelche (Verwaltungs-) Daten (Verzeichniseinträge, Prozesstabellen etc.) zumindest geringfügig verändert werden, da ansonsten keine Änderung des Systemverhaltens vorkommen kann. Die Abgrenzung erfolgt danach, ob die Schädigung im Wert der Daten selbst besteht, also z.B. eine Kundendatenbank (→ Datenbeschädigung), oder bloß eine Folge der Änderung von Daten ohne eigenen Wert ist, beispielsweise betriebssysteminterne Tabellen (→ Funktionsstörung)[634]. Im Gegensatz zu § 126a StGB kann hier nicht von dem Erfordernis einer Unmittelbarkeit der Störung durch die Tathandlungen ausgegangen werden, da weder Übermittlung noch Eingabe selbst jemals[635] eine Störung der Funktion zur Folge haben können. Erst die Ausführung derart "eingeschleuster" Programme oder die Bearbeitung der Daten führt technisch zu einer Störung.

Das Delikt besitzt in speziellen Fällen zusätzliche Bedeutung, etwa wenn keine Schädigungsabsicht vorliegt. Der Beweis für zumindest den Eventualvorsatz für eine (wenn auch schwere) Störung der Funktionsfähigkeit wird vielfach leichter zu erbringen sein, als der für eine Schädigung. Ein weiterer Anwendungsfall ist, wenn der Störer zwar Alleinver-

---

[632] Im Sinne des Hinzufügens neuer Daten und nicht technisch als Bearbeitungsvorgang.

[633] Dies muss nicht unbedingt für den Eigentümer gelten: Sind Teile vermietet (z.B. Rechenzeit-Anteile), so gibt es niemanden mehr mit Alleinverfügungsberechtigung!

[634] Bei Datenbeschädigung muss der Schaden unmittelbar (Triffterer, Kommentar § 126a RZ 84ff) an den Daten entstehen, besteht d.h. in deren Tausch- oder Wiederbeschaffungswert (Kienapfel, Grundriß § 126a RZ 22), welche beide bei reinen Verwaltungsdaten praktisch fehlen. Dort treten nur, eben durch § 126a nicht erfasste, Folgeschäden auf!

[635] Die Übermittlung kann zu einer Belegung der Bandbreite führen, welche aber kein Teil des Computersystems ist: die Leitung selbst verarbeitet keine Daten, sondern transportiert sie nur. Denkbar wäre höchstens das vollständige Belegen von Festplattenkapazität durch Dateneingabe, welche zu einem Absturz führt.

fügungsberechtigung über die *Daten* besitzt, aber diese so konstruiert, dass sich daraus eine Funktionsstörung des Systems ergibt, über welches er *nicht* alleine verfügen darf. Eine solche wäre beispielsweise die Konfiguration einer automatischen E-Mail-Weiterleitung an sich selbst ohne Limitierung: Eine Rekursion, welche zum Systemabsturz bzw. zur Verhinderung weiterer E-Mail-Zustellungen für andere Nutzer des Systems führen kann.

Unter einer "schweren" Störung sind gravierende Einschränkungen der Funktionalität zu verstehen. D.h. was nur geringfügige Verzögerungen, langsamere Verbindungen, Unbequemlichkeiten oder höheren Stromverbrauch/Belastung bedeutet, fällt nicht unter dieses Delikt. Als Grenze kann die Ablehnung oder Unzumutbarkeit der Ausführungsdauer von Aufträgen bzw. Programmen gesehen werden, die ohne die Störung noch durchgeführt werden könnten[636]. Es muss also ein "außergewöhnlicher Systemzustand" geschaffen werden, der ansonsten nicht eingetreten wäre.

In den Gesetzeserläuterungen werden Viren, Trojaner und Spam als Zielgruppe angeführt, was jedoch kaum zutrifft. Bei Viren und Trojanern löst erst die Aktion, z.B. Ausführen des Attachments, eines Dritten, der meist der Benutzers selbst ist (welcher normalerweise über das System verfügungsberechtigt ist), die eigentliche Störung bzw. Schädigung aus. Im Hinblick auf die Schadfunktion ist dies für den Risikozusammenhang von Bedeutung, da diese Ausführung ev. ein grob fahrlässiges Verhalten des Verletzten darstellen wird. Dies kann jedoch nur für klare Fälle wie unbekannte Dateianhänge fremder Absender gelten: Bei Trojanern besteht keine Kenntnis von der (Existenz der) Funktion und daher auch keine Verantwortung des Benutzers. Die Schadfunktion wird in der Praxis oft eine Datenbeschädigung sein. Würmer sind ähnlich zu Trojanern, doch ist hier überhaupt keine Aktion des Systembesitzers nötig. Höchstens eine Unterlassung käme in Frage, welche jedoch mangels Handlungsverpflichtung wegfällt. Würmer selbst stören auch normalerweise keine Rechnerfunktion[637]. Wird ein System durch eine ungebremste Vervielfältigung von Viren oder Würmern gestört, so ist das Tatbild erfüllt, da dies immer noch auf den ursprünglichen Sender zurückzuführen ist und es sich nicht um unabhängige und einzeln ja straflose Taten von verschiedenen Personen handelt.

Eine besondere Art von "Schadfunktion" ist das Auslesen und Versenden von Daten[638] durch Spyware, was jedoch wieder keine Funktionsstörung darstellt. Auch wird hier zwar ev. ein Schädigungs-, aber sicher kein Störungsvorsatz vorliegen. Siehe hierzu auch den Datenschutz. Da weiters die Störung des CS, und nicht des Benutzers oder des Betriebsablaufs, vorsätzlich erfolgen muss, wird dies bei Spam nie vorliegen, der daher ebenso nicht unter diese Bestimmung fällt[639]. Eine Störung der Funktionsfähigkeit durch unbefugte Benutzung ("Diebstahl" von Rechenzeit) könnte vorliegen, wenn andere Benutzer stark beeinträchtigt werden. Wird lediglich "überschüssige" Rechenzeit verwendet, so bleibt dies hier auch weiterhin straffrei (siehe aber § 118a StGB!). Durch fehlerhaft programmierte Viren[640] bzw. spezielle Pakete ("Ping of Death") können Rechner zum, u.U. sofortigen, Absturz gebracht werden. Da solche Programmteile oder Pakete normal nicht vorkommen,

---

[636] Beispiel: Ein Programm kann nicht gestartet werden, da keine Ressourcen, z.B. Hauptspeicher oder virtueller Speicher, mehr zur Verfügung stehen.

[637] Etwaige Schadfunktionen, in letzter Zeit eher selten enthalten, sind wie bei Viren und Trojanern separat zu beurteilen.

[638] Die geringfügigen Änderungen an internen (Verwaltungs-)Daten (Verzeichnis, Tabelle laufender Prozesse) sind hier vom Schaden zu weit entfernt um relevant zu sein.

[639] Zum Lahmlegen durch Überflutung mit Spam siehe die Überlegungen am Ende von IX.3.4.

[640] Aber auch Würmer, Trojaner oder bloß "normal" fehlerhafte Programme, bei denen dies bekannt ist.

ist die Störungsabsicht klar. Die Störung erfolgt zumindest bei den Paketen direkt durch die Übermittlung selbst, daher ist jedenfalls eine Funktionsfähigkeitsstörung anzunehmen. Je nach Art der Attacke kann Denial of Service dieses Delikt verwirklichen oder nicht. Wird durch unzählige Anfragen die Bandbreite eines Webservers so stark belegt, dass Kunden keinen Zugriff mehr erlangen, so wird die Funktionsfähigkeit des Computer(!)-systems hierdurch nicht gestört[641], ist also nicht tatbildlich. Erfolgt der Angriff durch SYN-Flood oder Ähnliches[642], liegt eine Funktionsstörung analog zu fehlerhaften Paketen vor.

IX.3.6. Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)

1. *Wer*
   1. *ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a) oder einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder*
   2. *ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,*

   mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
2. *Nach Abs 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.*

Analog zu Waffen sollen bestimmte Informationen bzw. Geräte nur eingeschränkt bzw. gar nicht verkehrsfähig sein. Die Herstellung, die Einfuhr, der Vertrieb, die Veräußerung oder das Zugänglichmachen, z.B. auf eine Webseite stellen, aber ev. auch bereits entsprechende Linkslisten[643], von Zugangscodes oder von Computerprogrammen, die für die Begehung eines Computerdeliktes geschaffen oder adaptiert wurden, wird verboten. Beispiele hierfür wären etwa das Veröffentlichen von Passwörtern, Codes zur Entschlüsselung kostenpflichtiger Dienste/Programme[644] oder private Schlüssel[645], genauso wie Programme

---

[641] Dieses funktioniert ja perfekt. Lediglich die (korrekten) Ergebnisse sind (wirtschaftlich!) sinnlos, da die Anfragen von Computern erzeugt und die Antworten ignoriert werden.

[642] Unzählige vorgetäuschte Verbindungsversuche, die zu einem Pufferüberlauf und folgendem Absturz bzw. Abweisen echter Verbindungen führen. Die gestörten Tabellen selbst besitzen keinen eigenen Wert, sondern wären bestenfalls Chancen auf einen späteren Vertragsabschluss, falls es sich z.B. um eine Werbe- oder Verkaufs-Web-Site handelt.

[643] Dies ist ein besonderes Problem und kann hier nicht allgemeingültig beantwortet oder ausgeführt werden.

[644] Siehe dazu auch das gesonderte Zugangskontrollgesetz!

[645] Insbesondere z.B. Zugangsdaten zum Online-Banking: Phishing ist ein "verschaffen" von Zugangsdaten für späteren Computerbetrug (§ 148a). Siehe auch Bergauer: Phishing im Internet – eine kernstrafrechtliche Betrachtung. RZ 2006, 82 (Die dort begründete Verwirklichung von § 108 StGB, Täuschung, ist jedoch sehr fraglich – Es tritt kein Schaden an den Rechten ein, da nichts verloren/gewonnen wird. Ebenso ist § 225a StGB, Datenfälschung, mit Vorsicht zu betrachten:

für DDoS-Angriffe[646] oder Viren/Trojaner. Zusätzlich besteht die Einschränkung, dass der Vorsatz für die Begehung eines der angeführten Computerdelikte mit diesen Mitteln vorliegen muss, wobei jedoch keine Absicht erforderlich ist[647]. Bei der Einführung des Delikts wurde noch darauf verzichtet, schon den Besitz alleine zu bestrafen, doch ist nunmehr auch schon dieser genauso wie die Beschaffung strafbar.

In Bezug auf die Computerprogramme muss beachtet werden, dass ein objektiver Maßstab anzulegen ist: Tools für Sicherheitsanalyse werden vielfach unter diese Bestimmung fallen, da sie zur Begehung eines solchen Delikts geschaffen wurden bzw. ohne jegliche Änderung dafür eingesetzt werden können. In diesem Fall kommt es dann nur mehr auf den Vorsatz für die Verwendung an.

Paragraph 2 dieses Delikts betrifft so genannte "Tätige Reue". Da es sich um ein Vorbereitungsdelikt handelt, ist die tatsächliche Begehung der "Haupttat", also Datenbeschädigung etc., für die Strafbarkeit nach diesem Delikt nicht erforderlich. Wird die Verwirklichung dieser Haupttat vom Ersttäter verhindert, so soll dies honoriert werden und keine Strafe erfolgen. Mit derartigen Vorschriften, welche auch für einzelne andere Delikte existieren, soll eine Art "goldene Brücke" für den Täter gebaut werden: Dieser kann am ehesten für die tatsächliche Verhinderung sorgen. In Frage kommt daher ev. das Löschen eines solchen Programms vor der Verwendung[648]. Die bloße Einstellung der Tätigkeit oder von Vorbereitungen dafür reicht sicher nicht aus[649].

IX.3.7. Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB)

1. *Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, dass er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkungen auf den Ablauf des Verarbeitungsvorgangs beeinflußt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.*
2. *Wer die Tat gewerbsmäßig begeht oder durch die Tat einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer einen 50 000 Euro übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.*

Ein Betrug (§ 148 StGB) setzt voraus, dass eine natürliche Person getäuscht wird, z.B. der Bediener des Computers, der dann falsche Eingaben tätigt. Aus diesem Grund kann nie ein Betrug verwirklicht werden, wenn nur eine Datenverarbeitungsanlage (=das Programm) "getäuscht" wird, beispielsweise ein Bankomat.

Stellt das Versenden einer E-Mail wirklich ein Handeln im "Rechtsverkehr" dar? Es sollen hier keinerlei Verfügungen über irgendwelche Rechte getroffen werden. Die Eingabe von Benutzername und Passwort könnte jedoch ev. als Ausübung eines Rechts darunter fallen).

[646] Distributed Denial of Service Attack: Angriffe, die von mehreren Computer im Zusammenspiel durchgeführt werden.

[647] Dolus eventualis, also „In-Kauf-nehmen“ reicht bereits aus.

[648] Planung eines Computerbetrugs mittels Software: Das Programm ist schon beschafft und daher dieses Delikt vollendet, noch bevor es noch zum betrügerischen Datenverarbeitungsmissbrauch kommt. Wird es vor dem Einsatz gelöscht, weil der Täter es sich anders überlegt, so ist er ausnahmsweise nicht zu bestrafen.

[649] Auch sonst ist die tätige Reue noch weiter eingeschränkt, so kann z.B. nach einer Durchsuchung wegen genau diesem Delikt keine Berufung mehr darauf erfolgen („Weil man mich erwischt hat, verzichte ich“).

Für das Vorliegen des Delikts ist ein viergliedriger Aufbau notwendig. Fehlt auch nur ein Schritt oder basiert ein Schritt nicht auf dem vorigen, so liegt keine Straftat vor:

1. Eine der angeführten Manipulationen (siehe näher unten) muss vorgenommen werden. Eine Raubkopie eines Programms ist keine Manipulation der Ausführung und fällt daher nicht unter dieses Delikt.
2. Durch diese Manipulation muss das Ergebnis der Verarbeitung verändert werden. Eine Verzögerung oder Unterbrechung ist keine Veränderung und daher nach § 148a StGB straflos. "Diebstahl" von Rechenzeit ist nicht ergebnisrelevant und daher (strafgesetzlich!) erlaubt[650]. Bloßes Hacken, d.h. *nur* Verschaffung von Zutritt zu einem Rechners, ist zwar eine Manipulation durch falsche Eingabe[651], doch hier nicht ergebnisrelevant.
3. Die Veränderung des Ergebnisses muss einen Vermögensschaden verursachen. Dieser muss direkt aus der Manipulation resultieren, d.h. ohne die Zwischenschaltung einer natürlichen Person, die etwa auf Grund der falschen Ausgabe erst die schädigende Handlung setzt.
4. Durch den Vermögensschaden muss der Täter oder ein Dritter sein Vermögen vermehren. Computersabotage im Auftrag einer Konkurrenzfirma erfüllt daher dieses Delikt nicht, weil die Bereicherung der Konkurrenzfirma durch Aufträge, die sonst die geschädigte Firma erhalten hätte, nicht aus dem Schaden stammt. Siehe zu diesem Problem auch die Erläuterungen bei der Datenbeschädigung (§ 126a StGB).

Es handelt sich um ein Vorsatzdelikt, sodass Fahrlässigkeit, egal welcher Ausprägung, nicht zur Strafbarkeit führt.

Folgende Begehungsarten sind möglich:

- Eingabe falscher Daten: Dies kann sowohl die "echte" Eingabe von Daten am Programmbeginn sein als auch die Veränderung, Löschung oder Unterdrückung von Daten während der Verarbeitung. Hierunter fallen auch richtige Daten, die z.B. gleich dem ausgefüllten Formular sind, wenn diese nicht den tatsächlichen Umständen und der Realität entsprechen, also zum Beispiel das Formular falsch ausgefüllt wurde und dies der eingebenden Person bekannt ist.
- Unbefugte Eingabe richtiger Daten: Beispiel hierfür ist die Eingabe des (richtigen!) PIN-Codes, um mit einer gestohlenen Bankomatkarte Geld zu beheben. Ebenso die Verwendung der eigenen Bankomatkarte, wenn sie vorher als gestohlen gemeldet wurde. Dies gilt hingegen nicht für Kreditkarten. Mit deren Vorlage im Geschäft wird eine Person getäuscht, auch wenn die Verarbeitung dann computerunterstützt erfolgt.
- Manipulation des Programmablaufs: Durch nachträgliche Einwirkungen von außen auf ein richtiges Programm ("Konsolenmanipulation"). Dies dürfte meiner Meinung nach entweder eine Veränderung des Programms oder der Eingabedaten sein.[652]

---

[650] Dies gilt im Gegensatz zu üblichen Multi-User-Systemen wahrscheinlich nicht für Realtime-Systeme: Durch die Abarbeitung einer zusätzlichen Aufgabe, z.B. mit hoher Priorität, kann das Ergebnis u.U. sehr stark beeinflusst werden!

[651] Es wird nicht der eigene (mangelnde) Benutzername eingegeben, sondern der einer anderen Person.

[652] Siehe dazu Turingmaschine: Veränderung des Eingabebandes und der internen Zustände ist eine Inputmanipulation. Eine Veränderung der internen Verarbeitungsvorschriften (Zustandsüberführungs- und Ausgabefunktion) ist eine Programm-Manipulation. Eine Abänderung der Ausgabe kann nur mehr durch Hardware-Veränderung (diese fällt aber aus diesem Delikt heraus) oder durch Ersetzen des Ergebnisbandes (fällt ebenfalls weg) erfolgen.

- Manipulation des Programms: Durch die Gestaltung des Programms wird vorsätzlich ein unsachgemäßer Ablauf herbeigeführt. Eine Abgrenzung zur Eingabe falscher Daten kann bei modernen Programmen schwierig sein, da man ihre Konfiguration auch als Programmierung verstehen kann.

Praktische Beispiele für dieses Delikt:

- Verwendung einer gestohlenen Bankomatkarte (siehe jedoch die Spezialbestimmungen in § 241a-g StGB)
- Eingabe eines gestohlenen oder errechneten Passwortes, um Software herunterladen zu können oder eine Testversion freizuschalten. Dies trifft nicht bei manuell bearbeiteten Bestellungen, z.B. per E-Mail, zu, sodass eine Person dann das Programm schickt. Werden lediglich Registrierungs- oder Kaufhinweise entfernt, so ist das Delikt nicht erfüllt, da der Schaden (=Verwendung des Programms ohne Bezahlung) bereits vorher eingetreten ist oder gar nicht vorliegt, z.B. bei legalen Versionen.
- Eingabe einer gestohlenen oder errechneten Kreditkartennummer. Erfolgt die Überprüfung und Abrechnung ausschließlich elektronisch, so wird dadurch das Delikt des § 148a StGB verübt. Führt hingegen eine Person die Überprüfung oder Versendung durch, so ist an normalen Betrug zu denken. Wird die Versendung zwar von einer Person vorgenommen, jedoch ausschließlich auf Grund von Computerausdrucken (z.B. Pack-Listen), so bleibt es beim Datenverarbeitungsmissbrauch: Die Täuschung muss durch die Manipulation hervorgerufen werden, d.h. nur wenn eine Person die Kreditkartennummer wahrnimmt und zumindest oberflächlich prüft, fällt § 148a StGB weg.

IX.3.8. Datenfälschung (§ 225a StGB)

Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Dieser Tatbestand entspricht dem der Urkundenfälschung (§ 223 StGB), nur bezieht er sich auf Daten. Unter "falschen Daten" ist hier zu verstehen, dass nicht der Inhalt falsch ist, also nicht der Realität entspricht, sondern dass über ihren Urheber (=Aussteller der Urkunde bzw. hier Eingeber/Autorisierer der Daten) getäuscht wird. Unter "verfälschte Daten" fallen jedoch sowohl Daten, bei denen der Urheber verändert, als auch solche, bei denen der gedankliche Inhalt manipuliert wurde. Das Delikt ist nur dann strafbar, wenn der Vorsatz hinzutritt, dass diese Daten im Rechtsverkehr verwendet werden sollen, z.B. zum Beweis des Abschlusses eines Kaufvertrages. Nicht enthalten sind daher einfache Manipulationen, um Spuren zu verwischen (Log-File Manipulationen) oder Bereicherung bzw. Schädigung (siehe betrügerischer Datenverarbeitungsmissbrauch/Datenbeschädigung). Zu beachten ist, dass es nicht darauf ankommt, wer der Besitzer der Daten ist. Auch die Manipulation eigener Daten kann hierdurch strafbar sein[653]! Dies betrifft etwa die Veränderung von eigenen oder die Erstellung neuer, angeblich abgesendeter oder empfangener E-Mails, wenn sie für einen der angegebenen Zwecke verwendet werden sollen.

[653] Analog etwa zur Strafbarkeit der Veränderung von Informationen im eigenen Führerschein, der eine Urkunde ist.

IX.4. Sonstige Straftaten mit Informatik-Bezug

In diesem Abschnitt[654] werden jene Straftaten im Überblick dargestellt, bei denen sich durch die Verwendung von Computern oder el. Kommunikation eine neue Begehungsweise ergibt, oder welche eine größere praktische Bedeutung besitzen. Die Bedeutung beruht nicht unbedingt auf einer Vielzahl von Verurteilungen oder der Häufigkeit ihres Vorkommens, sondern teilweise auch auf der öffentlichen Meinung[655].

IX.4.1. Üble Nachrede (§ 111 StGB)

Üble Nachrede ist entweder ein Vorwurf gegen den Charakter einer Person, also ein Angriff gegen die Ehre ohne bestimmte Tatsachen, oder der Vorwurf einer bestimmten Handlung, die unehrenhaft oder unsittlich ist. Diese Äußerung muss für zumindest einen Dritten wahrnehmbar, wenn auch nicht unbedingt tatsächlich wahrgenommen worden, sein. Als Dritter zählt nur, wer nicht in die Beleidigung miteinbezogen ist. Der Vorwurf muss geeignet sein, das Opfer lächerlich zu machen oder herabzusetzen.

Kein Delikt liegt vor wenn der Täter nachweisen kann, dass seine Äußerung der Wahrheit entspricht bzw. er im guten Glauben gehandelt hat, d.h. er sachliche und glaubhafte Anhaltspunkte für seine Äußerung hatte. Über Tatsachen des Privat- und Familienlebens ist ein solcher Beweis jedoch unzulässig und die Handlung daher unabhängig vom Wahrheitsgehalt der Aussage verboten.

Wird die Äußerung auf eine Weise durchgeführt, dass sie einer breiten Öffentlichkeit zugänglich wird, erhöht sich die Strafdrohung. Beispiele dafür sind Plakatierungen, Ansprachen auf Massenversammlungen oder sonst mit großer Streuung. In Bezug auf Informatik lassen sich weitere Beispiele anführen: Ausführungen auf Webseiten oder in belebten Newsgruppen bewirken ebenfalls eine besondere Streuung und sind breiter Öffentlichkeit zugänglich. Ob die Webseiten gut besucht sind oder nicht ist unerheblich, da lediglich die *Möglichkeit* der Kenntnisnahme erforderlich ist, die im Internet grundsätzlich weltweit besteht. Fast "private" Webseiten mit geringster Besucheranzahl fallen aber ev. heraus. Bei einer öffentlichen Verbreitung ist nur noch der Wahrheitsbeweis, aber nicht mehr der Beweis guten Glaubens möglich.

Das Opfer übler Nachrede muss stets eine natürliche Person sein. Eine Begehung durch Verbreitung unwahrer Aussagen über Programme bzw. deren Verhalten oder Eigenschaften ist nicht erfasst[656]. Es ist jedoch immer genau zu prüfen, ob hinter dem direkten Vorwurf nicht ein indirekter steckt, der gegen eine Person gerichtet ist: der Programmierer oder der Benutzer. Wird beispielsweise eine unwahre Aussage über die Kreditwürdigkeit eines Software-Agenten verbreitet, so handelt es sich nur dann um üble Nachrede, wenn der Besitzer (=Benutzer) des Agenten offensichtlich ist, wenn auch nur für Personen, mit denen der Agent Geschäfte abschließt. In diesem Fall ist noch besonders zu berücksichtigen, dass üble Nachrede voraussetzt, dass eine natürliche Person und nicht nur ein Computerprogramm die Äußerungen wahrnehmen kann. Hier wird darauf abzustellen sein, ob

---

[654] Siehe hierzu insbesondere Kienapfel, Grundriß des österreichischen Strafrechts. Besonderer Teil Band II. Delikte gegen Vermögenswerte. 2. Auflage. Wien: Manz 1988 sowie Foregger/Kodek, Strafgesetzbuch Kurzkommentar. 6. Auflage. Wien: Manz 1997

[655] Kinderpornographie hat im Internet typischerweise eine geringe Bedeutung, etwa im Vergleich zu „normalem“ Betrug. Dennoch wird sie durch das Internet stark erleichtert und auch als besonders verwerflich angesehen.

[656] Hierfür dürfte in vielen Fällen das Gesetz gegen den Unlauteren Wettbewerb (UWG) schlagend werden.

mittels normaler Aktionen Kenntnis von der Aussage erlangt werden kann und dies zumindest einigermaßen wahrscheinlich ist[657].

In Bezug auf Informatik ergeben sich folgende besonderen Punkte:

- Durch E-Mails mit auch nur einem weiteren Empfänger, selbst wenn nur BCC und damit für den Hauptempfänger unsichtbar, kann das Delikt begangen werden.
- Posten in Newsgruppen, in Chats oder eine Darstellung auf Webseiten stellen eine breite Öffentlichkeit dar. Es ist daher in diesen Fällen besonders auf die Äußerungen zu achten. Handelt es sich um eine Webseite in einem Intranet (z.B. firmenintern), so liegt keine Öffentlichkeit vor, aber immer noch Wahrnehmbarkeit für Dritte.
- Wenn eine Person unter Pseudonym auftritt, so erfüllt auch eine Beleidigung dieses Pseudonyms den Tatbestand der üblen Nachrede. Die Kenntnis des tatsächlichen Namens der dahinter stehenden Person ist weder beim Täter noch bei Dritten notwendig, sofern eine bestimmte Person identifiziert werden kann, d.h. das Pseudonym nur von einer einzigen Person oder einer fest zusammengesetzten Personengruppe regelmäßig verwendet wird.

Es handelt sich um ein Privatanklagedelikt, das Opfer trägt daher das Prozessrisiko.

IX.4.2. Beleidigung (§ 115 StGB)

Bei einer Beleidigung handelt es sich im Gegensatz zur üblen Nachrede rein um Werturteile[658] (weshalb auch kein Wahrheitsbeweis möglich ist), die den Anspruch auf achtungsvolle Behandlung durch andere verletzen.

Eine Beleidigung kann auf folgende Arten begangen werden:

- Beschimpfung: Die Missachtung eines anderen durch Worte, Gesten oder Bilder. Typischer Fall ist die formale Ehrenbeleidigung.
- Verspottung: Das Opfer wird lächerlich gemacht oder als minderwertig verhöhnt.
- Bedrohung mit körperlicher Misshandlung: Jemandem wird eine üble, unangemessene Behandlung in Aussicht gestellt.

Die Handlung muss, um strafbar zu sein, öffentlich oder vor mehreren begangen werden. Als Richtwert für die Öffentlichkeit ist im Gegensatz zu § 111 StGB nach der Literatur eine Anzahl von ca. zehn Personen anzunehmen. Vor mehreren wird die Tat begangen, wenn außer dem Beleidiger und dem Beleidigten mindestens noch drei weitere Personen anwesend sind. Durch dieselbe Äußerung Mitbeleidigte werden allerdings nicht mitgezählt. Tatsächliche Wahrnehmung ist nicht erforderlich, lediglich die Möglichkeit dazu. Auch hier muss das Opfer eine natürliche Person sein.

---

[657] Die Erweiterung auf die "Wahrnehmbarkeit" wurde vorgenommen, um mehr oder minder zufällige Nicht-Wahrnehmung durch Dritte nicht zu privilegieren. Der Gesetzgeber dürfte hier von der Ansicht ausgegangen sein, dass die Wahrnehmung der Regelfall ist. In Bezug auf Programme ist daher eine teleologische Einschränkung vorzunehmen: Was nur in außergewöhnlichen Sonderfällen oder durch Spezialmanipulationen (z.B. Hexdump) wahrgenommen werden kann, ist nicht tatbildlich.

[658] Von der physischen Begehungsart der körperlichen Misshandlung wird hier abgesehen.

In Bezug auf Informatik ergeben sich folgende besondere Punkte:

- Beleidigungen in E-Mails müssen zumindest an vier Personen (CC oder BCC) gerichtet sein, um die Mindestpublizität zu erreichen.
- Webseiten oder Newsgruppen erfüllen jedenfalls die Erfordernis der Öffentlichkeit.

Wie bei der üblen Nachrede handelt es sich um ein Privatanklagedelikt.

IX.4.3. Verletzung des Briefgeheimnisses/Briefunterdrückung (§ 118 StGB)

Das Gesetz spricht im § 118 StGB nur von "verschlossenem Brief oder anderem *solchen* Schriftstück". Aus diesem Grunde können E-Mails[659] oder sonstige Daten nicht Tatobjekt sein[660]. Anderes könnte für verschlüsselte E-Mails gelten, da diese "verschlossen" sind. Problematisch ist dann jedoch immer noch die Qualifizierung als "Schriftstück", welche eher auf eine Verkörperung hinweist. Werden die Daten jedoch ausgedruckt, so kann eine Verschlüsselung wohl als "Verschluss" gelten und § 118 StGB ist dann auf das physische Schriftstück anwendbar.

IX.4.4. Auskundschaften von Geschäfts- oder Betriebsgeheimnissen (§ 123 StGB)

Geschäftsgeheimnisse sind Tatsachen kommerzieller Art (Wissen), welche nur einem Innenstehenden bekannt sind, beispielsweise Geschäftsbeziehungen oder Prozesse, während es sich bei Betriebsgeheimnissen um technische Einrichtungen oder sachbezogene Daten handelt. Damit ein Geheimnis vorliegt, müssen die folgenden vier Punkte zutreffen[661]:

1. Die Tatsache muss eine Beziehung zum Betrieb aufweisen.
2. Sie darf nicht offenkundig oder allgemein zugänglich sein.
3. Der Besitzer muss ein berechtigtes Interesse an der Geheimhaltung haben.
4. Der Besitzer muss die Tatsache geheim halten wollen.

Eine Verwertung liegt vor, wenn aus der Kenntnis wirtschaftlicher Nutzen gezogen wird, also eine kommerzielle Verwertung erfolgt (rein privat: erlaubt). Das Auskundschaften umfasst alle Tätigkeiten, die drauf abzielen, in den Besitz eines Geheimnisses zu gelangen. Erwirbt jemand aus seiner beruflichen Tätigkeit solche Kenntnisse, so fällt die Weitergabe *nicht* unter § 123 StGB (Hier: „Auskundschaften“, nicht „Verrat“).

Es handelt sich hierbei um ein Vorbereitungsdelikt. Es ist daher nicht erforderlich, dass der Täter auch tatsächlich ein Geheimnis erfährt. Bereits der Versuch ist voll strafbar, jedoch muss dieser zumindest einigermaßen zur Erlangung der Information geeignet sein, darf also nicht absolut untauglich sein.

In der Informatik ist dieses Delikt praktisch bedeutend, da insbesondere das "Hacken" von fremden Computersystemen sehr oft darunter fällt; siehe dazu aber jetzt auch die Spezialregelung in § 118a StGB. Da es sich bei dem Delikt um Wirtschaftsspionage handelt, fal-

---

[659] Zum Briefgeheimnis bei E-Mails siehe auch das Telekommunikationsgesetz § 93 (Kommunikationsgeheimnis). Das TKG betrifft den Inhalt der Übermittlung, während § 119 und § 120 StGB Anlagen zum Abhören unter Strafe stellen. § 119a StGB schützt wiederum den Inhalt.

[660] Siehe zur Schriftlichkeit Punkt IX.1.4: Qualifizierung von Daten, Urkundendelikte

[661] Jaburek/Schmölzer, Computer-Kriminalität. EDV und Recht Band 2. Wien: Orac 1985

len darunter alle kommerziellen Versuche, in Rechner eines fremden Unternehmens einzudringen, um aus der Kenntnis dort gespeicherter geheimer Informationen einen Vorteil zu ziehen. Das Eindringen in Rechner von Regierungseinrichtungen fällt nicht darunter, siehe dazu jedoch § 254f StGB (Ausspähung von Staatsgeheimnissen). Auch das Ausspähen zur anschließenden Preisgabe an die Öffentlichkeit ist strafbar[662]. Ein weiteres Beispiel ist der Diebstahl von Backup-Bändern[663]. Kein Geschäftsgeheimnis ist ein Kunden- und Lieferantenverzeichnis, das Telefonnummern, Adressen und Namen von Ansprechperson enthält[664].

Es handelt sich um ein Privatanklagedelikt, sodass Verurteilungen äußerst selten sind. Aus diesem Grund, wegen der oft schwierigen Beweislage und der negativen Publizität, sollte das Verfahren bekannt werden, ist die Bereitschaft zur Verfolgung solcher Delikte insbesondere in der Informatik eher gering. Wird das Delikt begangen, um die Informationen im Ausland zu verwerten, so wandelt es sich in ein Offizialdelikt mit höherer Strafdrohung (§ 124 StGB). Dann ist ebenso der Verrat solcher Geheimnisse strafbar.

IX.4.5. Ketten- oder Pyramidenspiele (§ 168a StGB)

Dieses 1996 eingeführte Delikt wurde zwar nicht mit Computer-Bezug geschaffen, doch besitzt es gerade dort eine große Bedeutung: Im Internet kursieren unzählige derartige Systeme, die insbesondere über Spam beworben werden, da mit geringstem finanziellem Einsatz enorme Mengen an potentiellen "Kunden" angesprochen werden können. Ketten- oder Pyramidenspiele basieren auf einem System, bei welchem für einen Einsatz ein Vermögensvorteil versprochen wird und der Erfolg davon abhängt, dass dem System weitere Teilnehmer unter den gleichen Bedingungen zugeführt werden und diese sich ebenfalls an die Bedingungen halten[665].

Strafbar sind folgende Aktionen:

- Veranstalten oder In-Gang-Setzen: Derjenige, der es anderen Leuten ermöglicht, an diesem Spiel teilzunehmen, also meist der Erfinder, verwirklicht das Delikt. Im Internet befinden sich diese Personen fast immer im Ausland und sind überdies keine Österreicher. Eine Strafbarkeit liegt selbst dann nicht vor, wenn das Spiel in Österreich vertrieben wird und Opfer findet. Ausnahme: Pyramidenspiele sind nach dem Ort des Beginns ebenfalls strafbar. Meist ist der Veranstalter jedoch zusätzlich auch Verbreiter und dann nach dem nächsten Punkt strafbar, sofern es sich um direkte Verbreitung vom Veranstalter nach Österreich handelt und nicht bloß Erreichung des Inlands über mehrere Zwischenstufen.
- In einer zur Anwerbung vieler Teilnehmer geeigneten Weise verbreiten: Unter vielen Teilnehmern sind mindestens 30 zu verstehen. Im Gegensatz zu Punkt 1 wird die Verbreitung regelmäßig im Inland erfolgen und daher strafbar sein. Eine Verbreitung in

---

[662] Etwa das Auskundschaften illegaler Abfallentsorgung.

[663] Siehe Sachverhalt in OGH 2.7.1992, 15 Os 43/92

[664] LG Linz 7.12.1999, 27 E Vr 591/99, ARD 5120/27/2000; Im diesem Fall wurde kein spezieller Beweis dafür geführt, dass die Namen der Ansprechpartner nicht bekannt und demnach ein Geschäftsgeheimnis gewesen wären. Dies ist wohl eher zweifelhaft. Im Ergebnis richtig, da kein Ausspähen vorlag: Der Mitarbeiter war gerade mit der Führung des "ausgespähten" Verzeichnisses beauftragt.

[665] Beispiel: Jeder muss x weitere Personen anwerben, welche ihren Einsatz an den Anwerbenden und/oder dessen Vorgänger bezahlen. Solange immer neue Personen hinzukommen, funktioniert das System, wobei Gewinne typischerweise an der Spitze der Pyramide massiert werden. Die „unteren Ränge“ machen jedoch keinen Gewinn, da keine weiteren Nachfolger gefunden werden (können: exponentielles Wachstum!).

Newsgruppen ist sicherlich geeignet, ebenso Massen-E-Mails. Sendet ein Teilnehmer daher seinen "guten Tipp" an eine größere Anzahl von Personen weiter, macht auch er sich strafbar.

- Die Verbreitung auf sonstige Weise gewerbsmäßig fördern: Dies betrifft hauptsächlich Mitspieler (die ansonsten straffrei sind), welche die Verbreitung zu Erwerbszwecken weiter fördern ("Berufskeiler"), dies aber auf individueller Basis durchführen. Die Abhaltung einer Werbeveranstaltung fiele hingegen unter Punkt 2.

IX.4.6. Pornographische Darstellungen Minderjähriger (§ 207a StGB)

Aufgrund des großen Aufmerksamkeitswertes wird auch dieses Delikt kurz erläutert, obwohl es nur geringen spezifischen Bezug zur Informatik gibt. Elektronische Kommunikation, vermeintliche Anonymität und die leichteren Möglichkeiten der Verschleierung haben aber zu häufigerem Auftreten geführt.

Erfasst sind bildliche Darstellungen, also Bilder und Videos, aber nicht textuelle Beschreibungen oder Tonaufzeichnungen, bei denen eine minderjährige Person[666] involviert ist. Es ist nicht erforderlich, dass eine solche Handlung tatsächlich vorgenommen wurde, sondern nur, dass dieser Eindruck erweckt wird, was die Beweislage vereinfacht. Daher umfasst das Delikt auch tatsächlich „gefälschte“ Bilder[667]. Die Darstellungen müssen jedoch wirklichkeitsnahe sein, um unter das Verbot zu fallen. Darunter versteht man Bilder, die von Wiedergabequalität und Erkennbarkeit her ein im allgemeinen Sprachgebrauch als fotografisch bezeichnetes Niveau erreichen, d.h. dem Betrachter den Eindruck vermitteln, „Augenzeuge“ zu sein[668].

In diesem Zusammenhang ist besonders auf die Provider-Verantwortlichkeit zu verweisen (siehe dazu auch später): Da es sich um eine Vorsatztat handelt, kann ein Transport-Provider, d.h. ein „Beförderer“, was für die Strafbarkeit sonst ausreicht, dieses Delikt nicht nach Abs 1 Z 2 begehen, solange er nichts vom Inhalt weiß oder vermuten muss, da er dann keinen Verbreitungsvorsatz hat. Problematisch ist lediglich die Ziffer 2, da hierfür nur die Zugänglichmachung gefordert ist (Access-Provider). Doch auch hier fehlt der Vorsatz bei mangelndem Wissen. Ein strengerer Maßstab gilt auch nicht für den Space-Provider, der Speicherplatz für Webseiten zur Verfügung stellt: Er ist nach dem E-Commerce Gesetz nicht zu (Vorab-) Kontrollen verpflichtet.

Für einen Internet-Benutzer ist Abs 1 Z 3 einschlägig: Zugänglichmachen liegt schon dann vor, wenn eine Webseite mit entsprechenden Darstellungen ins Netz gestellt wird. Doch schon der Besitz ist nach Abs 3 verboten und trifft zu, wenn ein derartiges Bild am Bildschirm angezeigt wird. Dennoch ist auch hier Vorsatz notwendig: Wem Bilder unterge-

---

[666] Also unter 18 Jahren. Der Strafrahmen ist höher, wenn es sich um unmündige Minderjährige (< 14 Jahre) handelt. Es existieren noch weitere Qualifizierungen.

[667] Also auch Bilder von Personen über 18 Jahren, welche verfremdet wurden um auszusehen, als wären sie von Personen unter diesem Alter („Realpornographie Erwachsener mit kindlichem Erscheinungsbild“). Genauso sind komplett computergenerierte Bilder betroffen („virtuelle Pornographie“). Dies kann nicht mehr mit dem Schutz von Minderjährigen begründet werden, die ja nicht involviert sind, sondern soll allgemein den „Markt“ derartiger Produkte reduzieren, um spätere tatsächliche Handlungen zu vermeiden. Volljährige Personen, welche wie Minderjährige aussehen und bei denen die Darstellung nicht verändert wurde, fallen jedoch heraus.

[668] Cartoons, Mangas etc. fallen daher wohl aus der Strafbarkeit heraus.

schoben werden (fehlendes Wissen) oder wer irrtümlich eine solche Seite erreicht (mangelndes Wollen), ist nicht strafbar.[669]

Für Firmen ist es nicht erforderlich, spezifische Vorbeugungshandlungen dagegen zu unternehmen, dass Mitarbeiter eventuell derartige Webseiten besuchen. Lediglich aus der Fürsorgepflicht gegenüber Minderjährigen könnte sich diese ergeben. Da jedoch die Erfolgquote entsprechender Software relativ gering ist, sind auch hier die Anforderungen äußerst niedrig, zumindest bis konkrete Probleme bekannt werden.

Dies ist eine Straftat, welche auch im Ausland begangen werden kann: Ist der Täter Österreicher und hat er seinen gewöhnlichen Aufenthalt im Inland, so wird die Tat auch dann bestraft, wenn sie im Ausland begangen wurde ("Sextourismus").

Privilegiert ist der Besitz bzw. die Herstellung derartiger Bilder in engen Grenzen:

- Mit Einwilligung von einer Person zwischen 14 und 18 Jahren zu deren eigenem Gebrauch. Eine Verbreitung ist also selbst bei freier Zustimmung hierzu verboten.
- Wenn es sich um Darstellungen handelt, welche nur den Eindruck einer Person von 14 bis 18 Jahren erwecken[670] und keine Gefahr der Verbreitung der Darstellung besteht.

IX.4.7. Geldfälschung (§ 232 StGB)

In Bezug auf E-Business stellt sich die Frage, welche rechtliche Kategorie neue Zahlungsmittel wie E-Cash[671] besitzen. Handelt es sich hierbei um "Geld" im Rechtssinne? Laut Kienapfel[672] ist Geld ein "vom österreichischen Staat oder einer von ihm ermächtigten Stelle als Wertträger beglaubigtes und zum Umlauf im allgemeinen Verkehr bestimmtes Zahlungsmittel". E-Cash ist daher kein Geld (=öffentliches Zahlungsmittel) im Rechtssinne, da es keinen öffentlichen Ursprung hat und nicht zum allgemeinen Verkehr bestimmt ist. Auch "Giralgeld" ist rechtlich gesehen kein Geld: Ein Bankguthaben ist nur eine Forderung gegenüber der Bank. Für ausländische Zahlungsmittel ist hingegen jeweils die Definition des Ausgabestaates anzuwenden. Sollte "elektronisches Geld" daher im Ausland anerkannt sein, so ist es auch in Österreich vor Fälschung geschützt.

Derartige Zahlungssysteme sind inzwischen wieder großteils vom Markt verschwunden: Aktuelle Systeme beruhen auf Guthaben (z.B. PayPal) oder alten Systemen (z.B. Kreditkarte, Bankomatkarte) mit neuer "Umkleidung", etwa Übertragung über SSL oder spezielle Protokolle. Bei Missbrauch ist insbesondere an betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB zu denken.

IX.4.8. Unbare Zahlungsmittel (§ 241a-g StGB)

Bei unbaren Zahlungsmitteln[673] handelt es sich um körperliche Zahlungsmittel[674], die den Aussteller erkennen lassen, gegen Fälschung oder missbräuchliche Verwendung geschützt

---

[669] Hier muss vor der Praxis der Selbsthilfe gewarnt werden: Wer nach solchen Darstellungen sucht und diese unverzüglich bei der Polizei anzeigt, handelt vorsätzlich und ist daher selbst strafbar!

[670] Also verfremdete Personen über 18 Jahren oder gemalte, computergenerierte, … Bilder.

[671] Von einer Bank ausgegebene elektronische Daten, mit denen einmalig eine Bezahlung erfolgen kann; die Verwendung entspricht der von Bargeld.

[672] Kienapfel, Probleme das strafrechtlichen Geldbegriffs. Österreichische Juristen Zeitung 1986, 423

[673] Definition in § 74 Abs 1 Z 10 StGB

sind und im Rechtsverkehr bargeldvertretende Funktion besitzen oder zur Ausgabe von Bargeld dienen. Der Verwendungsschutz muss auf Codierung, Ausgestaltung oder Unterschrift beruhen. Typische Beispiele sind die Quick-Geldbörse, Kreditkarten, Bankomatkarten, Prepaid-Karten, Wechsel, Schecks etc., also nicht ausschließlich el. Zahlungsmittel.

Der Hintergrund dieser Regelung bestand in einer Schutzlücke für bestimmte Gegenstände: Fälschung und Diebstahl waren bisher nur dann strafbar, wenn es sich um Urkunden oder Wertträger handelte. Kreditkarten sind z.B. Urkunden, die Quick-Geldbörse Wertträger. Bankomatkarten hingegen werden nicht als Urkunden angesehen, da typischerweise keine Vorlage gegenüber Personen erfolgt, und sind auch keine Wertträger, selbst zusammen mit der PIN nicht[675]. Die Wegnahme einer Bankomatkarte ohne deren Verwendung zum Abheben von Geld war daher bislang straflos[676].

Diese Delikte sollen nicht dem Schutz des Besitzers dienen, hierfür sind die existierenden Delikte vorgesehen, sondern das Vertrauen in die Sicherheit und Zuverlässigkeit des Zahlungsverkehrs garantieren, wobei der Rechtsgutträger die Allgemeinheit und nicht der im Einzelnen am Zahlungs- und sonstigen Wirtschaftsverkehr Beteiligte ist. Sie basieren auf einem EU-Rahmenbeschluss zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[677]. Die neuen Delikte verdrängen zwar entsprechende Urkundendelikte sofern vorliegend, da diese ebenso der Sicherung der Allgemeinheit dienen, eine separate Wertträgereigenschaft bleibt jedoch weiterhin als Angriff gegen Rechtsgüter einer Einzelperson gesondert strafbar.

Verboten sind im Einzelnen folgende Handlungen (teilweise ist tätige Reue möglich):

- Fälschung (§ 241a StGB): Herstellung eines nachgemachten Wechsels oder Erzeugung einer Bankomatkarte durch Speichern entsprechender Daten auf dem Magnetstreifen einer Blanko-Magnetkarte. Ein Vorsatz zur Verwendung im Rechtsverkehr, also zum späteren Einsatz, ist erforderlich.
- Annahme, Weitergabe oder Besitz falscher oder verfälschter unbarer Zahlungsmittel (§ 241b StGB): Auch hier ist ein Verwendungsvorsatz erforderlich. Falsche Zahlungsmittel sind künstlich hergestellt, verfälschte wurden manipuliert. Eine gestohlene Bankomatkarte mit PIN fällt daher nicht unter diese Bestimmung.
- Vorbereitung der Fälschung (§ 241c StGB): Anfertigung, Verschaffung oder Besitz von bestimmten Mitteln mit dem Vorsatz, eine Fälschung zu ermöglichen, ist verboten. Solche Mittel müssen nach ihrer besonderen Beschaffenheit ersichtlich zu einem solchen Fälschungszweck bestimmt sein. Dies betrifft also etwaige besondere Sicherungselemente, z.B. Hologrammfolien. Magnetstreifen-Leser/-Schreiber fallen wohl nicht darunter, da diese auch für legale Zwecke verwendet werden können. Eine Kombination mit Software zum Kopieren von Karten könnte jedoch als verboten angesehen werden; die Strafbarkeit hängt dann vom Vorsatz ab.

---

[674] Rein elektronisches Geld fällt daher heraus. Die Quick-Geldbörse ist jedoch körperlich (Chip), obwohl der Wert rein el. ist, was aber für alle diese Zahlungsmittel zutrifft.

[675] Der Wert der Plastikkarte und des Chips ist praktisch Null, auch der Code ist für sich alleine oder in Zusammenhang mit der Karte nicht verkäuflich.

[676] Datenbeschädigung kommt zwar in Frage, betrifft jedoch nur den Schaden des Besitzers, der die Karte nicht verwenden kann. Liegt kein solcher vor, fällt auch dieses Delikt weg.

[677] Rahmenbeschluss des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, 2001/413/JI, ABl. Nr. L 149 vom 2.6.2001, 1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001F0413:DE:HTML

- Entfremdung unbarer Zahlungsmittel (§ 241e Abs 1 StGB): Die Verschaffung eines solchen Zahlungsmittels ist verboten, wenn sie dazu erfolgt, eine unrechtmäßige Bereicherung zu erzielen oder eine Fälschung zu ermöglichen. Dies betrifft den Diebstahl derartiger Zahlungsmittel und das kurzfristige „ausborgen", z.B. um eine Kopie anfertigen zu können.
- Unterdrückung unbarer Zahlungsmittel (§ 241e Abs 3 StGB): Vernichtung, Beschädigung oder Unterdrückung unbarer Zahlungsmittel ist strafbar, wenn dies vorgenommen wird, um deren Einsatz zu verhindern. Kein Delikt wird bei Alleinverfügungsberechtigung begangen, d.h. die Zerstörung der eigenen Zahlungsmittel ist erlaubt.
- Annahme, Weitergabe oder Besitz entfremdeter unbarer Zahlungsmittel (§ 241f StGB): Analog zu § 241b StGB ist der Besitz etc. von entfremdeten Zahlungsmitteln mit dem Vorsatz, sich oder einen Dritten durch die Verwendung zu bereichern oder eine Fälschung zu ermöglichen, verboten.

In diesen Bestimmungen explizit nicht enthalten ist der tatsächliche Einsatz von gestohlenen oder gefälschten unbaren Zahlungsmitteln: Dieser ist genau wie bisher nach den anderen Delikten separat und zusätzlich zu bestrafen.

IX.4.9. Verbreitung falscher, beunruhigender Gerüchte (§ 276 StGB)

Die Verbreitung von Gerüchten ist in Sonderfällen unter Strafe gestellt: Der Verbreiter muss von der Unwahrheit der Darstellung wissen und beabsichtigen, dass ein großer Personenkreis beunruhigt wird, sodass dadurch die öffentliche Ordnung gefährdet wird. Beunruhigung setzt die Eignung zur Hervorrufung echter Besorgnis für die Zukunft voraus (Kriegsgefahr, Rationierungen, Katastrophen[678]). Ein großer Personenkreis muss eine große und wesentliche Gruppe der Bevölkerung sein, also mindestens mehrere tausend Personen.

Die regelmäßig auftretenden Falschmeldungen über Viren stellen sicherlich kein geeignetes Tatobjekt dar, da die Besorgnis unter der Schwelle dieses Paragraphen liegt und auch die Verbreitung meist zu gering ist. Ein Beispiel hätte hingegen das Jahr-2000-Problem sein können: Es war geeignet, echte Besorgnis in einem großen Personenkreis hervorzurufen, diese war jedoch tatsächlich vorhanden und nicht unwahr. Sie wurde ev. mit Bereicherungsabsicht[679] verbreitet, aber wohl kaum mit der Absicht zur Beunruhigung.

IX.4.10. Fälschung eines Beweismittels (§ 293 StGB)

Beweismittel ist alles, was in einem behördlichen Verfahren geeignet ist, bestimmte Sachverhalte zu belegen. Jegliche Änderung, um einen anderen Sachverhalt glaubhaft oder glaubhafter zu machen, ist strafbar. Es handelt sich um ein Delikt mit erweitertem Vorsatz, daher ist die Abänderung nur strafbar, wenn dieses Beweismittel in einem gerichtlichen oder verwaltungsbehördlichen Verfahren verwendet werden soll, egal von wem, und ob es dann tatsächlich gebraucht wird/wurde und ob es zu einer Irreführung kam.

Urkunden sind davon nicht erfasst, da für diese Spezialvorschriften gelten[680]. Da Daten jedoch keine Urkunden sind und sie besonders zu einer Fälschung geeignet sind[681], ist dieses

---

[678] Beispiele: Terroranschlag, Überschwemmungen, großflächige Stromausfälle, Vulkanausbrüche, Hurricanes etc.

[679] Verkauf von Beratung, neuer Software, Dienstleistungen etc.

[680] Urkundenfälschung nach § 223 StGB geht diesem Delikt vor, Datenfälschung (§ 225a StGB) jedoch nicht! Dort wird bereits die Manipulation der Daten bestraft, während hier auch die tatsächliche Verwendung unter Strafe steht. Daher kommt es in einem großen Bereich zur Überschneidung beider Delikte.

Delikt für die Informatik von hoher Bedeutung. In der Praxis wird es jedoch wohl in den meisten Fällen von der Datenfälschung verdrängt.

Es ist daher jedwede Veränderung (Löschen: § 295 StGB) von Daten verboten, wenn damit gerechnet wird, dass diese eventuell in einem Verfahren als Beweismittel verwendet werden. In Frage kommen insbesondere gespeicherte Dokumente und Logfiles. Ein tatsächlicher Schutz dagegen ist jedoch einzig dadurch möglich, eine Kopie zu erstellen, wobei die unveränderte Herstellung und Aufbewahrung mit einer höheren Glaubhaftigkeit ausgestattet sein muss als beim Original.

IX.4.11. Neutralitätsgefährdung (§ 320 Abs 1 Z 5 StGB)

In Bezug auf die Informatik ist nur der Tatbestand des Abs 1 Z 5 von Bedeutung, da z.B. ein Mail-Relay oder Proxy-Server eine Fernmeldeanlage im Sinne dieses Deliktes darstellen. Es ist jedoch erforderlich, dass die Übermittlung während eines bewaffneten Konfliktes erfolgt, an dem Österreich nicht beteiligt ist und dass die Übermittlung wissentlich erfolgt. Ein normaler Provider begeht daher dieses Delikt nicht, da er üblicherweise kein Wissen vom Inhalt der von ihm übertragenen Daten besitzt und diesen ja auch nur in ganz wenigen Sonderfällen überhaupt feststellen darf.

Wird jedoch ein Rechner speziell dafür eingerichtet, militärische Nachrichten zu übermitteln oder zu verbreiten, ist dieses Delikt schon mit der Errichtung der Anlage, in diesem Fall also der Anbindung an ein Kommunikationsnetz, vollendet.

IX.4.12. Verbotsgesetz

Ebenso wie Pornographie besitzen nationalsozialistische Äußerungen oder Handlungen mit Bezug darauf einen hohen Aufmerksamkeitswert, insbesondere in Österreich und Deutschland. Derartige Tätigkeiten werden durch das Verbotsgesetz unter Strafe gestellt. In Verbindung mit der Informatik sind drei Teile von besondere Bedeutung: Einrichtungen zur Nachrichtenübermittlung, Aufforderung und Verharmlosung.

IX.4.12.1. Einrichtungen zur Nachrichtenübermittlung (§ 3a Z 3, 4 VerbotsG)

Jede Herstellung, Verschaffung oder Bereithaltung von Einrichtungen zur Nachrichtenübermittlung für nationalsozialistische Organisationen ist verboten. Solche Einrichtungen sind zweifellos: Server für Webseiten, Newsgruppen, Chats, Dateiablage, ... Voraussetzung ist jedoch, dass der Täter mit dem Vorsatz handelt, dass sie von einer solchen Organisation verwendet werden sollen. Die bloße Weiterleitung ohne Wissen davon ist nicht strafbar. Da es sich um ein Erfolgsdelikt handelt, kommt als Tatort (Ort des Betriebs der Anlage) nur Österreich in Betracht. Ausländische Anlagen, auch wenn sie von Österreichern betrieben werden, sind nicht erfasst.

IX.4.12.2. Aufforderung (§ 3d VerbotsG)

Die Aufforderung, sich für die NSDAP oder ihre Ziele zu betätigen, ist verboten, sofern sie öffentlich oder vor mehreren erfolgt. Auch bildliche Darstellungen sind davon erfasst.

---

[681] Frühere Zustände sind unwiederbringlich verloren und eine Wiederherstellung ist unmöglich, außer über vorhandene Backups. Weiters ist es unmöglich, die Tatsache einer Veränderung aus den veränderten Daten selbst zu entdecken, sofern diese nicht signiert oder anderweitig gesichert sind.

Fraglich ist, wo im Falle von Webseiten auf ausländischen Servern der Tatort liegt: Wird die "Aufforderung" beim Sender (=Lieferant der Webseiten) oder beim Empfänger (=Ort der Darstellung) durchgeführt? Da es sich um ein schlichtes Tätigkeitsdelikt handelt, ist eher auf den Ort des Senders abzustellen, da er die Aufforderung durchführt. Das Abrufen und Betrachten derartiger Seiten ist straflos. Verboten ist jedenfalls zu verbreiten, wo solche Seiten zu finden sind.

IX.4.12.3. Wiederbetätigung (§ 3g VerbotsG)

Dieser allgemeine Auffangtatbestand betrifft jedwede Art von Wiederbetätigung und stellt sie unter Strafe. Es besteht Subsidiarität zu strenger bestraften Sonderregelungen. Es wird nur darauf abgestellt, dass sich jemand "im nationalsozialistischen Sinn betätigt", daher führt auch schon eine einzelne Mail an einen einzelnen Empfänger zur Strafbarkeit.

IX.4.12.4. Verharmlosung (§ 3h VerbotsG)

Die Verharmlosung sowie das Gutheißen, Leugnen oder Rechtfertigen von nationalsozialistischen Verbrechen ist strafbar. Das Delikt ähnelt der Aufforderung, jedoch muss die Art der Verbreitung geeignet sein, sie vielen Menschen zugänglich zu machen. Es fallen daher einige wenige Begehungsweisen heraus, wie beispielsweise das Versenden in kleineren Kreisen per E-Mail oder in Chats. Die Aufforderung zur Wiederbetätigung ist vergleichsweise auch strafbar, wenn sie nur vor mehreren, d.h. zumindest drei Personen, erfolgt.

IX.4.13. Pornographiegesetz

Gegenüber der im StGB verpönten Kinderpornographie sind sonstige pornographische Darstellungen (Filme, Bilder, Texte, ...) laut Pornographiegesetz verboten. Hierbei ist ein wichtiger Unterschied zu bemerken: Das Pornographiegesetz verbietet nicht den Besitz, sondern nur die Verbreitung auf besondere (praktisch alle) Arten, wenn gewinnsüchtige Absicht oder Gefährlichkeit für Jugendliche unter 16 Jahren gegeben ist.

Eine Einteilung erfolgt in "harte Pornographie"[682], welche bei Gewinnabsicht grundsätzlich verboten ist (§ 1 Pornographiegesetz), und "normale Pornographie" (§ 2 Pornographiegesetz), bei der eine Gefährdung Jugendlicher gegeben sein muss.

Nach dem Wortlaut ist bei „harter Pornographie“ an eine körperliche Verbreitung gedacht und die Bestimmung daher auf das Internet vermutlich nicht anwendbar[683], zusätzlich auch nicht bei Unentgeltlichkeit. Gemäß Abs 1 lit. e Pornographiegesetz ist jedoch strafbar, wer darauf hinweist, wo solche Darstellungen zu finden sind oder wie Zutritt dazu erlangt werden kann. Es sind daher schon bloße Hinweise, also ohne Bilder, in Newsgruppen oder in weiter verbreiteten E-Mails (ab drei Empfängern) strafbar, sofern es sich beim Ziel um harte Pornographie handelt.

Die „normale“ Variante kann im Gegensatz selbst gegen Entgelt in Verkehr gebracht werden, sofern sie nicht öffentlich in Erscheinung tritt und Jugendlichen der Zutritt verwehrt

---

[682] Exzessiv aufdringliche Darstellung realer Sexualakte, sexuelle Gewalttätigkeiten, Unzucht mit Unmündigen, Personen desselben Geschlechts oder Tieren. Die Kategorien entstammen nicht dem Gesetz, sondern Literatur und Rechtsprechung.

[683] Siehe dazu auch http://normative.zusammenhaenge.at/it-recht_answers/it-recht_answers120.html (4.2.2000; inaktiv) Noch auffindbar im Web-Archiv http://web.archive.org/web/20040621232531/http://normative.zusammenhaenge.at/it-recht_answers/it-recht_answers120.html

wird. Hiervon ist auch das Internet betroffen, wobei eher ein strenger Maßstab anzulegen ist. Dies bedeutet für die Informatik, dass ein, eventuell nur fremdsprachiger, Hinweistext mit anschließendem Link wohl nicht als Jugendschutz ausreicht, sondern stattdessen eine einigermaßen verlässliche Altersprüfung erfolgen muss[684].

IX.5. Literatur

IX.5.1. Allgemein

Augeneder, Silvia: Strafbarkeit im Internet unter besonderer Berücksichtigung neonazistischer Inhalte. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther, Liebwald, Doris (Hg.): Zwischen Rechtstheorie und e-Government. Wien: Verlag Österreich 2003, 445-452

Bergauer, Christian: Phishing im Internet – eine kernstrafrechtliche Betrachtung. RZ 2006, 82

Bertel, Christian: Grundriß des österreichischen Strafprozeßrechts. 5. Auflage, Wien: Manz 1997

Foregger, Egmont, Kodek, Gerhard: Strafgesetzbuch Kurzkommentar. 6. Auflage. Wien: Manz 1997

Geiger, Patrick: Indiskretionsdelikte und neue Medien. Zur strafrechtlichen Relevanz der Überwachung privater Kommunikation mittels "Internet Monitoring Software". Master Thesis. http://rechtsprobleme.at/doks/indiskretionsdelikte_und_neue_medien-geiger.pdf

Jaburek, Walter, Schmölzer, Gabriele: Computer-Kriminalität. EDV und Recht Band 2. Wien: Orac 1985

Kienapfel, Diethelm: Grundriß des österreichischen Strafrechts. Allgemeiner Teil. 6. Auflage. Wien: Manz 1996

Kienapfel, Diethelm: Grundriß des österreichischen Strafrechts. Besonderer Teil Band I. Delikte gegen Personenwerte. 4. Auflage. Wien: Manz 1997

Kienapfel, Diethelm: Grundriß des österreichischen Strafrechts. Besonderer Teil Band II. Delikte gegen Vermögenswerte. 2. Auflage. Wien: Manz 1988

Kienapfel, Diethelm: Probleme das strafrechtlichen Geldbegriffs. ÖJZ 1986, 423

Schmölzer, Gabriele: Das neue Computer-Strafrecht (Strafrechtsänderungsgesetz 1987). EDVuR 1988 H 1, 20

Seiler, Robert: Kritische Anmerkungen zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JBl 1989, 746

Sonntag, Michael: Cybrer-Crime-Konvention – Störung der Funktionsfähigkeit und widerrechtlicher Zugriff. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther, Liebwald, Doris (Hg.): Zwischen Rechtstheorie und e-Government. Wien: Verlag Österreich 2003, 437-444

Triffterer, Otto: StGB Kommentar

[684] In Deutschland schärfer: Eingabe einer Personalausweis- oder Kreditkartennummer ist nicht ausreichend, um Minderjährige fernzuhalten. OLG Düsseldorf 24.5.2005, I-20 U 143/04 http://www.jurpc.de/rechtspr/20050158.htm

Zagler, Wolfgang: Strafrecht. Besonderer Teil. Wien: LAST&CO Verlag 2000
http://www.rechtsverlag.at/Verlagsprogramm/Bucher/Strafrecht/strafrbt.pdf

IX.5.2. Rechtsvorschriften

Cybercrime-Konvention: Convention on Cybercrime, CETS No.: 185
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=8/9/04&CL=ENG

Strafgesetzbuch: Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe

bedrohten Handlungen (Strafgesetzbuch - StGB) BGBl. I Nr. 60/1974 idF BGBl. I 56/2006

Verbotsgesetz: Verbotsgesetz 1947 StGBl. Nr. 13/1945 idF BGBl. Nr. 25/1947

Pornographiegesetz: Bundesgesetz vom 31. März 1950 über die Bekämpfung unzüchtiger Veröffentlichungen und den Schutz der Jugend gegen sittliche Gefährdung. BGBl. Nr. 97/1950 idF BGBl. Nr. 599/1988

Abbildungsverzeichnis

Stichwortverzeichnis

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z