Der europarechtliche Rahmen für die Informationsgesellschaft

Master These
zur Erlangung des akademischen Grades
„Master of Advanced Studies (European Law)“

im Rahmen des EURO-JUS
Universitätslehrganges für Europarecht
an der Donau Universität Krems

Mag. René Tritscher

Jänner 2000

Inhaltsverzeichnis

1. EINLEITUNG

In jüngster Zeit sind Schlagwörter wie „Electronic Commerce“, „Internet“, „Cybercash“ und „Informationsgesellschaft“, in aller Munde. Kaum vergeht ein Tag, an dem nicht über neue technische Entwicklungen im Bereich des Internet in den Medien berichtet wird.

Die - sich enorm rasch vollziehenden - technischen Entwicklungen in diesem Bereich werfen für den Juristen jedoch diverse Fragestellungen auf. Ein Handlungsbedarf in juristischer Hinsicht wurde in der Lehre bereits in zweifacher Hinsicht geortet. Einerseits sind Juristen zu einer engeren Zusammenarbeit mit Technikern aufgerufen[1] und andererseits wurden Regelungsdefizite im bestehenden Normenbestand aufgezeigt und die Gesetzgeber auf nationaler und internationaler (insbesondere europäischer) Ebene zur Erarbeitung von entsprechenden - möglichst harmonisierten - Regelungen aufgefordert.[2]

Offene Fragen im Zusammenhang mit den neuen Medien bestehen in nahezu allen Rechtsbereichen wie dem Urheberrecht, Markenschutzrecht, Steuerrecht, Arbeitsrecht, Datenschutzrecht, Verbraucherschutzrecht oder dem Internationalen Privatrecht.

In der Tat ist es in jüngster Zeit zur Verabschiedung einer Fülle von gesetzlichen Regelungen in diesen Bereichen sowohl auf nationaler, aber insbesondere auf europäischer Ebene

---

[1] *Laga*, Neue Techniken im World Wide Web - Eine Spielwiese für Juristen?, JurPC Web-Dok. 25/1998, Abs 1-50. Im Internet unter http://www.jura.uni-sb.de/jurpc/aufsatz/19980025.htm .

[2] Zuletzt *Fallenböck*, Pannenstreifen der Datenautobahn, Die Presse vom 16.2.1999, 12. Auch in verschiedenen Studien über das Kaufverhalten der österreichischen Konsumenten im Internet werden die noch ungeklärten rechtlichen Aspekte im elektronischen Geschäftsverkehr als Hindernis für die weitere Verbreitung des elektronischen Handels gesehen. Vgl dazu beispielsweise die Studie von *Regioplan*, Virtuelles Shopping in Österreich (1998) 74.

gekommen. Ein Teil dieser Normen befinden sich noch im Entwurfsstadium, teilweise sind sie bereits geltendes Recht. Als Motor der Regulierung des elektronischen Geschäftsverkehrs ist die Europäische Union, insbesondere die Europäische Kommission anzusehen.

Ziel der vorliegenden Arbeit ist es einen Überblick über die europarechtlichen Bestimmungen betreffend den elektronischen Geschäftsverkehr zu bieten. Punktuell wird eine Beschreibung der nationalen und internationalen Bestimmungen vonnöten sein.

Im 1.Teil der Arbeit wird versucht eine brauchbare Definition des Begriffes „elektronischer Handel“ zu erarbeiten um danach die wirtschaftliche Bedeutung des elektronischen Geschäftsverkehrs und die Zukunftsprognosen zu beleuchten.

Da in der Lehre bereits ausführliche allgemeine Abhandlungen zur rechtlichen Problematik im elektronischen Geschäftsverkehr, insbesondere im Internet verfasst wurden, soll im 2.Teil nur ein Überblick über die rechtlichen Problemfelder beim elektronischen Geschäftsverkehr gegeben werden.

Der Hauptteil der Arbeit beschäftigt sich mit den aktuellen Regelungsvorhaben auf europäischer Ebene, wobei speziell Fragen des Datenschutzes, des Verbraucherschutzes und der digitalen Signatur behandelt werden. Dies deshalb, da einerseits von der Regulierung dieser Bereiche wesentlich die weitere Entwicklung des elektronischen Geschäftsverkehrs abhängen wird und andererseits in diesen Bereichen jüngst Richtlinien auf europäischer Ebene verabschiedet wurden.

Dieser Teil wird ergänzt durch die Behandlung der E-Commerce Richtlinie. Dabei wird vor allem untersucht, ob diese Regelung einen einheitlichen europäischen Rahmen für den elektronischen Geschäftsverkehr bieten kann.

In einer Zusammenfassung wird der derzeitige acquis communautaire im Bereich des elektronischen Geschäftsverkehrs bewertet und ein Ausblick für das Jahr 2000 gegeben.

2. DER ELEKTRONISCHE HANDEL (ELECTRONIC COMMERCE)

2.1 GESELLSCHAFTLICHE AUSWIRKUNGEN

Die Gesellschaft befindet sich in einem Wandel, der von der Europäischen Kommission bereits mit den Umwälzungen zur Zeit der industriellen Revolution verglichen wird.[3] Die Industriegesellschaft entwickelt sich seit den achtziger Jahren zunehmend zu einer Dienstleistungsgesellschaft. Nunmehr stehen wir an der Schwelle zur sogenannten **„Informationsgesellschaft“**.

Der Begriff „Informationsgesellschaft“ wurde bereits in den siebziger Jahren vor allem in der Sozialwissenschaft verwendet.[4] In der Wirtschaftspolitik wird von sogenannten „wissensbasierten Volkswirtschaften“ gesprochen.[5] Das Wissen und die Information an sich werden zur bedeutenden Handelsware, verarbeitete Daten und Medieninhalte stehen im Mittelpunkt des Interesses.

In der Wirtschaft spricht man von Phänomenen wie der Konvergenz, der Telematik und neuerdings auch vom Begriff „TIMES“. Darunter versteht man das Zusammenwachsen der Bereiche Telekommunikation, Informationstechnologie, Medien und Unterhaltung, ergänzt um den Aspekt der Sicherheit.[6]

---

[3] Broschüre der Europäischen Kommission, Die Informationsgesellschaft, Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften (1996) 3. Darin betont die Kommission, dass „die Welt von der dritten industriellen Revolution erfasst worden ist“.

[4] *Touraine*, Die postindustrielle Gesellschaft (1972); *Bell*, The Coming of the Post Industrial Society (1973).

[5] *Knoll*, Informationsgesellschaft als Aufgabe wirtschaftspolitischer Initiative, Wirtschaftspolitische Blätter 2-3/1998, 119 ff.

[6] *Martos*, „Time“ - 4 Branchen verschmelzen, Die Presse vom 26.2.1999, 23. Die Europäische Kommission hat zu diesem Thema das Grünbuch zur Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und

Diese gesellschaftlichen Änderungen haben nicht nur Auswirkungen auf die Wirtschaft, sondern auch auf andere Bereiche des gesellschaftlichen Lebens. Die soziologischen Auswirkungen werden sehr unterschiedlich bewertet wobei von den Skeptikern vor allem die Überflutung des einzelnen mit Informationen und die Vereinsamung des Individuums beklagt werden.[7]

Neue Arbeitsformen sind im Entstehen, die vieles in der traditionellen Organisation und Struktur der Arbeitswelt verändern werden.[8] Die Struktur der Aus- und Weiterbildung[9] unterliegt ebenso einem Veränderungsprozeß wie das Verhältnis des Staatsbürgers zu den Behörden.[10]

Die neuen Medien werden daneben auch fundamentale Auswirkungen auf die Staatsform der Demokratie generell, der demokratischen Mitbestimmung und der politischen Willensbildung im besonderen haben.[11] So wird beispielsweise in der Schweiz bereits über

---

ihren ordnungspolitischen Auswirkungen, KOM(97) 623, verfasst. Im Internet unter http://www.ispo.cec.be/convergencegp/97623de.doc. Einen Überblick über das Grünbuch und die Ergebnisse des Konsultationsprozesses bietet *Wessely*, Das EG-Grünbuch Konvergenz, Medien und Recht 1998/4, 175. Vgl zum Begriff „Konvergenz“ *Laga*, Rechtsprobleme im Internet (1998) 62.

[7] Vgl jüngst *Morton*, Kugel im Nichts, Die Presse vom 13.3.1999, III und *Jochum*, Wohin mit all den Infos ?, Die Presse vom 12.7.1999, III.
Einen schematischen Überblick über die vielfältigen Auswirkungen der Informationsgesellschaft bieten *Rübig*, Die Informationsgesellschaft - Die Zukunft im Griff, in *Kaspar/Rübig*, Telekommunikation, 56 und *Bruck/Selhofer/Winkler*, Österreich in der Informationsgesellschaft, Wirtschaftspolitische Blätter 5/1999, 411 (413).

[8] *Weinzierl*, Die Arbeitswelt in der Informationsgesellschaft, Wirtschaftspolitische Blätter 2-3/1998, 201.

[9] Eine Beschreibung des Projektes einer virtuellen Wirtschaftsuniversität Wien findet sich bei *Scheidl*, Studieren per Mausklick, Die Presse vom 13.3.1999, X. Zu den Veränderungen durch die neuen Medien im Schul- und Universitätsbereich jüngst *Glotz*, Alt schauen wir aus, Herr Kollega!, Die Presse vom 25./26. September 1999, I.

[10] Vgl den Bericht „Eine Informationsgesellschaft für alle“ einer Gruppe hochrangiger Experten im Auftrag der Generaldirektion V. Im Internet unter http://www.ispo.cec.be/hleg/hleg.html.

[11] Vgl jüngst *Postman*, Vorsicht vor Optimisten, Die Presse vom 24./25.7.1999, I.

eine Abstimmung via Internet bei Wahlen und Volksabstimmungen nachgedacht.[12]

Nach Ansicht von schweizerischen Wissenschaftern der Technische Hochschule Zürich werden in zehn bis fünfzehn Jahren Wahlen und sonstige Abstimmungen ausschließlich über das Internet durchführbar sein. Durch die rasche technische Entwicklung wird eine sichere Durchführung der Internet-Wahlen möglich sein.[13]

In den USA wird der Wahlkampf für die kommenden Wahlen zu einem sehr bedeutsamen Teil bereits im Internet geführt. Die Instrumente reichen von E-Mail Kampagnen bis zu eigenen websites vieler amerikanischer Politiker.[14]

2.2 DEFINITION

Der Transformationsprozess von der Dienstleistungs- zur Informationsgesellschaft äußert sich in der **Digitalisierung aller Unternehmensbeziehungen**.[15] Seit kurzem ist dafür der Begriff **„Electronic Commerce“** in aller Munde obwohl wirtschaftliche Tätigkeiten bereits seit vielen Jahren über elektronische Verbindungen durchgeführt werden. Unter den Begriff „Electronic Commerce“ fallen mehrere Arten der Anwendung des elektronischen Datentransfers.[16]

Einerseits wird darunter der Austausch von Daten und Informationen zwischen selbständigen Unternehmen sowie die interne Kommunikation innerhalb eines einzelnen Unternehmens verstanden (**business to business - relation**). Diese Definition ist auf die Beziehungen zwischen Unternehmen bzw. innerhalb eines Unternehmens beschränkt[17].

---

[12] „Wahlen per Mausklick“, Die Presse vom 6.3.1999, 5.

[13] Im Internet unter http://www.pte.at/show.pl.cgi?pta=990914019.

[14] Zuletzt *Borrus*, on the stump – online, Business Week, 12.4.1999, 40.

[15] *Bruck/Selhofer/Winkler*, Wirtschaftspolitische Blätter 5/1999, 415.

[16] Zu den verschiedenen Interpretationen des Begriffes "Electronic Commerce" seitens der Kommission vgl im Internet unter http://www.ispo.cec.be/ecommerce/answers/what.html.

[17] Studie „Electronic Commerce – Status Quo und Perspektiven“ der *KPMG Unternehmensberatung GmbH*, Deutschland (1997). Electronic Commerce wird

Andererseits wird unter „Electronic Commerce“ auch die Beziehung zwischen Unternehmen und Endverbrauchern, also Konsumenten verstanden (**business to consumer - relation**).
Damit fallen eine Vielzahl von geschäftlichen Transaktionen unter diesen Begriff, wie beispielsweise Internet-Dienste, Online-Shopping, E-Mail, Intranet oder Extranet.[18]
Die gebräuchlichsten Internet-Dienste sind zur Zeit Electronic Mail, das World Wide Web, File Transfer Protocol (FTP), Telnet, Usenet inklusive Newsgroups, Internet Relay Chat (IRC), Voice over IP sowie Videokonferenzen.[19]
Auch der elektronische Datenaustausch zwischen Unternehmen und Verwaltung (**business to administration - relation**) und jener zwischen Verwaltung und Bürger (**administration to consumer - relation**) sind Ausprägungsformen des Electronic Commerce.[20]
Im Bereich „E-Government“ ist international der Trend festzustellen, dass häufig Formulare zum Download

---

darin als „ein Konzept zur Nutzung von bestimmten Informations- und Kommunikationstechnologien zur elektronischen Integration und Verzahnung unterschiedlicher Wertschöpfungsketten oder unternehmensübergreifender Geschäftsprozesse“ bezeichnet.

[18] Einen Überblick der Transaktionen, die unter den Begriff „Electronic Commerce“ subsumiert werden können, findet sich im Handbuch EDI und INTERNET, Hrsg Austria Pro - Wirtschaftskammer Österreich (1998) 5.
Der business to business Bereich nutzt eine spezielle Form des Internet – das Extranet. Darunter versteht man einen nicht öffentlich zugängigen, mittels Zugangsberechtigung geschützten Teil des Internets, der mit internen Netzen mehrerer Unternehmen („Intranets“) verbunden ist. Auf den Server des Extranets können bestimmte ausgewählte Personengruppen zugreifen. Beispielsweise können Händler auf die Datenbanken ihrer Lieferanten zugreifen und Waren online bestellen.
Das Intranet kann dagegen ausschließlich von Mitarbeitern des jeweiligen Unternehmens verwendet werden.

[19] Vgl. dazu ausführlich das Handbuch EDI und INTERNET, 5; *Laga*, Internet, 29.

[20] Im Internet unter http://www.edi.at/kapitel2.htm. Diese beiden Formen des Electronic Commerce werden auch als „E-Government“ bezeichnet. Einen Überblick über Anwendungsbereiche und Typen von elektronischen Diensten in diesem Bereich bieten *Aichholzer/Schmutzer*, Informations- und Transaktionsdienste im Bereich der öffentlichen Verwaltung, Wirtschaftspolitische Blätter 5/1999, 456 (457).

bereitgestellt werden, jedoch selten die Möglichkeit der elektronischen Einreichung besteht, wobei der Bereich des Steuerwesens noch am weitesten entwickelt ist. Ein Bedarf der Bürger an elektronischen Transaktionsdienstleistungen wurde bereits in verschiedenen Studien festgestellt.[21]

Das entspricht auch dem Stand in Österreich. In Österreich ist das ehrgeizige Projekt eines elektronischen Amtshelfers in der Umsetzungsphase. Ziel ist es, den Bürgern eine möglichst große Anzahl an Behördenkontakten auf elektronischem Weg anzubieten.[22] Auch die Stadt Wien plant in Zukunft vermehrt die Antragstellung in Verwaltungsverfahren in elektronischer Form abzuwickeln.[23]

Die Bundesregierung hat in einer Absichterklärung vom 7. September 1999 den Willen deklariert auch die Kommunikation zwischen Wirtschaft und öffentlicher Verwaltung mittels Electronic Data Interchange (EDI) zu verbessern. Über speziell gesicherte Netzwerke sollen Aufträge, Bestellungen, Rechnungen, Zoll- und Finanzformulare sowie Banktransfers in digitaler Form ausgetauscht werden.[24]

Auch in Deutschland soll die Vision des allzeit vernetzten Bürgers mit einem „digitalen Rathaus“ bald Realität werden. Das deutsche Bundesministerium für Bildung, Wissenschaft und Forschung fördert konkrete Projekte zur Verwirklichung von elektronischen Amtsgeschäften. Ein zentrales Element ist die Entwicklung von multifunktionalen Bürger-Chipkarten.[25]

Der Begriff „elektronischer Handel“ wird daher nicht nur die bloße Übermittlung von Daten zwischen Unternehmen über Netzwerke umfassen, sondern auch „kommerzielle Aktivitäten,

---

[21] *Aichholzer/Schmutzer*, Wirtschaftspolitische Blätter 5/1999, 463.

[22] Im Internet unter http://www.help.gv.at.

[23] Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=991103031 und http://www.wien.gv.at.

[24] Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=990914012. Eine empirische Bestandsaufnahme der Informationsangebote auf Bundesebene findet sich in der Studie der *Akademie der Wissenschaften*. Im Internet unter http://www.oeaw.ac.at/ita/ebene2/d2-1htm.

[25] Im Internet unter http://www.bmbf.de.

auf globaler Ebene mit einer sich ständig erhöhenden Anzahl von kommerziellen und privaten Teilnehmern“ mit einschließen.[26] Unterschieden werden verschiedene Arten des elektronischen Handels. Beim **„indirekten“ elektronische Handel** wird eine Ware auf elektronischen Weg bestellt um dann per Post zum Kunden gebracht zu werden. Einen Schritt weiter geht der **„direkte“ elektronische Handel**, wo beide Schritte bereits elektronisch abgewickelt werden. Beispiele dafür sind das Teleshopping oder Telebanking. Erst diese Form des Handels nutzt die Vorteile von Electronic Commerce zur Gänze aus: 24 Stunden Service, reduzierte Vertriebs- und Servicekosten, Unterstützung aller Phasen der Geschäftsabwicklung von der Anbahnung bis zur Nachbetreuung der Kunden.

2.3 WIRTSCHAFTLICHE BEDEUTUNG

Die Bedeutung des Electronic Commerce hat in jüngster Zeit – nicht zuletzt durch die Entwicklung des Internets - weltweit enorm zugenommen. Daher ist es wenig verwunderlich, dass das Thema Internet mittlerweile auch in Österreich von der Politik zur Chefsache erklärt wurde. Bundeskanzler Klima hat am 14.7.1999 die Initiative „Österreich ans Internet“ gestartet. Ziel dieser Maßnahme ist eine möglichst große Zahl von Österreichern von der wachsenden Bedeutung der Informationstechnologien zu überzeugen und ihnen die Vorteile der elektronischen Abwicklung von Bankgeschäften, Behördenwegen, Einkäufen etc. näher zu bringen.[27] Im Folgenden werden die volkswirtschaftlichen Auswirkungen, die Bedeutung für einzelne Sektoren und Branchen sowie die Auswirkungen der neuen Technologien auf einzelne Unternehmen untersucht.

[26] Nach *Laga*, Internet, 52 hat sich das Netzwerk von einem reinen Mittel zur Übertragung von Daten zu einem Marktplatz entwickelt.

[27] Im Internet unter http://www.austria.gv.at.

2.3.1 Volkswirtschaftliche Auswirkungen

Bereits im Juni 1994 warnte der damalige Kommissar Martin Bangemann im sogenannten **Korfu Bericht**, dass „Die ersten Länder, welche bewusst in die Informationsgesellschaft eintreten, werden den größten Nutzen daraus ziehen. Sie werden die Agenda für die erst später folgenden festlegen. Länder, die diesen Schritt zögerlich und halbherzig tun, könnten in weniger als einem Jahrzehnt mit einer desaströsen Abnahme der getätigten Investitionen und massiven Jobproblemen konfrontiert werden.“ Tatsächlich zeigen verschiedene Untersuchungen weltweit den enormen Einfluss der neuen Medien auf den Wohlstand einer Gesellschaft.[28]

Die jüngste Studie der Marktforschungs- und Beratungsfirma Giga Information Group „Sales Revenues just the tip of the Electronic Commerce Economic Iceberg“[29] prognostiziert, dass bereits in drei Jahren in den Industrienationen ein Drittel aller wirtschaftlichen Vorgänge durch das Internet oder im Zusammenhang mit dem Internet abgewickelt werden.

Die Auswirkungen der neuen Medien auf die Beschäftigung und den Arbeitsmarkt sind weltweit enorm. Der Bericht des Verbandes der amerikanischen Elektronikindustrie, der American Electronics Association (AEA) zeigt, dass in den **USA** seit 1993 eine Million Arbeitsplätze im Bereich der Informationstechnologie geschaffen wurden und die Zahl der Arbeitnehmer in dieser Branche 1998 bereits auf knapp fünf Millionen angewachsen ist.[30] Die High-Tech Industrie ist in den USA einer der größten Wirtschaftszweige des Landes. Das Durchschnittseinkommen der Angestellten dieser Branche liegt um achtzig Prozent über jenem der Mitarbeiter der übrigen

---

[28] Eine detaillierte Analyse der Auswirkungen des Internets auf die gesamte Volkswirtschaft findet sich im Bericht des *European Communication Council*, Die Internet-Ökonomie - Strategien für die digitale Wirtschaft, European Communication Council Report (1999).

[29] Im Internet unter http://www.gigaweb.com/marketing/news_releases.stm.

[30] Im Internet unter http://www.aenet.org.

Privatwirtschaft. Diese Arbeitsplätze stellen daher hochbezahlte qualifizierte Jobs dar.

Allein die Internet-Wirtschaft beschäftigt laut einer Studie der Universität von Texas bereits 2,3 Millionen Arbeitnehmer und erwirtschaftete im Jahr 1998 301 Milliarden US-Dollar. Ein Drittel dieser Unternehmen wurde erst nach 1996 gegründet.[31]

Dasselbe Bild ergibt ein Blick auf die Mitgliedstaaten der **Europäischen Union**. Der Bericht der Kommission an den Rat „Beschäftigungsmöglichkeiten in der Informationsgesellschaft – Nutzung des Potentials der Informationsgesellschaft“[32] zeigt, dass der Sektor der Informationstechnologie den dynamischsten Wirtschaftszweig der EU darstellt und bereits fünf Prozent des BIP erwirtschaftet. Darüber hinaus sind bereits über 4 Millionen Menschen in diesem Sektor beschäftigt. In der Zeit zwischen 1995 und 1997 wurden über 300.000 neue Arbeitsplätze geschaffen.

Auch in **Österreich** sind positive Auswirkungen der neuen Geschäftsfelder auf den Arbeitsmarkt erkennbar. Nach der jüngsten Studie von Arthur D. Little 'Jobmaschine Telekom', die auf Basis von Interviews mit 24 Telekom-Experten im Juli 1999 durchgeführt wurde, hat die Telekom-Liberalisierung in den letzten beiden Jahren zu einem direkten Beschäftigungseffekt von 6000 neuen Arbeitsplätzen geführt. Der Telekommunikationssektor (Festnetz, Telekom-Equipment-Industrie, Mobilfunk, Internetprovider, Kabel-TV sowie Mehrwertdienste) beschäftigt heute in Österreich bereits 42.264 Personen.[33]

Die elektronischen Märkte werden die gesamte Wirtschaftsstruktur der Volkswirtschaften verändern, insbesondere dadurch, dass sie zu erhöhter Markttransparenz

---

[31] Die Presse vom 29.10.1999, 29.

[32] KOM (98) 590 endg. Im Internet unter http://www.europa.eu.int/comm/dg05/soc-dial/info_soc/jobopps/joboppde.pdf.

[33] Im Internet unter http://www.bmwa.gv.at/presse/2462.htm.

führen, was wiederum zu einem branchenweiten Preisverfall führen könnte.[34]

Die **Zukunftsprognosen** für den Electronic Commerce werden von Experten äußerst optimistisch eingeschätzt.[35]

Dieses rasante Wachstum des Electronic Commerce und die optimistischen Zukunftsprognosen führen zu einem harten Kampf um Marktanteile im World Wide Web. In diesem Zusammenhang kommt es immer wieder zu Fusionen und Firmenübernahmen im größeren Ausmaß. Ende des Jahres 1998 übernahm der amerikanische Internetprovider America Online die Softwarefirma Netscape um gegen den Mitbewerber Microsoft gerüstet zu sein.[36]

Nach einer Studie von Forrester Research wurde 1998 in den **USA** von online Händlern bereits ein Umsatz von 13 Milliarden Dollar erzielt.[37] Im Jahr 2000 sollen es bereits 22 Milliarden, 2003 108 Milliarden Dollar sein.

Auch in der **Europäischen Union** nimmt die Bedeutung des Electronic Commerce jährlich zu. Der Umsatz lag 1997 schon bei immerhin 36 Millionen Dollar, 1998 bereits bei 128 Millionen Dollar. Die OECD schätzt den Umsatz in Europa für das Jahr 2000 bereits auf 730 Millionen Dollar.[38]

---

[34] *Bakos*, A Strategic Analysis of Elektronik Marketplaces, MIS Quaterly 15, 294.

[35] Zahlreiche Studien bescheinigen dem Internet und dem Electronic Commerce ein gewaltiges Wachstumspotential. Beispielsweise die jüngste Studie von *Nielsen Media*, im Internet unter http://www.nielsen.com.
Die Zukunftsszenarien für die Entwicklung der Umsätze im elektronischen Geschäftsverkehr weichen zum Teil jedoch erheblich voneinander ab. Zur Entstehung von Electronic Commerce Prognosen vgl im Internet unter http://www.heise.de/tp/deutsch/inhalt/te/1655/1.html.
Eine gute Übersicht über statische Daten betreffend den elektronischen Geschäftsverkehr findet sich in der Publikation des *deutschen Handelsverbandes*, Informationen für den Handel, Sonderausgabe Electronic Commerce, 1-2/99.

[36] Vgl ausführlich *Neuhold*, Die Schlacht ums Internet, Format 9/98, 92.

[37] Im Internet unter http://www.forrester.com.

[38] Im Internet unter http://www.oecd.org/dsti/sti/it/ec/prod/dismantl.htm.

Im Jahr 2002 sollen die Umsätze weltweit im Electronic Commerce bereits etwa 3.200 Milliarden Dollar betragen. Das wären bereits fünf Prozent der weltweit getätigten Handelsumsätze.[39]

Ein Ländervergleich macht die ungeheure **Dominanz der USA** im elektronischen Geschäftsverkehr deutlich. Der größte Anteil des Umsatzes entfällt auf die Vereinigten Staaten, auf Platz 2 liegt Deutschland, gefolgt von Großbritannien.[40] Nach Studien von Nielsen media steigt die Bedeutung des Electronic Commerce jedoch auch in Lateinamerika und der EU.

In der Europäischen Union werden bis 2004 etwa 8 Millionen Dollar im Electronic Commerce umgesetzt werden.[41] In den USA soll der Internet Markt von 8 Milliarden Dollar im Jahr 1997 auf 17 Milliarden 1998 und 327 Milliarden im Jahr 2002 wachsen.[42]

Im Jahr 2002 werden bereits 70 Prozent der weltgrößten Unternehmen das Internet als Verkaufsplattform nutzen. Dabei werden 850 Milliarden in den USA erwirtschaftet, 250 Milliarden in der EU und 50 Milliarden im asiatisch pazifischen Raum.[43]

Heute nutzen bereits **92 Millionen Menschen** weltweit das Internet. Die Steigerungsraten sind enorm. Anfang 2000 werden es bereits 130 Millionen Menschen sein. Auch in Österreich verfügen bereits über 30 Prozent der Bevölkerung über einen

---

[39] Im Internet unter http://www.forrester.com. Zu ähnlichen Ergebnissen gelangen Untersuchungen der *International Data Corporation* (unter http://www.idc.com), *Activmedia* (unter http://www.activmedia.com) und *Deloitte Consulting* (unter http://www.dc.com).
Noch optimistischer ist eine Untersuchung der Marktforschungs- und Beratungsgesellschaft *Giga Information Group* (unter http://www.gigaweb.com).

[40] Im Internet unter http://www.nielsen.com und http://www.emarketer.com/estats/sell_eglob.html .

[41] Internationale Wirtschaft, 4.2.1999, 29.

[42] Im Internet unter http://www.forrester.com.

[43] Vgl zum folgenden im Internet unter http://www.dc.com, http://www.nielsen.com, http://www.emarketer.com/estats/sell_eglob.html, http://www.ispa.at und http://www.c-i-a.com/199908iu.htm.

Zugang zum Internet.[44] Im Jahr 2002 werden etwa 200 Millionen Menschen weltweit das Internet regelmäßig nutzen, für 2005 werden bereits weltweit 717 Millionen Nutzer prognostiziert.

Die Verteilung auf die verschiedenen Staaten und Weltregionen wird jedoch höchst unterschiedlich sein. Die USA haben die höchste Dichte an Internet Nutzern. Bereits 64 Millionen US-Amerikaner nutzen regelmäßig das Internet. Ende 1998 waren noch mehr als die Hälfte der Internet-Nutzer US-Amerikaner oder Kanadier. Asien und Europa holen jedoch seit kurzem rapide auf. Nach der Studie "eGlobal Report" des amerikanischen Marktforschers *emarketer* wird der Anteil der USA um die Jahrtausendwende erstmals unter 50 Prozent sinken. Bis 2002 werden sich die Prozentzahlen noch weiter annähern: Die USA werden mit 98,1 Millionen User ein Drittel der Internet-Nutzer stellen, dahinter Europa (29,9 Prozent) und Asien (21,5 Prozent).

Auch die Verteilung der Internet Nutzer auf die Gesellschaftsschichten ist sehr unterschiedlich. Nach Ansicht der Autoren des United Nations Human Development Reports sind Einkommen, Bildung, Geschlecht und geographische Gegebenheiten die Determinanten der neuen Zweiklassengesellschaft im Internet. Man kann insgesamt von einer sehr **„elitären" Internet-Gesellschaft** aus.[45]

Sowohl was die geographische als auch was die soziologische Verteilung betrifft, kann das Internet daher durchaus als „Villenviertel im globalen Dorf" bezeichnet werden.

Von der Mehrzahl der Nutzer wird das Internet derzeit zur Beschaffung und zum Austausch von Informationen für Beruf, Studium und Freizeit genutzt. Das Internet ist daher als alternative Informationsquelle neben den bestehenden Medien anzusehen und wird daher auch die Medienlandschaft verändern.[46]

---

[44] Studie der Universität Innsbruck unter http://info.uibk.ac.at/fodok/C/41502.html und zuletzt Der Standart vom 17.11.1999 unter http://www.derstandart.at/199991117/374.htm.

[45] Im Internet unter http://futurezone.orf.at/futurezone.orf?read=detail&id=2732&tmp=47027.

[46] Studie der *ISPA* unter http://www.ispa.at.

Nach Schätzungen von Nielsen media kaufen derzeit in den USA 28 Millionen Menschen online ein. Viele suchen zwar online nach Produktinformationen, kaufen dann trotzdem offline ein.[47]
Insgesamt prognostizieren alle Untersuchungen eine dauerhafte Dominanz der USA im Elektronischen Handel, jedoch einen Aufholprozess Europas bei IT Infrastrukturen und privater und geschäftlicher Nutzung des Electronic Commerce. 72 Prozent der websites sind derzeit dort beheimatet und 92 Prozent der Electronic Commerce-Aktivitäten gehen von US amerikanischen Sites oder ihren Ablegern aus. Man kann daher abschließend feststellen, dass „zwar noch nicht der Rubel, jedoch bereits der Dollar im Internet rollt“[48]
Gründe für die Dominanz der USA in diesem Bereich und der Überlegenheit gegenüber Europa sind die vergleichsweise niedrigen Telefongebühren, Infrastrukturkosten, aber auch kulturelle Gründe und unterschiede in den Steuersystemen der EU-Mitgliedstaaten.[49]

2.3.2 Auswirkungen für Wirtschaftszweige und einzelne Unternehmen

Die oben beschriebene rasante Entwicklung des Internet und die Wachstumsraten des Electronic Commerce haben nicht nur volkswirtschaftliche Bedeutung. Für einzelne Unternehmen und ganze Branchen sowohl im Industrie- als auch im

---

[47] Studie des Marktforschers *Harris Interactive* unter http://www.ecommercepulse.com.

[48] *Steuerer*, Wenn sich das Geld auflöst, Die Presse vom 11.7.1998, VIII.

[49] *Wallace*, Why are Europeans still so cool to E-Commerce, Fortune Dezember 1998 21, 65 und die jüngste Studie des Marktforschungsinstitutes *Datamonitor*, European business Internet service markets. Im Internet unter http://www.datamonitor.com/dmhtml/tc/tcwtsnew.htm.
Erst jüngst hat die Kommission kritisiert, dass die Preise für Mietleitungen im grenzüberschreitenden EU-Verkehr sechzehn mal so hoch wie in den USA seien. Im Internet unter http://www.pte.at/show.pl.cgi?pta=991130002.

Dienstleistungsbereich werden sich neue Chancen und Risiken durch den elektronischen Geschäftsverkehr ergeben.

Das elektronische Geschäft wurde bisher primär von Großunternehmen beherrscht. Weitgehend multinationale Unternehmen und Start-up-Companies teilen das Geschäft unter sich auf. Die kleinen und mittleren Unternehmen (KMU) mit Ausnahme von neu gegründeten Internet Unternehmen drohen den Anschluß zu verpassen. Diese haben im elektronischen Geschäftsverkehr kaum nennenswerte Zuwächse im Vergleich zu Großunternehmen. Das Marktforschungs- und Beratungsunternehmen Giga Information Group wertete dies bereits als ein **„Alarmsignal für den Mittelstand“**[50].

Chancen bieten sich im Electronic Commerce jedoch vor allem für kleine und mittlere Unternehmen (KMU). Etliche KMU nutzen das Internet bereits als internationales Vertriebsinstrument. Es besteht der Vorteil, dass Märkte erreicht werden können, auf denen die Einrichtung konventioneller Absatzkanäle finanziell nicht lukrativ erscheinen. Mit relativ geringem finanziellen Aufwand können Kunden weltweit erreicht werden. Im Netz sind alle gleich und auch ein kleines Unternehmen kann mit einem professionell gestalteten Auftritt im Internet positiv auffallen.

Der Electronic Commerce bezieht sich jedoch nicht nur auf das Internet. Unternehmen können auch den Zahlungsverkehr rein elektronisch durchführen, die innerbetriebliche Organisation und Logistik verbessern. Ein Musterbeispiel optimaler Kundenbindung in der Informationsgesellschaft ist die US-amerikanische Buchhandlung Amazon.[51]

Aus einer vom Managementberatungsunternehmen Diebold unter 160 österreichischen Topunternehmen durchgeführten Studie geht hervor, dass in **Österreich** die Unternehmen das Internet derzeit größtenteils als Informations- und

[50] Studie „Sales Revenues just the Tip of the Electronic Commerce Economic Iceberg“. Im Internet unter http://www.gigaweb.com.

[51] Die Presse vom 6.11.1999, 31. Der Geschäftserfolg von Amazon ist zwar bisher katastrophal, die gestiegenen Börsenkurse weisen jedoch auf eine extrem hohe Bewertung des Unternehmens durch die Investoren hin.

Kommunikationsplattform nutzen. 87 Prozent der Unternehmen setzen E-Mails ein, 55 Prozent verfügen über einen eigenen Internet Auftritt. Nur etwa 17 Prozent haben jedoch die Möglichkeit der elektronischen Bestellmöglichkeit für ihre Produkte bzw für die Beschaffung vorgesehen.

Derzeit verfügen etwa **20 Prozent der Unternehmen** in Österreich über einen Internet Zugang. Der Großteil der Unternehmen nutzt das Internet zur Informationsbeschaffung, zur Kommunikation und zur Darstellung des Unternehmens, nur 20 Prozent für den Vertrieb und 14 Prozent für die Beschaffung.[52]

Der Electronic Commerce erfordere jedoch eine grundlegend neue Unternehmensorganisation und sollte von den Unternehmen „als Anlaß für die Optimierung von Unternehmensabläufen“ gesehen werden. Derzeit haben 61 Prozent keine organisatorische Verankerung für den Electronic Commerce im eigenen Unternehmen.[53]

Das Marktforschungsinstitut *Datamonitor* prognostiziert, dass im Jahr 2004 bereits 5,4 Millionen Firmen der EU ans Internet angeschlossen sind. Laut der Studie "European business Internet service markets" sind bisher etwa 2,2 Millionen Unternehmen im Internet vertreten.[54]

Als **Gründe für den Einstieg** in den Electronic Commerce werden von den Unternehmen die folgenden angegeben: Reduktion der Kosten für Beschaffungsprozesse, Lagerhaltung und Kapitalbindung, Margenverbesserung durch Überwindung veralteter Technologien, Optimierung der Kundenbetreuung und Kundenbindung, 24 Stunden verfügbare Informations- und Kommunikationseinrichtungen, raschere Abwicklung von Geschäftszyklen, kürzere Zeiten für Produkteinführungen, Expansion in neue Märkte, Erschließung neuer Kundengruppen und Aufbau neuer Geschäftszweige.

Durch neue Softwareentwicklungen ist es möglich viele der betrieblichen Abläufe über das Internet selbst abzuwickeln

---

[52] Studie von *OGM*, WirtschaftsMonitor, im Auftrag des KSV und des Wirtschaftsblattes.

[53] Studie der Managementberatung *Diebold GmbH*.

[54] Im Internet unter http://www.datamonitor.com.

oder darin einzubinden. In vielen Unternehmen gestaltet sich jedoch die Einbindung bestehender Geschäftsabläufe und IT-Infrastrukturen in das Internet sehr schwierig.[55]

Das Internet wird daher in Zukunft nicht nur als **Informationsmedium** und als **Präsentationsplattform** des Waren- und Dienstleistungsangebotes genutzt werden. Es wird sich zu einem Intranet-System als **Instrument unternehmensinterner Kommunikation**, und einem Extranet-System womit auch Intranets für Geschäftspartner geöffnet werden können, entwickeln. So können auch Kunden, Lieferanten und das eigenen Rechnungswesen den elektronischen Datenaustausch miteingebunden werden.

Risiken treten vor allem dann auf wenn die oben beschriebene Entwicklung von Unternehmen ignoriert wird und keine entsprechenden Schritte gesetzt werden.[56] Der Trendforscher Ludwig Morasch hat jüngst gar prognostiziert, das sich der klassische offline Handel durch das Auftreten des Electronic Commerce innerhalb der nächsten zehn Jahre halbieren werde.[57]

Eine Gefahr für den traditionellen Handel ergibt sich aus einer möglichen **Veränderung im Fluss des Warenstromes** insofern, als Zwischenhändler ausgeschaltete werden können und ein Direktverkauf vom Hersteller an den Endverbraucher ermöglicht wird.[58]

Schon jetzt zeigt ein Blick auf die derzeit im Internet angeboten **Produktpalette**, welche Branchen in Zukunft mit grundlegenden Veränderungen zu rechnen haben. Die im Internet am erfolgreichsten verkauften Produkten sind derzeit überwiegend homogene Produkte, die nicht vor dem Kauf getestet werden müssen, sondern bei denen Produkterfahrung vorausgesetzt wird, und die über einen günstigen Preis

---

[55] *Steuerer*, Nuggets und taube Nüsse, Die Presse vom 27.11.1999, X.

[56] Fortune betitelte die Dezember-Ausgabe 1998 bereits mit der Warnung „Internet or Bust - using the Net to create a whole new way of doing business“.

[57] *Zenker*, „Der klassische Handel wird sich in den nächsten zehn Jahren nahezu halbieren“, Die Presse vom 25.8.1999, 21.

[58] *Brandtweiner*, Entwicklung und Auswirkung elektronischer Märkte, Wirtschaftspolitische Blätter 5/1999, 420 (423).

verkauft werden. Dies sind vor allem EDV-Hardware und Software, Bücher, Musikprodukte, reisen, Flugtickets, Unterhaltungselektronik, Kleidung, Haushaltsgeräte und Sportartikel.[59]

Ein Beispiel für eine Branche im Wandel ist der **Buchhandel**. Schon vor einigen Jahren hat der Auftritt von online - Buchhändlern wie beispielsweise dem amerikanischen Buchhändler amazon.com die Vertriebsstruktur in dieser Branche verändert. Weitere Änderungen wird die Verbreitung von digitalisierten Büchern (e-books) dieser Branche bringen.[60]

Der elektronische Handel wird auch massive Auswirkungen auf den **Kfz-Handel** mit sich bringen. In den USA werden bereits ein Viertel der Neuwagen im Zusammenhang mit dem Internet gekauft. Bereits jedes 30. Fahrzeug direkt über das Netz.[61] Auch in Österreich wird die traditionelle Form des Kfz-Vertriebs in den nächsten Jahren Veränderungen unterworfen sein. Die Branche hat jedoch bereits auf die neuen Herausforderungen reagiert. Seit August 1999 betreibt die Interessensvertretung der österreichischen Kfz-Händler gemeinsam mit dem Unternehmen eurotax eine Internet Plattform zum Verkauf von Neu- und Gebrauchtwagen. Darüber hinaus wird auch die elektronische Kommunikation und Geschäftsabwicklung zwischen Herstellern, Importeuren, Händlern und Endverbrauchern gefördert. Jeder Kfz-Händler hat die Möglichkeit der Präsentation seines Unternehmens auf dieser Plattform. Ziel des Projektes „kfzweb.at“ ist es für die gesamte österreichische Kfz-Wirtschaft eine elektronische Basis zu schaffen.

Auch die Europäische Kommission hat die Bedeutung des Electronic Commerce erkannt und fördert die Nutzung der neuen Technologien durch die europäischen Unternehmen in

---

[59] Studie von Activmedia, Firstsurf (1998). Im Internet unter http://www.wk.or.at/austriapro/layout/ec.htm.

[60] *Kugler*, Bücher aus dem Netz, Lesen ohne Papier: Die „e-books“ kommen, Die Presse vom 22.3.1999, 19; *Klauhs*, Frankfurter Messe: Gier nach Liebe, Geld und dem digitalisierten Buch, Die Presse vom 16.10.1999, 3.

[61] Studie der Marktforschungsgruppe *Gomez Advisors* unter http://www.gomez.com .

vielfältiger Weise.[62] Die Europäische Kommission hat erst jüngst die Initiative „eEurope“ vorgestellt.[63]

Unerläßlich für die weitere Verbreitung wird die Schaffung eines stabilen rechtlichen Rahmens für Transaktionen via Electronic Commerce sein. Als Hemmnis für die weitere Verbreitung des Electronic Commerce werden immer wieder das fehlende Vertrauen der Teilnehmer der Netzwerke in eine sichere Datenübermittlung sowie fehlende, mangelhafte oder unklare rechtliche Rahmenbedingungen genannt.[64]

[62] Vgl beispielsweise das Weißbuch Handel, KOM (99) 6 endg vom 27.1.1999.

[63] Im Internet unter http://europa.eu.int/comm/dg13/com081299_en.pdf .

[64] Beispielsweise *Fallenböck*, Die Presse vom 16.2.1999, 12.

3. RECHTLICHER RAHMEN DES ELEKTRONISCHEN GESCHÄFTSVERKEHRS

Begriffe wie "**Cyberlaw**", "**Netlaw**", "**Internet-Recht**" oder "**Online-Recht**" sind derzeit in aller Munde. Das erweckt den Eindruck, dass es sich dabei um ein völlig eigenständiges Rechtsgebiet handelt.

Mit dem Aufkommen des elektronischen Geschäftsverkehrs stellte sich die Frage, ob Transaktionen über elektronische Netze den bestehenden Rechtsnormen unterliegen. Falls dies nicht der Fall wäre, so mußte ein völlig neues Rechtsgebiet für Transaktionen über das Internet geschaffen werden, ein „Internet Recht“ oder „Electronic Commerce Recht“. Dies ist jedoch nicht der Fall. Weite Teile der Rechtsordnung galten und gelten auch für den Bereich des Electronic Commerce, insbesondere das Internet und damit auch für die maschinenunterstützte Kommunikation und die Datenfernübertragung. Das Internet war daher von Beginn an **kein rechtsfreier Raum**.[65]

Die "neuen Technologien" bedingen jedoch einen **Anpassungsbedarf der nationalen, europäischen und internationalen Rechtsordnungen**, da diese den Herausforderungen durch die technischen Veränderungen vielfach nicht mehr gewachsen sind. Neue, international akkordierte und speziell auf die Anforderungen des Electronic Commerce zugeschnittenen Regelungen sind daher notwendig.

---

[65] Im Internet unter http://normative.zusammenhaenge.at/inhalt.html. Treffend wird hier behauptet, dass vieles was unter "Cyberrecht" verstanden wird "alter Wein in neuen Schläuchen" sei. Für Österreich: *Laga*, Internet im rechtsfreien Raum? (Dissertation Universität Wien, 1998). Im Internet unter http://www.univie.ac.at/juridicum/forschung/laga/cover.html. Für Deutschland: *Strömer*, Online – Recht: Rechtsfragen im Internet und in Mailboxen (1997), 2.

Die Europäische Kommission hat das **Manko der lückenhaften und fehlenden rechtlichen Rahmenbedingungen** für den Electronic Commerce erkannt. *Jörg Wenzel*, Leiter des Aktionszentrums Informationsgesellschaft der Europäischen Kommission hat anläßlich eines Vortrages beim 8.Tag des Handels der EuroCommerce am 13.11.1997 in Brüssel und anläßlich einer Veranstaltung in der Wirtschaftskammer Österreich am 8.6.1998 in Wien betont, der Mangel an Sicherheit sei ein Haupthindernis für die massenhafte Verbreitung des elektronischen Handels. Daneben seien unklare rechtliche Rahmenbedingungen eine weitere wichtige Hürde für das Anwachsen des Electronic Commerce.

Die jüngste Studie des Marktforschungsinstituts *RegioPlan Consulting* sieht in den unausgereiften Zahlungssystemen, regulatorischen Defizite für elektronisch signierte Verträge, unklare rechtliche Aspekte und fehlende Regeln die wesentlichsten Hemmnisse für die Verbreitung des Electronic Commerce in Österreich. [66]

Die Kommission sieht die Rechtsfragen im Zusammenhang mit dem elektronischer Handel **aus globaler Sicht** und ortet daher einen Bedarf an internationaler Zusammenarbeit. Aus diesem Grund hat die Kommission in der Mitteilung „Globalisierung der Informationsgesellschaft – Die Notwendigkeit einer stärkeren Internationalisierung“ die **Schaffung einer internationalen Charta** vorgeschlagen. Darin sollen Grundsätze für Bereiche wie Netzinhalte, Netzsicherheit, Verschlüsselung, Datenschutz, Verbraucherschutz, Internationales Privatrecht und Urheberrecht geregelt werden.[67]

An der Erarbeitung dieses verbindlichen multilateralen Übereinkommens sollen verschiedenen Organisationen wie die UNO, deren Sonderorganisationen, die WTO, OECD, WIPO und der Europarat mitwirken.

---

[66] Studie von *RegioPlan Consulting*, Virtuelles Shopping in Österreich (1998) 73. So auch *Seidenberger*, Internationale Wirtschaft, 4/1999, 20.

[67] KOM(98) 50 endg. Im Internet unter http://www.ispo.cec.be/eif/policy/com9850de.pdf.

Ein erstes Beispiel eines weltweiten Übereinkommens liegt mit dem, unter der Schirmherrschaft der United Nations Commission on International Trade Law (UNCITRAL) erarbeiteten, **Model Law on Electronic Commerce** bereits vor.[68]

Auch die Internationale Handelskammer (ICC) arbeitet zur Zeit an weltweit einheitlichen, nicht verbindlichen Rahmenbedingungen für den elektronischen Handel.[69]

Daneben hat auch die **OECD** jüngst **Richtlinien** für den elektronischen Handel veröffentlicht, die sich schwerpunktmäßig mit dem Verbraucherschutz beschäftigen.[70]

Bislang ist die Europäische Union, insbesondere die Kommission als Motor der Verrechtlichung des Electronic Commerce anzusehen.[71] Sie hat sich in einer Vielzahl an Initiativen durch Grundsatzdokumente und sekundärrechtlichen Bestimmungen allgemeiner und themenbezogener um einen einheitlichen europäischen Rechtsrahmen für die Entwicklung der Informationsgesellschaft bemüht.

Schon 1996 wurde der Aktionsplan "Europa als Wegbereiter der globalen Informationsgesellschaft: Dynamischer Aktionsplan"[72] verabschiedet.

Gestützt auf diesen Aktionsplan und andere Vorarbeiten der Kommission[73] hat die Kommission am 16. April 1997 in der

---

[68] Darin finden sich vor allem Klärungen von Definitionen, rechtlicher Wirkungen, Schriftform- und Unterschriftenerfordernisse für digitale von elektronischen Nachrichten. Vgl. dazu näher *Riedl*, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, ecolex 4/1999, 241. Im Internet unter http://www.uncitral.org/en-index.htm.

[69] Die ICC hat dazu die Arbeitsgruppe „Electronic Trade Practices" gegründet, von der im Oktober 1999 ein Entwurf für die ICC Uniform Rules on Electronic Trade Settlement (URETS) vorgelegt wurde. Im Internet unter http://www.iccwbo.org/home/menu_electronic_commerce.asp.

[70] Im Internet unter http://www.oecd.org/news_and_events/release/guidelinesconsumer.pdf.

[71] *Laga*, Internet 81; *Brenn*, Der elektronische Geschäftsverkehr, ÖJZ 13/1999, 481 (490).

[72] KOM(96) 607 vom 27.11.1996. Im Internet unter http://www.ispo.cec.be/infosoc/legreg/rollcomm.html.

[73] Vgl. vor allem die Mitteilungen "Normung und die globale Informationsgesellschaft", KOM(96) 359 endg. vom 24.7.1996; "Lernen in der

Mitteilung „Europäische Initiative für den elektronischen Geschäftsverkehr“ die Schaffung eines günstigen ordnungspolitischen Rahmens für den elektronischen Geschäftsverkehr angekündigt.[74]

Da Auswirkungen des elektronischen Geschäftsverkehrs auf nahezu alle Lebensbereiche (wie Arbeit, Bildung, Freizeit) bestehen hat die Kommission für verschiedenste Regelungsbereiche im Zusammenhang mit dem Electronic Commerce bereits europarechtliche Regelungen erlassen oder bereitet diese vor.

In der Mitteilung „Globalisierung der Informationsgesellschaft“ hat die Kommission **die Notwendigkeit eines kohärenten rechtlichen Rahmens im Online-Bereich** für folgende Bereiche bekräftigt: Steuerrecht (insbesondere indirekte Steuern), Zivilprozessrecht (Gerichtsstand), Arbeitsrecht, Urheberrecht, Datenschutz (Schutz personenbezogener Daten), Markenrecht, Sicherheit und Authentifizierung (insbesondere Kryptographie und digitale Signatur), Verbraucherschutz, Zivilrecht (Haftung für Übermittlungsfehler im Zusammenhang für den Vertragsabschluß, Missbräuche durch die Verwendung falscher/fremder E-Mail Adressen im Bereich des Namensrechts) und Strafrecht (Verbreitung schädigender Inhalte oder Programme über das Internet, Kinderpornographie, nationalsozialistische Wiederbetätigung, Hacking).

Die vorliegende Arbeit kann dieses umfangreiche Spektrum an Rechtsfragen nicht abdecken. Sie konzentriert sich daher auf aktuelle und zentrale Regelungen (insbesondere Richtlinien) im Bereich des Electronic Commerce auf europäischer Ebene.

Informationsgesellschaft - Aktionsplan”, KOM(96) 471; “Illegale und schädigende Inhalte im Internet”, KOM(96) 487 vom 16.10.1996; “Kohäsion und Informationsgesellschaft”, KOM(97) 7 vom 22.1.1997 und die Grünbücher “Leben und Arbeiten in der Informationsgesellschaft”, KOM(96) 389 vom 24.7.1996 und “Jugendschutz und Schutz der Menschenwürde in den audiovisuellen und den Informationsdiensten”, KOM(96) 483 vom 16.10.1996.

[74] KOM(97) 157 endg.

3.1 DATENSCHUTZ IM NETZ

3.1.1 Problematik des Datenverkehrs im elektronischen Geschäftsverkehr und Sicherheitsstrategien

In offenen Netzen besteht die Möglichkeit, Daten dezentral an verschiedenen Stellen zu speichern. Der Datenverkehr kann in einem offenen Netz wie dem Internet an einem beliebigen Ort abgehört und mitgeschnitten werden. Über Internet übertragene Daten können auch durch unbefugte Dritte verändert, gefälscht, verzögert oder unterdrückt werden.

Bei der Nutzung von Internet Diensten bleibt der Benutzer im Regelfall nicht anonym.[75] Anhand der verwendeten E-Mail Adresse oder einer eindeutigen numerischen Adresse des im Internet eingebundenen Rechners (IP-Nummer) können Versender und Empfänger einer Nachricht, Zeitpunkt der Datenübermittlung oder auch der Abruf von Informationen durch einen Benutzer festgestellt werden.[76]

Es besteht daher nicht nur ein Gefährdungspotential für die Vertraulichkeit und Integrität der Daten. Vor allem besteht die Gefahr, dass Datenspuren - ohne Wissen und Einwilligung der Betroffenen - zur Bildung von Kommunikations- und Nutzungsprofilen herangezogen werden.

Die bestehenden Datenschutzbestimmungen sind nur beschränkt geeignet, diesen Gefahren zu begegnen. Die **Notwendigkeit einer Novellierung der bestehenden Datenschutzgesetze** bringt der Bremer Datenschutzbeauftragte *Stefan Walz* auf den Punkt :“Die

---

[75] Das gilt nicht nur für das Internet sondern auch für andere Arten der elektronischen Datenübertragung wie beispielsweise die uncodierte Übertragung von Daten im Rahmen von satelittengesteuerten Sicherheits- und Informationssystemen. *Simoner*, Sicherer im Auto mit Beifahrer „Big Brother“, Der Standart vom 15.3.1999, 9.

[76] *Schallbruch*, Electronic Mail im Internet - Wie steht es mit dem Datenschutz ?, Datenschutz-Nachrichten 5/95, 11. In den USA finden mittlerweile bereits Technologien aus dem Bereich der "künstlichen Intelligenz" Anwendung, um Daten von Anwendern zu erfassen. Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=990928018.

Notwendigkeit für ein neues Gesetz ergibt sich vor allem durch die technologische Entwicklung. Durch die Digitalisierung und Vernetzung der Informationsübertragung werden die traditionellen Grenzen von Computer, Telefon und Fernseher aufgehoben. Ein Beispiel: Beim Kauf einer Zeitung am Kiosk bleibt der Leser anonym. Keiner kann erkennen, welcher Artikel wann und wie lange gelesen wird. Bei Onlinediensten wie AOL oder bei Pay-TV liegt der Fall anders. Wer einen solchen Onlinedienst anwählt, gibt beim Eintritt automatisch seine Visitenkarte ab. Die Bewegungen innerhalb des Dienstes werden dokumentiert. Könnten Kundendaten von Onlinediensten genauso weiterverkauft werden, wie es bei Versandhäusern der Fall ist, entstünden dort ausgefeiltere Benutzerprofile als je zuvor. Hochwertige Verschlüsselungstechnik oder aufladbare Geldkarten sind Beispiele für diese Option. Wo früher die verschiedenen Formen von Information und Kommunikation strikt getrennt waren (Rundfunk - Telefon - Brief), laufen diese Daten bereits heute zum Teil auf einem einzigen Weg zusammen - im Computer. Der PC mutiert langfristig zur großen Datenzentrale für Pay-TV, E-Mail, Bankgeschäfte, Datenverarbeitung, Handel über das Internet oder digitale Verwaltung. Alle Daten rauschen durch die gleiche Leitung. Gleichzeitig wird aber auch der gesellschaftliche Druck immer größer, diese Technik nicht nur zu nutzen, sondern sich mit ihr auseinander zu setzen.“[77]

Die unverschlüsselte Übermittlung von Daten über Netzwerke birgt **Gefahren sowohl für Unternehmen als auch für Privatpersonen**. Von Betriebsspionage, über organisierten Datenhandel bis hin zu ungewollten Eingriffen in die Privatsphäre reicht das Risikopotential.[78]

In jüngster Zeit häufen sich die Beispiele für die Weiterverwendung der Daten von PC- und Internet-Benutzern. Gerade das Internet erscheint ein geeignetes Instrument zu sein, das Kaufverhalten der Benutzer zu erkunden und dann

[77] Im Internet unter http://www.heise.de/tp/deutsch/inhalt/te/1940/1.html .

[78] *Laga*, Internet, 67.

auszuwerten. Durch Cookies beispielsweise wird das Online Verhalten der Benutzer genau aufgezeichnet.[79]

Im März 1999 beispielsweise stand die Firma Microsoft am Pranger der Datenschützer. Durch eine „Fehlfunktion“ im Betriebssystem Windows 98 wurden trotz ausdrücklicher Ablehnung durch die Kunden unerlaubt Identitätsnummern und persönliche Daten der Kunden durch Windows 98 und andere Microsoft Programme an eine Datenbank von Microsoft übermittelt.[80]

Einen Schritt weiter ging Microsoft gemeinsam mit der Deutschen Telekom. In einem Feldversuch verknüpfte die Microsoft Tochtergesellschaft Web-TV mittels einer Settop-Box Fernseh- und Internetdaten der Kunden. So wurden beispielsweise die gesehenen TV-Sendungen, Filme und Internet Adressen sowie Online Bestellungen aufgezeichnet und dieses Interessensprofil noch dazu mit einer digitalen Signatur versehen. Anonyme Daten wurden so zu einem Persönlichkeitsprofil weiterentwickelt.[81]

Auch die Firma Netscape sammelt Daten von Internet Benutzern. Die Version 4.06 des Internet Browsers Netscape beinhaltet die Funktion „Smart Browsing“, die im aktivierten Zustand jede besuchte Internet Adresse (URL) durch den Benutzer automatisch an einen Datenbank Server der Firma Netscape weiterleitet. Dort kommt es zu einem Datenabgleich mit bereits abgespeicherten Daten und dem Benutzer wird ein Vorschlag von

---

[79] Cookies sind Informationen, die vom Informationsanbieter mit Hilfe des Browser auf der Festplatte des Computers des Benutzers abgespeichert werden können, um bestimmte Daten mit dem Computer des Anwenders zu verknüpfen.
Eine klassische Anwendung ist das Einkaufen am Internet mit Hilfe eines „virtuellen“ Einkaufswagens. Ziel ist das Nutzungsverhalten der User zu ermitteln und somit spezifische Präferenzen innerhalb eines Browserprogramms zu vermerken. Cookies werden als Werbewirkungskontrollinstrument genutzt.
Zu den datenschutzrechtlichen Bedenken gegenüber Cookies vgl FN 110.

[80] Wieder Eklat um Microsoft: Kundendaten ausspioniert, Die Presse vom 10.3.1999, 25.

[81] Dazu ausführlich im Internet unter http://www.heise.de/tp/deutsch/inhalt/te/1590/1.html .

inhaltlich ähnlich gestalteten Internet Adressen über das Netzwerk übermittelt. Diese Funktion arbeitet nicht nur in öffentlichen Netzen, sondern greift auch in Intranets ein.[82]

Der Handel mit Daten über bestimmte Kundengruppen spielt besonders in der Werbung eine wichtige Rolle. Zu einem beliebten Mittel von Unternehmen im Handel zur Kundenbindung und Erforschung des Persönlichkeitsprofils der Kunden hat sich in jüngster Zeit die Kundenkarte entwickelt. Derzeit wird von größeren Handelsunternehmen wie Billa oder Spar in Eigenregie mittels Kundenkarte festgestellt, wer, welchen Artikel, wann und in welcher Filiale eingekauft hat.[83]

Als **Sicherheitsstrategien** für die beschriebenen Gefahrenpotentiale sind vor allem sogenannte „Firewalls“ und die Verschlüsselung von Daten anzusehen. Eine Firewall ist ein mehrstufiger Schutzwall zwischen einem zu schützenden System , beispielsweise einem Intranet und einem offenen System. Dabei fungiert die Firewall als eine Art Pförtner, der den Zugriff aus dem unsicheren System in das geschützte Netzwerk kontrolliert.[84]

Auch in den Unternehmen ist gegen Datenspionage von außen offenbar noch nicht ausreichend Vorsorge getroffen worden. Eine Studie der deutschen Beratungsunternehmens Orbit GmbH zeigt, dass 80 Prozent der Unternehmen unzureichend auf die Gefahren der mangelnden Datensicherheit im Internet vorbereitet sind. Firewalls wurden zwar durchwegs von den Unternehmen eingerichtet, doch verwenden 60 Prozent der Unternehmen keine Verschlüsselung der gesendeten Informationen und halten eine zuverlässige Authentifizierung, mit der Benutzer ihre Berechtigung zum Datenzugriff nachweisen müssen, für überflüssig.[85]

---

[82] *Steuerer*, Von wegen fest verschlossen..., Die Presse vom 21.11.1999, X. Zum technischen Hintergrund der Datenspeicherung über Internet vgl *Baig/Stepanek/Gross*, Privacy, Business Week vom 5.4.1999, 56.

[83] *Baum/Graber*, Im Visier der Datensammler, Format 8/98, 78.

[84] *Spork*, Die Zeit der Onlinetechniker, Format 33/99, 78. Zur Verschlüsselung unter 3.3.1.

[85] Im Internet unter http://www.orbit.de .

Nicht nur wirtschaftliche Nachteile für Unternehmen, sondern auch Risken für die Privatsphäre des einzelnen bestehen bei einem mangelnden Datenschutzniveau. Daher wird vehement die Verwendung von modernen Verschlüsselungsmethoden gefordert.[86]
Durch neue Technologien sind die Möglichkeiten des Abhörens von Nachrichten, der Datenspeicherung, der Verfälschung von Nachrichten stark erweitert worden. Zur Zeit der Entstehung des Internet hatten Fragen des Datenschutzes und der Datensicherheit kaum nennenswerte Bedeutung. Nichtsdestoweniger wirft nunmehr die rasante Verbreitung des elektronischen Geschäftsverkehrs und der multifunktionalen Medien eine Reihe von datenschutzrechtlichen Problemen auf. Datenschutzrechtliche Regelungen sind diesen Erfordernissen anzupassen. Voraussetzung für die weitere rasche Entwicklung des Electronic Commerce ist die Garantie eines sicheren Datenverkehrs für alle Beteiligten.

3.1.2 Rechtlicher Rahmen

3.1.2.1 Geschichte des Datenschutzes in der Europäischen Union

Der Datenschutz ist eine relativ junge Regelungsmaterie der Europäischen Union. Erste Initiativen zur Schaffung gemeinschaftsweiter Datenschutzbestimmungen gingen vom Europäischen Parlament aus. Im Jahr 1974 forderte der Abgeordnete *Lord Mansfield* derartige Regelungen.[87]
In den siebziger und Anfang der achtziger Jahre verfaßte das Parlament mehrere Resolutionen und forderte die Kommission zur Abfassung eines Richtlinienvorschlages auf.[88]

---

[86] Im Internet unter http://www.heise.de/telepolis.

[87] *Kopp*, Das EG-Richtlinienvorhaben zum Datenschutz, RDV (1993) 1.

[88] Entschließung zum Schutz der Rechte des einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung, Abl EG C 60/48 vom 11.3.1975, Abl EG C 140/34 vom 5.6.1979 und Abl EG C 87/39 vom 5.4.1982.

Die Kommission erließ daraufhin eine an die Mitgliedstaaten gerichtete Empfehlung, die vom Europarat erlassene Konvention über den Datenschutz bis Ende 1982 zu ratifizieren.[89] Erst am 18.6.1990 legte die Kommission ihren ersten Vorschlag eines Richtlinienentwurfes im Rahmen eines umfangreichen Maßnahmenpaketes zum Datenschutz dem Rat vor.[90] Im Oktober 1992 folgte ein geänderter Entwurf, der die Stellungnahme des Wirtschafts- und Sozialausschusses und fast 120 Abänderungsanträge des Parlaments berücksichtigen sollte.

Der Hauptgrund für den langwierigen Gesetzwerdungsprozess neben dem mangelnden politischen Willen in den Mitgliedstaaten war wohl die umstrittene Frage der Kompetenzgrundlage der Datenschutzrichtlinie, da auch der Vertrag von Amsterdam keine ausdrückliche Kompetenz der Gemeinschaft für den Datenschutz vorsieht.[91]

Der Erlass unterschiedlicher datenschutzrechtlicher Bestimmungen in den Mitgliedstaaten, die Judikatur zum Schutz der Grundrechte und die Einfügung von Art F in den Vertrag von Amsterdam haben letztlich doch zur Verabschiedung einer Richtlinie über den Datenschutz geführt.[92] Am 24.10.1995 unterzeichneten die Präsidenten des Rates und des Parlaments die **Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr**[93].

Die Kommission verfolgt mit der DSRL primär marktwirtschaftliche Ziele. Ziel der DSRL ist es den freien Datenverkehr innerhalb der Gemeinschaft sicherzustellen und Verzerrungen des Wettbewerbs zu vermeiden. Als Mittel hierzu

---

[89] Empfehlung der Kommission vom 29.6.1981 betreffend ein Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Abl EG L 241/31 vom 29.8.1981.

[90] KOM (90) 314 endg. vom 13.6.1990.

[91] *Souhrada-Kirchmayer*, Der Vorschlag einer allgemeinen EG-Datenschutzrichtlinie und seine Auswirkungen auf das österreichische DSG, JBl 3/1995, 147 (148).

[92] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz-Regierungsvorlage, ecolex 1999, 361.

soll durch die DSRL in allen Mitgliedstaaten ein gleichwertiger Schutz natürlicher Personen bei der Datenverarbeitung installiert werden.[94] Die Kommission stützte die DSLR daher auf Art 100a iVm Art 7a EWGV, da die Verarbeitung personenbezogener Daten oftmals als Hilfsinstrument im Rahmen der 4 Grundfreiheiten eingesetzt wird.[95] Daneben steht in den Rechtsordnungen der Mitgliedstaaten auch der grundrechtliche Aspekt des Datenschutzes im Vordergrund. Einige Mitgliedstaaten wie Portugal und Spanien haben ein Grundrecht auf Datenschutz sogar im Verfassungsrang normiert. Ein Menschenrecht auf Datenschutz ist in der EMRK nicht enthalten, jedoch wurde eine Ergänzung in dieser Hinsicht bereits vom Europarat 1980 und vom Europäischen Parlament 1982 empfohlen[96]. In der Lehre wird jedoch vereinzelt ein europäisches Grundrecht auf Datenschutz aus Art 8 MRK abgeleitet.[97]

Im Folgenden werden die europarechtlich relevanten Datenschutzbestimmungen, dh im wesentlichen die DSRL im Detail behandelt.

Dieser Richtlinie wird die jüngst erlassene Novelle zum österreichischen Datenschutzgesetz[98] gegenübergestellt, um festzustellen, in welchen Teilbereichen ein Anpassungsbedarf der österreichischen Rechtsordnung gegeben war und ob die Richtlinie tatsächlich ordnungsgemäß in das österreichische Recht umgesetzt wurde.

Im Vorfeld der Umsetzung standen mehrere Varianten der formalen Umsetzung der DSRL ins österreichische Recht zur Diskussion. Einerseits wurde eine Novellierung des bestehenden

---

[93] Abl L 281 vom 23.11.1995, im Folgenden als DSRL bezeichnet.

[94] Gemeinsamer Standpunkt des Rates vom 20.2.1995, Abl EG C 93, 1, 19, Begründung des Rates, II. Ziele.

[95] *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr (1990) 532.

[96] *Bergmann*, Grenzüberschreitender Datenschutz (1985) 197.

[97] *Souhrada-Kirchmayer*, JBl 3/1995, 150.

[98] Bundesgesetz über den Schutz personenbezogener Daten, BGBl I 165/1999. Im Folgenden als DSG 2000 bezeichnet.

Datenschutzgesetzes[99] gefordert. Andererseits wurde bereits vor der Verabschiedung der Datenschutzrichtlinie ein beträchtlicher Anpassungsbedarf der österreichischen datenschutzrechtlichen Bestimmungen geortet und eine umfangreiche Novellierung des DSG 1978 in Form einer gänzlichen Neufassung des DSG 1978 als notwendig erachtet.[100]

3.1.2.2 Die Datenschutzrichtlinie

3.1.2.2.1 Definitionen

3.1.2.2.1.1 Verantwortlichkeit

Der für die Verarbeitung der Daten **„Verantwortliche“** ist für die Festlegung der Zweckbestimmung verantwortlich. Ihm kommt daher eine entscheidende Position in der DSRL zu.[101] Damit wird derjenige zur zentralen Person, der über die Zwecke und Mittel der Verarbeitung entscheidet. Nach dem DSG ist der „Auftraggeber“ jedoch die Person, welche nur den technischen Vorgang ausführt.
DSRL und das DSG 1978 verfolgen somit einen anderen Ansatz. Ein Anpassungsbedarf wurde daher bereits im Zuge der Diskussion über die Richtlinienentwürfe geortet.[102]
Die Definition des „Auftragsverarbeiters“ in der DSRL entspricht im wesentlichen jener des DSG 1978. In Österreich musste der Auftrag zwischen Auftraggeber und Dienstleister als wesentlichen Inhalt die automationsunterstützte Verarbeitung personenbezogener Daten sein. Die DSRL erfaßt auch Verträge wo dies nur zweitrangig geregelt ist.

---

[99] Bundesgesetz über den Schutz personenbezogener Daten vom 28. November 1978, BGBl 1978/565. Im Folgenden als DSG 1978 bezeichnet.

[100] *Souhrada-Kirchmayer*, JBl 3/1995, 158; *Brühann/Zerdick*, Umsetzung der EG-Datenschutzrichtlinie in Österreich, CR 9/1996, 556 (561); *Kronegger*, im Internet unter http://www.ad.or.at/office/recht/eu.htm .

[101] *Brühmann*, RDV 1996, 15.

[102] *Brühann/Zerdick*, CR 9/1996, 557.

Im DSG 2000 wurde daher die **Abgrenzung zwischen dem „Auftraggeber“ gemäß § 4 Z4 und dem „Dienstleister“** gemäß § 4 Z5 neu definiert. Die datenschutzrechtliche Verantwortung trifft nach dem DSG 2000 den „Auftraggeber“, und zwar jene Person, die „ein Werk unter Heranziehung von Datenverarbeitung herstellen läßt“. Nach § 3 Z4 DSG 1978 galt eine Person als „Auftraggeber“, wenn die Datenverarbeitung „wesentlicher Inhalt“ des Werkes war.[103]

3.1.2.2.1.2 Verarbeitung

Die DSRL kennt als zentralen Oberbegriff aller denkbarer Verarbeitungsschritte von personenbezogenen Daten nur den Begriff der **„Verarbeitung“**. Darunter fallen sämtliche Zwischenschritte wie das „Ermitteln“, „Benützen“, „Löschen“ oder „Überlassen“ von Daten. Neben dem Begriff des „Verarbeitens“ von Daten kennt das DSG 1978 all diese Begriffe. Somit ergeben sich jedoch unterschiedliche Auffassungen über den Begriff der Verarbeitung zwischen der DSRL und dem DSG 1978.

3.1.2.2.2 Anwendungsbereich

Die Richtlinie erfasst im persönlichen Anwendungsbereich ausschließlich den **Schutz natürlicher Personen**. Nur in einigen wenigen Mitgliedstaaten sind von den nationalen Datenschutzgesetzen **auch juristische Personen** erfasst.[104] Auch nach dem DSG 1978 genossen juristische Personen bereits Datenschutz. Das wird auch im DSG 2000 gemäß § 4 Z4 beibehalten.
Juristische Personen fallen zwar nicht in den Anwendungsbereich der DSRL, gemäß Erwägungsgrund 24 der DSRL werden jedoch einschlägige Vorschriften der Mitgliedstaaten

[103] Vgl ausführlich *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 362.

[104] So etwa in Dänemark oder Luxemburg. Dazu ausführlich *Ellger*, RDV (1991) 59.

ausdrücklich als zulässig erklärt. Demnach wären für juristische Personen auch - von der gemeinschaftsrechtlichen Vorgabe - abweichende Regelungen zulässig. Das DSG 2000 gilt sehr wohl für Bereiche, die nicht dem Anwendungsbereich der Richtlinie unterworfen sind. Ein Beispiel dafür findet sich in Art 3 Abs 2, wonach die DSRL keine Anwendung auf Datenverarbeitungen für die Ausübung von bestimmten Tätigkeiten findet.

Der Umstand, dass der für die Wirtschaft so wichtige Bereich der Datenschutzbestimmungen juristischer Personen nicht der Richtlinie unterliegt wurde zu Recht kritisiert. Damit wird in einem wichtigen Bereich des Datenschutzes keine europaweit harmonisierte Regelung geschaffen und den Mitgliedstaaten bei der Umsetzung ein erheblicher Ermessenspielraum eingeräumt, der dem Ziel der DSRL, einer weitgehenden Harmonisierung der einzelstaatlichen Rechtsvorschriften sicherlich hinderlich sein wird. Die unterschiedlichen Regelungen in den Mitgliedstaaten werden in der Praxis wohl zu Handelshemmnissen führen.[105]

Die Richtlinie gilt in ihrem sachlichen Anwendungsbereich gemäß Art 3 Abs. 1 sowohl für die **automatisierte Verarbeitung** als auch für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in Dateien gespeichert sind oder gespeichert werden sollen (**manuelle Daten**).

In diesem Bereich war in Österreich ein erheblicher Anpassungsbedarf an die Vorgaben der DSRL gegeben. In Österreich waren vor dem DSG 2000 durch § 1 Abs 3 und 4 DSG 1978 manuell verarbeitete Daten ausschließlich durch das Grundrecht auf Datenschutz geschützt, was zu einer Einschränkung der Rechte des Betroffenen geführt hat.

Der **Kompetenztatbestand** § 2 Abs 1 des DSG 2000 bestimmt eine Gesetzgebungskompetenz des Bundes für automationsunterstützte Daten. Für die Gesetzgebung im Bereich der nichtautomatisierten (manuellen) Daten sind nach wie vor die Länder zuständig. Eine Erweiterung dieser

[105] *Souhrada-Kirchmayer*, JBl 3/1995, 150.

Gesetzgebungskompetenz des Bundes auf manuelle Daten konnte in Verhandlungen mit den Ländervertretern nicht erreicht werden.[106] Die Richtlinie wurde daher durch § 2 Abs 1 nur teilweise umgesetzt. Für manuell, im Bereich der Länder gespeicherte Daten erfolgte noch keine Umsetzung und sind in diesem Bereich die Länder zur Erlassung eigener Datenschutzgesetze aufgefordert, die ebenfalls den Vorgaben der Richtlinie entsprechen müssen.

3.1.2.2.3 Datenverwendung

Die DSRL gibt in den Art 6 bis 9 **Grundsätze für die Verarbeitung von Daten** vor. Die nähere Ausgestaltung dieser Grundsätze ist den Mitgliedstaaten überlassen.
Der Anpassungsbedarf des DSG 1978 wurde in diesem Punkt unterschiedlich beurteilt.[107] Einigkeit herrscht in der Lehre darüber, dass eine Aufgabe der Zweiteilung in einem öffentlichen und privaten Teil wie Ihn die einfachgesetzlichen Bestimmungen des DSG 1978 vorsahen, nach den Vorgaben der DSRL nicht notwendig sind.[108]
Der österreichische Gesetzgeber hat die **Zulässigkeitsvoraussetzungen** für die Ermittlung, Verarbeitung und Übermittlung von Daten in der Tat **neu formuliert**. Der Grund dürfte im Abgehen der strikten Zweiteilung des einfachgesetzlichen Teiles des DSG 1978 in einen öffentlichen und einen privaten Teil liegen.[109] In § 6 wird nach den Vorgaben der DSRL eine Aufzählung der Grundsätze der Datenverarbeitung festgeschrieben. Im § 7 werden die Zulässigkeitsvoraussetzungen für die Datenverwendung im

[106] *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 362.

[107] *Souhrada-Kirchmayer*, JBl 3/1995, 150 ortet keine Notwendigkeit der Anpassung. AM ist *Brühann/Zerdick*, CR 9/1996, 557, der dies anhand einiger Beispiele anschaulich darstellt.

[108] *Souhrada-Kirchmayer*, JBl 3/1995, 150; *Brühann/Zerdick*, CR 9/1996, 557 empfiehlt jedoch im Hinblick auf die Übersichtlichkeit und Gesetzesökonomie eine Neuformulierung.

[109] *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 362.

einzelnen aufgezählt. § 8 regelt die Geheimhaltungsinteressen bei nicht sensiblen Daten.

3.1.2.2.4 Datenarten

Die DSRL teilt die **personenbezogenen Daten** gemäß Art 8 in mehrere Kategorien von verschiedener Schutzwürdigkeit ein. Für sensible Daten statuiert die DSRL den Grundsatz des Verbotes der Verarbeitung. Hiervon gibt es jedoch Ausnahmen gemäß Art 8 Abs 2, beispielsweise bei Einwilligung des Betroffenen.
Im DSG 1978 war diese Kategorie von Daten unbekannt, ein Verbot existierte nicht. In Umsetzung der DSRL wurde in § 1 Abs 2 DSG 2000 ein gleichlautendes Verbot der Verarbeitung sensibler Daten eingeführt. Nach § 4 Z4 DSG 2000 gelten als „sensible „ Daten, Daten natürlicher Personen, über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse und philosophische Überzeugung, Gesundheit oder ihr Sexualleben.[110]

---

[110] Vgl auch Art 6 der Datenschutzkonvention des Europarates, BGBl 1988/317. In diesem Zusammenhang wird auch das Problem der Verwendung von Cookies relevant. Gemäß Art 10 (Information bei der Erhebung personenbezogener Daten bei der betroffenen Person) müssen Personen, bei denen die sie betreffenden Daten erhoben werden, vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhalten:
a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters, b) Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind, c) weitere Informationen, beispielsweise betreffend die Empfänger oder Kategorien der Empfänger der Daten, die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung, das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.
Beim Ablegen von Cookies wird jedoch nicht informiert, für welchen Zweck die Daten erhoben bzw. verarbeitet werden. *Brandl/Mayr-Schönberger*, CPU-IDS, Cookies und Internet-Datenschutz, ecolex 1999, 366 empfehlen daher den Anbietern von Internetseiten, im Zweifelsfall von der Verwendung von

3.1.2.2.5 Datenübermittlung in andere Mitgliedstaaten und in Drittländer

Das DSG 2000 ist grundsätzlich nach seinem r**äumlichen Anwendungsbereich** auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Daneben ist das DSG 2000 gemäß § 3 Abs 1 auf die Verwendung vom Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der EU für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung eines Auftraggebers geschieht.
Gemäß § 3 Abs 2 ist das Recht des Sitzstaates eines Auftraggebers des privaten Bereichs aus einem anderen Mitgliedsstaat anzuwenden, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist. Das DSG 2000 ist gemäß § 3 Abs 3 nicht auf die Durchfuhr von Daten im Datenverkehr innerhalb der Union anzuwenden.
Für den **Datenverkehr innerhalb der EU** gibt es **keine Beschränkungen**. Was den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs betrifft, so ist dieser aber nur in Bereichen, die dem Gemeinschaftsrecht unterliegen, genehmigungsfrei. Die Zusammenarbeit innerhalb der "dritten Säule" (Bereich Justiz und Inneres) ist nicht von der Bestimmung erfasst.[111]
Der Datenverkehr von einem **Mitgliedstaat in einen Drittstaat** ist nur dann zulässig, wenn in diesem Drittstaat ein gewisser **Standart** im Bereich des Datenschutzes besteht.
Von diesem Grundsatz gibt es in Art 27 jedoch Ausnahmen, in denen ein Datentransfer trotz des Nichtvorliegens eines angemessenen Datenschutzniveaus in ein Drittland trotzdem stattfinden darf. Art 26 Abs 2 stellt Kriterien für die in Abs

---

Cookies aus Datenschutzgründen abzusehen oder Informationen über die Verwendung und Umgang mit Cookies anzugeben.

[111] Diese Bestimmung lässt jedoch verschiedene Fragen offen. Unklar ist beispielsweise, wie der Datenverkehr zwischen privatem Bereich und öffentlichem Bereich zu beurteilen ist.

1 festgelegte „Angemessenheit“ auf. Das Feststellungsverfahren, ob in einem Drittstaat ein angemessenes Schutzniveau besteht, wird in den Abs 4 und 5 geregelt, wobei die Kommission sich vorbehält im Einzelfall zu entscheiden.

Welche Drittländer über ein angemessenes Datenschutzniveau verfügen wird von der Kommission festgestellt und durch den Bundeskanzler kundgemacht. Das DSG 2000 sieht daneben auch die Möglichkeit vor, dass neben den Feststellungen der Kommission durch Verordnung[112] des Bundeskanzlers weitere Drittstaaten als mit angemessenem Datenschutzniveau ausgestattet angesehen werden.

Sowohl der Grundsatz als auch die Ausnahmetatbestände des Art 26 waren Gegenstand heftiger Diskussionen. Kritisiert wurde die Unbestimmtheit des Rechtsbegriffes sowie die teilweise zu engen und teilweise zu weit gefassten Ausnahmetatbestände.[113]

Kritik an den Richtlinienentwürfen der Kommission gab es auch von Drittstaaten, die nicht jenes hohe Datenschutzniveau erreichen, das mit Einführung der DSRL für die EU gelten wird. Insbesondere seitens der **USA** wurden Bedenken geäußert, dass diese Regelung den grenzüberschreitenden elektronischen Handel stark beeinträchtigen würde.[114]

Bei diesem Streit werden die fundamental entgegengesetzten Denkansätze im Rahmen des Rechtes der Privatsphäre in Europa

---

[112] In wie weit diese Verordnungsermächtigung als richtlinienkonform anzusehen ist bzw. ihre Ausübung Beschränkungen durch das EU-Recht und die DSRL unterliegt, ist zweifelhaft.

[113] *Ellger*, Datenexport in Drittländer, CR 1993, 8.

[114] Das Marktforschungsunternehmen *Forrester Research* hat in einer Studie aufgezeigt, dass auf den meisten US-Websites die Datenschutzstandards nicht eingehalten werden. Im Internet unter http://www.ecommercetimes.com/news/articles/990916-3.shtml. Die US-Regierung hat gemeinsam mit der amerikanischen Industrie unverbindliche Empfehlungen entwickelt, die von amerikanischen Online-Anbietern verlangen, dass sie im Rahmen der Selbstregulation sogenannte "Privacy Policies" veröffentlichen, welche die Nutzer über Datenerhebung und Speicherung informieren sollen. Diese sind jedoch vage formuliert und nur wenige Anbieter halten die Vorgaben über die Bereitstellung von Informationen ein.

und Amerika sichtbar. Dahinter steckt auch die wirtschaftliche Sorge multinationaler Marketing-Unternehmen und Internet Firmen wie America Online mit Sitz in den USA, dass die Sammlung und Weitergabe personenbezogener Daten von europäischen Kunden nun nicht mehr in demselben Ausmaß wie bisher möglich ist und die Teilnahme am europäischen Markt daher mit zusätzlichen Kosten für den Aufbau separater Datenbanken der europäischen Niederlassungen beeinträchtigt wird. Die USA haben sogar mit einer Beschwerde bei der WTO gedroht.[115]

Für die österreichische Rechtsordnung ergab sich aus den Vorgaben der Art 25 und 26 ein dringender Anpassungsbedarf.[116] Der Datenverkehr mit Drittstaaten ist nunmehr in den §§ 12 und 13 DSG 2000 geregelt. In Umsetzung der Vorgaben der DSRL regeln § 12 die genehmigungsfreie und § 13 DSG 2000 die genehmigungspflichtige Datenübermittlung und -überlassung in Drittländer. Soweit der Datenverkehr mit dem Ausland nicht genehmigungsfrei ist, unterliegt die Datenübermittlung der vorherigen Genehmigung der Datenschutzkommission. Obwohl die DSRL nur auf natürliche Personen Anwendung findet, werden die Ausnahmen von der Genehmigungspflicht auch auf den Datenexport von juristischen Personen ausgedehnt.[117]

3.1.2.2.6 Pflichten der Verantwortlichen

3.1.2.2.6.1 Publizität der Datenanwendungen (Meldepflicht und Vorabkontrolle)

Die DSRL sieht in Art 18 grundsätzlich ein umfangreiches **Meldeverfahren** vor. Von dieser Meldepflicht können gemäß Art

---

[115] Im Internet unter http://interactive.wsj.com/articles/SB909436495579300500.htm ; http://www.akademie.de/news/langtext.html?id=2024 und http://www.news.com/News/Item/Textonly/0,25,36862,00.html .

[116] *Souhrada-Kirchmayer*, JBl 3/1995, 156; *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 363.

[117] Zur Begründung vgl den Allgemeinen Teil der EB zur RV.

18 Abs 2 bei bestimmten Verarbeitungskategorien Vereinfachungen oder Ausnahmen vorgenommen werden. Zur Bestimmung dieser Kategorien werden von der DSL bestimmte Kriterien festgelegt. Auch in Österreich existiert bereits ein ähnliches System zur Gewährleistung der Publizitätserfordernisse, das der DSRL wohl als Vorbild diente.[118]

In Umsetzung der Richtlinie wurde das schon bisher vorgesehene Meldeverfahren beibehalten. In § 17 DSG 2000 wird eine Meldepflicht an das Datenverarbeitungsregister (DVR) festgelegt. Schon vor Inkrafttreten des DSG 2000 stand in Österreich eine dem Art 18 Abs 2 entsprechende Regelung in Geltung, wonach für sogenannte **„Standartverarbeitungen“** eine Ausnahme von der Meldepflicht vorgesehen war. Durch Verordnung wurden bestimmte Typen von Datenverarbeitungen zu Standartverarbeitungen erklärt. In Einzelfällen war dennoch eine Meldepflicht vorgesehen. (§ 23 Abs 1 Satz 3 DSG 1978).

Nach dem DSG 2000 werden Standartverarbeitungen in Zukunft überhaupt nicht meldepflichtig sein (§ 17 Abs 2 Z6), was zu einer Verminderung des Registrierungsaufwandes führen wird. Standartverarbeitungen werden in Zukunft sogenannten „Musteranwendungen“ gemäß § 19 Abs 2 DSG 2000 entsprechen.

In diesem Bereich war die österreichische Regelung Vorbild für die entsprechende Richtlinienbestimmung und somit kein Anpassungsbedarf der österreichischen Rechtsordnung gegeben.[119]

Neben der Meldepflicht an das DVR hat der österreichische Gesetzgeber in § 18 Abs 2 DSG 2000 für bestimmte besonders schutzwürdige Daten das Instrument der **Vorabkontrolle** eingeführt. Diese Datenanwendungen dürfen erst nach einer Prüfung (Vorabkontrolle) durch die Datenschutzkommission (DSK) aufgenommen werden. Diese Regelung geht über die Vorgaben der Richtlinie hinaus und wurde als Wettbewerbsnachteil für die österreichische Wirtschaft kritisiert.[120]

---

[118] *Brühann/Zerdick*, CR 9/1996, 560.

[119] *Brühann/Zerdick*, CR 9/1996, 560.

[120] *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 365.

3.1.2.2.6.2 Informations- und Auskunftspflichten - Widerspruchsrecht des Betroffenen

Die DSRL sieht zur Konkretisierung des Grundrechts auf Datenschutz verschiedene **Rechte der Betroffenen** vor. Im einzelnen sind dies das Recht auf Information, Auskunft, Widerspruch, Richtigstellung und Löschung. Auch das DSG 1978 kannte die Sicherung der Rechtsstellung des Betroffenen durch das Auskunfts-, Richtigstellungs- und Löschungsrecht.

Die **Informationspflichten** des Datenverarbeiters an den Betroffenen, Kernstück des Datenschutzes[121], werden in Art 11 der DSRL festgelegt. Art 13 sieht in engen Grenzen Ausnahmen von dieser Verpflichtung vor. Im DSG 1978 sind entsprechende Pflichten nicht zu erkennen und wurde daher eine völlige Novellierung dieser Bestimmungen gefordert.[122] In das DSG 2000 wurde in § 24 daher als zusätzliche Informationspflicht neben der Meldepflicht an das DVR eine „Informationspflicht des Auftraggebers“ an den Betroffenen neu eingefügt.

Daneben räumt die DSRL zum Schutz der Betroffenen diesen weitgehende Rechte ein. Art 12 der DSRL sieht ein **Auskunftsrecht** vor, das weitgehend mit jenem des DSG 1978 überstimmt. Punktuelle Änderungen waren in der Umsetzung jedoch von Nöten um eine Richtlinienkonformität zu erreichen.[123] Dasselbe gilt für **das Recht auf Richtigstellung und Löschung**.

Die DSRL sieht darüber hinaus jedoch noch ein Widerspruchsrecht vor, das dem DSG 1978 weitgehend unbekannt war. In Anpassung an die DSRL wurde in das DSG 2000 das von der Richtlinie vorgegebene Widerrufsrecht in § 28 eingefügt.[124]

---

[121] *Kopp*, DuD 1995, 204 (209).

[122] *Souhrada-Kirchmayer*, JBl 3/1995, 152; *Brühann/Zerdick*, CR 9/1996, 559.

[123] *Souhrada-Kirchmayer*, JBl 3/1995, 153; *Brühann/Zerdick*, CR 9/1996, 560.

[124] *Souhrada-Kirchmayer*, JBl 3/1995, 153; *Brühann/Zerdick*, CR 9/1996, 560.

Die Regelung wurde jedoch als schwer nachvollziehbar und unpraktikabel kritisiert.[125]

3.1.2.2.6.3 Rechtsschutz durch die Datenschutzbehörden – Haftung des Verantwortlichen - Strafbestimmungen

Die DSRL gibt den Mitgliedstaaten eindeutige Vorgaben für die Ausgestaltung der **nationalen Datenschutzbehörden**. Art 30 Abs 1 bestimmt, dass die Anwendung der in Durchführung der DSRL ergangenen Bestimmungen (also das DSG 2000 in Österreich) von einer oder mehreren unabhängigen Kontrollinstanzen überwacht werden müssen. Die Mitgliedstaaten haben diese nationalen Kontrollbehörden im Bereich des Datenschutzes überdies mit umfangreichen Untersuchungs- und Einwirkungsbefugnissen auszustatten.
Aufgrund dieser Vorgaben der DSRL wurde in Österreich eine umfassende Neuorganisation der Behördenstruktur im Datenschutzbereich vorgeschlagen.[126]
Im DSG 2000 wurden trotz dieser Überlegungen im Bereich der Datenschutzbehörden **keine tiefgreifenden Veränderungen** vorgenommen. Die Trennung des Rechtsweges für die Durchsetzung der Rechte der Betroffenen wurde beibehalten. Für Datenschutzverletzungen durch Auftraggeber im öffentlichen Bereich bleibt die DSK zuständig. Die ordentlichen Gerichte entscheiden über Verletzungen im privaten Bereich. Gemäß den Vorgaben der DSRL wurden jedoch die Kontrollbefugnisse der DSK erheblich ausgeweitet. Der Aufgabenbereich der DSK umfaßt nunmehr alle Datenanwendungen und ist nicht bloß auf den öffentlichen Sektor beschränkt. Ihr wird auch die Führung des DVR zugeordnet. Wie schon im Rahmen der Verabschiedung der DSRL vorgeschlagen, wurde die DSK als unabhängige

[125] *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 364.

[126] *Souhrada-Kirchmayer*, JBl 3/1995, 157. Nach Meinung der Autorin entsprach bloß die DSK, nicht aber der Datenschutzrat den Vorgaben der DSRL. Weder die DSK noch die Gerichte waren jedoch mit Kontrollbefugnissen ausgestattet, welche die DSRL vorsieht.

Kontrollstelle iSd Art 28 der DSRL eingesetzt[127]. Um die Vorgabe der „Unabhängigkeit“ iSd DSRL zu garantieren wurde die DSK als Kollegialbehörde mit richterlichem Einschlag iSd Art 133 Z4 B-VG eingesetzt.[128]

Art 23 der DSRL räumt Personen, denen durch die rechtswidrige Verarbeitung ihrer personenbezogenen Daten ein Schaden entsteht, ein **Recht auf Schadenersatz** gegenüber dem Verantwortlichen der Verarbeitung ein. Art 23 Abs 2 der DSRL sieht die Möglichkeit einer teilweisen oder gänzlichen Haftungsbefreiung vor.

Aufgrund des weiten Ermessensspielraumes für die Mitgliedstaaten bei der Umsetzung dieser Bestimmung, wurde eine Änderung des österreichischen Haftungsregimes im DSG nicht als zwingend notwendig erachtet.[129] Das Fehlen einer ausdrücklichen Bestimmung über den Schadenersatzanspruch im DSG 1978 hat den österreichischen Gesetzgeber jedoch dazu veranlasst, in das DSG 2000 eine spezielle Schadenersatzbestimmung einzufügen. § 33 DSG 2000 sieht nunmehr einen Ersatz des Schadens nach den Bestimmungen des AGBG vor. Bereits vor Inkrafttreten des DSG 2000 gründete sich ein derartiger Schadenersatzanspruch im privaten Bereich auf das ABGB, im öffentlichen Bereich auf das AHG, sodass diese Bestimmung bloß ein Festschreiben des derzeitigen Status quo darstellt und keine inhaltlichen Neuerungen mit sich bringt.[130]

Neu ist jedoch die Bestimmung, dass bei öffentlicher Bloßstellung bei sensiblen, strafrechtlich relevanten Daten und Daten über die Kreditwürdigkeit der Betroffenen, auch der Ersatz immaterieller Schäden bis zu einer Obergrenze von 200.000.- ATS vorgesehen ist. Dies ist deshalb von Bedeutung, da in Österreich grundsätzlich immaterielle Schäden nur dort ersetzt werden, wo sich im Gesetz eine ausdrückliche Regelung

---

[127] *Souhrada-Kirchmayer*, JBl 3/1995, 157.

[128] Vgl ausführlich *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 364.

[129] *Souhrada-Kirchmayer*, JBl 3/1995, 155.

[130] *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 364.

dafür findet.[131] Diese Regelung findet keine Deckung in der DSRL und geht daher über die Vorgaben der Richtlinie hinaus.[132]
Art 25 DSRL schreibt den Mitgliedstaaten die Einführung **„ausreichender Sanktionen“** gegen Personen vor, welche die Datenschutzbestimmungen nicht einhalten. Der österreichische Gesetzgeber nahm diese Bestimmung zum Anlass um die bestehenden Straftatbestände wesentlich umzugestalten (§ 51 und 52 DSG 2000).
Einerseits wurden die Verwaltungsstraftatbestände erheblich ausgedehnt, andererseits sind nach dem DSG 2000 nur mehr die absichtliche Schadenszufügung und die rechtswidrige Übermittlung von Daten in Gewinnerzielungsabsicht gerichtlich strafbar. Der Änderungsbedarf ergab sich nicht zuletzt aufgrund der rasanten technischen Entwicklung.[133]

3.1.2.3 Die ISDN Datenschutzrichtlinie

Die Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation[134] stellt eine spezielle Datenschutzvorschrift für den **Bereich Telekommunikation** dar, welche die DSRL ergänzt. Die ISDN Datenschutzrichtlinie schützt gemäß Art 2 Z a zum Unterschied der DSRL auch juristische Personen.
In Österreich wurde die Richtlinie bereits im Telekommunikationsgesetz berücksichtigt.[135]

---

[131] *Koziol/Welser*, Grundriß[10] I, 444f.

[132] Zu der Kritik an den überschiessenden - nicht durch die DSRL vorgegebenen - Bestimmungen im DSG 2000 vgl *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 365.

[133] Allgemeiner Teil der EB zur RV.

[134] Im Internet unter http://www2.echo.lu/legal/de/datenschutz/protection.html .

[135] *Laga*, Rechtsprobleme, 326.

3.1.2. Resümee

Insgesamt hat die DSRL zu **erheblichen Änderungen im österreichischen Datenschutzrecht** geführt. Diese Änderungen sind jedoch nicht zur Gänze auf die europarechtlichen Vorgaben zurückzuführen, da der österreichische Gesetzgeber in manchen Bereichen über die Vorgaben der DSRL hinaus Regelungen getroffen hat, was von Seiten der Wirtschaft als Wettbewerbsverzerrung kritisiert wurde.

Trotz dieser teilweise überschießender Regelungen hat die Kommission bei mehreren Mitgliedstaaten, unter anderem Österreich die Umsetzung der DSRL kritisiert.[136]

Das hochgesteckte Ziel der DSRL in allen Mitgliedstaaten einen gleichwertigen Schutz bei der Datenverarbeitung zu installieren, den freien Datenverkehr innerhalb der Gemeinschaft sicherzustellen und Verzerrungen des Wettbewerbs und damit Standortverlagerungen zu vermeiden[137] wird durch die Ausklammerung in der Praxis bedeutsamer Teile wie dem Schutz juristischer Personen, die Einräumung weiter Ermessensspielräume für die Mitgliedstaaten bei der Umsetzung

---

[136] Nach Ansicht der Kommission haben bislang nur Griechenland, Portugal, Schweden, Italien, Belgien und Finnland die Richtlinie vollständig umgesetzt. Die Richtlinie hätte gemäß Art 32 binnen 3 Jahren nach ihrer Annahme - nicht ab Veröffentlichung im ABl ! - also bis 24.10.1998 umgesetzt werden müssen. Bereits im Juli 1999 hat die Kommission an Frankreich, Luxemburg, die Niederlande, Deutschland, das Vereinte Königreich, Irland, Dänemark, Spanien und Österreich mit Gründen versehene Stellungnahmen gerichtet, weil diese Länder ihr nicht alle zur Umsetzung der DSRL notwendigen Maßnahmen mitgeteilt haben. Im Internet unter http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/99/592|0|RAPID&lg=EN. Unabhängig vom Stand der Umsetzung können sich Einzelne vor nationalen Gerichten auf gewisse Bestimmungen der Richtlinie berufen (Marleasing, RS C-106/89, 13.11.90). Außerdem können Personen, die infolge der Nichtumsetzung der Richtlinie durch einen Mitgliedstaat einen Schaden erlitten haben, in bestimmten Fällen vor nationalen Gerichten auf Schadenersatz klagen (Francovich, RS C-6/90 und C-9/90, 19.11.91).

[137] Gemeinsamer Standpunkt des Rates vom 20.2.1995, Abl EG C 93, S 1, 19, Begründung des Rates, II. Ziele.

und die überschießenden Regelungen in manchen Mitgliedstaaten, kann freilich nur schwer erreicht werden.

Auf die aktuelle Situation im Bereich Internet nimmt weder die DSRL noch das DSG 2000 Bezug[138]. Der Hauptgrund hierfür liegt darin, dass die Arbeiten an der DSRL schon in den frühen achtziger Jahren begonnen haben und daher keine Rücksicht auf die erst kürzlich erlassene E-Commerce Richtlinie genommen wurde. Das trägt mE nicht zu einer Stärkung des Vertrauens der Anwender in die neuen Medien bei und wird daher eine **baldige Novellierung der DSRL notwendig** machen.

Offenbar erachtet auch die Kommission eine derartige Weiterentwicklung des Datenschutzrechtes für notwendig, da bereits eine Studie ausgeschrieben wurde, welche die spezifischen technischen und wissenschaftlichen Probleme des Datenschutzes im elektronischen Geschäftsverkehr untersuchen soll.[139]

[138] *Duschanek/Rosenmayr-Klemenz*, ecolex 1999, 365.

[139] Im Internet unter http://europa.eu.int/index-de.htm.

3.2 VERBRAUCHERSCHUTZ IM INTERNET – DIE FERNABSATZRICHTLINIE

Das Internet entwickelt sich sowohl für digitale als auch für nichtdigitale Waren und Dienstleistungen immer mehr zu einem **virtuellen Einkaufsparadies**. Die Kommerzialisierung des Internet wird durch die Vielseitigkeit, Schnelligkeit und Benutzerfreundlichkeit des Mediums auch in Zukunft rasch voranschreiten.[140] Die Zuwachsraten beim sogenannten „Internet-Shopping" sind beeindruckend.[141] Die online Umsätze der Versandhäuser beispielsweise steigen rasant. Die deutsche Neckermann Versand AG erzielte 1998 Umsätze in der Höhe von 140 Millionen Schilling. Das ergibt eine Verdreifachen gegenüber 1997. Auch die österreichische Tochter konnte ihre Umsätze über das Internet 1998 im Vergleich zu 1997 vervierfachen.[142]

In der Tat setzten sich immer mehr Unternehmen weltweit mit dieser neuen Technologie auseinander.

Die spezielle Situation bei Verbrauchergeschäften über das Internet hat auch die Europäische Kommission dazu veranlaßt aktiv zu werden. Seit 1992 arbeitet die Europäische Kommission an einer Richtlinie über den Verbraucherschutz im Fernabsatz. Nach zwei Entwürfen[143] wurde vom Rat ein Gemeinsamer Standpunkt bereits am 29. Juni 1995 festgelegt.[144] Die Beschlußfassung über die endgültige Fassung erfolgte - unter Beachtung von 31 Änderungswünschen des Europäischen Parlaments - am 20. Mai 1997 als **Richtlinie 97/7/EG des Europäischen Parlaments und des Rates über den Verbraucherschutz bei Vertragsabschlüssen**

---

[140] *Arnold*, Verbraucherschutz im Internet, CR 9/1997, 526.

[141] *Borges*, Verbraucherschutz beim Internet-Shopping, Zeitschrift für Wirtschaftsrecht, 20/1999 H 4, 130.

[142] Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=990730014.

[143] Abl EG C 156 vom 23.6.1992, 14 und ABl EG C 308 vom 15.11.1993, 18.

[144] Abl EG C 288 vom 30.10.1995, 1.

im Fernabsatz.[145] Gemäß Art 15 verpflichtet die Fernabsatzrichtlinie die Mitgliedstaaten, die Richtlinie bis spätestens 3 Jahre nach deren Inkrafttreten in das nationale Recht umzusetzen. Da gemäß Art 18 die Richtlinie am Tag ihrer Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften in Kraft tritt (somit am 4. Juni 1997) endet die Umsetzungsfrist für die Mitgliedstaaten am 4. Juni 2000.

Die Fernabsatzrichtlinie ist das **wichtigste Regelungswerk auf europäischer Ebene über den Verbraucherschutz im elektronischen Geschäftsverkehr**.[146] Man könnte sie daher auch als das europäische Konsumentenschutzgesetz für das Internet bezeichnen.

Anhand der Richtlinie werden deren wesentliche Bestimmungen über den Verkauf über das Internet an einen Konsumenten dargestellt. Dabei wird auf die Umsetzung dieser Bestimmungen in die nationalen Rechtsordnungen, insbesondere in das österreichische Recht Bezug genommen.

Mehrere Mitgliedstaaten wie Österreich und Deutschland sind gerade im Begriff die Richtlinie umzusetzen bzw. haben die Richtlinie bereits umgesetzt. Der österreichische Gesetzgeber versucht die europarechtlichen Vorgaben durch das **Fernabsatz-Gesetz** zu erfüllen.[147]

Man hat sich nicht für die Verabschiedung eines eigenen Umsetzungsgesetzes entschieden, sondern die Bestimmungen der Richtlinie in das 1. Hauptstück des KSchG eingefügt.[148] Damit

---

[145] Abl EG L 144, 9 vom 4.6.1997. Im Folgenden als Fernabsatzrichtlinie bezeichnet.

[146] *Jaburek/Wölfl*, Cyber-Recht (1997) 43.

[147] So die EB zur RV 23. Bundesgesetz, mit dem Bestimmungen über den Vertragsabschluß im Fernabsatz in das Konsumentenschutzgesetz eingefügt und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 sowie das Produkthaftungsgesetz geändert werden (Fernabsatz-Gesetz), BGBl I 185/1999 vom 19.8.1999.

[148] Begründet wurde diese Form der Umsetzung mit dem weitem Anwendungsbereich der Richtlinie, dem geringeren Aufwand bei der Umsetzung und dem Bestehen des KSchG in Österreich als "zentraler Hort des österreichischen Verbraucherschutzrechts". Vgl EB zur RV 24.

muss jedoch eine zunehmende Unübersichtlichkeit des KSchG in Kauf genommen werden.[149]

3.2.1 Problematik beim Online-Shopping und Ziel der Fernabsatzrichtlinie

Für den Konsumenten bringt der Einkauf im Wege des Electronic Commerce mehrere **Vorteile** wie eine große Auswahl, eine bessere Vergleichbarkeit der Angebote, eine bequeme, rasche und weltweite Bestellmöglichkeit, keine Bindung an Öffnungszeiten und oftmals Preisvorteile, da die Anbieter oft Wettbewerbsvorteile an die Kunden weitergeben. Die Kommunikation per Internet ist kostengünstiger und schneller als die Bestellung per Post und steht 24 Stunden am Tag zur Verfügung. Der Anbieter hat mehr Möglichkeiten bei der Produktpräsentation und Information als im Katalog.[150]
Dem stehen jedoch auch Nachteile und **Risiken** für den Verbraucher gegenüber. Die Waren können nicht besichtigt und erprobt werden, die Gefahr unseriöser Anbieter ist eher gegeben als beim klassischen Einkauf im Verkaufslokal und vertragliche Rechte können schwierig gegenüber ausländischen Anbietern durchgesetzt werden. Darüber hinaus besteht die Gefahr von übereilten und unüberlegten Kaufentscheidungen der Konsumenten ohne die Ware gesehen zu haben und die Gefahr des „Verklickens“.[151]
Von verschiedenen Seiten wurde daher wiederholt auf die Problematik des Verbraucherschutzes bei der

---

[149] *Neumann*, Vertragliche Rahmenbedingungen für Online-Shopping im WorldWideWeb (Diplomarbeit Universität Salzburg, 1999) 23. Im Internet unter http://www.privatrecht.sbg.ac.at/forum/Neumann.html.

[150] *Köhler*, NJW 1998, 185.

[151] *Arnold*, CR 9/1997, 526 (531); *Mohr*, Elektronischer Kauf - Verbraucherschutz im Fernabsatz, e-commerce, ecolex 1999, 247. So auch EB zur RV 16.

Geschäftsabwicklung durch Verbraucher via Internet hingewiesen.[152]

Damit stellt sich für den Verbraucher beim Kauf über Internet die Situation **ähnlich** dar wie beim **Versandhandelsgeschäft**.[153]

Diese Gefahren bestehen in ähnlicher Form zwar bei allen Formen eines Kaufes außerhalb der Geschäftsräume, werden aber durch die technischen Möglichkeiten im Internet verstärkt. Die Bestellung kann sehr rasch erfolgen und in wenigen Sekunden kann der Verbraucher über sehr hohe Summen verfügen.[154] Die Hemmschwelle für den Verbraucher eine rechtlich relevante Willenserklärung bloß per Mausklick abzugeben, ist ungleich niedriger als bei sonstigen Arten der Willenserklärung.[155]

Ziel der Fernabsatzrichtlinie ist es daher, "dem Verbraucher vor Vertragsschließung **ausreichende Informationen** zu verschaffen." Darin manifestiert sich das auch in anderen Verbraucherschutz-Richtlinien maßgebliche **Transparenzgebot**.[156]

3.2.2 Anwendungsbereich

Die Richtlinie findet gemäß Art 2 Z1 allgemein auf **„Vertragsabschlüsse durch Verbraucher im Fernabsatz“**

---

[152] Vor allem die Verbraucherverbände haben sich für spezielle konsumentenschutzrechtliche Bestimmungen für Geschäfte im Internet ausgesprochen. Vgl für Österreich: Kein Konsumentenparadies, Konsument 1/99, 18. In Deutschland hat zuletzt die Arbeitsgemeinschaft der deutschen Verbraucherverbände auf die Problematik beim Internet-Banking hingewiesen. Im Internet unter http://www.agv.de. Insbesondere wurde die mangelnde Anbieter und Preistransparenz beklagt. Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=990315016.

[153] Die Vorteile des online Shopping entsprechen im wesentlichen jenen des Versandhandels. Vgl dazu EB zur RV 16.

[154] Zum Ablauf eines Bestellvorganges im Internet ausführlich *Borges*, Zeitschrift für Wirtschaftsrecht 20/1999, 131.

[155] Zu den Gefahren vor übereilten Käufen im Online-Shopping vgl EB zur RV 17; *Madl*, Vertragsabschluss im Internet, ecolex 1996, 79; *Arnold*, CR 9/1997, 526; *Borges*, Zeitschrift für Wirtschaftsrecht 20/1999, 131.

[156] EB zur RV 20.

Anwendung. Unter den Begriff "Vertragsabschluß" fällt sowohl der Vorvertrag als auch die Vertragsabwicklung an sich und allfällige Leistungsstörungen. Nicht erfaßt sind jedoch Werbe- und Marketingmaßnahmen.[157]

Entscheidend ist, dass der „Lieferer“ bzw. „Betreiber einer Fernkommunikationstechnik“ für den Vertrag einen oder mehrere „Fernkommunikationstechniken“[158] verwendet.

Im Gegensatz zur deutschen Haustürgeschäftewiderrufsgesetz oder dem österreichischen KSchG kommt die Fernabsatzrichtlinie nicht mit einem einheitlichen Begriff für den Vertragspartner des Verbrauchers aus, sondern unterscheidet zwischen „Lieferer“ und „Betreiber“ einer Fernkommunikationstechnik. Lieferer ist der „fernabsetzende“ Vertragspartner des Verbrauchers, beispielsweise das Versandhaus oder der Service Provider.

In Anhang 1 findet sich eine demonstrative Aufzählung der Geschäfte bei denen **„Fernkommunikationstechniken“** zur Anwendung kommen.

In der Liste findet sich unter anderem zwar die E-Mail, nicht aber das Internet. Im Punkt 9 der Erwägungen zur Fernabsatzrichtlinie erklärt die Kommission dies damit, dass man aufgrund der raschen technischen Entwicklung keine erschöpfende Liste verfassen wollte. Es sollen vielmehr alle Fernmeldetechniken erfasst sein, die der Definition des Art 2 Z4 gerecht werden.

Darunter fallen demnach nicht nur Geschäfte von Verbrauchern über das Internet wie Videotext (Mikrocomputer, Fernsehbildschirm), Voice-Mail Systeme[159], Audiotext und

---

[157] EB zur RV 38.

"Fernabsatz" ist ein den nationalen Gesetzen unbekannter Rechtsbegriff, der offenbar aus der französischen Bezeichnung „vente à distance“ stammt. *Arnold*, CR 9/1997 FN 26.

[158] Unter Fernkommunikationstechniken ist nach Art 2 Z 4 jede Technik zu verstehen, welche ohne gleichzeitige physische Anwesenheit der Vertragsparteien den Abschluss eines Vertrages ermöglicht

[159] Der Verwendung von Voice-Mail Systemen wird eine rasante Verbreitung vorausgesagt. Im Bereich der Telephonie gibt es in jüngster Zeit sogenannte "Voice Portale". Dabei formuliert der Verbraucher Fragen an den Computer,

elektronische Post, sondern auch das Teleshopping, der Versandhandel per Katalog, die Zusendung von Drucksachen mit Bestellscheinen und die Telefonwerbung.
Damit findet die Richtlinie sowohl auf die klassische Form des Fernabsatzes, wie den Versandhandel als auch auf moderne Formen wie beispielsweise TV-Shopping oder Internet-Shopping Anwendung.[160] Der Anwendungsbereich der Richtlinie ist demnach verhältnismäßig weit.[161]
Zu **keiner Anwendung der Richtlinie** kommt es demnach, wenn der Unternehmer den Kontakt, der zum Vertragsabschluß führt, über das Internet anbahnt, es dann aber zu einen konventionellen Vertragsabschluß im Geschäft des Unternehmers oder durch einen Vertreter kommt.[162] Das ist deshalb bedeutsam, da sich, wie oben ausgeführt, zur Zeit viele Verbraucher über das Internet über Produkte und Dienstleistungen informieren, der Vertragsabschluß selbst jedoch in vielen Fällen offline abgewickelt wird. Damit ist eine ganz bedeutsame Anzahl von Verträgen vom Anwendungsbereich der Richtlinie ausgenommen. Das erscheint sachlich auch richtig, da auch schwer nachvollziehbar erscheint, ob sich ein Verbraucher online oder in anderer Weise über das gekaufte Produkt informiert hat und eine Überrumpelungssituation wohl nicht gegeben ist. In diesen Fällen stand dem Konsumenten auch vor Verabschiedung der

---

der bestimmte Schlüsselworte aus der Frage herausfiltert, die der Datenbank bekannt sind und formuliert daraus eine Datenbankabfrage. Beispiele dafür existieren bereits beim zweitgrößten Telefonanbieter Italiens "Omnitel Pronto Italia" und bei der schwedischen Bahn. Vgl. ausführlich *Mayer*, Als die Computer zuhören lernten, HightechPresse 10-99, 16.

[160] Nachdem es sich beim Internet um ein Kommunikationsmedium handelt, bei dem es ohne Zweifel zu einem Vertragsabschluß zwischen einem Lieferer und einem Verbraucher ohne gleichzeitige körperliche Anwesenheit kommt, ist das Online-Shopping eindeutig von der Richtlinie erfasst. *Widmer-Bähler*, Rechtsfragen beim Electronic Commerce (1997) 180.
Zur Klarstellung wurde die demonstrative Aufzählung der "Fernkommunikationsmittel" in Anhang 1 in Österreich in § 5a Abs 2 KSchG um die in der Richtlinie nicht angeführten elektronischen Medien ergänzt.

[161] So auch EB zur RV 31.

[162] *Madl*, ecolex 1996, 80.

Richtlinie kein Rücktrittsrecht nach § 3 KSchG zu, da oftmals der Konsument den Vertragsabschluß angebahnt hat.
Zusammenfassend gesagt, ist die Richtlinie somit auf alle Verträge anwendbar, die ***ohne persönlichen Kontakt*** *(also nicht von Angesicht zu Angesicht) zwischen den Vertragspartnern geschlossen werden*.[163]
Der österreichische Gesetzgeber übernimmt den Anwendungsbereich der Richtlinie, indem er sich in § 5 KSchG im wesentlichen an die vorgegebene Terminologie der Richtlinie hält.[164]

3.2.2.1 Ausnahmen vom Anwendungsbereich

Eine Reihe von Verträgen sind jedoch vom Anwendungsbereich der Richtlinie zur Gänze oder teilweise ausgenommen.
Art 3 der Richtlinie nimmt verschiedene Bereiche vom Anwendungsbereich der Richtlinie generell aus. Dieser Katalog war naturgemäß Gegenstand kontroverser Diskussionen.[165]
Gemäß Art 3 Abs 1 der Richtlinie werden Versteigerungen, Automatenkäufe, Immobiliengeschäfte mit Ausnahme der Vermietung und aufgrund der Benutzung von öffentlichen Fernsprechern mit den Betreibern von Telekommunikationsmitteln abgeschlossene Verträge zur Gänze von der Richtlinie ausgenommen.
Art 3 Abs 1 sieht auch eine Ausnahme des Anwendungsbereichs der Richtlinie für den **Verkauf von Finanzdienstleistungen** vor. Die Richtlinie gilt somit auch nicht für Online-Banking und den Online-Aktienhandel[166]. Da gerade diese im elektronischen Geschäftsverkehr zusehends an Bedeutung gewinnen, war diese Ausnahme auch Gegenstand heftiger Diskussionen.[167] Um keine

---

[163] EB zur RV 16 und *Arnold*, CR 9/1997, 529

[164] EB zur RV 23, 37.

[165] *Madl*, ecolex 1996, 80 FN 13.

[166] Zur Haftung bei Online-Banking vgl *Graf*, Wer haftet bei Telebanking?, e-commerce, ecolex 1999, 239 ff.

[167] *Hoeren*, Rechtsfragen des Internet (1999) 136. Im Internet unter http://www.uni-muenster.de/Jura.itm/hoeren.

Regelungslücke für diesen wichtigen Bereich zu hinterlassen, wird der „Fernverkauf von Finanzdienstleistungen" künftig in einer eigenen gemeinschaftsrechtlichen Regelung, der Richtlinie über den Fernabsatz von Finanzdienstleistungen geregelt werden.[168] Anleger, die Versicherungs- oder Bankgeschäfte online oder telefonisch durchführen wird darin ein Rücktrittsrecht von 14 Tagen eingeräumt.

Eine weitere Ausnahme ist jene für **Automatenkäufe**. Vor allem beim Bezug von Immaterialgütern wie Software, Filmen im Online-Demand Verfahren, MP3 Musik unter Eingabe der Kreditkartennummer und sofortigem Download wird wohl ein solcher Automatenkauf vorliegen.[169]

Damit sind erhebliche Bereiche des Online-Shoppings vom Anwendungsbereich der Fernabsatzrichtlinie ausgenommen.[170]

Auch **Online-Versteigerungen** wie beispielsweise jene unter http://www.ebay.com, fallen nicht unter die Richtlinie. Die Versteigerungen im Internet von Reisen, Kfz oder Flugtickets nehmen zu, sodass dadurch wiederum eine große Anzahl von Verträgen vom Anwendungsbereich ausgenommen wird.

Diese Ausnahmen wurden in § 5b KSchG mit Ausnahme der Verträge über die Benutzung von öffentlichen Fernsprechern mit den Betreibern von Telekommunikationsmitteln übernommen.[171]

Auf bestimmte Verträge ist die Richtlinie nur eingeschränkt anwendbar. Insbesondere die Informationspflichten und das Rücktrittsrecht sind nicht anwendbar.[172] Diese Ausnahmen wurden durch § 5c Abs 4 in das KSchG übernommen.

---

[168] Die Kommission hat dazu einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 90/619/EWG des Rates, sowie der Richtlinien 97/7/EG und 98/27/EG vorgelegt.

[169] *Hansen*, Klare Sicht am Info-Highway (1996) 167. In solchen Fällen liegt bereits ein Anbot iSd § 861 ABGB vor. Vgl unter 3.4.2.2.1.

[170] Daher auch die berechtigte Kritik von *Kilches*, Fernabsatzrichtlinie-Europäisches Electronic Commerce Grundgesetz?, Medien und Recht 5/97, 280.

[171] EB zur RV 37.

[172] Das sind gemäß Art 3 Abs 2 :

1. Verträge über die Lieferung von Lebensmitteln, Getränken oder sonstigen Haushaltsgegenständen des täglichen Bedarfs, die am Wohnsitz, am

3.2.3 Schutzmechanismen

Im wesentlichen beinhaltet die Richtlinie **drei Schutzmechanismen** für Verbrauchergeschäfte, die unter den Anwendungsbereich der Richtlinie fallen.[173] Art 4 räumt den Konsumenten ein Informationsrecht ein. Art 5 Abs 1 sieht eine schriftliche Bestätigung bestimmter Information durch den Vertragspartner des Konsumenten vor und Art 6 schreibt ein Widerrufsrecht vor.

3.2.3.1 Widerrufsrecht[174]

Das **Kernstück der Richtlinie** - und zugleich eine wesentliche Erweiterung der Verbraucherrechte gegenüber der bisherigen

---

Aufenthaltsort oder am Arbeitsplatz eines Verbrauchers von Händlern im Rahmen häufiger und regelmäßiger Fahrten geliefert werden

2. Verträge über die Erbringung von Dienstleistungen in den Bereichen Unterbringung, Beförderung, Lieferung von Speisen und Getränken sowie Freizeitgestaltung, wenn sich der Lieferer bei Vertragsabschluß verpflichtet, die Dienstleistungen zu einem bestimmten Zeitpunkt oder innerhalb eines genau angegebenen Zeitraums zu erbringen.

[173] *Arnold*, CR 9/1997, 529. Ihm folgend *Laga*, Internet, 124.

[174] Der Terminus "Widerrufsrecht" ist ein Novum im Sekundärrecht. Bisher wurde ausschließlich der Begriff "Rücktritt" verwendet. Offensichtlich sind diese Begriffe ident und setzen beide einen wirksam zustande gekommenen Vertrag voraus. Vgl ausführlich *Bülow*, Unsinniges im Fernabsatz, ZIP 31/99, 1294.

Offenbar ist auch in der Fernabsatzrichtlinie ein Rücktrittsrecht gemeint. Nach dem Wortlaut - es wird ausdrücklich auf einen *Vertragsabschluß* abgestellt - handelt es sich wohl um eine Art Rücktrittsrecht von dem bereits geschlossenen, aber in der Regel noch nicht erfüllten Vertrag. *Reich*, Die neue Richtlinie 97/7 EG über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, EuZW 19/1997, 586.

Rechtslage in Österreich[175] - ist das Widerrufsrecht gemäß Art 6.[176]

Ziel dieser Bestimmung ist die Korrektur von unüberlegten Bestellungen. Die Gefahr unüberlegter Vertragsabschlüsse ist im Fernabsatz besonders groß, da der Verbraucher die Ware nicht vor Augen hat und auch keine persönliche Beratung durch einen fachkundigen Verkäufer in Anspruch nehmen kann.[177]

Unabhängig ob die Vertragsanbahnung vom Unternehmer oder Konsumenten ausgegangen ist, steht dem Konsumenten jedenfalls ein **Rücktrittsrecht** zu.

Nur in bestimmten Fällen ist das Rücktrittsrecht **ausgeschlossen**, kann jedoch trotzdem auch bei diesen Verträgen vertraglich vereinbart werden. Nach Art 6 Abs 3 sind dies Verträge zur Erbringung von Dienstleistungen, deren Ausführung mit Zustimmung des Verbrauchers vor Ende der sieben Tage Frist begonnen hat; Verträge zur Lieferung von Waren über ungewisse Preise; Verträge zur Lieferung von Waren, die nach individuellen Wünschen der Kunden angefertigt werden, oder die nicht für eine Rücksendung geeignet sind; verderbliche oder abgelaufene Waren; Verträge zur Lieferung von Audio- oder Videoaufzeichnungen oder Software, die vom Verbraucher entsiegelt worden sind; Verträge zur Lieferung von Zeitungen, Zeitschriften und Illustrierten, sowie Verträgen zur Erbringung von Wett- und Lotterie-Dienstleistungen.

Es handelt sich dabei um Verträge, bei denen eine Rückabwicklung entweder nicht möglich oder unzumutbar wäre.[178]

---

[175] *Madl*, ecolex 1996, 81.

[176] *Arnold*, CR 9/1997, 530; ihm folgend *Borges*, Zeitschrift für Wirtschaftsrecht (ZIP) 20/1999136. *Arnold*, CR 9/1997, 531 übt jedoch auch Kritik am Widerrufsrecht, das seines Erachtens eine zu starke Position des Verbrauchers bedingt. Würden in den Mitgliedstaaten ausreichende Sanktionen für die Nichteinhaltung der Verpflichtungen nach Art 4 und 5 der Richtlinie verankert werden – was die Richtlinie im übrigen nicht vorschreibt - dann wäre seines Erachtens ebenfalls eine sehr starke Position des Konsumenten beim Vertragsabschluß über das Internet gegeben.

[177] EB zur RV 49.

[178] Begründung des Rates zum Gemeinsamen Standpunkt der Fernabsatz-Richtlinie vom 30.10.1995, ABl C 288 unter III. Für eine restriktive

Das Rücktrittsrecht kann vom Verbraucher "ohne Angaben von Gründen und ohne Strafzahlung" ausgeübt werden. Diese Wendung wurde nicht gesondert in das KSchG übernommen, da schon bisher der Rücktritt vom Verbrauchergeschäft nicht an die Angabe von Gründen oder die Zahlung einer Vertragsstrafe gebunden war.[179] Der Verbraucher muss das Rücktrittsrecht jedoch innerhalb einer **Frist von sieben Tagen** ausüben.[180]

Die Laufzeit der Frist beginnt bei Warenlieferungen mit dem Tag des Einlangens der Ware beim Verbraucher (wenn die schriftlichen Informationen gemäß Art 5 Abs 1 ordnungsgemäß übermittelt wurden), bei Dienstleistungen mit dem Tag des Vertragsabschlusses oder - wenn dies danach liegt - mit Erteilung der schriftlichen Informationen gemäß Art 5 Abs 1 der Richtlinie.[181]

Wenn diese Informationspflichten vom Unternehmer nicht erfüllt werden, sieht die Fernabsatzrichtlinie ein **erweitertes Rücktrittsrecht** vor. Die Dauer der Frist beträgt in diesem Fall drei Monate. Die Laufzeit der Frist beginnt bei Warenlieferungen wiederum mit dem Tag des Einlangens der Ware beim Verbraucher (unter der Voraussetzung, dass die schriftlichen Informationen gemäß Art 5 Abs 1 ordnungsgemäß übermittelt wurden), bei Dienstleistungen mit dem Tag des Vertragsabschlusses.

Auslegung der Ausnahmen *Arnold*, CR 9/1997, 531. Diese Ausnahmen wurde in § 5f KSchG übernommen.

[179] EB zur RV 50.

[180] Ursprünglich war im Entwurf noch eine Frist von 14 Tagen vorgesehen. Das hat jedoch heftige Kritik seitens der Wirtschaftskammer Österreich ausgelöst. Vgl die Stellungnahme der WKÖ zum Ministerialentwurf des Fernabsatzgesetzes. Neben dieser Abweichung des Fernabsatz-Gesetzes von den Vorgaben der Richtlinie wurden auch die Abweichungen in den §§ 5b, 5g Abs 2, 5i und 5k kritisiert. Im Internet unter http://www.wk.or.at/rp/fabsatz.htm.

[181] Da die Richtlinie vom „Widerruf des Vertragsabschlusses“ spricht, meint *Madl*, ecolex 1996, 81, dass die Frist nicht vor dem Vertragsabschluß zu laufen beginnen kann. Die Richtlinie gibt aber keine Möglichkeit eines Widerrufs im Fall eines vom Unternehmer noch nicht angenommenen Anbots. Er

In Österreich führt Art 6 zu erheblichen Änderungen, da bisher dem Verbraucher im österreichischen Recht nach hM kein Rücktrittsrecht gemäß § 3 KSchG für Geschäfte im Internet zustand.[182]

Nach § 3 Abs 1 KSchG wird dem Konsumenten ein Rücktrittsrecht bei Verträgen gewährt, die außerhalb der Geschäftsräume des Unternehmers geschlossen werden. Dieses Rücktrittsrecht bei sogenannten „Haustürgeschäften“ soll einen Ausgleich für den "überrumpelten" Verbraucher schaffen, der in solchen Situationen möglicherweise einen ungewollten Vertrag abschließen könnte. Das Rücktrittsrecht steht dem Verbraucher gemäß § 3 Abs 3 Z1 bzw Z2 jedoch nicht zu, wenn das Geschäft mit dem Unternehmer vom Verbraucher selbst angebahnt wurde oder dem Vertragsabschluß keine Besprechung zwischen den Vertragsparteien vorangegangen ist.

Begründet wurde dies damit, dass Geschäfte im Electronic Commerce durch den Unternehmer meist nicht "angebahnt" wurden, da das Suchen und Abrufen einer Internetseite eines Unternehmers als Anbahnungstätigkeit des Verbrauchers iSd § 3 KSchG zu verstehen sei. Zudem findet in der Regel auch keine Besprechung iSd § 3 Abs 3 Z2 KSchG vor Abschluß eines Rechtsgeschäfts im Internet statt.[183]

In der Praxis wurde im Versandhandel dem Verbraucher jedoch schon bisher in den Allgemeinen Geschäftsbedingungen eine Rücktrittsfrist von 14 Tagen eingeräumt.[184]

Das im Art 6 Abs 1 dem Verbraucher eingeräumte "Widerrufsrecht" wird durch § 5e KSchG umgesetzt. *Nunmehr steht dem Verbraucher bei Geschäften im Fernabsatz im Gegensatz zum "Haustürgeschäft" gemäß § 3 Abs 3 Z1 und 2 KSchG ein Rücktrittsrecht auch dann zu, wenn er das Geschäft*

---

schlägt daher vor, ähnlich wie in § 3 KSchG dem Verbraucher das Rücktrittsrecht bereits ab Abgabe des Anbots einzuräumen.

[182] *Madl*, Vertragsabschluß im Internet, ecolex 1996, 82; *Jaburek/Wölfl*, Cyber-Recht, 106; *Brenn*, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ 1997, 654.

[183] *Brenn*, ÖJZ 1997, 654.

[184] EB zur RV 15, 32 und 50.

angebahnt hat und keine Besprechungen dem Vertrag vorausgegangen ist.[185]

Auch in Deutschland bestand vor Umsetzung der Richtlinie mangels Anwendbarkeit des Haustürgeschäftewiderrufsgesetzes[186] auf das Internet nicht in jedem Fall ein Rücktrittsrecht für den Verbraucher im elektronischen Geschäftsverkehr.[187]

In Zukunft steht für online abgeschlossene Verträge dem Verbraucher sowohl das Rücktrittsrecht nach § 5e Abs 1 KSchG als auch jenes nach § 3 KSchG zu, das von der neuen Bestimmung unberührt bleibt.

3.2.3.2 Informationspflichten der Anbieter

Schon das Auffinden der Adresse eines potentiellen Vertragspartners kann im Internet für den Verbraucher schwierig sein. Die Richtlinie sieht daher **detaillierte** - gegenüber dem österreichischen Recht erweiterte - **Informationspflichten** des Unternehmers gegenüber dem Konsumenten bereits *vor* Abschluß des Vertrages vor. Der Verbraucher soll dadurch vor Abgabe der Bestellung einen umfassenden Überblick über seinen Vertragspartner, über Details der Leistung, des Preises und der sonstigen Kosten erhalten.[188]

---

[185] Begründet wird diese unterschiedliche Wertung vom Gesetzgeber in den EB zur RV, 49 mit den nicht vergleichbaren Situationen beim Haustürgeschäft und im Fernabsatz in Bezug auf den Rücktritt.

[186] Gesetz über den Widerruf von Haustürgeschäften und ähnlichen Geschäften (HWIG) vom 16.1.1986, dBGBl I, 122.

[187] Vgl zur hL *Waldenberger*, Grenzen des Verbraucherschutzes beim Abschluss von Verträgen im Internet, BB 1996, 2365 (2367); *Hoeren*, Internet, 133; *Köhler*, Die Rechte des Verbrauchers beim Teleshopping (TV-Shopping, Internet-Shopping), NJW 1998, 185; *Borges*, Zeitschrift für Wirtschaftsrecht (ZIP) 20/1999, 136.
Begründet wurde die Nichtanwendbarkeit mit der Tatsache, dass sich der Verbraucher beim Teleshopping aus freiem Entschluss in das Netz einwählt und eine Homepage eines Anbieters aufruft. Es fehle daher an der für das HWIG typischen Überrumpelungssituation.

[188] Erwägungsgrund 11 der Fernabsatzrichtlinie; EB zur RV 43.

Zum Schutz des Verbrauchers muß der Unternehmer diesen gemäß Art 4 „klar und verständlich“ vor Abschluß des Vertrages über verschiedene für die Kaufentscheidung besonders wichtige Punkte informieren.[189]

Die Richtlinie verlangt, dass dem Verbraucher diese Informationen vor Vertragsabschluß zur Verfügung stehen müssen.

§ 5c Abs 1 KSchG bestimmt darüber hinaus, dass diese Angaben dem Verbraucher bereits vor Abgabe seiner Vertragserklärung vorliegen müssen, dh vor Abgabe seiner Bestellung, da er beim Vertragsabschluß bereits an sein Anbot gebunden ist.[190]

Im einzelnen wird vom Anbieter die **Angabe folgender Punkte** verlangt.

1. die *Identität des Unternehmers* sowie im Fall einer Vorauszahlung dessen Anschrift[191], 2. die wesentlichen *Produkteigenschaften* und Preis inkl. aller Steuern, 3. eventuelle *Lieferkosten*, 4. die *Modalitäten über die Zahlung und Lieferung*, 5. eine Belehrung über das Rücktrittsrecht[192], 6. *Fernkommunikationskosten*, sofern diese höher sind als der Grundtarif und 7. die *Gültigkeitsdauer von Anbot und Preis*.

Diese Informationen müssen beim elektronischen Geschäftsverkehr bevor der Verbraucher eine Willenserklärung abgibt, diesem auf dem Bildschirm angezeigt werden. Der Verbraucher muß sie eindeutig wahrnehmen können. Dies könnte in der Form erfolgen, dass sich der Lieferer die Kenntnisnahme dieser Angaben vom Verbraucher bestätigen läßt, im Internet beispielsweise mittels eines Bestätigungsfensters.[193] Es genügt jedenfalls, wenn der Verbraucher die Informationen selbst

---

[189] Beachte auch Art 10 der Richtlinie E-Commerce unter 3.4.2.2.

[190] *Engel*, Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz (Dissertation Universität Salzburg, 1997) 53.

[191] Für eine weite Interpretation *Madl*, ecolex 1996, 80, der darunter den vollen Namen, die Rechtsform und genaue Adresse versteht.

[192] *Madl*, ecolex 1996, 80 meint, dass hierfür der Text von Art 6 zitiert werden müsste, was mE nicht zielführend ist, da dieser Text nicht wortwörtlich in das KSchG übernommen wurde. Um Verwirrungen zu vermeiden, sollte eher der Text des § 5e KSchG abgedruckt werden.

abrufen kann ohne, dass sie ihm vom Unternehmer eigens übermittelt wurden. Eine allgemein zugängliche und abrufbare Internetseite wäre dafür wohl ausreichend.[194]

3.2.3.3 Bestätigungspflicht der Anbieter

Der Verbraucher muß gemäß Art 5 diese Informationen (die vorher auf dem Bildschirm angezeigt wurden) **bis zur Erfüllung des Vertrages** (bei Waren spätestens bis zur Lieferung) auch schriftlich oder mittels einem "dauerhaft zur Verfügung stehenden Datenträger" **bestätigt** erhalten.
Grund dafür ist offenbar die Tatsache, dass bei elektronischen Bestellungen dem Verbraucher die Vertragsbedingungen lediglich in elektronischer Form vorliegen und sie der Verbraucher vor Vertragsabschluß noch einmal schriftlich in Händen halten soll.[195]
Zusätzlich zu den Informationspflichten gemäß Art 4 ist der Konsument dabei auch über den Kundendienst und die geltenden Garantiebedingungen aufzuklären.[196]
Diese Informationen müssen dem Verbraucher "**auf Dauer zur Verfügung stehen**". Ausreichend sind sicherlich die Abspeicherung auf einer Festplatte, Disketten, CD Roms, Videokassetten und E-Mail.[197] Leider findet sich weder in § 5d KSchG noch in den EB zur RV eine Klarstellung, ob eine

---

[193] *Arnold*, CR 9/1997, 530.

[194] EB zur RV 43.

[195] *Arnold*, CR 9/1997, 530.

[196] *Madl*, ecolex 1996, 81, will dies auch auf die Gewährleistungsregelungen ausdehnen und schlägt vor, einen Hinweis auf die landesspezifischen Regelungen der Gewährleistung anzubringen. Dies ist mE nicht mit dem Wortlaut der Richtlinie vereinbar und würde darüber hinaus zu einer unangemessenen Belastung für die Anbieter führen.

[197] Nach den EB zur RV 47 soll dies für E-Mail nur eingeschränkt gelten. ME ist es wenig zielführend dem Unternehmer zuzumuten, sich über die technische Ausbildung und Ausrüstung seines Vertragspartners zu informieren. Das würde bedeuten, dass sich der Unternehmer vor Vertragsabschluß über die Ausstattung die Hard- und Software sowie den Server des Verbrauchers informieren müsste.

jederzeit abrufbare Internetseite ein "dauerhafter Datenträger" im Sinne dieser Bestimmung ist.[198] In den Erläuterungen zum Entwurf wird lediglich festgehalten, dass „wenn der Unternehmer seiner Informationspflicht durch das Versenden der Informationen in Form von Disketten, CD-ROM oder Videokassetten nachkommt, das Formerfordernis gewahrt sein soll. Aber auch eine Sendung im Wege der E-Mail wird als eine die schriftliche Übermittlung substituierbare Datenträgerform ausdrücklich anzusehen sein, sofern der Verbraucher eine entsprechende Adresse bekannt gegeben hat sowie eine derartige Sendung empfangen und ohne besonderen Aufwand lesen, speichern oder ausdrucken kann.“

Die Bestätigung muß allerdings nur erfolgen, sofern dem Verbraucher die aufgezählten Informationen nicht bereits beim Vertragsabschluß in der bezeichneten Form erteilt wurden. Darüber hinaus nimmt Art 5 Abs 2 gewisse Verträge von dieser schriftlichen Bestätigung der Informationen aus. Darunter fallen beispielsweise die telefonische Fernwartung eines Computerprogrammes oder die Abfrage von Datenbanken wie das elektronisches Firmenbuch.[199]

Problematisch wird die Erfüllung der Verpflichtung des Art 5 bei einer **Leistungserbringung in digitaler Form** sein. Hier wäre an die Übermittlung eines Dokumentes in digitaler Form zu denken, das mit einer elektronischen Signatur versehen ist.[200] Überhaupt schließt die Richtlinie meines Erachtens die Bestätigung durch digital signierte Dokumente nicht aus, da lediglich die schriftlicher Bestätigung oder jene auf anderen Datenträgern gefordert ist.

---

[198] ME ist das zu bejahen, da eine jederzeit abrufbare, nicht durch Zugangscodes lediglich einer eingeschränkten Benutzergruppe vorbehaltene Internetseite wohl vom durchschnittlichen Verbraucher ohne besonderen Aufwand gelesen, gespeichert und ausgedruckt werden kann.
Würde man das verneinen ergäbe sich für Unternehmen eine erheblicher Aufwand, da wiederholt dieselben Informationen verschickt werden müssten.

[199] *Madl*, ecolex 1996, 81.

[200] *Arnold*, CR 9/1997, 530.

Durch § 5 d KSchG wird Art 5 der Fernabsatzrichtlinie ohne Veränderung in das KSchG übernommen.

3.2.4 Ergänzende Bestimmungen

3.2.4.1 Werbung über elektronische Netze - Spamming

Bereits im Frühjahr 1996 hat die Kommission die Prinzipien ihrer zukünftigen Politik auf dem Gebiet der kommerziellen Kommunikation im Rahmen des **Grünbuchs zur kommerziellen Kommunikation im Binnenmarkt** veröffentlicht.[201] Dieses Thema ist gerade in Hinblick auf die zukünftige rasante Entwicklung der Informationsgesellschaft, insbesondere des Internet von besonderer Bedeutung. Die zunehmende grenzüberschreitende kommerzielle Kommunikation und die damit auftretenden Probleme durch unterschiedliche einzelstaatliche Regelungen werden im Grünbuch einer detaillierten Analyse unterzogen. **„Kommerzielle Kommunikation„** ist demnach ein wesentlicher Bestandteil des elektronischen Geschäftsverkehrs.

---

[201] Grünbuch über kommerzielle Kommunikation im Binnenmarkt, KOM (96) 192 endg. Unter dem von der Kommission weit definierten Begriff „kommerzielle Kommunikation“ ist jede Form von Werbung, Direktmarketing, Sponsoring, Verkaufsförderung und Öffentlichkeitsarbeit zu subsumieren.
In Übereinstimmung mit dem Grünbuch fallen auch nach Art 2 lit e der E-Commerce Richtlinie „alle Formen der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren und Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer sonstigen Organisation oder einer natürlichen Person dienen, die eine Tätigkeit in Handel, Gewerbe oder Handwerk oder einen freien Beruf ausübt“ unter den Begriff der „kommerziellen Kommunikation“.
Nicht erfasst vom Begriff der „kommerziellen Kommunikation“ sind jedoch nach der E-Commerce Richtlinie unabhängige Produktförderungen wie die Erwähnung einer Domain-Name oder einer E-Mail Adresse. Ebenfalls nicht ausreichend sind der bloße Besitz einer Internet Adresse oder eine Hypertext Verknüpfung mit einer Internet Adresse, über die „Kommerzielle Kommunikation“ betrieben wird.

Die Kommission zieht im Grünbuch zusammenfassend den Schluss, dass die kommerzielle Kommunikation für alle Marktteilnehmer im Binnenmarkt möglichst keinen Beschränkungen unterworfen werden soll und Regelungen darüber in allen Mitgliedsländern möglichst einheitlich gestaltet sein sollen.

Das Internet wird tatsächlich zunehmend als **Werbeplattform** genutzt. In Österreich wurden 1998 etwa 50 Millionen Schilling in Online-Werbung investiert. Weltweit wird eine Steigerung des Werbevolumens im Internet bis zum Jahr 2003 auf 15 Milliarden US-Dollar (3,2 Milliarden Schilling) prognostiziert.[202]

Die Vorteile des Mediums als Werbeplattform genutzt zu werden, liegen auf der Hand. Die Erreichbarkeit einer großen Anzahl von Kunden, hochgradige Individualisierungsmöglichkeit der Information und eine völlige neue Dimension der Geschwindigkeit in der Verteilung der Werbebotschaften machen das Internet zu dem Werbemedium der Zukunft.[203]

Online Anbieter versuchen dabei oftmals die entstehenden Kosten mittels einer Refinanzierung durch Werbung wieder hereinzuspielen. Nicht immer ist die Wirksamkeit der Online Werbung leicht zu quantifizieren. Es gibt mehrere Verfahren die zur Zeit herangezogen werden, wie insbesondere Hits, Page Impressions oder Page Views, AdImpressions oder AdViews und Visits.

Im Internet bestehen verschiedene **Arten von Werbemöglichkeiten**. Die häufigsten sind Banner[204], related links[205], Buttons[206], Microsites[207], Sponsoring, keyword buying[208], adbreaks[209] und natürlich E-Mail Werbung.

---

[202] *Schönberger*, www.werben.at, Trend August 1999, 24; *Schönherr*, Schmarotzer im Internet: Recht setzt Online-Werbung Grenzen, Die Presse vom 6.9.1999, 9.

[203] *Schönberger*, Trend August 1999, 24.

[204] Banner sind kleine Werbegrafiken oder Texte die - meist in einem Standartformat - als Dateien in HTML-Dokumente eingebunden werden.

[205] Microsites sind themenbezogene Querverweise auf eine Homepage.

[206] Buttons sind kleine statische Werbeflächen als institutionalisierte Hinweise auf einen Sponsor oder ein Produkt.

In jüngster Zeit ist weltweit eine dramatische Zunahme von Massenaussendungen per E-Mail zu Werbezwecken festzustellen.[210] Mit der Verbreitung der Übersendung von elektronischer Post ergab sich zunehmend das Problem des sogenannten "**Spamming**". Darunter versteht man das massenweise Versenden von Werbung per E-Mail an eine Vielzahl von Adressaten, ohne vorausgehenden Kontakt zum Absender und ohne, dass die Adressaten an dem Inhalt der Email Interesse haben.[211] Inzwischen ist eine heftige Diskussion über Vor- und Nachteile der E-Mail Werbung, insbesondere von Massensendungen per E-Mail entstanden.

Die Befürworter eines Verbots von unerwünschten E-Mails argumentieren im wesentlichen mit einer Analogie zur Rechtsprechung, welche die unerbetene Fax-Zusendung nach § 1 UWG verboten hat, da sie darin einen Eingriff in das Eigentum des Empfängers an Papier und Toner gesehen hat und die Übertragung unerwünschter Werbung per E-Mail bei den Anwendern Kosten und einen erheblichen Zeitaufwand verursache. [212]

---

[207] Dabei klickt der User auf ein, in einer Seite integriertes Fenster und es öffnet sich ein kleines Icon des Werbekunden, in dem das WWW-Angebot präsentiert wird.

[208] Dem Werbekunden von Suchmaschinen wird auch die Möglichkeit der Buchung von Suchbegriffen (Keyword buying) angeboten.

[209] Adbreaks sind Unterbrechungen in Form einer Werbeeinblendung. Das bedeutet, dass nach einer bestimmten Anzahl von angeklickten Seiten im WWW automatisch eine bildschirmgroße Werbeschaltung erfolgt.

[210] Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=981213006; http://www.pressetext.at/show.pl.cgi?pta=990121025. Eine besondere Form von E-Mail Missbrauch ist jener Fall, wo Hacker über fremde Rechner Massen E-Mails mit gefälschtem Absender verschicken. Die Empfänger-Adressen werden mit einem Zufallsgenerator erzeugt und existieren gar nicht. Der betroffene Mailserver schickt die elektronische Post umgehend als unzustellbar zurück und überflutet den Absender mit Tausenden von E-Mails.

[211] Zum Begriff „Spam“ siehe im Internet unter http://www.cnet.com/Resources/Info/Glossary/Terms/spam.html.

[212] So auch offenbar das Justizministerium in de EB zur RV 28. " In gleicher Weise ist davon auszugehen, dass der vom Adressaten nicht gewünschte Einsatz von E-Mails als Eingriff in die Privatsphäre des Adressaten unzulässig ist."

Im Gegensatz dazu wird betont, dass diese Argumentation bei E-Mail nicht greife, da hierbei weder Papier noch Toner verbraucht wird.[213]

Als Argumente gegen ein gesetzliches Verbot von Emails wird vor allem das verfassungsgesetzlich gewährleistete Recht auf freie Meinungsäußerung gemäß Art 10 EMRK angeführt, das nach stRspr des VfGH auch die kommerzielle Werbung erfasst.[214]

Da ein generelles Verbot im vorhinein und gegen alle Unternehmen gerichtet wäre, wird auch ein Verstoß gegen die Presse- und Zensurfreiheit erwogen.

Eine Studie der Europäische Kommission soll nun die spezifischen Problemen des Datenschutzes und des Schutzes der Privatsphäre, die durch unerwünschte elektronische Postsendungen entstehen, wissenschaftlich untersuchen. Außerdem soll im Rahmen der Studie untersucht werden, wie innerhalb der Europäischen Union mit Vorschriften auf diese Probleme reagiert wird.[215]

Offenbar ist man sich bewußt, dass nur ein koordiniertes - zumindest europaweit einheitliches - Verbot der unerwünschten E-Mails zum gewünschten Ziel führen kann.

3.2.4.1.1 Art 10 der Fernabsatzrichtlinie

Unter dem Motto "Stimm gegen SPAM - Vote agains SPAM - Votez contre le SPAM". riefen im Februar 1999 die Fachzeitschrift "c´t Magazin für Computertechnik" und die parteienunabhängige Informations- und Kommunikationsplattform "politik-digital" aus Deutschland die Bürger der Europäischen Union zu einer Petition gegen unerwünschte Werbung per E-Mail auf. Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=990228006. Eine Umfrage der Internet-akademie.de vom Februar 1999 belegt, dass 80 Prozent der Internetnutzer in Deutschland sich auch dann gegen E-Mail-Werbung aussprechen, wenn sie als solche gekennzeichnet wird. Im Internet unter http://www.akademie.de/tips_tricks/.

[213] Urteil des Landgerichts Berlin im Hauptverfahren vom 13.10.1998, wonach lediglich Zeit, Arbeitsaufwand und Speicherplatz beeinträchtigt wird. Im Internet unter http://www.online-recht.de/vorent.html.

[214] VfSlg 10.948/1986.

[215] Im Internet unter http://www.pte.at/show.pl.cgi?pta=990817002.

Den sekundärrechtlichen Rahmen für die Werbung per E-Mail legt die Fernabsatzrichtlinie fest, indem sie in **Art 10** die Verwendung bestimmter Fernkommunikationstechniken beschränkt. Die Richtlinie zielt auf den Schutz der Privatsphäre des Verbrauchers, um diesen vor aggressiven Verkaufsmethoden bewahren. Er soll sich insbesondere gegen Belästigungen durch besonders aufdringliche Marketingstrategien und Kommunikationstechniken zur Wehr setzen können.
Die Mitgliedstaaten werden daher in Art 10 verpflichtet, Vorkehrungen gegen die unbestellte Zusendung von Waren und Dienstleistungen zu treffen und müssen Verbraucher, die bestimmte Kommunikationsmittel nicht verwenden wollen, durch geeignete Mittel wirksam vor derartigen Maßnahmen schützen.
Den Mitgliedstaaten steht es jedoch gemäß Art 14 frei, strengere Bestimmungen zu erlassen oder beizubehalten.
Auf Gemeinschaftsebene war diese Regelung über Beschränkungen beim Einsatz von Fernkommunikationsmitteln sehr **umstritten**[216].
Im geänderten Vorschlag der Europäischen Kommission war noch vorgesehen,[217] dass auch die unaufgeforderte Lieferung von E-Mails (auch zu Werbezwecken) und die Telefonverwendung nur mit vorheriger Zustimmung des Verbrauchers erlaubt sein sollen. Letztendlich wurde dieser Vorschlag vom Rat und vom Europäischen Parlament aber nicht übernommen.
Nunmehr bedarf gemäß Art 10 lediglich die Nutzung von Voice Mail Systemen[218] und Telefax der Einholung einer vorherigen Zustimmung des Empfängers ("**opt in**").[219]

---

[216] EB zur RV 27.

[217] Art 4 des geänderten Vorschlags der Europäischen Kommission, ABl C 308 vom 15. November 1993, 18.

[218] Unter Voice-Mail-System versteht man die Verwendung eines Automaten als "Gesprächspartner" des Verbrauchers. Diese Geräte ermöglichen eine individuelle und gegenseitige Kommunikation. Daher sind bloße Anrufbeantworter nicht darunter zu subsumieren. EB zur RV 45.

[219] Als Vorbild dieser Regelung dienten wohl die Anti Spam Gesetze in den USA, wo sich beispielsweise in Kalifornien Internet-Nutzer in eine Email-Adressen Liste - analog zur Robinson Liste gegen Werbung an der Haustüre - eintragen lassen können, wodurch die Zusendung kommerzieller Emails an diese Nutzer verboten werden. Bei Zuwiderhandlungen gegen diese

Diese Zustimmung kann vom Verbraucher jederzeit widerrufen werden. Andere Kommunikationstechniken, die eine individuelle Kommunikation ermöglichen, wie E-Mails, die zur Werbung verwendet werden können, dürfen nur dann nicht verwendet werden, wenn der Empfänger dies "nicht offenkundig" abgelehnt hat ("**opt out**").

*Nach Art 10 bedarf demnach die Verwendung folgender Techniken durch den Lieferer bedarf der vorherigen Zustimmung des Verbrauchers: 1. Kommunikation mit Automaten als Gesprächspartner (**Voice-Mail-Systeme**) und 2. Fernkopie (**Telefax**). E-Mail wird nunmehr in der Fernabsatzrichtlinie bewußt nicht der Telefax- und Telefonwerbung gleichgestellt.*

Vom Gesetzgeber wurde in Österreich durch Art 10 der Richtlinie im überarbeiteten Entwurf prinzipiell kein Anpassungsbedarf gesehen.[220] Begründet wurde dies vom Gesetzgeber, dass der von der Richtlinie angestrebten Schutz der Privatsphäre des Verbrauchers schon das geltende Recht biete.[221]

Eintragungen in Robinson Listen drohen Verwaltungsstrafen. Im Internet unter http://www.pte.at/show.pl.cgi?pta=981004001.

[220] EB zur RV 27, worin betont wird, dass „Art 10 über "Beschränkungen in der Verwendung bestimmter Fernkommunikationstechniken" in Österreich keiner gesonderten Umsetzung bedarf."

[221] EB zur RV 28. In Österreich sind insbesondere die Judikatur zu § 16 ABGB (ein allgemeines Persönlichkeitsrecht auf Achtung des Privatbereichs wird von der Rechtsprechung abgeleitet) und zu § 1 UWG 1984 im Zusammenhang mit dem Einsatz von "Fernkommunikationstechniken" zu beachten.
Darin wurde betont, dass der Einsatz solcher Techniken ohne die - vorherige - Zustimmung des Adressaten unzulässig ist.
Daraus ergibt sich, dass die unerbetene telefonische Werbung bei Privatpersonen verboten ist (vgl OGH 18.10.1994, 4 Ob 107/94, ÖBl 1995, 12).
Auch ist die Telefax-Werbung ist unzulässig, wenn der Anschlussinhaber die Werbesendung weder gewünscht hat noch der Werbende nach den besonderen Umständen des Einzelfalls ein Einverständnis voraussetzen konnte. Vgl. OLG Graz 5.3.1992, 6 R 227/91, ÖJZ 1995/27; LGZ Wien 22.8.1994, 40 R 341/94, ÖJZ 1995/28.

Einziger Anpassungsbedarf wurde im Bereich der **Verwendung von Automaten als "Gesprächspartner"** gesehen, die offenbar durch die auf den Schutz des privaten Lebensbereichs abstellenden Regelungen des § 16 ABGB und des § 1 UWG 1984 noch nicht vollständig abgedeckt erschienen.[222] Aus diesem Grund wurde die Verwendung dieses spezifischen Kommunikationsmittels besonders geregelt. Wenn der Verbraucher bei Gesprächen mit Automaten selbst Anrufer ist, kann es bei Voice-Mail-Systemen durchaus vorkommen, dass der Verbraucher nicht sofort erkennt, dass er mit einem Automaten kommuniziert. Nur wenn er sich dessen bewußt ist, kann er sich entscheiden, ob er seine Zustimmung zum Einsatz dieses Kommunikationsmittels erteilen und das Telefonat fortsetzen möchte oder nicht.[223]
Deshalb wurde § 5c Abs 2 zweiter Satz in das KSchG eingefügt, der die geltende Rechtslage ergänzen soll. Bestimmungen, nach denen der Einsatz bestimmter Fernkommunikationsmittel beschränkt oder verboten ist, sollen davon unberührt bleiben. Auch die – zur Frage der Zulässigkeit unerbetener Telefonanrufe – gefestigte Rechtsprechung soll durch diese Ergänzung nicht beeinträchtigt werden.[224]
Der Bestimmung des Art 4 Abs 3 der Fernabsatzrichtlinie, durch die der Verbraucher vor aggressiven Vertriebsmethoden in seiner Privatsphäre geschützt werden soll, wird durch § 5c Abs 3 KSchG entsprochen. Die Bestimmungen über die Zulässigkeit eines Telefonanrufes - vor allem § 5j Abs 2 KSchG und § 101 TKG sowie die einschlägige Rechtsprechung - bleiben durch diese Norm unberührt.
Die Bestimmungen des Art 10 der Fernabsatzrichtlinie zum Schutz der Privatsphäre des Verbrauchers sollen durch § 5j KSchG umgesetzt werden. § 5j Abs 1 KSchG ist insofern enger gefasst als die Richtlinie, als eine vorherige Zustimmung des

---

Der OGH (27.4.1999, 1 Ob 82/99m) gewährt dem gestörten Nutzer eines Faxgerätes als Schadenersatz die „Manipulationskosten“ für die Durchsicht der unerwünschten Faxsendungen.

[222] EB zur RV 45.

[223] EB zur RV 46.

[224] EB zur RV 46.

Verbrauchers zur Verwendung von Fernkopien oder Automaten als Gesprächspartner nur erforderlich ist, "sofern die Verwendung geeignet ist, die Privatsphäre des Verbrauchers zu beeinträchtigen".

Im Bezug auf alle anderen, potentiell störenden, Fernkommunikationsmittel sieht hingegen § 5j Abs 2 KSchG eine weitere Regelung vor, indem diese Kommunikationsmittel verwendet werden dürfen "wenn der Verbraucher dies nicht offenkundig abgelehnt hat". Auf die positive Kenntnisnahme durch den Unternehmer wird nicht abgestellt. Schon die offenkundige Ablehnung durch den Verbraucher soll ausreichen.[225] Der für die Abwicklung von Online-Shopping Verträgen wichtige Einsatz von E-Mail soll durch diese Bestimmung laut den Erläuterungen zum Entwurf nicht erfaßt werden.[226]

Obwohl der österreichische Gesetzgeber im Zuge der Umsetzung der Fernabsatzrichtlinie in das KSchG keinen Anpassungsbedarf gesehen hat, wurde kurzfristig doch ein Verbot von E-Mail Werbung gesetzlich verankert. Nicht als spezifische Verbraucherschutzbestimmung im Konsumentenschutzrecht, sondern als allgemein - auch zwischen Unternehmern - geltende Regelung im Telekommunikationsgesetz.[227]

Dies offenbar deshalb, da nach vor der Umsetzung in Österreich die Diskussion entstanden ist, ob § 101 TKG (alte Fassung), auch analog auf unerwünscht zugesandte Werbe E-Mails anwendbar sei. Seitens mehrerer Fernmeldebehörden wurde die Auffassung vertreten, dass Werbe E-Mails nicht unter § 101 TKG (alte Fassung) fallen, da diese nicht explizit genannt seien.[228]

---

[225] EB zur RV 52.

[226] EB zur RV 53.

[227] § 101 TKG letzter Satz: „Die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken bedarf der vorherigen - jederzeit widerruflichen - Zustimmung des Empfängers." Eine verwaltungsrechtliche Sanktion ist in 104 Abs 3 Z23 enthalten.

[228] Kurier vom 3.4.1999, 19. Unabhängig davon ist ein allfälliger Unterlassungs- oder Schadenersatzanspruch nach dem allgemeinen Zivilrecht oder dem UWG zu beurteilen.

§ 101 TKG alte Fassung erklärte Anrufe sowie das Senden von Fernkopien zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers für unzulässig.[229]

Im **neuen § 101 TKG** wurde nach einem Beschluß des Justizausschusses des Nationalrates Anfang Juli auch ein **explizites Verbot der Zusendung elektronischer Post** als Massensendung oder zu Werbezwecken - ohne vorherige Zustimmung des Empfängers eingefügt.[230] Demnach bedarf die "Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken der vorherigen - jederzeit widerruflichen - Zustimmung des Empfängers."

Im Gegensatz zur Fernabsatzrichtlinie, die eine liberale "opt-out-Lösung" vorsieht (Spams sind nur dann verboten, wenn man sich in eine Liste einträgt, in der man die Zusendung von Massen-Mails nicht wünscht, sieht § 101 TKG eine sogenannte "opt-in" Maßnahme vor. Spamming ist demnach nur mit Zustimmung des Empfängers gestattet. Diese Bestimmung wurde in allerletzter Sekunde aufgrund verschiedener privater und öffentlicher Initiativen eingefügt.[231]

---

[229] Diese Regelung entspricht im wesentlichen dem Art 12 der Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation.
Damit ist für den Bereich der Werbung eine Regelung in Kraft, die in ihrem Anwendungsbereich insofern weiter geht, als sie nicht auf das Verhältnis zwischen Unternehmer und Verbraucher beschränkt ist, sondern allgemein gilt.

[230] Das Justizministerium hat im 1.Entwurf zur Novelle des KSchG im Zuge der Umsetzung der Fernabsatzrichtlinie die Einfügung dieser Bestimmung (ausdrückliches Verbot der Zusendung unerwünschter E-Mail) in das KSchG vorgeschlagen. Dieser Entwurf ging weit über die Vorgaben der Richtlinie hinausging.

[231] Offener Brief der Vereinigungen *EuroCAUCE*, *medianexus*, *quintessenz* und *VIBE.AT* an die Mitglieder des Justizausschuss des Nationalrates, ein Verbot von unerwünschter Zusendung via E-Mail auch in das KSchG aufzunehmen. Im Internet unter http://www.vibe.at/aktion_9906/index.html.
Vor allem Institutionen wie die *Arbeiterkammer*, Konsumentenverbände und auch die *ISPA* (Verband der Internet-Serviceprovider Österreichs) forderten vehement ein Verbot.

Diese sehr weitgehende und allgemein formulierte Regelung wurde bereits im Hinblick auf den unklaren Anwendungsbereich und den damit verbundenen Auslegungsproblemen heftig **kritisiert**.[232]

Auch die Vereinbarkeit mit Art 10 der Fernabsatzrichtlinie ist zweifelhaft. Art 14 der Richtlinie räumt zwar den Mitgliedsstaaten die Möglichkeit ein, einzelne Regelungen zu verschärfen, doch hat bereits ein deutsches Gericht erhebliche Zweifel geäußert, ob ein generelles Verbot von Werbe E-Mails im nationalen Recht mit dem ursprünglichen Richtlinienentwurf vereinbar sei. Das Gericht konstatierte ein Fehlen von Maßnahmen zum Schutz der Einzelnen gegen Spam und forderte entsprechende gesetzliche Regelungen, um Verbraucher, die keine Kontaktaufnahmen wünschen, vor derartigen Kontakten wirksam zu schützen.[233]

---

[232] Zuletzt *Hecht*, Fragwürdige Fleißaufgabe in Gewinn 12/99, 210. Die *Wirtschaftskammer Österreich* hat daher vorgeschlagen § 101 letzter Satz folgendermaßen zu formulieren: „Die Übermittlung von unaufgeforderten elektronischen kommerziellen Kommunikationen durch elektronische Post an Nutzer ist verboten."

Kernpunkte dieser Kritik sind, dass nicht nur massenhaftes Versenden von E-Mail verboten wird, sondern auch das Versenden einer einzigen E-Mail zu Werbezwecken bereits unter der Strafdrohung steht. Durch die allgemeine Formulierung ist unklar was mit den Begriffen „zu Werbezwecken" oder „Massensendung" gemeint ist (auch „Hoax-Mails" sind davon betroffen). Mit der Regelung wird bei extensiver Auslegung jede - nicht nur kommerzielle Werbung mittels E-Mail verboten, da es gibt keine Einschränkung auf kommerzielle Werbung gibt. Es ist auch keine Einschränkung dahingehend eingefügt worden, ob bereits eine Beziehung zum Empfänger der E-Mail besteht.

Unklar ist auch der Terminus „Zustimmung des Empfängers". Offen ist ob eine Angabe der E-Mail Adresse auf der eigenen Homepage oder die Verteilung der Visitenkarte ausreicht oder eine ausdrückliche Zustimmung erforderlich ist?

[233] Urteil des Landgerichts Berlin im Hauptverfahren vom 13.10.1998. Unerbetene E-Mails stellen nach deutscher Rechtsprechung einen Wettbewerbsverstoß bzw einen Eigentumseingriff dar.

3.2.4.1.2 Art 7 der E-Commerce Richtlinie[234]

Neben Art 10 der Fernabsatzrichtlinie ist für die Werbung per E-Mail auch der 2. Abschnitt der E-Commerce Richtlinie heranzuziehen.

Die E-Commerce Richtlinie sieht in Abschnitt 2 Bestimmungen für die **"Kommerzielle Kommunikation"** vor. [235]Um das Vertrauen der Nutzer in den elektronischen Geschäftsverkehr zu erhöhen, wird kommerzielle Kommunikation bestimmten Transparenzerfordernissen unterworfen.

Art 6 sieht daher eine **Kennzeichnungspflicht** für kommerzielle Kommunikation vor. Demnach muß Werbung, Sponsoring und Marketing klar als solche zu erkennen sein und die natürliche oder juristische Person, in deren Auftrag kommerzielle Kommunikationen erfolgen (Auftraggeber) muß klar identifizierbar sein.

Besondere Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke sowie Gewinnspiele und Preisausschreiben müssen klar als solche erkennbar sein, und die Bedingungen für ihre Inanspruchnahme müssen leicht zugänglich sein.

In **Art 7 findet sich eine Kennzeichnungspflicht für unerbetene kommerzielle Kommunikationen.** Demnach muß durch elektronische Post übermittelte unerbetene[236] kommerzielle Kommunikationen bei Eingang beim Nutzer klar und unzweideutig als solche bezeichnet werden. Art 7 legt fest, dass die Mitgliedstaaten in ihren Rechtsvorschriften vorsehen, durch elektronische Post übermittelte unerbetene kommerzielle Kommunikationen beim Eingang beim Nutzer klar und unzweideutig als solche zu bezeichnen.

---

[234] Die Kommission hat am 18.11.1998 einen Entwurfes für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliches Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt (KOM(98)586 endg) vorgelegt. Der Binnenmarkt Ministerrat hat diesem Entwurf am 7.12.1999 zugestimmt. Im Folgenden E-Commerce Richtlinie.

[235] Zum Begriff vgl FN 201.

[236] *Brenn,* ÖJZ 1999, 486 schlägt vor, den Begriff „unaufgeforderte“ anstelle „unerbetene“ zu verwenden.

Bereits bestehende sekundärrechtliche und nationale Bestimmungen[237] bleiben von dieser Bestimmung unberührt. Art 7 stellt daher eine zusätzliche Kennzeichnungspflicht dar.[238]
Dieser Entwurf erlaubt somit prinzipiell den Versand von Werbe E-Mails, sieht jedoch für kommerzielle Kommunikation via E-Mail eine ***Kennzeichnungspflicht von nicht bestellten Werbe-Emails*** *vor.*
Im geänderten Entwurf wurde gemäß den Änderungswünschen des Europäischen Parlamentes analog zu Art 10 der Fernabsatzrichtlinie die Versendung von Werbung per E-Mail an eine vorherige Konsultation eines sogenannte **Opt-Out-Register** gebunden. Ist eine Person nicht in das Register eingetragen, so ist die Zustellung von elektronischer Post erlaubt. Wenn eine natürliche Person keine Werbung per Mail erhalten möchte, so kann sie dies durch die Eintragung in das Register verhindern.
Der Vorteil dieser Lösung liegt sicherlich darin, dass eine neue Art der Werbemöglichkeit nicht prinzipiell verboten wird. Sie birgt jedoch die Gefahr einer explosionsartigen Zunahme von Werbe E-Mails in sich. Damit würden Werbebotschaften durch die Überlastung des E-Mail-Postkastens ihren Empfänger nicht erreichen. Dem Provider entstehen Kosten für die Datenspeicherung. Unternehmen und Verbrauchern müßten mit großem Zeitaufwand ihre Post im elektronischen Briefkasten aussortieren, da auch wichtige E-Mails darunter sein können.

3.2.4.1.3 Resümee

Anhand der verschiedenen Regelungsansätze in zwei Richtlinien ist die Schwierigkeit der Formulierung einer gesetzlichen Regelung, die den Kontakt von Unternehmen per E-Mail zu

---

[237] Fernabsatzrichtlinie, DSRL, Entwurf zum Fernabsatz von Finanzdienstleistungen und § 101 TKG.

[238] Zu möglichen Problemen bei der Durchsetzung dieser Kennzeichnungsverpflichtung vgl. Brenn, ÖJZ 1999, 486.

Zwecken kommerzieller Kommunikation mit Verbrauchern oder anderen Unternehmen, zu ersehen.
Zur Zeit bestehen jedenfalls inhaltlich **unterschiedliche Regelungen mit verschieden weiten Anwendungsbereichen** für den Kontakt zwischen Unternehmern mit Verbrauchern und zwischen Unternehmern, nebeneinander.
Problematisch ist insbesondere, dass ein Großteil der Unternehmen, die Spamming betreiben, ihren Sitz bzw Niederlassung in Drittstaaten, insbesondere in den USA[239] haben und von den europaweit einheitlichen Bestimmungen nicht erfaßt werden. Nicht einmal eine gesamteuropäische Lösung könnte das Problem lösen.
Vorgeschlagen wurden daher *Regelungen auf globaler Ebene* zu schaffen, da einzelne nationale Lösungen die grenzüberschreitende kommerzielle Kommunikation erschweren und - wie oben gezeigt - rasch an die Grenzen ihrer Wirksamkeit stoßen.

3.2.4.2 Zahlungen von Verbrauchern mittels Kreditkarten

Nachdem sich das Internet von einem wissenschaftlichen Computernetzwerk zu einem virtuellen Marktplatz gewandelt hat, steigen auch die Anforderungen der am elektronischen Geschäftsverkehr beteiligten Geschäftspartner an das Medium. Speziell die Frage der Sicherheit der übertragenen Informationen wurde zunehmend hinterfragt. Ein wesentliches Hindernis für die weitere Verbreitung des Electronic Commerce ist das mangelnde Vertrauen vieler Nutzer in die Sicherheit von **Zahlungen mit Kreditkarten** über elektronische Netze.[240]

---

[239] In den USA gibt es von Anbietern bereits Bestrebungen, Freiwillige Regelungen für kommerzielle Kommunikation im Internet einzuführen.

[240] Vgl beispielsweise die Studie der Unternehmensberater *Ernst&Young LLP*, Internet Shopping study - The digital channel continues to gather steam, 7, 14, wo als Hauptforderung der User für sicheren Electronic Commerce die "security of sending credit card info over the Net" genannt wurde. So auch *Halbwidl*, Austria Pro Nachrichten Nr 17, Mai 1999, 38.

Die Bezahlung mittels Kreditkarte bringt tatsächlich (vor allem bei unverschlüsselt übermittelten Nachrichten) einige **Nachteile** mit sich.[241]

Einer der am häufigsten öffentlich diskutierten, ist die hohe **Mißbrauchs- und Betrugsgefahr** durch Dritte.[242] Es ist der Fall denkbar, dass ein Konsument via Internet seine Kreditkartennummer bekannt gibt und diese in der Folge von einem Dritten bei einem Zahlungsauftrag unrechtmäßig verwendet wird. Dabei stellt sich die Frage, wer für den – oft schwer nachvollziehbaren - Mißbrauch der Karte haften soll. Die Kreditkartenfirmen zeigten sich zwar bei den bisher aufgetretenen Fällen von Mißbrauch kulant, wälzen jedoch die Risken beim Mißbrauch bisher häufig auf die Vertragshändler und Karteninhaber ab.[243] Nach Punkt 8 Abs 6 der Allgemeinen Geschäftsbedingungen der österreichischen Kreditinstitute (AGBöKr) haften die Kreditinstitute nicht für die Folgen der Durchführung von gefälschten oder verfälschten Überweisungsaufträgen. Die Kreditinstitute sind gemäß der AGBöKr Punkt 17 nicht für Schäden aus Übermittlungsfehlern oder Irrtümern im Telefon-, Fernschreib- und telegrafischen Verkehr haftbar zu machen, es sei denn sie hat den Schaden selbst verschuldet.

Bei der Abwicklung von Online-Geschäften mittels Kreditkarte werden die Kreditkarteninformationen gesammelt und in Datenbanken gespeichert um so Rückschlüsse auf das Kundenverhalten zu erhalten. Ein weiterer Kritikpunkt ist die mangelnde Anonymität des Kunden bei der Zahlung mittels Kreditkarten im elektronischen Geschäftsverkehr. Da sich die beiden Vertragspartner miteinander über elektronischen Weg meist nicht kennen, herrscht auch Skepsis, ob die Person tatsächlich jene sind, die sie zu sein vorgeben.[244]

---

[241] Vgl zu den Risken näher *Jaburek/Wölfl*, Cyber-Recht, 121; *Kristoferitsch*, Sicherheitsmängel : Das Damoklesschwert des Web-Zahlungsverkehrs, Austria Pro Nachrichten Nr. 16, Jänner 1999, 9; *Mohr*, ecolex 1999, 248.

[242] Zuletzt *Bauer/Himmelbauer*, Der Nep im Web, Format 25/99, 66.

[243] *Jaburek/Wölfl*, Cyber-Recht, 121.

[244] *Halbwidl*, Austria Pro Nachrichten Nr. 17, Mai 1999, 38.

Es gibt jedoch bereits eine Reihe von Projekten, deren Zielsetzung die sichere Abwicklung finanzieller Transaktionen über das Internet ist. Ein vielversprechender Ansatz, der bereits in der Praxis Verwendung findet, ist ein gemeinsames Projekt der US-Kreditkartenfirmen Visa und Mastercard in Zusammenarbeit mit führenden Soft- und Hardwareherstellern wie IBM, Microsoft, Netscape, Sun und Hewlett Packard namens Secure Electronic Commerce (SEC). Als erstes Resultat liegt eine Verschlüsselungsmethode namens **SET** (Secure Electronic Transaction) vor. Kernstück von SET ist die Aufbewahrung der Kreditkarteninformationen in elektronischer und verschlüsselter Form als digitales Zertifikat[245]. SET stellt einen weltweiten Standart für sichere Zahlungstransaktionen über das Internet dar, der die Vertraulichkeit der übertragenen Kontoinformationen, die Verschlüsselung der übertragenen Daten, die Identifikation der Beteiligten als berechtigte Teilnehmer sichern soll.[246]

Neben SET bestehen bereits eine Vielzahl anderer Systeme für den sicheren Zahlungsverkehr wie **„E-Cash“** oder **„Cybercash“**.[247]

Trotz des Vorliegens der technischen Voraussetzungen für ein sicheres Bezahlen mittels Kreditkarten über elektronische Netze, wird diese Möglichkeit von den Anbietern im Netz noch relativ selten genutzt.[248]

Da mit der Kommerzialisierung des Electronic Commerce auch der Einsatz von Zahlungs- und Kreditkarten in diesem Bereich

---

[245] Vgl unter 3.3.1.

[246] *Halbwidl*, Austria Pro Nachrichten Nr. 17, Mai 1999, 39. Zur technischen Funktionalität von SET auch *Jaburek/Wölfl*, Cyber-Recht, 121; *Kristoferitsch*, Sicherheitsmängel : Das Damoklesschwert des Web-Zahlungsverkehrs, Austria Pro Nachrichten Nr. 16, Jänner 1999, 9.

[247] Ein Überblick findet sich bei *Jaburek/Wölfl*, Cyber-Recht, 121; *Kristoferitsch*, Sicherheitsmängel : Das Damoklesschwert des Web-Zahlungsverkehrs, Austria Pro Nachrichten Nr. 16, Jänner 1999, 12.

[248] Laut einer Untersuchung des deutschen Interessensvertretung der Online Wirtschaft *eco* ist als Bezahlungsform im Internet bei deutschen Anbietern noch immer die Bezahlung per Nachnahme deutlich an erster Stelle. Vgl im Internet unter http://www.eco.de.

zunehmen wird[249], enthält Art 8 nunmehr eine Bestimmung über die **Bezahlung von Verbrauchern mittels Zahlungs-[250] und Kreditkarten** im Electronic Commerce.

Ziel des Art 8 ist es, dem Mißbrauch der Kreditkartennummer des Verbrauchers beim Vertragsabschluß im Fernabsatz vorzubeugen.

Die Mitgliedstaaten tragen demnach dafür Sorge, dass geeignete Vorkehrungen bestehen, damit der **Verbraucher** im Falle einer "betrügerischen" Verwendung seiner Zahlungskarte im Rahmen eines unter diese Richtlinie fallenden Vertragsabschlusses im Fernabsatz die **Stornierung bzw die Gutschrift oder Rückerstattung** einer bereits getätigten Zahlung **verlangen** kann.

Entgegen den AGBöKr soll das Risiko nicht dem Konsumenten bzw dem Kreditkartenberechtigten auferlegt werden, wenn eine Karte "mißbräuchlich"[251] durch den Lieferer oder durch Dritte verwendet wurde. Der wirtschaftliche Nachteil soll in diesem Fall den Aussteller der Zahlungskarte treffen.[252]

Unklar bleibt, von wem der Verbraucher die Rückerstattung verlangen kann. Sowohl eine Rückerstattung von Seiten eines betrügerischen Lieferers als auch von Dritten dürfte in der Praxis in den meisten Fällen an der Rückverfolgbarkeit scheitern. Denkbar wäre eine Haftung der Banken bzw Kreditkarteninstitute. Hierbei käme es jedoch zum kaum wünschenswerten Fall, dass Banken und Kreditkarteninstitute zur eigene Absicherung vor jeder Abbuchung mit dem Kunden eine Absprache über sein Einverständnis bzw den ordnungsgemäße Erhalt der Gegenleistung durch den Lieferer halten müssten.[253]

---

[249] EB zur RV 20, 68.

[250] Neben Kreditkarten kommen in der Wirtschaft immer häufiger Chipkarten mit elektronischem Geld als "Konsumentenkarten" und "Kundenkarten" zum Einsatz, mit denen der Kunde berechtigt wird bargeldlos im jeweiligen Unternehmen zu bezahlen. So auch EB zur RV 68.

[251] Nach den EB zur RV 69 fällt darunter "jede Verwendung ohne Wissen und Willen des Karteninhabers".

[252] EB zur RV 20, 24.

[253] *Kilches*, Medien und Recht 5/97, 280.

Offen bleibt nach der Richtlinie daher im Ergebnis, wie der Schaden zwischen dem Kreditkartenunternehmen und dem mit diesem in Vertragsbeziehung stehendem Händler aufgeteilt wird.[254]

Die Regelung sollte ursprünglich dem Verbraucher ein Recht zum Einspruch gegen die Gültigkeit eines Zahlungsvorganges einräumen, wenn dieser auf einer nicht elektronisch überprüften Kartennummer beruht. Diese Regelung wurde jedoch in die endgültige Fassung der Richtlinie nicht übernommen.[255]

Mit § 5k KSchG soll Art 8 über den Schutz des Verbraucher bei der Verwendung einer Zahlungskarte im Fernabsatz übernommen werden. Regelungsgegenstand sind trotz einer etwas anderslautenden Formulierung ("mißbräuchlich verwendet") die Rückforderungsansprüche des Verbrauchers bei einer mißbräuchlichen Verwendung seiner Zahlungskarte im Fernabsatz. § 5k KSchG soll außerdem Aufschluß über die Risikoverteilung in derartigen Mißbrauchsfällen geben. Den Erläuterungen zur Folge sollen auch mißbräuchliche Verwendungen von Zahlkarten im Rahmen von Fernabsatzverträgen, die nach § 5b KSchG von den

---

[254] Den Konsument treffen jedoch Sorgfaltspflichten bei der Verwendung und Aufbewahrung von der Kreditkarteninformationen, insbesondere die Geheimhaltung des PIN-Codes. *Mohr*, Elektronischer Kauf - Verbraucherschutz im Fernabsatz, e-commerce, ecolex 1999, 248, die diese Regelung als durchaus ausgewogen begrüßt.

Die mögliche Mitverantwortung im Einzelfall für den Konsumenten wird auch in den EB zur RV 69 betont. Details dieser Sorgfaltspflichten sind oft in den Allgemeinen Geschäftsbedingungen der Kreditkartenunternehmungen geregelt. Diese sind in Zukunft an "den allgemeinen zivil- und konsumentenschutzrechtlichen Regeln sowie der Empfehlung 88/590/EWG der Kommission vom 17. November 1988 zu Zahlungssystemen, insbesondere zu den Beziehungen zwischen Karteninhabern und Kartenausstellern (ABl L 317 vom 24. November 1988, 55), sowie die Empfehlung der Kommission 97/489/EG vom 30. Juli 1997 zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden (besonders zu den Beziehungen zwischen Emittenten und Inhabern solcher Instrumente), ABl L 208 vom 2. August 1997, 52," zu prüfen sein.

Eine beispielhafte Aufzählung von unzulässigen Klauseln findet sich in den EB zur RV 70.

[255] *Hoeren*, Rechtsfragen des Internet, 136.

besonderen Regelungen der §§ 5c ff KSchG ausgenommen sind (zB Verträge über Finanzdienstleistungen), erfaßt sein.[256] **Nicht erfaßt** werden sollen Mißbräuche durch Dritte bei Geschäften unter Anwesenden sowie Fälle in denen die Zahlkarte nicht dem Verbraucher, sondern einem anderen Karteninhaber gegenüber mißbräuchlich verwendet werden. § 5k KSchG ist nach diesem Standpunkt auf Online-Verträge über Finanzdienstleistungen anzuwenden.

Legt Art 8 noch nicht genau fest, gegen wen der Verbraucher einen Anspruch auf Erstattung seiner Zahlungen haben soll, so ist die geplante Umsetzung im KSchG präziser. Nach § 5k KSchG soll dem Verbraucher ein Anspruch gegen den Zahlungskartenaussteller zustehen. In der Regel wird die Haftung für einen Kreditkartenmißbrauch somit das Kreditkartenunternehmen treffen.[257] Diese Präzisierung ist vor allem für den Bereich des Online-Shoppings zu begrüßen. Gerade beim Vertragsabschluß mit einem "virtuellen Vertragspartner", der in einem anderen Staat ansässig ist, wird ein Rückzahlungsanspruch des Verbrauchers regelmäßig ins Leere gehen. Dem Kartenberechtigten soll daher der von der Richtlinie vorgegebene Anspruch gegen den Aussteller der Zahlkarte eingeräumt werden. Dem Kartenaussteller bleibt es jedoch frei im Rahmen der Regelungen des § 5k KSchG in seinen AGB nähere Vorkehrungen für den Gebrauch seiner Karte im Fernabsatz zu treffen. Allfällige Regreßansprüche zwischen dem Kartenaussteller und dessen Vertragsunternehmer richten sich nach den vereinbarten Regelungen sowie nach den allgemeinen Regelungen des Schadenersatz- und Bereicherungsrechts.[258]

Der Anwendungsbereich der österreichischen Regelung geht über jenen der Richtlinie hinaus, da nicht nur Mißbräuche bei Verbrauchergeschäften oder Mißbräuche der Karte eines Verbrauchers erfaßt sind.[259]

---

[256] EB zur RV 54.

[257] EB zur RV 55.

[258] EB zur RV 56

[259] EB zur RV 30, 69. Das Bundesministerium für Justiz hatte ursprünglich vorgeschlagen, den Anwendungsbereich von Art 8 auf alle Geschäfte bei denen

3.2.4.3 Zusendung unbestellter Waren

Art 9 verpflichtet die Mitgliedstaaten, Maßnahmen zu ergreifen, welche die Lieferung von Waren an einem Verbraucher ohne dessen vorherige Bestellung verhindern.
Für den elektronischen Geschäftsverkehr wird dies keine Auswirkungen haben, da der Verbraucher regelmäßig den ersten direkten Kontakt zum Unternehmer durch Anklicken einer Webseite herstellt.
Diese Regelung über unbestellte Waren und Dienstleistungen bedürfte in Österreich keiner weiteren Umsetzung, da sie **bereits mit der KSchG Novelle 1997 umgesetzt** wurde.[260]
§ 864 Abs 2 ABGB bestimmt, dass ein Empfänger von unbestellten Waren diese behalten, verwenden und verbrauchen darf, ohne daß dadurch ein Vertrag zustande kommt. Der Empfänger ist auch nicht verpflichtet die Sache zu verwahren oder zurückzuschicken.

3.2.4.4 Unabdingbarkeit der Verbraucherrechte

Der Verbraucher kann gemäß **Art 12** Abs 1 auf die Rechte, die ihm aufgrund der Umsetzung der Richtlinie zustehen, **nicht rechtswirksam verzichten**. Ein Abgehen von diesen Rechten zum Vorteil des Verbrauchers ist jedoch möglich.[261] Ebenso ist gemäß Art 12 Abs 2 die Wahl von Drittlandsrecht durch die Vertragsparteien - sofern sich darin nicht mit der Richtlinie zu vergleichende Verbraucherschutzrechte finden - erheblich eingeschränkt.

---

es zu einer Verwendung von Kreditkarten kommt, auszudehnen, was jedoch zu einer Verteuerung des Zahlungsmittel geführt hätte.

[260] BGBl I Nr 6/1997. Vgl § 864 Abs 2 ABGB und § 32 Abs 1 Z5 KSchG.
Zum Anpassungsbedarf durch die Richtlinie vgl im Detail EB zur RV 27.

[261] *Engel*, Verbraucherschutz, 72.

3.2.4.5 Mindestschutz für den Verbraucher

Wie viele andere Verbraucherschutzregelungen auf europäischer Ebene soll auch die Fernabsatzrichtlinie nur eine Mindestharmonisierung, einen europaweit gültigen Mindeststandart schaffen. Daher bestimmt **Art 14**, dass **strengere Vorschriften** zugunsten des Verbrauchers in den Mitgliedstaaten **bestehen bleiben** dürfen bzw neu eingeführt werden dürfen.
Auch der österreichische Gesetzgeber hält sich - mit wenigen Ausnahmen[262] - an die von der Richtlinie vorgegebenen Standards mit der Begründung, dass durch abweichende Regelungen lediglich Handelshemmnisse geschaffen würden.

3.2.4.6 Umsetzung

Den Mitgliedstaaten wird gemäß **Art 15** Abs 1 eine Frist von drei Jahren nach dem Inkrafttreten der Richtlinie eingeräumt, um diese in nationales Recht umzusetzen. Die Richtlinie ist am 4.6.1997 in Kraft getreten und daher bis 4.6.2000 von den Mitgliedstaaten in nationales Recht umzusetzen. Österreich ist dieser Verpflichtung durch die Novellierung des KSchG frühzeitig nachgekommen.

3.2.5 Resümee

Die Richtlinie ist als erster Ansatzpunkt für eine Klarstellung der Rechte und Pflichten der am Vertragsabschluß im Fernabsatz Beteiligten Verbraucher und Unternehmer zu werten. Zahlreiche Detailfragen werden sich mit der zunehmenden Nutzung des Electronic Commerce durch Unternehmer und Verbraucher noch in Zukunft ergeben.[263]

---

[262] EB zur RV 24.

[263] *Mohr*, ecolex 1999, 249.

*Die Richtlinie **erweitert** für Geschäfte zwischen Verbrauchern und Unternehmern ua im elektronischen Geschäftsverkehr die Möglichkeit des schon vor der Richtlinie in Österreich bestehenden **Rücktrittsrechtes** und schreibt daneben Mindestinformationen vor die dem Verbraucher zur Verfügung gestellt werden müssen.*[264]

Die Richtlinie kann als ausgewogener Kompromiss zwischen Verbraucherrechten und den Bedürfnissen der Anbieter gewertet werden. Sie lässt die Ausnutzung der technischen Möglichkeiten im Electronic Commerce zu und behindert den elektronischen Geschäftsverkehr zwischen Unternehmer und Konsumenten via Internet nicht mit umständlichen Hürden. Anderseits sind die Gefahren für die Verbraucher durch die Schutzmechanismen der Art 4, 5 und 6 deutlich reduziert.

[264] *Madl*, ecolex 1996, 80.

3.3 VERTRAULICHKEIT UND SICHERHEIT BEIM VERTRAGSABSCHLUSS IM INTERNET - VERSCHLÜSSELUNG UND DIGITALE SIGNATUR

3.3.1 Technischer Hintergrund

Der technische Austausch von Daten stellt - abgesehen von gelegentlichen Engpässen bei der Übertragungsbreite - kein besonderes Problem mehr dar. Die weitere Entwicklung des Electronic Commerce wird jedoch wesentlich von der Sicherheit des Datentransports und dem Vertrauen der Teilnehmer in die modernen Kommunikationstechnologien abhängen. In der Vergangenheit waren das **mangelnde Vertrauen** und die damit in Zusammenhang stehenden ungeklärten rechtliche Aspekte, insbesondere regulatorische Defizite für elektronisch signierte Verträge, ein wesentliches Hindernis für die raschere Verbreitung des elektronischen Geschäftsverkehrs.[265]
Technisch gesehen erfolgt die Versendung von Daten über elektronische Netze folgendermaßen.[266] E-Mails werden in mehrere kleine Datenpakete aufgeteilt und gemeinsam mit anderen Informationen abgeschickt. Die Nachricht erreicht jedoch nicht direkt den Empfänger, sondern läuft oft über mehrere Relaisstationen (Hops), wo die Datenpakete gesammelt

[265] Studie von *RegioPlan Consulting*, Virtuelles Shopping in Österreich (1998) 74.

[266] Vgl zum folgenden *Dix*, Gesetzliche Verschlüsselungsstandarts-Möglichkeiten der Gesetzgebung, CR 1/1997, 38; *Koch*, Grundrecht auf Verschlüsselung, CR 2/1997 106; *Posch*, Digitale Signatur und Zertifizierung in Austria Pro Nachrichten, Nr. 14, 1998, 12; *Laga*, Internet, 145; *Forgo*, Was sind und wozu dienen digitale Signaturen, ecolex 4/1999, 235; *Steindl*, Digitale Signatur Sicherheitstechnologie, Austria Pro Nachrichten, Nr. 17 Mai 1999, 12; *Greiner*, Sicherheit im Internet in e-commerce, November 1999, 39.

und zum nächsten Hop geleitet werden, bis sie die Zieladresse erreicht haben.
Dabei ist der Inhalt der Daten bei den Zwischenstationen lesbar, vergleichbar der Beförderung eines Pakets mittels der konventionellen Post, das auf seinem Weg ebenfalls von den beteiligten Personen gelesen werden kann.[267]
Um nun zu verhindern, dass elektronische Post an den Knotenpunkten des Netzes beispielsweise von Providern, Netzbetreibern oder anderen Nutzern des Netzes unbefugt gelesen wird, also ein hohes Maß an **Datensicherheit** zu erreichen gibt es mehrere Möglichkeiten.
Eine Möglichkeit ist es Informationen oder Nachrichten zu verbergen (**Steganographie**).
Eine andere Möglichkeit ist jene, Daten mittels **Verschlüsselung** (Kryptografie) im Wege eines mathematischen Verfahrens, beispielsweise dem Verschieben von Buchstaben, unlesbar zu machen. Bei der Kryptographie werden die Informationen oder Nachrichten nicht versteckt, sondern so verändert, dass sie für Dritte unlesbar und unverständlich bleiben.
Neuere Verschlüsselungsverfahren beruhen darauf, dass der codierte Text nicht in einem bestimmten, durch die verfügbaren Rechnerkapazitäten determinierten, Zeitraum dechiffriert werden kann. Es wird dabei ein Schlüsselwert (Key) benutzt. Je höher die Anzahl möglicher Keys, desto höher ist die Sicherheit.
Unterschieden wird zwischen symmetrischer und asymmetrische Verschlüsselung.
Bei **symmetrischen Verschlüsselungsverfahren** (Private Key Verschlüsselung) wird die Nachricht von Sender und Empfänger mit demselben Schlüssel ver- und entschlüsselt. Nachteil dieses Verfahrens sind die fehlende Möglichkeit der spontanen

[267] Zu den Gefahren im Online-Bereich bei der Übertragung von Informationen auf nicht gesicherten Leitungen vgl. *Stoll*, Bankraub Online : Die Tricks , Kniffe und Methoden der Online-Profis (1997).

Verschlüsselung, die Geheimhaltungspflicht der beteiligten Parteien und die bedingte Einsatzmöglichkeit zwischen mehreren Partnern.

Bei der **asymmetrischen Verschlüsselung** (Public Key Verfahren) wird ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel verwendet. Es handelt sich daher um ein zwei Schlüsselverfahren (geheimer und öffentlicher Schlüssel).[268] Es hat sich international der RSA Algorithmus bewährt.

Der geheime Schlüssel (Secret Key) ist nur einer Person bekannt, den öffentlichen Schlüssel kann jeder kennen. Zwei komplementäre Schlüssel werden erstellt und einem Nutzer zugeordnet. Mittels öffentlichem Schlüssel (Public Key) werden Nachrichten ver-, mittels privatem Schlüssel (private key) entschlüsselt. Einer der Signaturschlüssel - bleibt privat, während der öffentliche Schlüssel - ein Signaturprüfschlüssel - veröffentlicht wird. Dabei wird sichergestellt, dass der private Schlüssel nicht aus dem öffentlichen Schlüssel berechnet werden kann. Verschlüsseln bedeutet, dass ein Dokument mit dem öffentlichen Schlüssel verschlüsselt wird, und nur der Besitzer des geheimen Schlüssels das Dokument entschlüsseln kann. In der Praxis kommen oft gemischte Modelle zur Anwendung.

Das Schlüsselpaar wird über **digitale Zertifikate** ausgegeben. Die Vergabe der digitalen Zertifikate ist Aufgabe der Zertifizierungsstellen. Das Zertifikat beinhaltet Informationen über die Identität des Zertifikatinhabers und die Zertifizierungsstelle.

Durch Verschlüsselungsverfahren soll garantiert werden, dass nur berechtigte Personen Zugriff auf gespeicherte und über

[268] RSA wurde 1978 von Ron Rivest, Adi Shamir und Leonard Adleman erfunden. Es handelt sich dabei um ein Asymmetrische Verschlüsselungsverfahren, d.h. ein Schlüssel wird öffentlich gemacht (PK = Public Key), der andere Schlüssel bleibt geheim (SK = Secret Key).
Die derzeit sichere Variante ist 1024 Bit RSA. Bei Sicherheitsüberlegungen muss die stärkste Rechnerleistung (NSA Möglichkeiten der USA) und die derzeit exponentiell steigende Rechnerleistung berücksichtigt werden.

elektronische Netzwerke übertragenen Informationen haben um so Daten gegen unbefugte Zugriffe von Dritten zu schützen. (**Vertraulichkeit**).

Asymmetrische Verschlüsselungsverfahren können auch zur Feststellung der Integrität von übermittelten Daten und des Nachweises der Identität des Bearbeiters verwendet werden.

Die Garantie, dass der Versender der Nachricht auch tatsächlich jener ist, der er vorgibt zu sein, bietet nicht die Verschlüsselung, sondern die **digitale Unterschrift** (**digitale Signatur**).[269] Dies geschieht bei einem konventionellen Vertragsabschluß durch die eigenhändige Unterschrift.

Digital signiert bedeutet, dass die Nachricht weiterhin leserlich bleibt, jedoch mit einem besonderen Schutzmechanismus versehen wird. Digitale Signaturen werden der Nachricht beigefügt, lassen jedoch den Inhalt eines elektronischen Dokuments unverändert. Signieren bedeutet, dass ein Dokument wird mit dem geheimen Schlüssel verschlüsselt (signiert) wird und jeder mit Hilfe des öffentlichen Schlüssels die Signatur überprüfen kann. Das Signieren (elektronisches Unterschreiben) ist nichts anderes, als die Umkehrung des Verschlüsseln.

Digitale Signaturen basieren auf den oben beschriebenen asymmetrischen Kryptographieverfahren (mathematisches Verschlüsselungsverfahren oder PKI Verfahren).

---

[269] Die Diskussion um digitale Signaturen ist streng zu trennen von der Frage der Zulässigkeit des Unlesbarmachens von Nachrichten durch Verschlüsselung. Kryptografie ist das Gegenteil von digitaler Signatur. Die Kryptografie ist im Gegensatz zur digitalen Signatur auf europäischer Ebene ein ungeregeltes Thema. In manchen Staaten wie beispielsweise in Frankreich oder Russland gibt es Verbote der Verwendung von bestimmten Verschlüsselungsprogrammen. In den USA ist der Export von Verschlüsselungssoftware verboten. Dies offenbar deshalb, da auch den Polizeibehörden der Zugriff auf verschlüsselte Nachrichten faktisch unmöglich wäre. In Österreich gibt es keine Beschränkungen für die Verschlüsselung bei der Datenübertragung.
Zur Diskussion und den Gesetzesvorhaben auf internationaler Ebene vgl *Brenn*, ÖJZ 17/1997, 643.

Mit dem öffentlichen Schlüssel des Senders kann der Empfänger herausfinden, ob die signierten Daten verändert wurden und ob der öffentliche und private Schlüssel des Senders ein komplementäres Schlüsselpaar bilden und somit Veränderungen der Daten feststellen. Was sich hier wie ein komplizierter mathematischer Prozeß anhört, geschieht in der Praxis in Sekundenschnelle im Rechner.

Das **digitale signieren einer Nachricht** erfolgt in mehreren Schritten.

Dazu wird die Datei mittels eines mathematischen Verfahrens (HASH – Verfahren) komprimiert. Aus einer Datei wird ein Abbild geschaffen. Aus derselben Datei entsteht immer derselbe Hash-Wert. Vom Hash-Wert kann man nicht auf die ursprüngliche Datei schließen.

Dieser Hash-Wert wird mit dem geheimen Schlüssel des Senders verschlüsselt. Das Ergebnis dieses Vorganges nennt man Signatur. Der Empfänger entschlüsselt mit Hilfe des öffentlichen Schlüssels die Signatur und bekommt einen Hash-Wert A. Er nimmt dann die lesbare Datei und mit Hilfe des gleichen Hash-Verfahrens wie der Sender komprimiert er die Datei in den Hash-Wert B. Dann überprüft er, ob die Hash-Werte A und B identisch sind.

Damit kann der Empfänger sicher sein, dass die Nachricht auch vom richtigen Absender kommt und er das was er bekommen hat, auch das ist was der Sender unterschrieben hat, die Datei vom Sender zum Empfänger also nicht manipuliert wurde.

Verschlüsselung garantiert daher Vertraulichkeit, indem nur berechtigte Personen Zugriff auf gespeicherte und über elektronische Netzwerke übertragenen Informationen haben um so Daten gegen unbefugte Zugriffe von Dritten zu schützen.

Die digitale Unterschrift (digitale Signatur) soll dem Empfänger einer Nachricht im Netz Sicherheit darüber geben, dass die Nachricht von demjenigen stammt, der vorgibt, der Absender der Nachricht zu sein (**Echtheit der Nachricht - Authentizität**), und ob die erhaltene Nachricht ident ist mit der abgesendeten Nachricht, somit keine inhaltlichen

Änderungen durchgeführt wurden (**Unverfälschtheit der Nachricht - Datenintegrität**).
Darüber hinaus garantieren digitale Signaturen, dass Informationen und Nachrichten zu bestimmten Zeitpunkten genau definierte Inhalte hatten. Daher kommt ihnen auch **Beweisfunktion** zu.
Genau in diesen Bereichen liegen die Probleme von offenen Netzen. Unverschlüsselte Kommunikation via Internet bietet weder Vertraulichkeit noch Authentizität. Damit waren jedoch auch dem Vertragsabschluß im elektronischen Geschäftsverkehr Grenzen gesetzt.
Die **Einsatzgebiete** für elektronische Unterschriften in der Praxis sind vielfältig. Es fallen darunter beispielsweise der Dokumentenversand im elektronischen Behördenverkehr, Steuererklärungen, Online-Banking, Telemedizin und Vertragsübermittlungen auf elektronischem Weg.

3.3.2 Rechtlicher Rahmen

Sowohl auf internationaler, insbesondere europäischer Ebene als auch in mehreren Mitgliedstaaten der Europäischen Union gibt es zahlreiche gesetzgeberische Aktivitäten und Diskussionen über die Themen Kryptografie und elektronische Signaturen.
Die UN-Kommission für internationales Handelsrecht (UNCITRAL) Working Group on Electronic Commerce hat nach Fertigstellung des Model Law on Electronic Commerce den Auftrag zur Erstellung von Regelungen über elektronische Unterschriften erhalten. Zum derzeitigen Zeitpunkt existiert **ein Entwurf über Uniform Rules On Electronic Signatures**, der aus acht allgemein formulierte Bestimmungen besteht.[270]

[270] Im Internet unter http://www.uncitral.org/uncitral. *Riedl*, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, ecolex 4/1999, 241.

Auch die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat **Leitlinien für die Kryptographiepolitik** im Jahr 1997 verabschiedet. Weitere internationale Organisationen, darunter die Welthandelsorganisation (WTO), befassen sich ebenfalls mit diesem Thema.

Auch in Österreich wurde mittlerweile ein **Signaturgesetz**[271] erlassen, dass am 1.1.2000 in Kraft getreten ist. Die Verabschiedung verzögerte sich, da es von verschiedenen Seiten heftige Kritik am ursprünglichen Entwurf geäußert wurde.[272] Österreich setzt damit die Signaturrichtlinie noch vor deren Inkrafttreten um, und ist mit dem geplanten Signaturgesetz einer der ersten Staaten der EU, der rechtliche Rahmenbedingungen für elektronische Unterschriften schafft. Neben Deutschland hat sonst nur Italien[273] ein Gesetz betreffend elektronische Dokumente und Schriftstücke.

Bereits seit 1.August 1997 ist in **Deutschland** ein Gesetz zur digitalen Signatur, als Teil des deutschen Informations- und Kommunikationsdienstegesetzes (IuKDG) in Kraft.[274] Das deutsche Gesetz beschränkt sich jedoch im Gegensatz zu Signaturrichtlinie auf die Regelung der Techniken der asymmetrischen Kryptographie. Das IuKDG regelt ein gewerberechtsähnliches Zulassungs- und Überwachungsverfahren

---

[271] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl I 190/1999, 1451. Im Folgenden als SigG bezeichnet.

[272] Kritisiert wurden von der *Vereinigung österreichischer Industrieller*, dem *Fachverband der Elektro- und Elektronikindustrie*, der *Information Technology Austria* und des *Verbandes der Informationswirtschaft* vor allem die kurze Begutachtungsfrist und mögliche Verfassungswidrigkeiten des Entwurfes. *Martos*, Elektronische Signatur: Husch-pfusch statt sicherem E-Commerce?, Die Presse vom 15. 6 1999, 27.
Demgegenüber hat die *Wirtschaftskammer Österreich* die Verabschiedung begrüßt, da die ursprünglich für Zertifizierungsstellen im Entwurf vorgesehene gesetzliche Haftpflichtversicherung in Höhe von 56 Millionen Schilling, nicht in das Gesetz übernommen wurde. Von Konsumentenschutzorganisationen war ursprünglich eine Gefährdungshaftung für Zertifizierungsdiensteanbieter gefordert worden.

[273] Im Internet unter http://www.aipa.it/english%5B4/law%5B3/pdecree51397.asp.

[274] Im Internet unter http://www.iid.de:80/rahmen/iukdg.html#.

für die bei Einsatz und Nutzung digitaler Signaturen erforderliche Infrastruktur und die Anforderungen an die erforderlichen technischen Komponenten. Bestimmte technische Verfahren werden nicht vorgeschrieben. Es schafft ein (streng hierarchisches) Lizenzverfahren für die Zulassung von Zertifizierungsstellen und geht von extrem hohen Sicherheitsanforderungen aus.
Deutschland und Italien, die schon seit längerem über ein Signaturgesetz verfügen, haben einen erhöhten Anpassungsbedarf an die Signaturrichtlinie, da Teile überhaupt nicht und anderes abweichend von der Richtlinie geregelt ist.[275]
Das österreichische SigG lehnt sich im Gegensatz zur italienischen und deutschen Regelung sehr eng an die Signaturrichtlinie an.

3.3.2.1 Die Signaturrichtlinie

3.3.2.1.1 Entstehungsgeschichte

Auf europäischer Ebene wird seit mehreren Jahren über einen einheitlichen Rahmen für digitale Signaturen intensiv diskutiert. In der Mitteilung vom 16. April 1997 an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über eine „Europäische Initiative für den elektronischen Geschäftsverkehr"[276] betrachtete die Kommission digitale Signaturen als wesentliches Element zur Gewährleistung der Sicherheit und des Vertrauens in offene Netze.
In einem zweiten Schritt unterbreitete die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen am 8.10.1997 eine **Mitteilung über „Sicherheit und Vertrauen in elektronische Kommunikation - ein europäischer Rahmen für digitale**

[275] *Geis*, Kurzkommentar zum EU-Richtlinienvorschlag für elektronische Signaturen, MMR 6/1998, VII.
[276] KOM(97) 157 endg vom 16.4.1997.

Signaturen und Verschlüsselung"[277], in der sie auf den Bedarf eines kohärenten Rahmen hinwies, der Vertrauen in digitale Signaturen ermöglicht und der wiederum so flexibel gestaltet ist, dass er auf neue technische Entwicklungen reagieren kann. Am 1. Dezember 1997 begrüßte der Rat die Mitteilung und forderte die Kommission auf, einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über digitale Signaturen vorzulegen.

Nach einer internationalen Expertenanhörung in Kopenhagen am 23. und 24.4.1998 verabschiedete die Kommission am 13.5.1998 einen Vorschlag für eine **Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen.**[278]

Nachdem sich der Rat der Telekommunikationsminister am 27.11.1998 über eine gemeinsame Position zu diesem Vorschlag einigen konnte, wurde der Vorschlag dem Europäischen Parlament zur ersten Lesung vorgelegt. Nach Stellungnahmen des Wirtschafts- und Sozialausschusses und des Ausschusses der Regionen stimmte das Parlament in seiner Entschließung vom 13.1.1999 dem Vorschlag zu, brachte jedoch 32 Änderungsvorschläge vor.[279]

Am 22.4.1999 wurde vom Telekommunikations-Ministerrat in Luxemburg ein gemeinsamer Standpunkt zum Vorschlag verabschiedet. Schließlich hat die Kommission am 29.4.1999 einen geänderten Vorschlag vorgelegt,[280] der am 27.10.1999 endgültig vom Parlament in zweiter Lesung gebilligt wurde.

Anläßlich des Telekommunikations-Ministerrates am 30.11.1999 haben die Mitgliedstaaten einstimmig die **Richtlinie**[281]

---

[277] KOM(97) 503 endg.

[278] KOM(98) 297 endg. Im Folgenden Vorschlag zur Signaturrichtlinie.

[279] Die Abänderungsanträge des Parlaments betreffen zum Großteil jedoch nur Begriffsdefinition und formale Änderungswünsche. Sie bringen inhaltlich nur geringfügige Änderungen.

[280] KOM(99) 195 endg.

[281] Im Internet unter http://europa.eu.int/comm/dg15/en/media/sign/elecsignen.pdf. Im Folgenden Signaturrichtlinie.

verabschiedet und somit den Weg für europaweit einheitliche Grundregeln für die elektronische Unterschrift geebnet.
Die Signaturrichtlinie steht in einer Linie mit der Richtlinie über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz und der Richtlinie über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt.
Bereits vor der endgültigen Verabschiedung der Signaturrichtlinie hatten mehrere Mitgliedstaaten innerhalb der Europäischen Union, beginnend mit Deutschland und Italien, legistische Initiativen bezüglich digitaler Signaturen gesetzt.[282]
Auch in den **USA** gibt es Initiativen von einzelnen Bundesstaaten, diese Materie zu regeln. Ein Entwurf für ein US-weites Signaturgesetz hat im November 1999 im Repräsentantenhaus jedoch nicht die notwendige Zweidrittelmehrheit erhalten. Der Gesetzesentwurf sah eine bundesweite Regelung der rechtlichen Rahmenbedingungen für elektronische Signaturen und eine weitgehende Gleichstellung mit eigenhändigen Unterschriften vor.[283]

3.3.2.1.2 Grundsätze und Ziele

Die Zielsetzungen der Richtlinie sind vielfältiger Natur.
Divergierende Regelungen über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsdiensteanbietern sollen vermieden werden (**Harmonisierung**).
Die Interoperabilität der Produkte für elektronische Signaturen soll gefördert werden. Die Richtlinie steht für verschiedene Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offen (**Technologische**

[282] Einen Überblick über die Aktivitäten der Mitgliedstaaten auf dem Gebiet der digitalen Signatur findet sich im Vorschlag zur Signaturrichtlinie, 4.
[283] Es besteht in den USA zur Zeit keine politische Einigkeit darüber, ob bestehende einzelstaatliche Regelungen durch die harmonisierten Regelungen beseitigt werden sollen. Im Internet unter http://futurezone.orf.at/futurezone.orf?read=detail?id=6877&tmp=90631.

Neutralität[284]). Die Kommission nimmt auch gemäß Art 12 zwei Jahre nach Umsetzung der Richtlinie eine Überprüfung derselben vor.

Die Erbringung von Zertifizierungsdienstleistungen soll im Sinne der freien Marktwirtschaft nicht an eine vorherige Genehmigung gebunden sein (**freier Marktzugang für Zertifizierungsdienstleister**).

Kernstück der Signaturrichtlinie ist die Gleichstellung digitaler Unterschriften mit handschriftlichen Unterschriften nach dem Prinzip, dass fortgeschrittene elektronische Signaturen, die mit einem qualifizierten Zertifikat verbunden sind und von einer sicheren Signaturerstellungseinheit erstellt werden,[285] als Beweismittel bei Gerichtsverfahren anerkannt werden und handschriftlichen Unterschriften gleichgestellt sind, insofern sie die Anforderungen für handschriftliche Unterschriften erfüllen (**Rechtliche Anerkennung elektronischer Signaturen**).[286] Dabei wird in die einzelstaatlichen Rechtsvorschriften jedoch nicht eingegriffen.

Die Signaturrichtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu deren rechtlicher Anerkennung

---

[284] Vorschlag zur Signaturrichtlinie, 4. Die Richtlinie ist sowohl gegenüber digitalen Signaturen als auch gegenüber symmetrischen Verschlüsselungsmethoden, stenografische Methoden und anderen in Zukunft zu entwickelnden Verfahren offen.

[285] Die Signaturrichtlinie sieht verschiedene Qualitätsstufen von Techniken, Dienstleistungen, Zertifikaten und Zertifizierungsdiensteanbietern vor.
Die rechtliche Anerkennung und Vertrauenswürdigkeit steigt, je mehr Anforderungen erfüllt sind. Es gilt jedoch der Grundsatz der Nichtdiskriminierung von sicheren Signaturen mit handschriftlichen Unterschriften.
Es wir zwischen "elektronische Signaturen" und "fortgeschrittene elektronische Signaturen, zwischen "Signaturerstellungseinheit" und "sicherer Signaturerstellungseinheit sowie zwischen Zertifikaten und qualifizierten Zertifikaten unterschieden. Ein qualifiziertes Zertifikat ist ein Zertifikat, das die Anforderungen des Anhangs I erfüllt und von einem Zertifizierungsdiensteanbeiter bereitgestellt wird, der die Anforderungen des Anhangs II erfüllt.

[286] Vorschlag zur Signaturrichtlinie, 5.

beitragen. Sie beschränkt sich jedoch auf Mindestanforderungen und geht nicht über das, zum Zweck der Schaffung harmonisierter rechtlicher Rahmenbedingungen für die Bereitstellung elektronischer Signaturen, notwendige Maß hinaus.

3.3.2.1.3 Anwendungsbereich

Die Richtlinie legt lediglich rechtliche Rahmenbedingungen für öffentlich angebotene Zertifizierungsdienste[287] für elektronische Signaturen fest, damit eine reibungsloses Funktionieren des Binnenmarktes gewährleistet ist. *Sie erstreckt sich nicht auf andere Aspekte im Zusammenhang mit dem Abschluß und der Geltung von Verträgen oder iZ mit anderen außervertraglichen Formvorschriften*, die Unterschriften voraussetzen.
Einzelstaatliche Regelungen über den Abschlusses und der Gültigkeit der Verträge und innerstaatliche Formvorschriften und Regeln und Beschränkungen bzgl der Verwendung von Dokumenten gehen der Richtlinie daher vor.[288]
Die Richtlinie bezieht sich auf **„elektronische Signaturen"**.[289] Die elektronische Signatur umfasst auch die digitale Signatur, beruht jedoch nicht zwingend auf asymmetrischen Verschlüsselungsverfahren. Die Kommission will mit diesem weiten Ansatz bewusst, „ein ganzes Spektrum elektronischer

[287] Ein „Zertifizierungsdiensteanbieter" ist gemäß Art 2 Z 6 eine Person oder Stelle, die Zertifikate erteilt oder anderweitige elektronische Signaturdienste öffentlich anbietet.

[288] Nicht betroffenen sind Regelungen über die Verschlüsselung. Dies ist nach wie vor nicht Gegenstand europäischer Gesetzgebung, sondern findet sich in den Rechtsordnungen mehrerer Mitgliedstaaten.

[289] Nach Art 2 Abs 3 „Eine Signatur in elektronischer Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt."
Der Vorschlag beschränkt sich noch auf den engeren Begriff der „digitalen Signatur". Das deutsche SigG spricht fälschlicherweise von digitalem „Sigel".

Signaturen abdecken, welches sowohl digitale Signaturen auf Basis kryptographischer Systeme mit öffentlich bekannten Schlüssel als auch Authentifizierungsverfahren anderer Art“ umfaßt.[290] Die elektronische Signatur muss verschiedene, in Art 2 Z 1 festgelegte Anforderungen erfüllen.

Die Begriffsbestimmungen der Richtlinie wurden im wesentlichen von § 2 SigG übernommen. Im Detail bestehen jedoch geringfügige Unterschiede.

Derjenige, der die elektronische Signatur erstellt **(„Signator“)** wird in § 2 Z2 SigG als "eine natürliche Person, der Signaturerstellungsdaten (das ist der private Schlüssel) und die entsprechenden Signaturprüfdaten (öffentliche Schlüssel) zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt" bezeichnet.

In der Richtlinie ist **"Unterzeichner“** eine natürliche Person, die eine Signaturerstellungseinheit besitzt und die entweder in eigenem Namen oder im Namen der von ihr vertretenen Person oder Stelle handelt".

Beim Vergleich dieser beiden Regelungen ist eine Abweichung des österreichischen Gesetzgebers, der nur natürliche Personen als Signator definiert, festzustellen. Daraus folgt, dass nach dem österreichischen Gesetz - juristische Personen nicht Unterzeichner bzw. Signator sein können.[291] In diesem Punkt ist das SigG nicht richtlinienkonform.

§ 2 Z3 sieht für die sichere elektronische Signatur ua vor, dass diese auf einem qualifizierten Zertifikat gemäß § 5 SigG beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses

---

[290] Vorschlag zur Signaturrichtlinie, 3.

[291] In den EB zur RV wird zu diesem Punkt ausgeführt: "Der Entwurf sieht vor, dass Signaturschlüssel nur natürlichen Personen zugeordnet werden können, zumal auch die Vertretungsmacht für juristische Personen letztlich an natürliche Personen gebunden ist.“
Die Tatsache, dass im elektronischen Geschäftsverkehr auch Maschinen miteinander kommunizieren, wird dabei übersehen. Es gibt daher Fälle, wo Angebote nicht von natürlichen Personen unterschrieben werden.

Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird.
Art 2 der Richtlinie stellt weniger strenge Anforderungen an eine sichere elektronische Signatur.[292] Eine fortgeschrittenen elektronische Signatur im Sinne der Richtlinie muss nicht auf einem qualifizierten Zertifikat beruhen und unter Verwendung von sicheren technischen Komponenten und Verfahren erstellt werden. *Auch hier weicht das SigG von der Richtlinie ab.*
Auch wenn aus den Erläuterungen zum Gesetzesentwurf erkennbar ist, dass die österreichische sichere elektronische Signatur der europäischen fortgeschrittenen elektronischen Signatur (inklusive Einhaltung der Anhänge I, II und III der Richtlinie) entspricht, bleibt offen, wie andere europäische fortgeschrittene Signaturen, welche die Anhänge I bis III nicht einhalten, in der österreichischen Rechtsordnung eingestuft werden.
Darüber hinaus gibt es im SigG gewisse begriffliche Unschärfen, terminologische Unklarheiten und ein Redaktionsfehler.[293]

3.3.2.1.4 Rechtswirkungen elektronischer Signaturen

Ziel einer gesetzgeberischen Maßnahme im Bereich der digitalen Signatur ist die Gleichstellung eben dieser mit der eigenhändigen Unterschrift.
Als Kernstück der Richtlinie verpflichtet daher **Art 5** die Mitgliedstaaten, eine Gleichstellung von sicheren elektronischen Signaturen (nicht digitalen) in ihren Rechtswirkungen mit der eigenhändigen Unterschrift vorzusehen

---

[292] Entspricht der „fortgeschrittenen elektronische Signatur“ der Signaturrichtlinie. Ein "qualifiziertes Zertifikat" muss die Anforderungen des Anhangs I erfüllen und von einem Zertifizierungsdiensteanbieter bereitgestellt werden, der die Anforderungen des Anhangs II erfüllt.
Anhang I legt die Anforderungen an qualifizierte Zertifikate fest und Anhang II die Anforderungen an Zerifizierungsdienstanbieter, die Zertifikate ausstellen.

[293] *Forgo*, Sicher ist sicher? – Das Signaturgesetz, ecolex 1999, 607 (609).

und diese in Gerichtsverfahren in gleicher Weise wie handschriftliche Unterschriften als Beweismittel zuzulassen.[294]
Nach Art 5 Abs 2 darf der elektronischen Signatur die Rechtsgültigkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder nicht auf einem qualifizierten Zertifikat beruht oder nicht auf einem von einem akkreditierten Zertifizierungsdienstanbieter erteilten qualifizierten Zertifikat beruht, oder nicht von einer sicheren Signaturerstellungseinheit erstellt worden ist.
Bezüglich der Rechtswirkung erstellt die Richtlinie also ein zweistufiges System. Die Rechtswirkungen von Art 5 Abs 1 gelten nur für **fortgeschrittene elektronische Signaturen**, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt worden sind.
Für den **nicht formgebundenen Bereich** sieht daher § 3 SigG die grundsätzliche Zulässigkeit der Verwendung elektronischer Signaturen im Rechts- und Geschäftsverkehr vor. Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt oder nicht auf einem qualifizierten Zertifikat beruht.
In den Erläuterungen zu § 3 SigG heißt es: "Die Zulässigkeit elektronischer Kommunikation - zumindest im

[294] Erwägungsgrund 6 der Signaturrichtlinie: „Die rechtliche Wirkung elektronischer Signaturen ist ein zentraler Faktor in einem offenen, aber vertrauenswürdigen System. Die Anwendung dieser Richtlinie soll auch dadurch zu harmonisierten rechtlichen Rahmenbedingungen in der Gemeinschaft beitragen, dass gewährleistet wird, dass einer elektronischen Signatur nicht die Rechtsgültigkeit, Rechtswirkung oder Durchsetzbarkeit mit der Begründung abgesprochen werden kann, dass die Signatur in elektronischer Form vorliegt, nicht auf einem qualifizierten oder nicht auf einem von einem akkreditierten Diensteanbieter ausgestellten Zertifikat basiert. Ferner ist sicherzustellen, dass elektronische Signaturen in gleicher Weise wie handschriftliche Signaturen rechtlich anerkannt werden. In den nationalen Beweisvorschriften sollten elektronische Signaturen ebenfalls anerkannt werden.“

rechtsgeschäftlichen Verkehr - wird grundsätzlich an eine Vereinbarung zwischen den Beteiligten zu knüpfen sein. Die bloße Einrichtung einer E-Mail Adresse wird hierfür noch nicht ausreichen."

Eine sichere elektronische Signatur erfüllt gemäß § 4 Abs 1 das Erfordernis der eigenhändigen Unterschrift, insbesondere der Schriftlichkeit iS von § 886 ABGB, sofern durch Gesetze oder Parteienvereinbarung nichts anderes bestimmt ist.

Die sichere elektronische Signatur, die eine Reihe von Voraussetzungen erfüllen muss, ist daher in Einklang mit der Richtlinie der eigenhändigen Unterschrift gleichzustellen.

In **Österreich** gilt bezüglich der Gültigkeit eines Rechtsgeschäftes gemäß § 883 ABGB der **Grundsatz der Formfreiheit**. Verträge können daher schriftlich, mündlich oder formfrei abgeschlossen werden. Einschränkungen dieses Prinzips ergeben sich aufgrund von möglichen Parteienvereinbarungen und gesetzlichen Sonderregelungen wie beispielsweise bei Realverträgen, im Verbraucherschutzrecht oder im Miet- und Wohnrecht.[295]

§ 886 ABGB bestimmt, dass das Schriftformerfordernis der einfachen Schriftform nur durch die eigenhändige Unterschrift erbracht werden kann. Eine Nachbildung auf mechanischen Weg ist gemäß § 886 letzter Satz ABGB nur dort zulässig, wo es im Geschäftsverkehr üblich ist.

Daher war es nach österreichischer Rechtslage bisher nicht erlaubt, Geschäfte die Schriftformerfordernisse erfordern über das Internet abzuschließen. Dies ermöglicht nun Art 5 der Richtlinie. Ziel dieser Bestimmung ist es auch formgebundene Verträge über das Internet wirksam schließen zu können.

Den Mitgliedstaaten wird jedoch ein Spielraum eingeräumt in welchen Bereichen die elektronische Unterschrift nicht zugelassen wird. Die Richtlinie will nicht in das Vertragsrecht der Mitgliedstaaten eingreifen.[296]

---

[295] *Koziol/Welser*, Grundriß[10], 151.

[296] Erwägungsgrund 9 der Signaturrichtlinie.

Dieser Spielraum wird jedoch durch **Art 9 der E-Commerce Richtlinie** eingeschränkt.

Die Mitgliedstaaten werden in Art 9 verpflichtet, ihre innerstaatlichen *Rechtsvorschriften so zu gestalten, dass die Verwendung elektronischer Verträge einerseits de facto ermöglicht wird und andererseits diesen Verträgen auch Rechtswirksamkeit zukommt*.[297] Das betrifft insbesondere Formerfordernisse, da nicht nur der Abschluß formfreier sondern auch formgebundener Verträge auf elektronischem Weg ermöglicht werden soll.

Vom Grundsatz, dass alle Verträge auch auf elektronischem Weg zustande kommen können müssen, sieht **Art 9 Abs 2 Ausnahmen für bestimmte Vertragstypen** vor. Die Mitgliedstaaten können 1. Verträge, die der Mitwirkung eines Notars bedürfen; 2. Verträge, die erst nach Eintragung in ein behördliches Register Rechtskraft erlangen und 3. Verträge im Bereich des Familien- und Erbrechts von diesem Grundsatz ausnehmen. Art 9 Abs 2 der E-Commerce Richtlinie gibt einen Spielraum für Ausnahmen für Notariatsakte, registrierungspflichtige Verträge und das Familien- und Erbrecht. Diese Bestimmung ergänzt die Signaturrichtlinie, die die Rechtswirkung elektronischer Signaturen regelt.

In Umsetzung dieser Bestimmung entfaltet gemäß **§ 4 Abs 2 SigG** daher eine sichere elektronische Signatur nicht die Rechtswirkungen der Schriftlichkeit iSd § 886 ABGB bei 1. *Rechtsgeschäften des Familien- und Erbrechts*, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind[298]; 2. anderen Willenserklärungen oder Rechtsgeschäften, die einer *öffentlichen Beglaubigung, einer gerichtlichen oder*

---

[297] Die Prüfung anpassungsbedürftiger Rechtsvorschriften durch die Mitgliedstaaten umfasst sämtliche Phasen des Vertragsschlusses. Dh die Aufforderung für eine Anbotstellung, die Verhandlung, das Anbot, den Abschluss des Vertrages, die Registrierung des Vertrages, die Kündigung und die Archivierung des Vertrages.

[298] Darunter fallen nach den EB der RV zu § 4 beispielsweise ein eigenhändig verfasstes Testament, nicht aber eine Unterhaltsverpflichtungserklärung eines Elternteils.

notariellen Beurkundung oder eines Notariatsakts bedürfen; 3. Willenserklärungen, Rechtsgeschäften, Eingaben, die zu ihrer *Eintragung ins Grundbuch, Firmenbuch oder in ein anderes Register einer öffentlichen Beglaubigung, einer gerichtlichen/notariellen Beurkundung oder eines Notariatsaktes* bedürfen und 4. einer *Bürgschaftserklärung* iSd § 1346 Abs 2 ABGB.

Die Ausnahmen der Z 1-3 sind wohl als richtlinienkonform anzusehen.[299] Dieser letzte Punkt der Ausnahmen, die Bürgschaftserklärung, ist jedoch höchst fragwürdig. Grundsätzlich macht die EU-Richtlinie keine Vorschriften darüber, welches Formerfordernis für eine bestimmte Willenserklärung erfüllt werden muß. Sie statuiert allerdings in Art 5 Abs 1 lit a, dass fortgeschrittene elektronische Signaturen die "rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen, wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen".

Durch die Ausnahme der Gültigkeit sicherer elektronischer Signaturen für die Abgabe von Bürgschaftserklärungen wird die elektronische Signatur gegenüber der handschriftlichen Unterschrift zur Unterschrift zweiter Klasse. Als Grund für diese Differenzierung wird in den Erläuterungen zur RV zum SigG wird der Übereilungsschutz genannt. Das ist zwar ein legitimes Interesse - der Weg allerdings, auf dem dieses Interesse durchgesetzt werden soll, führt zu Rechtsunsicherheit und zu einer österreichischen Lösung, die nicht im Einklang zu den Zielen der E-Commerce Richtlinie steht.[300]

Da in § 4 Abs 2 SigG der Schiedsvertrag nicht erwähnt ist, ist ein nach dem 1.1.2000 auf elektronischem Weg geschlossener Vertrag mit Schiedsklausel oder eine Schiedsvereinbarung, die

---

[299] *Jud/Högler-Pracher*, Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschriften, ecolex 1999, 610 (613).

[300] Vgl dazu *Forgo*, ecolex 1999, 608; *Jud/Högler-Pracher*, ecolex 1999, 610 (613).

mit einer elektronischen Signatur unterschrieben ist, eine gültige Schiedsvereinbarung im Sinne von § 577 Abs 3 ZPO.[301]

3.3.2.1.5 Zertifizierungsdiensteanbieter

Verschlüsselungsverfahren weisen eine Sicherheitslücke auf. Es besteht ein gewisses **Zuordnungsrisiko**, da ein Schlüsselpaar falsch zugeordnet werden könnte. Daher muß die Zuordnung eines Schlüsselpaares von einer Institution erfolgen zu der die beteiligten Parteien Vertrauen haben.
Unumgängliche Voraussetzung für die weite Verbreitung und die Garantie der Authentizität dieser digitalen Signaturen ist daher die Einrichtung von Zertifizierungsanstalten.
Die **Zertifizierungsanstalten,** auch **Certificate Authorities** genannt, ermöglichen den Nachweis, dass der öffentliche Schlüssel wirklich mit dem des Senders übereinstimmt
Die Aufnahme und Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters bedürfen laut § 6 Abs 1 SigG keiner gesonderten Genehmigung. Damit entspricht die österreichische Rechtslage der Signaturrichtlinie.
Ein Zertifizierungsdiensteanbieter hat die Aufnahme seiner Tätigkeit unverzüglich der Aufsichtsstelle gemäß § 13 SigG anzuzeigen.[302] Zertifizierungsdiensteanbieter können

---

[301] Außerhalb der EU gibt es zwar verschiedene Initiativen der UNO und in den USA, zu einer globalen Anerkennung elektronisch geschlossener Schiedsvereinbarungen ist es jedoch noch ein weiter Weg. So *Neuteufel* anlässlich eines Vortrages am 1.9.1999 in der Wirtschaftskammer Österreich. In Deutschland soll demnächst ein virtuelles Schiedsgericht schnell und flexibel über Streitigkeiten im elektronischen Geschäftsverkehr entscheiden. Im Internet unter http://www.akademie.de/news/langtext.html?id=2836.
Zu den rechtlichen und technischen Rahmenbedingungen für Schiedsverfahren unter Verwendung elektronischer Medien vgl *Jud/Högler-Pracher*, Schiedsverfahren mit modernen Kommunikationstechniken, ecolex 1999, 601.

[302] In Österreich treten zur Zeit folgende Unternehmen als Anbieter von Zertifizierungsdienstleistungen auf: *Datakom Austria* mit „A-Sign“(http://a-sign.datakom.at), *APPS* (Austrian Payment Systems Services GmbH) mit „E-Sign“(http://www.e-sign.at). Daneben sind Verisign

Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen anbieten. Stellt eine Zertifizierungsstelle sichere elektronische Signaturen bereit, so muss sie in ihrem Sicherheitskonzept die Einhaltung der Sicherheitsanforderungen nach dem SigG und den Verordnungen, die auf Basis des SigG ergehen, darlegen.

3.3.2.1.5.1 Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

Eine Zertifizierungsstelle, die qualifizierte Zertifikate ausstellt, hat nach § 7 SigG besonderen Anforderungen zu genügen.
Ein Zertifizierungsdiensteanbeiter hat gemäß § 8 SigG die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, zuverlässig festzustellen.
Gemäß § 12 SigG hat eine Zertifizierungsstelle die Einstellung ihrer Tätigkeit unverzüglich der Aufsichtsstelle anzuzeigen.

3.3.2.1.5.2 Haftung

Art 6 beschäftigt sich mit der **Haftung des Zertifizierungsdiensteanbieters.** Die Mitgliedstaten müssen als Mindestregelung gewährleisten, dass ein Zertifizierungsdiensteanbieter, der ein qualifiziertes Zertifikat öffentlich erteilt oder für ein Zertifikat öffentlich einsteht, in bezug auf Schäden gegenüber einer Person, die billigerweise auf das Zertifikat vertraut, für bestimmte Leistungen haftet. Wenn der Zertifizierungsdiensteanbieter nachweist, dass er nicht fahrlässig gehandelt hat, haftet er für die oben genannten Punkte nicht.

(http://www.verisign.com), die *ARGE Daten* (http://www.keyserver.ad.or.at), AD Cert (http://www.arges.tempo.at/) und net.surance (http://www.generali.co.at/security/) in Österreich tätig. Vgl dazu im Detail Gewinn 5/1999, 106.

Als Mindestregelung ist weiters vorzusehen: Vertraut eine Person auf ein qualifiziertes Zertifikat, das widerrufen worden ist, und der Widerruf des Zertifikats ist nicht registriert worden, so haftet der Zertifizierungsdiensteanbieter für daraus entstehende Schäden, falls er nicht nachweisen kann, dass er nicht fahrlässig handelte.

Überdies muß der Zertifizierungsdiensteanbieter Beschränkungen des Geltungsbereiches des Zertifikates vorgeben können. Diese Beschränkung muß für Dritte erkennbar sein. Wird das Zertifikat über diesen Geltungsbereich heraus genutzt, so ist der Zertifizierungsdiensteanbieter nicht haftbar.

Die Zertifizierungsdiensteanbieter müssen auch den Wert der Transaktionen begrenzen können, für die das Zertifikat verwendet werden kann.

In früheren Entwürfen zur Signaturrichtlinie war eine verschuldensunabhängige Gefährdungshaftung seitens des Zertifizierungsdiensteanbieters vorgesehen, geblieben ist davon eine Beweislastregelung, die auf das Verschulden abzielt. Der Zertifizierungsdiensteanbieter kann seine Verantwortung zudem örtlich und betragsmäßig beschränken.

Auch nach § 24 SigG trifft den Zertifizierungsdiensteanbieter eine Verschuldenshaftung.[303] Er haftet nicht, wenn er nachweist, dass ihn und seine Leute an der Verletzung seiner Verpflichtungen kein Verschulden trifft (§ 24 Abs 3 SigG - **Beweislastumkehr**).

Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt oder für ein ausländisches Zertifikat gemäß § 24 Abs 2 Z2 SigG einsteht, haftet gegenüber jeder Person, die auf das Zertifikat vertraut dafür, dass alle Angaben im qualifizierten Zertifikat im Zeitpunkt der

[303] Ursprünglich war im Entwurf zum SigG für Zertifizierungsstellen eine gesetzliche Haftpflichtversicherung in Höhe von 56 Millionen Schilling vorgesehen, die jedoch nicht in das SigG übernommen wurde.
Von Konsumentenschutzorganisationen war ursprünglich eine Gefährdungshaftung für Zertifizierungsdiensteanbieter gefordert worden.

Ausstellung richtig sind, der im qualifizierten Zertifikat angegebene Signator im Zeitpunkt der Ausstellung im Besitz jener Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen, die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander in komplementärer Weise entsprechen, das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und die Widerrufsdienste verfügbar sind und die Anforderungen an den Zertifizierungsdiensteanbieter gemäß § 7 SigG und an die technischen Komponenten und Verfahren gemäß § 18 SigG erfüllt sind.

3.3.2.1.6 Weltweite Verwendung elektronischer Zertifikate - Anerkennung von Zertifizierungsdienstleistungen aus Drittstaaten

Art 7 legt die **Voraussetzungen für die Anerkennung von Zertifikaten aus Drittstaaten** fest. Die Mitgliedstaaten werden verpflichtet unter gewissen Voraussetzungen, Zertifikate die von einem Zertifizierungsdiensteanbieter eines Drittlandes ausgestellt werden, den von einem in der Gemeinschaft niedergelassenen Diensteanbieter ausgestellten Zertifikaten rechtlich gleichgestellt werden. Die Bereitstellung von Zertifizierungsdiensten aus anderen Mitgliedstaaten dürfen nicht eingeschränkt werden.
Die **Anerkennung** kann dadurch erfolgen, dass der Zertifizierungsdiensteanbieter die Anforderungen dieser Richtlinie erfüllt und einem freiwilligen Akkreditierungssystem eines Mitgliedstaats unterworfen hat oder ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen gemäß Anhang II erfüllt, für das Zertifikat in gleichem Umfang einsteht wie für seine eigenen Zertifikate oder das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der

Gemeinschaft und Drittländern oder internationalen Organisationen anerkannt ist.

Nach **Art 4** hat jeder Mitgliedstaat die Bestimmungen auf die in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter anzuwenden.

Ebenso wie die Signaturrichtlinie zielt auch das österreichische SigG auf die **Interoperabilität von Signaturen** ab. Dabei wird nicht nur die Akkordierung der Signaturaktivitäten der Mitgliedstaaten angestrebt, auch Drittländer sollen einbezogen werden. Um die weltweite Interoperabilität zu gewährleisten, sind multilaterale Vereinbarungen mit Drittländern und die gegenseitige Anerkennung von Zertifizierungsdiensten geplant.

Im Gegensatz zu den USA, wo mehrere Bundesstaaten bereits eigene Signaturgesetze erlassen haben, ohne auf Fragen der Interoperabilität besonderes Augenmerk zu legen, will die EU von Anfang an eine Abstimmung der Signaturaktivitäten herbeiführen.

Nach § 24 Abs 1 SigG sind Zertifikate, die von einem in der EU niedergelassenen Zertifikatsanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, inländischen Zertifikaten gleichgestellt. Qualifizierte Zertifikate solcher Zertifizierungsdiensteanbieter entfalten dieselben Rechtswirkungen wie inländische Zertifikate.

Laut **§ 24 Abs 2 SigG** werden auch Zertifikate, die von einem in einem Drittstaat niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, im Inland anerkannt. Qualifizierte Zertifikate werden gleichgestellt, wenn die Zertifizierungsstelle die Anforderungen des § 7 SigG erfüllt, unter einem freiwilligen Akkreditierungssystem eines EU-Mitgliedstaats akkreditiert ist, ein EU-Zertifizierungsdiensteanbieter, der die Anforderungen des § 7 SigG erfüllt, für das Zertifikat haftungsrechtlich einsteht oder eine entsprechende bilaterale oder multilaterale Vereinbarung zwischen der EU und Drittstaaten oder internationalen Organisationen besteht.

3.3.2.1.7 Überwachungsbehörden

Als Aufsichtsstelle ist in Österreich gemäß § 13 SigG die **Telekom-Control-Kommission** vorgesehen. Ihr obliegt die Aufsicht über die Einhaltung der Bestimmungen des SigG und der auf Basis des SigG ergangenen Verordnungen.
Die Aufsichtsstelle hat insbesondere die Umsetzung der Angaben im Sicherheits- und Zertifizierungskonzept zu überprüfen, bei sicheren elektronischen Signaturen die Verwendung geeigneter technischer Komponenten (§ 18) zu überwachen, Zertifizierungsstellen gemäß § 17 SigG zu akkreditieren und die organisatorische Aufsicht über Bestätigungsstellen (§ 19) durchzuführen.
Die Aufsichtsstelle stellt Zertifikate für Zertifizierungsdiensteanbieters aus. Für diese Zertifikate gelten die Vorschriften für qualifizierte Zertifikate.
Zertifizierungsdiensteanbieter, die sichere elektronische Signaturen bereitstellen, können auf Antrag akkreditiert werden. (**freiwillige Akkreditierung gemäß § 17 SigG**). Ziel der ex ante Akkreditierung, die in der Signaturrichtlinie in Art 3 Abs 2 geregelt wird, ist es, den Zertifizierungsstellen einen Bonus zu ermöglichen, wenn sie sich akkreditieren lassen.
Für die Erzeugung und Speicherung von Signaturerstellungsdaten und für die Erzeugung sicherer Signaturen sind gemäß § 18 SigG solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen und die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verhindern.
Die **technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen** müssen nach dem Stand der Technik hinreichend geprüft sein. Entsprechen technische Komponenten und Verfahren den allgemein anerkannten Normen, die von der EU-Richtlinie festgelegt werden, so gelten die Sicherheitsanforderungen als erfüllt.

Die Erfüllung der Sicherheitsanforderungen muß von einer Bestätigungsstelle gemäß § 19 SigG bescheinigt sein. Die von Bestätigungsstellen anderer Mitgliedstaaten ausgestellten Bescheinigungen (Produktbewertungen) müssen in den anderen Mitgliedstaaten anerkannt werden.

3.3.2.1.8 Die Signaturverordnung

Wie auch in Deutschland ist die Regelung von Details einer Verordnung vorbehalten. Gemäß **§ 25 SigG** hat der Bundeskanzler im Einvernehmen mit dem Justizminister und dem Bundesminister für Wissenschaft und Verkehr die nach dem Stand der Technik zur Durchführung des SigG erforderlichen Rechtsvorschriften zu erlassen.[304]

3.3.2.1.9 Umsetzung und Kritik

Die den Mitgliedstaaten gewährte Frist für die Umsetzung der Richtlinie in das nationales Recht gemäß Art 13 beträgt **18 Monate** ab Inkrafttreten der Richtlinie.
Nach § 26 SigG tritt das österreichische Signaturgesetz daher richtlinienkonform mit **1.1.2000** in Kraft. *Damit ist Österreich der erste Mitgliedstaat, der über ein nationales*

[304] Das betrifft insbesondere folgende Bereiche: die Festsetzung kostendeckender Entgelt für die Leistungen der Aufsichtsstelle, der Telekom-Control-GmbH und der Bestätigungsstellen, die Festsetzung der für die Abdeckung des Haftungsrisikos der Zertifizierungsdiensteanbieter notwendigen Finanzmittel, die näheren Sicherheitsanforderungen an die technischen Komponenten und Verfahren, die Dauer der Führung der Widerrufsdienste durch die Aufsichtsstelle, Anwendungsbereiche, Anforderungen und Toleranzen von sicheren Zeitstempeldiensten, die Gültigkeitsdauer und die Erneuerung der qualifizierten Zertifikate, sowie den Zeitraum und das Verfahren, nach denen eine neue elektronische Signatur angebracht werden sollte (nachsignieren), Form, Darstellung und Verfügbarkeit des Zertifizierungskonzepts, die Dauer der Aufbewahrung einer Dokumentation gemäß § 11 und die Art und Form der Kennzeichnung akkreditierter Zertifizierungsdiensteanbieter.

Umsetzungsgesetz verfügt, das Großteils der Signaturrichtlinie entspricht.[305]

Kritisiert wurde in Stellungnahmen zum Entwurf vor allem der Zusammenhang zwischen des SigG zu bestehenden Gesetzen, da weder die Rechtsfolgen im Strafrecht, noch die verwaltungsrechtlichen oder zivilrechtlichen Folgen geregelt sind. Unklar ist auch, ob mit der elektronischen Signatur, dem Zertifikat und der damit verbundenen Identitätsfeststellung die Kriterien einer Privaturkunde oder einer öffentlich beglaubigten Urkunde erfüllt werden. Eine Anwendung des Urkundenbegriffes auf die elektronische Signatur würde die Urkundendelikte des Strafrechts anwendbar machen, was in der Folge zu mehr Rechtssicherheit für Signatoren, Empfänger und Zertifizierungsstellen führen würde.

Schon vor der Veröffentlichung des Entwurfes wurde – vor allem von seiten der Wirtschaft - eine Verabschiedung der Signaturrichtlinie vehement gefordert. *Die Signaturrichtlinie ist grundsätzlich zu begrüßen, da sie die Basis für einen europaweiten elektronischen Geschäftsverkehr schafft. Auch der weite Geltungsbereich wurde gegenüber dem engeren Ansatz des deutschen SigG gelobt. Vor allem von der deutschen Lehre wurde positiv vermerkt, dass die Richtlinie nicht nur die technischen Voraussetzungen für den sicheren Geschäftsverkehr schaffe, sondern auch Regelungen der Rechtsfolgenwirkung elektronischer Erklärungen beinhaltet.*[306]

Kritisch wurde vermerkt, dass die in der Signaturrichtlinie vorgesehenen Instanzen keine ausreichende Sicherheit der Signaturverfahren gewährleisten können.[307]

---

[305] Zu den Abweichungen des SigG von der Signaturrichtlinie vgl *Forgo*, Sicher ist sicher? – das Signaturgesetz, ecolex 1999, 607.

[306] *Geis*, MMR 6/1998 VII; ihm folgend *Roßnagel*, Elektronische Signaturen in Europa – Der Richtlinienvorschlag der Europäischen Kommission, 331.

[307] *Roßnagel*, Elektronische Signaturen, 334.

3.4 DIE E-COMMERCE RICHTLINIE – EIN EINHEITLICHER RAHMEN FÜR DEN ELEKTRONISCHEN GESCHÄFTSVERKEHR IN EUROPA?

Aus den bisherigen Ausführungen ergibt sich, dass zur Zeit verschiedene – für den Bereich des Electronic Commerce relevante - sekundärrechtliche Regelungen im Gemeinschaftsrecht nebeneinander existieren. Daneben haben auch die Mitgliedstaaten in den nationalen Rechtsordnungen eine Vielzahl von derartigen Regelungen erlassen. Auch internationale Organisationen arbeiten intensiv an der Regulierung des elektronischen Geschäftsverkehrs. **Der derzeitige Rechtsrahmen trägt weder zur Übersichtlichkeit noch zur Rechtssicherheit bei**.[308]

Überdies ergibt sich daneben das Problem, dass Unklarheit in vielen Rechtsbereichen besteht, ob und wieweit die bestehenden Regelungen auf den „Online“ Bereich anwendbar sind.[309]

Aus diesen Gründen hat die Europäische Union die **Schaffung von einheitlichen rechtlichen Rahmenbedingungen, die einen kohärenten Rechtsrahmen für den elektronischen Geschäftsverkehr im Binnenmarkt schaffen sollen**, als notwendig erachtet und arbeitet seit mehreren Jahren an einem entsprechenden Regelwerk.[310]

Am 11.Jänner 1997 präsentierte die Kommission einen **Entwurf für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt**.[311]

---

[308] Entwurf, 8.

[309] Entwurf, 3.

[310] Entwurf, 4.

[311] KOM (98) 586 endg. Im Internet unter http://ispo.cec.be/Ecommerce/docs/legalde.pdf. Der Vorschlag basiert auf der Mitteilung der Kommission „Europäische Initiative für den

Das Europäischen Parlaments gab am 6. Mai 1999 zum ursprünglichen Vorschlag eine befürwortende Stellungnahme ab, die den binnenmarktorientierten Ansatz der Kommission voll und ganz unterstützt, brachte jedoch einige Änderungsanträge ein.[312]

Am 6. September 1999 legte die Europäische Kommission dem Parlament und dem EU-Ministerrat einen **geänderten Entwurf** der Richtlinie vor.[313] Damit die Richtlinie der raschen technischen Entwicklung und den Änderungen im Electronic Commerce auch gerecht wird, soll sie drei Jahre nach dem Erlass auf ihre Aktualität überprüft werden. Maßgebliche Kriterien dafür sind technische und wirtschaftliche Einflüsse aber auch die Rechtsprechung in den einzelnen Mitgliedstaaten. Im Folgenden wird der Geltungsbereich der Richtlinie und die wesentlichen Inhalte behandelt.[314]

---

elektronischen Geschäftsverkehr“ worin die Kommission bis zum Jahr 2000 einen kohärente Rechtsrahmen für Online-Beziehungen schaffen will.

[312] KOM(98) 586 endg vom 18.11.1998. In der Folge als Entwurf bezeichnet.

[313] KOM(99) 427 endg. Im Internet unter http://europa.eu.int/comm/dg15/en/media/eleccomm/com427de.pdf. In der Folge als geänderter Entwurf bezeichnet.
Die Kommission hat darin einige Änderungswünsche des Parlamentes berücksichtigt. Im überarbeiteten Entwurf wurden vor allem Begriffsdefinitionen präzisiert. Daneben gab es Änderungen bei folgenden Themen: 1. Spamming (Wer Werbung per E-Mail verschickt, muss vorher ein sogenanntes Opt-Out-Register konsultieren. Darin kann sich jede natürliche Person eintragen, wenn sie keine Werbung per Mail erhalten möchte) 2. Vereinfachung der Regelung über den Zeitpunkt des Vertragsabschlusses (ein elektronischer Vertrag kommt erst dann zustande, sobald der Nutzer vom Diensteanbieter auf elektronischem Wege die Empfangsbestätigung seiner Bestellung erhalten hat. Die Empfangsbestätigung gilt als zugegangen, wenn der Nutzer sie abrufen kann. Erst ab diesem Zeitpunkt sind beide Parteien an den Vertrag gebunden) und 3. Überprüfung der Richtlinie spätestens drei Jahre nach deren Erlass, damit notwendige Änderungen aufgrund neuer Techniken eingefügt werden können.

[314] Wenn Bestimmungen der E-Commerce Richtlinie auch Auswirkungen auf andere in der Arbeit behandelten Bereiche haben, wurden sie bereits in diesem Zusammenhang dargestellt.

3.4.1 Anwendungsbereich

Nach Art 1 Z2 soll die E-Commerce Richtlinie, „*die für die Dienste der Informationsgesellschaft geltenden innerstaatlichen Regelungen einander angleichen*“. Davon betroffen sind das Binnenmarktprinzip, die Niederlassung der Diensteanbieter, kommerzielle Kommunikationen, elektronische Verträge, die Haftung von Vermittlern, Verhaltenskodizes, Systeme zur außergerichtlichen Beilegung von Streitigkeiten, Klagemöglichkeiten sowie die Zusammenarbeit zwischen den Mitgliedstaaten.“

Unter „**Dienste der Informationsgesellschaft**“ ist gemäß Art 2 lit a jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung zu verstehen. Je nach verwendeter Technologie fallen darunter der Vertrieb von Waren und Dienstleistungen im Fernabsatz und das Teleshopping. Nicht erfasst sind Post- und Telefondienste, die Internet-Telefonie und Rundfunkdienste wie Fernseh- und Radiosendungen(eingeschränkt Webcasting[315]). *Entscheidend für die Anwendung der E-Commerce Richtlinie sind also die Übertragungstechniken und nicht die übertragenen Inhalte.*

Der Begriff der „Dienste der Informationsgesellschaft“ ist der Transparenzrichtlinie[316] entnommen, in der sich in Anhang auch eine beispielhafte Aufzählung der Dienste findet, die unter diesen Terminus fallen.

3.4.1.2 Ausnahmen vom Anwendungsbereich

[315] *Brenn*, ÖJZ 13/1999, 481 (483).

[316] Richtlinie des Europäischen Parlaments und des Rates vom 22.6.1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, Abl 1998 L 204/37, geändert durch die Richtlinie 98/48/EG, Abl 1998 L 217/18.

Die Richtlinie findet **keine Anwendung** auf das *Steuerwesen* (Art 22 Abs 1 lit a[317], den *Datenschutz* (lit b) sowie Tätigkeiten von *Notaren, gewisse anwaltliche Tätigkeiten und Geldspiele* (lit c).

Die Nichtanwendbarkeit der Richtlinie auf den von der Datenschutzrichtlinie (95/46/EG) erfaßten Bereich erscheint nicht einsichtig, da im elektronischen Geschäftsverkehr auch personenbezogene Daten wie Adressen, Namen, Bestellungen verarbeitet werden.

Gewisse Bereiche sind grundsätzlich erfasst, jedoch **vom Binnenmarktprinzip nach Art 3 ausgenommen**. Darunter fallen *Urheberrechte, gewerbliche Schutzrechte, Finanzdienstleistungen, vertragliche Verpflichtungen betreffend Verbraucherverträge und unerbetene Werbung durch elektronische Post.*

Die E-Commerce Richtlinie zielt nicht darauf ab, spezifische Regeln des **Internationalen Privatrechts** betreffend das anwendbare Recht oder der Zuständigkeit der Gerichte einzuführen und läßt die einschlägigen internationalen Übereinkommen daher unberührt.[318] Die Kommission subsumiert jedoch unter die Wendung *„vertragliche Verpflichtungen betreffend Verbraucherverträge“* auch das internationale Privatrecht auf europäischer Ebene.[319] Daraus ergeben sich weitreichende **Konsequenzen**. Durch die geplanten Änderungen des Brüsseler und des Lugano Übereinkommens[320] ergeben sich weitreichende Auswirkungen für den elektronischen Geschäftsverkehr in Europa. Die Kommission hat Ende 1997 eine Arbeitsgruppe zur Revision der Übereinkommen eingesetzt. Mittlerweile liegt auch ein Entwurf für eine Verordnung vor,

---

[317] Steuerliche Fragen wurden offensichtlich mangels Übereinstimmung in den Mitgliedstaaten von der Kommission ausgeklammert. Eine Einbeziehung hätte die Verabschiedung der Richtlinie sicherlich verzögert.

[318] Erwägungsgrund 7 der Richtlinie.

[319] Vgl. dazu *Brenn*, ÖJZ 13/1999, 483.

[320] Übereinkommen über die gerichtliche Zuständigkeit und Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen vom 16.9.1998(LGVÜ), BGBl 448/1996, Abl 1998 L 319, 9.

die Änderungen im EuGVÜ vorsieht, mit der die Übereinkommen in Fragen des anwendbaren Rechts und der Gerichtszuständigkeit auf die neuen Technologien angepasst werden sollen.[321]

Als **Streitpunkt zwischen Verbraucherverbänden und der Wirtschaft** hat sich insbesondere die geplante Änderung von Art 15 Abs 1 lit c und Art 16 EuGVÜ herauskristallisiert. Die Änderungen würden hinsichtlich des Gerichtstandes bei Geschäften zwischen Verbrauchern und Unternehmern auf elektronischen Weg dazu führen, dass Unternehmer in allen Mitgliedstaaten in denen sie als Dienstanbieter auftreten (de facto in all jenen, wo ihre Homepage abrufbar ist und wo sie Waren oder Dienstleistungen anbieten) den Verbraucher im Mitgliedstaat klagen müßten, wo er seinen Wohnsitz innehat und von dem Verbraucher auch dort jederzeit geklagt werden könnten. Dies hat zu heftigen Protesten der Wirtschaft geführt.[322]

---

[321] Vorschlag für einen Rechtsakt des Rates über die Ausarbeitung des Übereinkommens Über die gerichtliche Zuständigkeit, die Anerkennung und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen in den Mitgliedstaaten der Europäischen Union, KOM(97) 609 endg.

[322] Im Internet unter http://www.pressetext.at/show.pl.cgi?pta=3D990708022; http://www.pressetext.at/show.pl.cgi?pta=990613003; http://www.pressetext.at/show.pl.cgi?pta=991103009. Die Verbraucherverbände fordern das Empfängerlandprinzip, wogegen sich die Wirtschaft für das Ursprungslandprinzip ausspricht, mit dem Hinweis, dass das Internet ein globales Medium ist und ein Unternehmer, der elektronischen Handel betreibt, sich nicht auf die Rechtslage jedes Staates der Welt Rücksicht nehmen kann. Da das Internet ein globales Medium ist, kann ein Unternehmer, der elektronischen Handel betreibt, nicht auf die Rechtslage jedes Staates der Welt Rücksicht nehmen könne und ein weltweit gültiges „Online-Recht“ nicht existiere. In einem Expertenhearing am 4. und 5.11.1999 in Brüssel hat die Kommission die offenen Fragen in Bezug auf die Gerichtsstände und das anwendbare Recht mit beiden Konfliktparteien besprochen. Im Internet unter http://www.akademie.de/news/langtext.html?id=2511.
Vgl grundsätzlich zur „Problematik IPR und elektronischer Geschäftsverkehr“ *Fallenböck/Haberler*, Rechtsfragen bei Verbrauchergeschäften im Internet (Online-Retailing), RdW 1998/8, 505 (507); *Fallenböck* in *Mänhardt/Posch*, Internationales Privatrecht-Privatrechtsvergleichung-Einheitsprivatrecht (1999) 104.

Die Wirtschaft spricht sich für das Herkunftslandprinzip aus, das festschreibt, dass das Handeln eines Dienstes der Informationsgesellschaft nach dem Recht des Staates zu beurteilen ist, in dem der Anbieter seinen Sitz hat.
Unter gewissen Voraussetzungen können die zuständigen Behörden der Mitgliedstaaten unter Beachtung des Gemeinschaftsrechts Maßnahmen ergreifen, die den freien Verkehr eines Dienstes der Informationsgesellschaft beschränken (Art 22 Abs 3).[323]

3.4.2 Wichtige Regelungsbereiche

3.4.2.1 Grundsatz der Zulassungsfreiheit für Diensteanbieter

Der **Zugang zur Tätigkeit eines Anbieters** von Diensten der Informationsgesellschaft ist gemäß Art 4 **nicht zulassungspflichtig**. Art 5 erlegt jedoch den Diensteanbietern zum Ausgleich dazu bestimmte allgemeine Informationspflichten auf.
Anders als im konventionellen Fernabsatz, bei dem der Konsument über Daten wie Telefonnummer oder der Anschrift des Anbieters verfügt, ist der Kunde im „Online-Fernabsatz“ auf einen Domainnamen oder eine E-Mail Adresse angewiesen. Mit einem gewissen Aufwand ist es möglich, die Person, die über diese „virtuellen“ Adressierungselemente verfügungsberechtigt ist, herauszufinden. Diese Person ist jedoch deshalb nicht automatisch für den Inhalt verantwortlich. Daher müssen die Diensteanbieter für den Nutzer und die zuständigen Behörden verschiedene Informationen ständig, unmittelbar und leicht zugänglich bereithalten. Das betrifft den Namen des Diensteanbieters, die Anschrift der Niederlassung, Kontaktmöglichkeiten, einschließlich seiner E-Mail Adresse, Firmenbuchnummer, Angaben der Zulassungsbehörde und die Umsatzsteuernummer.

[323] Darunter fallen Maßnahmen zum - Schutz der öffentlichen Ordnung, der öffentlichen Gesundheit, der öffentlichen Sicherheit und der Verbraucher.

3.4.2.2 Vertragsabschluß im Netz

Solange lediglich das Anbieten von Waren und Dienstleistungen über elektronische Netze zulässig ist und der Vertragsabschluß zwischen Anbieter und Nutzer noch auf konventionelle Weise erfolgen muss, wird sich der elektronische Geschäftsverkehr nicht durchsetzen. Die Kommission hat sich deshalb entschlossen, die bestehenden Rechtsunsicherheiten im Bereich der Rechtswirksamkeit elektronischer Verträge und deren Beweiswert zu beseitigen.
Art 10 schreibt **Informationspflichten des Diensteanbieters** im Rahmen des Abschlusses eines Vertrages auf elektronischem Weg fest. Dies betrifft vor allem die Erläuterung des Zustandekommens des elektronischen Vertrages. Dem Verbraucher, (für den dies zwingend vorgesehen ist) und dem gewerblichen Nutzer (bei dem dies abbedungen werden kann), müssen die technischen Abläufe erläutert werden. Das rechtliche Prozedere des Zustandekommens des Vertrages ist davon nicht erfasst.[324]

3.4.2.2.1 Zeitpunkt des Vertragsabschlusses

Bedeutsam ist vor allem zu welchem Zeitpunkt ein elektronischer Vertrag als abgeschlossen gilt. Dabei kann die Annahme eines Vertragsangebots durch den Empfänger der Dienstleistung auch darin bestehen, dass dieser online eine Bezahlung ausführt. Die Eingangsbestätigung durch den Anbieter kann darin bestehen, dass dieser eine bereits bezahlte Dienstleistung tatsächlich online erbringt.
Um Verträge gültig zustande kommen zu lassen, sind nach österreichischem Zivilrecht zwei **übereinstimmende Willenserklärungen** der Parteien notwendig.[325] Es besteht natürlich die Möglichkeit, Willenserklärungen auch im elektronischen Verkehr abzugeben Dies kann sowohl zwischen

[324] *Brenn*, ÖJZ 1999, 487.
[325] *Koziol/Welser*, Grundriß[10], 103 (104).

Personen als auch von Personen zu Maschinen oder umgekehrt geschehen.[326]

Sowohl Erklärungen mittels Fernsprecher, in Chat rooms, über voice over IP, mittels Web-Formular oder per E-Mail können daher als Anbot oder Annahme im Sinne der §§ 862 bis 864 ABGB rechtliche Wirkungen entfalten.

Das Anbieten von Waren und Dienstleistungen auf einer Webseite ist rechtlich nicht als Anbot im Sinne von § 861 ABGB zu werten. Im Regelfall ist es lediglich als Aufforderung zur Stellung von Anboten (Inovatio ad offerendum) vergleichbar mit Katalogen oder Schaufenster oder als Anbot an einen unbestimmten Personenkreis zu sehen, ohne dass der Anbieter bereits eine endgültige Willenserklärung abgibt.[327]

Ein **Anbot** wird erst dadurch abgegeben, indem ein Bestellformular auf einer Website durch einen Käufer ausgefüllt und abgeschickt wird oder durch Versendung einer E-Mail, wo der Besteller seinen Willen dokumentiert, eine Ware zu erwerben. Das Anbot geht also in der Regel nicht vom Anbieter aus.

Erst mit dem Zugang der Nachricht beim Empfänger wird das Anbot wirksam und entsteht die **Bindung des Anbotstellers**. Als Postkasten im elektronischen Bereich fungiert die Mailbox.[328] Digitale Willenserklärungen gelten als **zugegangen**, wenn die

---

[326] Willenserklärungen von Computern haben dieselben Rechtswirkungen wie Erklärungen, die direkt von natürlicher Person abgegeben werden. Vgl. *Fallenböck*, Rechtsfragen beim Verbrauchergeschäft im Internet (Online-Retailing), RdW 1999/8, 505.

[327] hM in Österreich: *Rummel* in *Rummel*, ABGB², Rz 7 zu § 861 mwN; *Koziol/Welser*, Grundriß[10] I, 104; *Madl*, Vertragsabschluß im Internet, ecolex 1996, 79; *Brenn*, ÖJZ 1997, 653; *Jaburek/Wölfl*, Cyber-Recht, 101. Ihnen folgend mit der Einschränkung, dass sehr wohl ein Anbot beim zum direkten download von Software gegen Bezahlung mittels Kreditkarten vorliege, *Fallenböck*, Rechtsfragen beim Verbrauchergeschäft im Internet (Online-Retailing), RdW 1999/8, 505. Unter FN 6 findet sich auch eine Übersicht über die hM in Deutschland.

[328] Vergleichbar mit dem konventionellen Briefkasten. Zu den geringfügigen Unterschieden zwischen einer Mailbox und einem Briefkasten *Fallenböck*, RdW 1999/8, 506, FN 22.

Erklärung im Machtbereich des Empfängers eingelangt ist und dieser sich Kenntnis vom Inhalt der Nachricht verschaffen kann. Die Bindungswirkung entsteht nicht schon im Zeitpunkt der Abspeicherung der E-Mail auf dem Server des Empfängers, sondern im Zeitpunkt des Abrufs der E-Mail durch den Empfänger.[329] Wenn die Nachricht in der Mailbox des Empfängers zur Nachtzeit oder an Sonn- und Feiertagen eingeht, gilt sie erst am nächsten Werktag als zugegangen.[330] Hat der Empfänger der Nachricht früher von Ihr Kenntnis erlangt, gilt die Nachricht im Zeitpunkt der tatsächlicher Kenntnis als zugegangen. Es muss davon ausgegangen werden, dass die Mailbox durch einen Verbraucher einmal pro Tag abgerufen wird.[331]

Die **Annahme des Anbotes** kann sowohl durch eine Erfüllungshandlung des Verkäufers als auch mittels einer Bestätigung des Anbotes per E-Mail mit anschließender Leistungserbringung erfolgen.

Auch die E-Commerce Richtlinie sieht eine Regelung des Zeitpunktes des Vertragsabschlusses vor. Dieses System weist jedoch erhebliche Unterschiede zum österreichischen Zivilrecht auf.

Der ursprüngliche **Entwurf** der Kommission bezog sich nur auf eine besondere Situation wo der Diensteanbieter bereits ein Angebot unterbreitet hat, nicht jedoch wenn der Diensteanbieter den Nutzer lediglich zur Angebotsstellung auffordert.

Wie oben dargelegt ist nach hM in Österreich das Anbieten von Waren und Dienstleistungen auf einer Website nicht als Anbot zu werten, sondern lediglich als Aufforderung zur Stellung von Anboten. *Dies hat zur Folge, dass die Regelung des Art 11 Abs 1 des Richtlinienentwurfes in Österreich gar nicht zur Anwendung gekommen wäre.*[332]

---

[329] *Ernst*, Der Mausklick als Rechtsproblem-Willenserklärungen im Internet, NJW-CoR 3/97, 165 (166).

[330] *Brenn*, ÖJZ 1997, 652; *Koch*, Internet-Recht (1998) 143.

[331] *Koziol/Welser*, Grundriß[10] I, 94.

[332] *Brenn*, ÖJZ 1999, 488.

Nach Art 11 des Entwurfes waren nämlich **mehrere Schritte für den für Vertragsabschluß auf elektronischem Weg notwendig**. Das *Anbot* auf einer Website wird bereits als Anbot, das *Absenden der Bestellung* als Annahme qualifiziert. Zum endgültigen Vertragsabschluß sind jedoch nach dem Entwurf noch weitere Schritte notwendig, nämlich eine *Empfangsbestätigung der Annahme* durch den Diensteanbieter und eine *Rückbestätigung des Nutzers* über den Erhalt der Bestätigung. Somit sind vier Schritte zu einem Vertragsabschluß im elektronischen Geschäftsverkehr notwendig.

Diese Regelung wurde heftig **kritisiert**.[333] Wenn einer der beiden Vertragspartner sich mit einer für den Vertragsabschluß erforderlichen Handlung sehr lange Zeit lässt und die notwendige Reaktion nicht setzt, entsteht sofort das Problem der zeitlichen Lücke, die von einem der Vertragsteile zum Vertragsrücktritt genutzt werden könnte. Offen bleibt, wie lange die Partei an ihr Anbot gebunden bleibt. Es können bei dieser komplizierten Konstruktion sehr leicht vorvertragliche Pflichten entstehen, die zu komplizierten Rückabwicklungen führen können, ohne dass überhaupt ein Vertrag entstanden ist. In einem raschen Medium wie dem Internet würde diese umständliche Regelung sicherlich nicht förderlich für Vertragsabschlüsse sein. Vor allem, wenn man bedenkt, dass in Kombination mit digitalen Signaturen ein dreifaches signieren notwendig wäre, was nicht nur aufwendig, sondern auch teuer wäre. Im übrigen sieht schon die Fernabsatzrichtlinie einen umfassenden Schutz des Verbrauchers vor, sodass Art 11 zu recht kritisiert wurde.

Im **geänderten Entwurf** der Kommission wurde die Regelung über den Zeitpunkt des Vertragsabschlusses bei Online-Verträgen gemäß den Änderungswünschen des Parlaments aufgrund dieser Schwächen **neu formuliert** und damit deutlich vereinfacht.

---

[333] *Pilz*, anlässlich eines Seminares am Juridicum der Universität Wien am 28.5.1999. Im Internet unter http//:www.univie.ac.at/ri/ajli/3/index.htm ; *Brenn*, ÖJZ 1999, 488.

Ein auf elektronischem Weg geschlossener Vertrag kommt demnach bereits dann gültig zustande, sobald der Nutzer vom Diensteanbieter die Empfangsbestätigung seiner Bestellung auf elektronischem Wege erhalten hat. *Damit entfällt als zusätzliches Kriterium für das Zustandekommen des Vertrages die Rückbestätigung durch den Nutzer.*
Die Empfangsbestätigung des Diensteanbieters gilt ab dem Zeitpunkt als zugegangen, ab dem der Nutzer diese abrufen kann. Ab diesem Zeitpunkt sind beide Parteien an den Vertrag gebunden. Um Verzögerungen beim Vertragsabschluss hintanzuhalten ist der Diensteanbieter verpflichtet, die Empfangsbestätigung „unverzüglich“ abzusenden.

3.4.2.3 Sonstige Regelungsbereiche

Darüber hinaus beinhaltet die E-Commerce Richtlinie noch Regelungen über die *Werbung*[334], die *Verantwortlichkeit der Provider* für Vermittlungstätigkeiten, wobei die Haftung für Hyperlinks ungeklärt bleibt[335] und über die *effektive Rechtsdurchsetzung*, wobei die Mitgliedstaaten verpflichtet werden, dass bei Streitigkeiten zwischen Diesteanbietern und Nutzern online außergerichtliche Streitbeilegungs- und Vermittlungsverfahren zur Verfügung stehen.

3.4.2. Resümee

Die Initiative der Kommission zur Schaffung der E-Commerce Richtlinie ist zu begrüßen. Die Kommission unterstreicht damit ihre **führende Stellung** in der Verabschiedung von Regelungen

[334] Vgl unter 3.2.4.1.2.

[335] Bei der Überprüfung der E-Commerce Richtlinie drei Jahre nach deren Erlas wird der Frage, ob Regelungen hinsichtlich der Verantwortlichkeit der Anbieter von Hyperlinks notwendig sind, besondere Beachtung geschenkt werden. Zur Verantwortlichkeit von Internet-Providern vgl im Detail *Brenn*,

über den elektronischen Geschäftsverkehr. Nachdem bereits spezifische Regelungen betreffend den elektronischen Geschäftsverkehr verabschiedet wurden, hat die Kommission nunmehr erstmals ein allgemeine Richtlinie mit einem umfangreichen Anwendungsbereich zu diesem Thema vorgelegt.
Die Kommission verfolgt mit der E-Commerce Richtlinie das ehrgeizige und durchaus begrüßenswerte Ziel einen einheitlichen Rechtsrahmen für den grenzüberschreitenden europäischen elektronischen Geschäftsverkehr zu schaffen. Dabei wird versucht, die bereits bestehenden mitgliedstaatlichen Regelungen zu vereinheitlichen und den Mitgliedstaaten gleichzeitig den notwendigen Spielraum zu lassen, um auf Unterschiede in den Zivilrechtssystemen bedacht zu nehmen.
Die E-Commerce Richtlinie wird sicherlich zu einer Erhöhung der Rechtssicherheit im Electronic Commerce in der EU beitragen und damit für dessen Verbreitung sicherlich förderlich sein. Die Richtlinie hat jedoch gewisse Schwächen im Detail. Da eine Überarbeitung bereits in der Richtlinie selbst vorgesehen ist, bleibt zu hoffen, dass die Lücken und Defizite in der Zwischenzeit durch die Rechtsprechung der Gerichte geschlossen werden.

ÖJZ 1999, 488; *derselbe*, Haftet ein Internet-Service-Provider für die von ihm verbreitete Informationen?, ecolex 1999, 249.

4. RESÜMEE UND AUSBLICK

Die Verbreitung des elektronischen Rechtsverkehrs hat für Juristen eine Reihe von *Fragen in verschiedenen Rechtsbereichen* aufgeworfen. Die rechtliche Entwicklung hinkt in diesem Bereich oftmals der technischen hinterher[336]. Electronic Commerce wird zunehmend auch juristisch als globales Phänomen erkannt. Verschiedene Institutionen arbeiten weltweit an verbindlichen Regelungen und unverbindlichen Empfehlungen, um offene Fragen einer Regelung zu unterziehen.
Zur treibenden Kraft der Verrechtlichung des Electronic Commerce und zum *Motor für eine Harmonisierung des grenzüberschreitenden elektronischen Handels* in Europa hat sich die *Europäische Kommission* entwickelt. Sie versucht vorwiegend durch Richtlinien die unterschiedlichen Regelungen in den Mitgliedstaaten zu vereinheitlichen.
Sie begegnet damit dem dringenden Regelungsbedarf auf europäischer Ebene, um das Entstehen unterschiedlicher nationaler Regelungen zu verhindern und das Verhältnis zu Drittstaaten zu klären. Wieweit die Kommission ihren in der globalen Charta dargelegten Ansatz zur Schaffung eines weltweiten E-Commerce Rechts verwirklichen kann, bleibt von ihrer Einflussnahme in den internationalen Gremien abhängig.
Die Problematik von Verträgen zwischen Unternehmern (bzw Verbrauchern) aus der EU und jenen aus Drittstaaten bleibt derzeit aufgrund von mangelnder weltweiter Harmonisierung der Regelungen über den elektronischen Geschäftsverkehr bestehen.
Für die Europäische Union wurden jedenfalls durch die Verabschiedung der Fernabsatz-, der Signatur- und der E-Commerce Richtlinie bereits die grundlegenden Voraussetzungen

[336] „Elektronischer Handel als neues Mega-Geschäft“, Gewinn 10/97, 53. Die Kommission hat daher beispielsweise in der E-Commerce Richtlinie bereits eine Verpflichtung zur Überarbeitung drei Jahre nach deren Erlass vorgesehen, um technische Änderungen entsprechend zu berücksichtigen.

für eine positive Weiterentwicklung des grenzüberschreitenden elektronischen Geschäftsverkehrs geschaffen.

Die genannten sekundärrechtlichen Regelungen bilden jedoch noch nicht den Abschluss der Bemühungen der Kommission dem Electronic Commerce eine rechtliche Basis zu bieten, sodass eine ständige Weiterentwicklung des acquis communautaire in diesem Bereich vorprogrammiert scheint.

Literaturverzeichnis

Aichholzer/Schmutzer, Informations- und Transaktionsdienste im Bereich der öffentlichen Verwaltung, Wirtschaftspolitische Blätter 5/1999, 456 (457),
Arnold, Verbraucherschutz im Internet, CR 9/1997, 526 ff.
Bakos, A Strategic Analysis of Elektronik Marketplaces, MIS Quaterly 15, 294-310.
Bell, The Coming of the Post Industrial Society (1973).
Bergmann, Grenzüberschreitender Datenschutz (1985) 197.
Borges, Verbraucherschutz beim Internet-Shopping, Zeitschrift für Wirtschaftsrecht, 20/1999 H 4, 130 ff.
Brandl/Mayr-Schönberger, CPU-IDS, Cookies und Internet-Datenschutz, ecolex 1999, 366 ff
Brandtweiner, Entwicklung und Auswirkung elektronischer Märkte, Wirtschaftspolitische Blätter 5/1999, 420 (423).
Brenn, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ 1997, 641. *Brenn*, Der elektronische Rechtsverkehr, ÖJZ 1999, 481
Bruck/Selhofer/Winkler, Österreich in der Informationsgesellschaft, Wirtschaftspolitische Blätter 5/1999, 411 (413).
Brühann/Zerdick, Umsetzung der EG-Datenschutzrichtlinie in Österreich, CR 9/1996, 556 (561.),
Bülow, Unsinniges im Fernabsatz, ZIP 31/99, 1294 ff.
Dix, Gesetzliche Verschlüsselungsstandarts-Möglichkeiten der Gesetzgebung, CR 1/1997, 38 ff
Duschanek/Rosenmayr-Klemenz, Datenschutzgesetz-Regierungsvorlage, ecolex 1999, 361.
EDI und INTERNET, Handbuch Hrsg. Austria Pro (Wirtschaftskammer Österreich), 1998, 5.
Ellger, Der Datenschutz im grenzüberschreitenden Datenverkehr, (1990), 532.
Ellger, Datenexport in Drittländer, CR 1993, 8 f.
European Communication Council, einer Gruppe von Kommunikationswissenschaftern, Die Internet-Ökonomie - Strategien für die digitale Wirtschaft, European Communication Council Report, Berlin/Heidelberg 1999.
Fallenböck, Rechtsfragen beim Verbrauchergeschäft im Internet (Online-Retailing), RdW 1999/8, 505,
Fallenböck, Pannenstreifen der Datenautobahn, Die Presse vom 16.2.1999, 12.
Forgo, Was sind und wozu dienen digitale Signaturen, ecolex 4/1999, 235.
Forgo, Sicher ist sicher? – Das Signaturgesetz, ecolex 1999, 607
Graf, Wer haftet bei Telebanking?, e-commerce, ecolex 1999, 239 ff.
Greiner, Sicherheit im Internet in e-commerce, November 1999, 39 ff

Gridl, Datenschutz in globalen Kommunikationssystemen, Baden-Baden 1999.
Halbwidl, Austria Pro Nachrichten Nr. 17 Mai 1999, 38.
Hoeren, Rechtsfragen des Internet, 136. Im Internet unter http://www.uni-muenster.de/Jura.itm/hoeren/.
Jaburek/Wölfl, Cyber-Recht, Marktplatz Internet - Schrankenlose Geschäfte (1997)
Jochum, Wohin mit all den Infos ?, Die Presse vom 12.7.1999, III.
Jud/Högler-Pracher, Schiedsverfahren mit modernen Kommunikationstechniken, ecolex 1999, 601
Koch, Grundrecht auf Verschlüsselung, CR 2/1997 106 ff;
Knoll, Informationsgesellschaft als Aufgabe wirtschaftspolitischer Initiative, Wirtschaftspolitische Blätter 2-3/1998, 119 ff.
Köhler, Die Rechte des Verbrauchers beim Teleshopping (TV-Shopping, Internet-Shopping), NJW 1998, 185
Kopp, Das EG-Richtlinienvorhaben zum Datenschutz, Recht der Datenverarbeitung (RDV) 1993, 1.
Kristoferitsch, Sicherheitsmängel : Das Damoklesschwert des Web-Zahlungsverkehrs, Austria Pro Nachrichten Nr. 16, Jänner 1999
Kronegger, im Internet unter http://www.ad.or.at/office/recht/eu.htm.
Laga, Neue Techniken im World Wide Web - Eine Spielwiese für Juristen?, JurPC Web-Dok. 25/1998, Abs 1-50.
Laga, Rechtsprobleme im Internet, Hrsg. Wirtschaftskammer Österreich (1998) 62,
Madl, Vertragsabschluß im Internet, ecolex 1996, 79;
Morton, Kugel im Nichts, Die Presse vom 13.3.1999, III.
Martos, „Time“ - 4 Branchen verschmelzen, Die Presse vom 26.2.1999, 23.
Mohr, Elektronischer Kauf - Verbraucherschutz im Fernabsatz, ecolex 1999, 249.
Posch, Digitale Signatur und Zertifizierung in Austria Pro Nachrichten, Nr. 14 1998, 12 ff
Riedl, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, ecolex, 4/1999, 241.
Rübig, Die Informationsgesellschaft - Die Zukunft im Griff, in *Kaspar/Rübig*, Telekommunikation, 56 ff
Schallbruch, Electronic Mail im Internet - Wie steht es mit dem Datenschutz ?, Datenschutz-Nachrichten 5/95, 11.
Seidenberger, Internationale Wirtschaft, 4/1999, 20.
Souhrada-Kirchmayer, Der Vorschlag einer allgemeinen EG-Datenschutzrichtlinie und seine Auswirkungen auf das österreichische DSG, JBl 3/1995, 147 (148).
Steindl, Digitale Signatur Sicherheitstechnologie, in Austria Pro Nachrichten, Nr. 17 Mai 1999, 12 ff
Stoll, Bankraub Online : Die Tricks , Kniffe und Methoden der Online-Profis, Feldkirchen 1997.

Touraine, Die postindustrielle Gesellschaft (1972).
Waldenberger, Grenzen des Verbraucherschutzes beim Abschluß von Verträgen im Internet, BB 1996, 2365 (2367)
Weinzierl, Die Arbeitswelt in der Informationsgesellschaft, Wirtschaftspolitische Blätter 2-3/1998, 201 ff.
Wessely, Das EG-Grünbuch Konvergenz, Medien und Recht 1998/4, 175 ff.