

Referat Linklaters Oppenhoff & Rädler/xxx/30/07/2001

12. Oktober 2001

**27. Deutsch-Französisches Juristentreffen
Aix-en-Provence 2001**

**Das Recht des Internet:
Berücksichtigung
in der
deutschen Gesetzgebung**

Dr. Heiner Baab LL.M.

LINKLATERS OPPENHOFF & RÄDLER
Mainzer Landstrasse 16
D-60325 Frankfurt am Main
Postfach 17 01 11
D-60075 Frankfurt am Main
Telephon: (49-69) 7 10 03-372
Telefax: (49-69) 7 10 03-333
Zeichen: JAP/HBB

Das Recht des Internet in der deutschen Gesetzgebung ist mittlerweile zu umfassend, um es in einem einzigen Referat in der vorgegebenen Zeit darzustellen. Die lose Aneinanderreihung von Vorschriften, die ohne Bezug zu einander stehen, würde den Zuhörer nur langweilen. Deshalb habe ich mir unter Berücksichtigung der anwaltlichen Praxis überlegt,

welche - deutschen - gesetzlichen Bestimmungen muß ein Unternehmen berücksichtigen, das in Deutschland ein "Geschäft im Internet" eröffnen möchte?

Gliederung

1. Domain-Name
2. Einrichtung des Online-Geschäfts
3. Fernabsatz : Verhältnis zum Kunden

Die nachfolgende Ausführung wird zeigen, daß das Internet weder ein "rechtsfreier Raum" ist, noch ausschließlich durch "neue Gesetze" reguliert wird, sondern daß das althergebrachte Recht aus der Zeit vor dem Internet auch für dieses neue Medium gilt und zusätzlich neue spezifische Regelungen geschaffen wurden.

Im ersten Teil gehe ich ein auf den Streit über Domain-Namen, im zweiten Teil auf die Einrichtung des Online-Geschäfts (Verträge sowie Verantwortlichkeit für Inhalte) und im dritten Teil auf den Fernabsatz im Verhältnis zum Kunden. In diesem letzten Teil werde ich die elektronische Signatur, das "Formvorschriftengesetz" (Änderung des BGB und der ZPO), das Fernabsatzgesetz, die Einbeziehung von Allgemeinen Geschäftsbedingungen (AGB) einschließlich einer Haftungsbegrenzung sowie Fragen des Datenschutzes behandeln.

Die Ausführung befaßt sich nur mit "Inhalten im Internet". Auf Gesetzesentwürfe noch im Stadium des Gesetzgebungsverfahrens oder auf Fragen zur Rechtsgrundlage des Netzes ("Carrier-Dienste", Deregulierung des Telekommunikationsmarktes) insbesondere das Telekommunikationsgesetz (TKG) werde ich mangels Zeit nicht eingehen.

1 Domain-Name

Stellen Sie sich vor, Sie wollen als Unternehmer ein Online-Geschäft eröffnen oder Ihre Aktivitäten vom Ausland über das Internet auf Deutschland erstrecken, allerdings wäre Ihr Wunschname einer Domain (zum Beispiel: www.calissons.de) bereits von jemand anderem registriert. Was tun? Sie können natürlich Ihren Wunschnamen mit einem Zusatz versehen (z.B.: www.calissons-IhrName.de). Vielleicht wollen Sie aber keinen Zusatz, weil eine solche Domain schlechter zu merken ist oder Sie einen Angriff des Domaininhabers Ihrer Wunschdomain auf die ersatzweise benutzte Domain mit Zusatz befürchten.

Für die Lösung der Domainstreitigkeiten im Internet ist teilweise ein neues Recht gefordert worden. In der Praxis fanden sich befriedigende Lösungen durch die Anwendung des bisherigen Rechts auf das neue Problem der Domainstreitigkeiten im Internet.

1.1 Ansprüche bei Domain-Streitigkeiten

Das Unternehmen kann gegenüber dem Domaininhaber Rechte hinsichtlich der Domain beanspruchen aus dem Markenrecht (Kennzeichen und Marken) nach §§ 5,15 oder 4,14 Markengesetz (MarkenG), dem Wettbewerbsrecht nach §§ 1,13 Gesetz gegen unlauteren

Wettbewerb (UWG) und/oder dem Namensrecht nach § 12 BGB sowie einer sittenwidrigen Schädigung nach § 826 BGB.

Alle Ansprüche sind grundsätzlich auf Unterlassung der Benutzung bzw. Löschung der Domain gerichtet. Während die Ansprüche aus dem Markenrecht und dem Wettbewerbsrecht nur "im geschäftlichen Verkehr" möglich sind, können Ansprüche aus sittenwidriger Schädigung und Namensrecht auch gegenüber einem Privaten geltend gemacht werden.

Nur ausnahmsweise kann die Übertragung einer Domain als Folgenbeseitigung (nach §§ 823 Abs. 2, 1004 BGB) verlangt werden, wenn kein anderer als der Anspruchsteller einen Anspruch auf diesen Domain-Namen haben kann (www.audi-lamborghini.net, KR 2000,613). Dies betrifft vor allem bekannte Marken (ab 30-40 % Bekanntheit im "relevanten Verkehrskreis", www.joop.de, LG Hamburg, MMR 2000,620 ff), die Verwässerungsschutz auch gegen die Betätigung Fremder in nicht geschützten Klassen genießen.

Auf die Probleme bei generischen Domain-Namen (Gattungsbezeichnungen) soll nur hingewiesen werden. In der bislang noch nicht veröffentlichten Entscheidung "www.mitwohzentrale.de" hat der BGH nach seiner Presseerklärung die Verwendung generischer Begriffe als Domain-Namen grundsätzlich erlaubt, jedoch kann ihre konkrete Verwendung gegen das Wettbewerbsrecht verstoßen. Wenn durch die Gestaltung der Webseite der Eindruck der Geschlossenheit entsteht, daß es nur diese(n) Anbieter gibt, dann führt dies zu einer unzulässigen Kanalisierung von Kundenströmen. Im übrigen wäre die zusätzliche Registrierung von verschiedenen Schreibweisen des generischen Begriffs (z.B. www.mitwohn-zentrale.de, www.mitwohzentralen.de) eine unzulässige Behinderung der Mitbewerber.

1.2 Anspruchsteller im Ausland

Ein Sonderproblem besteht, wenn der Anspruchsteller bislang nur im Ausland, jedoch noch nicht in Deutschland geschäftlich tätig ist. Vielleicht hat ein potentieller Domain-Grabber aus einer Presseerklärung entnommen, daß ein im Ausland tätiges Unternehmen seine Aktivitäten nach Deutschland erstrecken möchte und reserviert vor dem Unternehmen die DE-Domain.

Alle Ansprüche nach deutschem Recht (Markenrecht, Wettbewerbsrecht, Namensrecht und sittenwidrige Schädigung) bestehen grundsätzlich nur, wenn der Anspruchsteller innerhalb Deutschlands bereits aktiv ist. Hier muß je nach den Umständen des Einzelfalls nach einer Lösung gesucht werden. Möglicherweise kann bei der Markenmeldung in Deutschland innerhalb von sechs Monaten an die Priorität der Anmeldung einer Markenmeldung in einem anderen Vertragsstaat des Pariser Verbandsübereinkommens (PVÜ 1883) angeknüpft werden. Wenn der Anspruchsteller über eine ältere Gemeinschaftsmarke verfügt, braucht er ebenfalls nicht in Deutschland aktiv sein, um die Ansprüche aus der Gemeinschaftsmarke geltend zu machen.

Im übrigen kann der Anspruchsteller nach Deutschland kommen und Aktivitäten entfalten, um anschließend gegen den Domaininhaber vorzugehen. In diesem Fall kommt es darauf an, wer die "besseren Rechte" begründet hat. Sollte der Domain-Grabber - wie häufig - nur die Domain registriert haben, ohne darunter eine Aktivität zu entfalten, so begründet die Registrierung alleine noch keine Rechte des Domaininhabers.

1.3 Durchsetzung der Ansprüche

Die Durchsetzung der Ansprüche bei einem Domain-Grabber in Deutschland erfolgt üblicherweise mittels einer Abmahnung, einstweiligen Verfügung oder Klage in der Hauptsache und eines sog. Dispute-Antrages. Bei einem Domain-Grabber im Ausland kann man auch ein ICANN-Schiedsverfahren in Betracht ziehen.

(a) Abmahnung, einstweilige Verfügung und Dispute-Antrag

Die Abmahnung ist ein einfaches Schreiben, das den konkreten Sachverhalt, den Wettbewerbsvorwurf sowie das Begehren nach der Abgabe einer Unterlassungs- und Verpflichtungserklärung innerhalb einer bestimmten Frist enthält. Wird innerhalb der Frist keine ausreichende Erklärung abgegeben, kann man Antrag auf Erlaß einer einstweiligen Verfügung stellen. Für die Dringlichkeit als Voraussetzung des Erlasses einer einstweiligen Verfügung darf – je nach Gericht und Einzelfall – die Kenntnis des Wettbewerbsverstoßes teilweise nicht länger als 4 bis 6 Wochen zurückliegen. Verneint das Gericht die Dringlichkeit, kann man Klage in der Hauptsache erheben.

Gleichzeitig mit der Abmahnung sollte man bei der DENIC, der Registrierungsstelle für DE-Domains, einen Dispute-Antrag (ehemals WAIT-Antrag) stellen, durch den verhindert werden soll, daß der jetzige Domaininhaber die Domain auf einen Dritten überträgt. Willigt der Domain-Grabber in die Löschung der Domain ein, wird der Dispute-Antragsteller automatisch als neuer Domain-Inhaber eingetragen.

(b) ICANN-Schiedsverfahren

Für internationale Domains (.com, .net und .org) kommt auch ein ICANN-Schiedsverfahren in Betracht. Die ICANN (www.icann.org : Internet Corporation for Assigned Names and Numbers) ist ein Unternehmen, das von der US-Regierung mit der Verwaltung des Internet beauftragt wurde. Das ICANN-Schiedsverfahren ist ein weltweit einheitlich schriftliches Verfahren, das von akkreditierten Streitbeilegungszentren, darunter die WIPO (www.wipo.org), durchgeführt wird. Das Verfahren ist nur möglich bei der Geltendmachung von Markenrechten, nicht jedoch von Namensrechten. Die Erstreckung des Verfahrens auf berühmte Namen wird derzeit diskutiert. Rechtsgrundlage zwischen den Beteiligten sind die Allgemeinen Geschäftsbedingungen bei der Registrierung (bzw. Verlängerung der Registrierung) der Domain. Das Verfahren dauert etwa 2-3 Monate und bietet sich an, wenn der Domaininhaber sich im Ausland befindet oder über keine zustellungsfähige Adresse verfügt. Der Vollzug der Entscheidung erfolgt ohne staatliche Anerkennung. Allerdings bei einem Verfahrensgegner in Deutschland ist das einstweilige Verfügungsverfahren die schnellere Lösung.

2 Einrichtung des Online-Geschäfts

Für die Einrichtung eines Online-Geschäfts werden häufig verschiedene Verträge abgeschlossen. Interessant für einige Unternehmer sind auch Haftungsfragen für die angebotenen Inhalte und sogenannte "Links" (Verweise auf andere Webseiten).

2.1 Verträge für die Einrichtung des Online-Geschäfts

In Betracht kommen Webhostingverträge über die Speicherplatz auf einem Server mit Internetanbindung, Webdesignverträge über die Erstellung der Webseiten, sog. Contentverträge über die Einbindung von Inhalten (z.B. Nachrichten), Kooperationsverträge über die Auslieferung von Waren, Verträge über die Abwicklung des Zahlungsverkehrs (elektronische Einzugsermächtigung, Kreditkarten, Inkasso), Softwarelizenzverträge für spezielle Aufgaben und Verträge über

Auftragsdatenverarbeitung. Hier handelt es sich in der Regel um vom stärkeren Vertragspartner vorgegebene Standardverträge, auf die das "Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen" (AGB-Gesetz) Anwendung findet, sofern deutsches Recht gilt.

2.2 Haftung für Inhalte

Bei Inhalten kann sich die Frage der Haftung stellen. Die zentrale Haftungsnorm für Inhalte von Webseiten ist § 5 Teledienstegesetz (TDG) oder § 5 Mediendienste-Staatsvertrag (MDStV). Es handelt sich dabei um eine Haftungsprivilegierung für Diensteanbieter (Provider). Das TDG ist ein Bundesgesetz; der MDStV ist ein Staatsvertrag zwischen den Bundesländern, welche die Kompetenz für die Regelung des Rundfunks sowie die Kulturhoheit innehaben. In Abgrenzung von beiden Regelungsbereichen findet das TDG bei individueller Kommunikation und der MDStV bei einer "rundfunkähnlichen" Darbietung an die Allgemeinheit zur öffentlichen Meinungsbildung statt. Indiz für die Anwendung des MDStV ist eine redaktionelle Bearbeitung von Beiträgen. Eine Abgrenzung der beiden Regelungsbereiche sowie die akademische Diskussion über die Verfassungswidrigkeit des MDStV (mangels ausreichender Kompetenz der Bundesländer) kann in der Praxis dahin stehen, da die Regelung des § 5 TDG / MDStV in den Absätzen 1 bis 3 identisch ist. Sollte danach eine Haftung bestehen, richtet sich diese nach den allgemeinen Gesetzen, z.B.: Wettbewerbsrecht (UWG, Markengesetz) und Strafgesetzbuch.

(a) § 5 Abs. 1 - 3 TDG / MDStV

- Für "eigene Inhalte" sind Diensteanbieter gemäß § 5 Abs. 1 immer verantwortlich. Hierzu gehören auch fremde Inhalte, die sich der Diensteanbieter zu eigen gemacht hat.
- Für "fremde Inhalte" sind Diensteanbieter gemäß § 5 Abs. 2 nur dann verantwortlich, wenn (a) sie von diesen positive Kenntnis haben und (b) es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Die positive Kenntnis kann durch eine Email, Telefonat oder Fax an einen Verantwortlichen des Unternehmens hergestellt werden.
- Nicht verantwortlich sind Diensteanbieter gemäß § 5 Abs. 3 für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln (sog. "Zugangsprovider", z.B.: AOL, T-Online, Germany.net).

Die deutsche Regelung im Informations- und Kommunikationsdienstegesetz (IuKDG 1997) war die erste dieser Art überhaupt und richtungsweisend für die spätere sog. E-Commerce Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

(b) Sonderproblem : Haftung für sog. Links

Ein derzeit in der Rechtsprechung virulentes Thema sind sog. "Links". Dabei handelt es sich um Verweise in einer Webseite, die den Besucher bei deren Anklicken zu einer anderen Webseite desselben Anbieters oder eines anderen Anbieters führen. Hier stellt sich die Frage, ob derjenige, der den Link auf seiner eigenen Webseite setzt, auch für Inhalte auf der verwiesenen Webseite eines anderen Anbieters verantwortlich ist (z.B. Bau einer Bombe, extremistische Äußerungen). Teilweise wurde in der Rechtsprechung und

Literatur vertreten, daß es sich bei Links um eine Verschaffung des Zugangs zu fremden Inhalten handelt, wofür der Linksetzer nach § 5 Abs. 3 nicht verantwortlich ist. Allerdings in jüngster Zeit setzt sich zu recht die Meinung durch, daß es sich bei Links um willentliche Handlungen des Linksetzers handelt, für die dieser je nach Ausgestaltung des Links nach § 5 Abs. 1 oder Abs. 2 verantwortlich ist.

3 Fernabsatz : Verhältnis zum Kunden

Im Verhältnis zum Kunden stellt sich die Frage der Identifizierung des Vertragspartners, die Bedeutung von speziellen Formvorschriften für den elektronischen Handel, die vom Unternehmer zu gebenden Informationen für den Fernabsatz, zur Haftungsbegrenzung und zum Datenschutz.

3.1 Die elektronische Signatur

Elektronische Signaturen spielen derzeit im E-Commerce noch keine Rolle. Die Technik wird bisher fast nur von einigen großen Unternehmen und einigen Behörden zur internen Kommunikation eingesetzt. Für Verbraucher ergibt die Anschaffung der technischen Komponenten mangels Kommunikationspartner bisher nicht sehr viel Sinn. Registrierung und Anschaffung einer Signaturkarte kosten etwa derzeit 150 DM pro Jahr. Auch ist das Verfahren recht kompliziert und das rechtliche Regelwerk neu und für "Nichttechniker" unverständlich.

Gleichwohl möchte ich die rechtlichen Regelungen in bezug auf den elektronischen Geschäftsverkehr als Ausblick darstellen. Das neue "Gesetz über Rahmenbedingungen für elektronische Signaturen" (Signaturgesetz - SigG) trat am 22.5.2001 in Kraft (BGBl. 2001 I 876 ff.) und ersetzt das Signaturgesetz von 1997. Die Neufassung setzte die Richtlinie 99/93/EG für elektronische Signaturen in nationales Recht um. Das Gesetz regelt nicht elektronische Signaturen im Detail, deren Anwendung und Rechtsfolgen, sondern die Sicherungsinfrastruktur für Signaturverfahren. Die wesentliche Neuerung besteht in der Einführung einer Haftungsregelung für Zertifizierungsstellen und einer freiwilligen Akkreditierung derselben. Bisher war eine Genehmigung und die damit verbundene behördliche Vorabkontrolle für Zertifizierungsstellen obligatorisch.

Das neue Gesetz kennt vier Kategorien der elektronischen Signatur: (a) die einfache "elektronische Signatur", (b) die "fortgeschrittene elektronische Signatur", (c) die "qualifizierte elektronische Signatur" sowie (d) die "qualifizierte elektronische Signatur mit Anbieter-Akkreditierung" oder kurz die "akkreditierte Signatur".

- Die einfache "elektronischen Signatur" im Sinne von § 2 Nr. 1 SigG dient nur der Authentifizierung beispielsweise mittels eingescannter Unterschrift und muß nicht fälschungssicher sein.
- Die "fortgeschrittene elektronische Signatur" im Sinne von § 2 Nr. 2 SigG muß (a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein, (b) seine Identifizierung ermöglichen, (c) mit Mitteln erzeugt sein, die seiner alleinigen Kontrolle unterliegen und (d) mit den Daten so verknüpft sein, daß eine nachträgliche Veränderung der Daten erkannt werden kann. Diese Anforderungen erfüllt zum Beispiel das frei erhältliche bekannte Verschlüsselungs- und Signaturprogramm "Pretty Good Privacy (PGP)".
- Die "qualifizierte elektronische Signatur" im Sinne von § 2 Nr. 3 SigG setzt die Merkmale der fortgeschrittenen Signatur voraus. Zusätzlich muß sie auf einem zum

Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit (schreckliches Wort) erzeugt wurde. Diese Signaturerstellungseinheit ist - wenn sie "sicher" sein soll - ein Chip auf einer Smartcard, den der Benutzer erhält. Dabei wird der zum signieren notwendige geheime Schlüssel im Chip generiert und auch die Signatur wird innerhalb dieses Chips verschlüsselt, so daß der geheime Schlüssel diese Einheit auf der Karte nie verläßt. Bei der qualifizierten elektronischen Signatur wurde die Signaturerstellungseinheit behördlich vorab überprüft, um sicherzustellen, daß sie nach dem Stand der Technik auch wirklich nicht ausgelesen werden kann und als "sicher" einzustufen ist. Eine Signaturerstellungseinheit darf nur für natürliche Personen ausgestellt werden; nicht für Behörden oder juristische Personen.

- Die 'akkreditierte Signatur' wird gemäß § 15 Abs. 1 Satz 4 SigG legaldefiniert, umständlich heißt es dort "qualifizierte Signatur mit Anbieter-Akkreditierung". Der Zertifizierungsanbieter dieses Verfahrens wird im Wege einer Akkreditierung hinsichtlich seiner technischen und administrativen Sicherheit behördlich vorab überprüft. Deshalb ist dieser höchsten Sicherheitsstufe auch im Prozeß der höchste Beweiswert einzuräumen.

Die Rechtsfolgen einer elektronischen Signatur ergeben sich aus den Änderungen des BGB, der ZPO sowie anderen Rechtsvorschriften.

3.2 "Formvorschriftengesetz"

Gleichwohl hat der Gesetzgeber mit mehreren Gesetzen bzw. Gesetzesänderungen ein Regelwerk geschaffen, um das deutsche Privatrecht den Entwicklungen des modernen Geschäftsverkehrs anzupassen. Kern dieses Regelwerkes ist das "Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr", das am 19.7.2001 in Kraft trat (BGBl. 2001 I 1542 ff.). Es handelt sich dabei um ein Artikelgesetz, das eine Reihe von gesetzlichen Bestimmungen in verschiedenen Gesetzen (BGB, ZPO, etc.) ändert.

(a) Änderungen im Bürgerlichen Gesetzbuch (BGB)

Im BGB gilt der Grundsatz der Formfreiheit, durchbrochen von einzelnen zwingen Formtatbeständen, für die grundsätzlich auf das Medium Papier fixierte Formen vorgesehen sind (Schriftform, notarielle Beurkundung und öffentliche Beglaubigung). Durch das Artikelgesetz sind zwei neue Formvorschriften eingeführt worden.

Gemäß § 126b BGB wurde die "Textform" eingeführt, die für bestimmte automatisch erstellte Erklärungen wie Mieterhöhungen und anderes gilt (§ 558a BGB, § 4 Abs. 1 Satz 3 Verbraucherkreditgesetz, § 13 Aktiengesetz, etc.). Ist durch Gesetz Textform vorgeschrieben, so muß die Erklärung in einer "zur dauerhaften Wiedergabe in Schriftzeichen geeigneten Weise abgegeben", der Name des Erklärenden muß genannt und der Abschluß der Erklärung durch Nachbildung der Namensunterschrift oder in anderer Form erkennbar gemacht werden. Die Textform kann in Papierform oder in digitaler Form erfolgen, so daß ein bloßer Papiausdruck oder gar eine ungesicherte E-mail ausreicht. Vorkehrungen für die Fälschungssicherheit sind nicht erforderlich.

Gemäß § 126a BGB wird die "elektronische Form" eingeführt. Soll die Schriftform durch die elektronische Form ersetzt werden, muß der Aussteller seiner Erklärung seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen. Diese elektronische Signatur ersetzt die

eigenhändige Unterschrift. Mangels ausreichender Warnfunktion und Gewöhnung an dieses Medium ist die elektronische Form in kritischen Bereich ausgeschlossen, so zum Beispiel bei der Bürgschaft und dem Schuldanerkenntnis. Während bei der Schriftform beide Parteien dasselbe Dokument unterzeichnen müssen, genügt es bei der elektronischen Form, wenn beide Parteien jeweils ein gleichlautendes Dokument elektronisch signieren.

Auch wenn nach § 126 BGB grundsätzlich die schriftliche Form durch die elektronische Form ersetzt werden kann, soll nach den Gesetzesmaterialien (BT-Drucks. 14/4987, S. 15 und 14/5561, S. 19) dies nur zulässig sein, wenn die Beteiligten ausdrücklich oder durch schlüssiges Handeln ihre Anwendung billigen und deshalb mit dem Zugang einer elektronischen Willenserklärung rechnen müssen.

(b) Änderungen in der Zivilprozeßordnung (ZPO)

Die Änderungen der ZPO dient der Einführung des elektronischen Rechtsverkehrs zwischen den Gerichten und den Verfahrensbeteiligten. Gemäß § 130a Abs. 1 ZPO wird die Möglichkeit eröffnet, daß Parteien, aber auch die am Verfahren beteiligten Dritte (z.B. Zeugen und Sachverständige) ihre Schriftsätze und Erklärungen als elektronisches Dokument einreichen können. Die Teilnahme am elektronischen Rechtsverkehr erfordert allerdings noch Vorbereitungen bei allen Beteiligten - den Gerichten, den Anwaltskanzleien und den Behörden. Aus diesem Grunde bestimmt § 130a Abs. 2 ZPO, daß die Bundesregierung und die Länderregierungen für ihren Bereich durch Rechtsverordnung nicht nur den Zeitpunkt bestimmen, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sondern auch die für die Bearbeitung der Dokumente geeignete Form.

Klargestellt wird auch, daß ein elektronisches Dokument im Beweisrecht nach § 371 Satz 2 ZPO keine Urkunde darstellt. Es gelten insoweit die Regeln des Augenscheinsbeweises. Mit § 292a ZPO wird ein gesetzlicher Anscheinsbeweis zugunsten des Empfängers eines elektronischen Dokumentes angeordnet. Danach kann der Anschein der Echtheit einer in elektronischer Form (§ 126a BGB = mit qualifizierter elektronischer Signatur) vorliegenden Willenserklärung nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, daß die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben wurde. Die Voraussetzungen dieser Vorschrift sind allerdings noch unklar. In der Literatur (Roßnagel, NJW 2001,1817,1826) wird angenommen, daß die Beweisvermutung des § 292a ZPO nur für eine akkreditierte Signatur in Anspruch genommen werden kann, da nur für diese nach § 15 Abs. 1 Satz 4 SigG eine gesetzliche Vermutung der technisch-organisatorischen Sicherheit bestehe.

3.3 Fernabsatzgesetz (FAG)

Das Fernabsatzgesetz will "Verbraucher" vor irreführenden und aggressiven Verkaufsmethoden im Fernabsatz schützen. Die Regelungen des FAG finden nur beim Fernabsatz im Verhältnis zum Endverbraucher (B2C) statt, nicht jedoch im Verhältnis des Handels der Unternehmen untereinander (B2B). Das FAG legt dem Unternehmen Informationspflichten auf und gewährt dem Verbraucher ein Widerrufs- und Rückgaberecht.

Das FAG gilt nach § 1 Abs. 1 (Voraussetzungen kumulativ)

- für Verträge über die Lieferung von Waren oder über die Erbringung von Dienstleistungen, die zwischen einem Unternehmer und einem Verbraucher

- unter ausschließlicher Verwendung von Fernkommunikationsmittel (Abs. 2 : insbesondere Briefe, Kataloge, Telefon, Telefax, E-Mail sowie Rundfunk, Tele- und Mediendienste) abgeschlossen werden,
- es sei denn, daß der Vertragsschluß nicht im Rahmen eines für den Fernabsatz organisierten Vertriebs- oder Dienstleistungssystems erfolgt (Fernabsatzverträge).

Bereichsausnahmen sind nach Abs. 3 zum Beispiel, obwohl ein Fernabsatzvertrag vorliegt, Finanzgeschäfte, Immobiliengeschäfte, Verträge über die Lieferung von Lebensmittel des täglichen Bedarfs (Pizzaservice). Für einige dieser Bereichsausnahmen soll es spezielle Regelungen in Umsetzung von EG-Richtlinien geben, zum Beispiel Richtlinie für Fernabsatz von Finanzdienstleistungen an Verbraucher.

Der Unternehmer hat bestimmte Informationspflichten zu erfüllen. Einige Informationen hat er vor Vertragsabschluß "in beliebiger Form" (z.B. Webseite), einige Informationen hat er spätestens bis zur Vertragserfüllung "in dauerhafte Form" zu geben.

- Vor Abschluß des Vertrages : Identität und Anschrift des Unternehmers; das Bestehen des Widerrufs- und Rückgaberechts; wesentliche Merkmale der Waren und Dienstleistungen; Preis einschließlich aller Steuern und sonstiger Preisbestandteile; Einzelheiten der Zahlung und Lieferung, etc.
- Spätestens bis zur vollständigen Vertragserfüllung hat das Unternehmen die oben genannten Angaben auf einem "dauerhaften Datenträger" zur Verfügung zu stellen und zusätzlich "in hervorgehobener Form" zu informieren über : Widerrufs- und Rückgaberecht, Anschrift für Beanstandungen, ladungsfähige Anschrift mit Namen eines Vertretungsberechtigten, Informationen über Kundendienst, Gewährleistungs- und Garantiebedingungen und Kündigungsbedingungen, bei Verträgen von mehr als 12 Monaten.

Folgen des Verstoßes gegen die Informationspflichten sind (a) die Gefahr der wettbewerbsrechtlichen Abmahnung durch Mitbewerber ("Vorsprung durch Rechtsbruch") und Verbraucherschutzverbände, (b) Verlängerung der Widerrufsrechts, längstens jedoch bis 4 Monate, (c) Reduzierung der Haftung des Verbrauchers auf Vorsatz und grobe Fahrlässigkeit.

Der Widerruf ist innerhalb von zwei Wochen auszuüben; es genügt die Absendung des Widerrufs oder die Rücksendung der Ware. Im Falle des Widerrufs hat der Unternehmer die Kosten und das Risiko der Rücksendung zu tragen. Eine Ausnahme besteht bei Bestellungen bis Euro 40, bei denen dürfen durch Allgemeine Geschäftsbedingungen (AGB) dem Verbraucher die Kosten der Rücksendung auferlegt werden. Das Widerrufsrecht besteht nicht bei Verträgen über zum Beispiel die Lieferung von speziell für den Kunden angefertigten Waren, verderbliche Waren, Zeitungen und Zeitschriften sowie Software, Audio- und Videoaufzeichnungen, sofern gelieferte Datenträger vom Verbraucher entsiegelt wurden.

3.4 Allgemeine Geschäftsbedingungen (AGB): Haftungsbegrenzungen

Häufig wird von Unternehmern nach Haftungsbegrenzungen für Schäden nachgefragt, die durch den Besuch der Webseite verursacht werden könnten. Als Beispiel wird gerne ein Szenario genannt, bei dem der Server des Unternehmens im Internet über den Abruf der Webseiten Viren verbreitet und die Systeme der Besucher beschädigt. Häufig wird dabei auf Webseiten anderer Unternehmen verwiesen, die auf ihrer Homepage einen Link "Rechtliche Hinweise" mit einer Haftungsbegrenzung enthalten.

Diese Unsitte auf deutschen Webseiten entstammt Vorbildern von Unternehmen in den USA. Im Common Law gibt es die Rechtstradition der sogenannten "einseitigen Verträge" ("unilateral contracts"), bei denen solche Hinweise rechtliche Beachtung finden können. Auch das deutsche Recht kennt den einseitigen Vertrag in Form der Auslobung nach §§ 657 - 661a BGB, die hier keine Rolle spielt.

Im deutschen Recht wäre eine Haftungsbegrenzung in eingeschränkter Form in Allgemeinen Geschäftsbedingungen (AGB) möglich. Hierzu bedarf es einer vertraglichen Beziehung zwischen den Parteien, in welche die AGB einbezogen wurden. Allerdings kommt beim Besuch einer Webseite regelmäßig keine vertragliche Beziehung zwischen dem Betreiber der Webseite und dem Besucher zustande. Die "Rechtlichen Hinweise" auf deutschen Webseiten sind deshalb regelmäßig überflüssig und unbeachtlich.

Das Zustandekommen einer vertragliche Beziehung kann jedoch durch die Gestaltung der Webseite erreicht werden, indem ein "Vertrag über die Nutzung der Webseite" geschlossen wird. Der Betreiber der Webseite bietet dem Besucher eine Webseite an, auf der die Allgemeinen Geschäftsbedingungen enthalten sind und die der Besucher nach unten skrollen muß und einen Button sinngemäß "Ich habe gelesen, verstanden und akzeptiere" drücken muß, bevor er in einen geschützten Informationsbereich gelangt. Häufig werden am Ende dieser Seite im Rahmen einer Registrierung auch noch persönliche Daten erfragt, wie zum Beispiel Name, Email-Adresse und sonstige für den Betreiber der Webseite interessante Angaben. Auf diese Weise kann eine vertragliche Beziehung unter Einbeziehung von AGB geschlossen werden. Die AGB einschließlich der Haftungsbegrenzung unterliegen dann der Inhaltskontrolle des ABG-Gesetzes. Sollte eine Bestimmung gegen das AGB-Gesetz verstoßen, dann ist sie unwirksam. Gerade Haftungsbegrenzungen sind in deutschen AGB nur eingeschränkt möglich.

Das Haftungsrisiko des Betreibers einer Webseite, die nur Informationen über das Unternehmen sowie die angebotenen Waren und Dienstleistungen enthält, das er mit AGBs begrenzen könnte, ist äußerst gering. Für Schäden, die aus der Benutzung von allgemeinen Informationen oder der Befolgung von unverbindlichen Ratschlägen entstehen, wird im deutschen Recht nach § 675 Abs. 2 BGB nicht gehaftet. Selbst das Horrorszenario der Verbreitung von Viren verliert in der Rechtsprechung seine Schrecken: Zum einen dürfte es für die Haftung aus unerlaubter Handlung nach § 823 BGB bei Einhaltung des Standes der Technik am Verschulden des Betreibers der Webseite fehlen, wenn auf dem Server ein aktuelles Virenschutzprogramm lief. Zum anderen kann die Haftung des Betreibers der Webseite angesichts eines überwiegenden Mitverschuldens des Besuchers nach § 254 BGB entfallen, wenn dieser kein aktuelles Virenschutzprogramm oder bei Unternehmen kein Datensicherungssystem (back-up) benutzte.

Gefährlicher für den Betreiber einer Webseite ist ein Verstoß gegen das allgemeine Wettbewerbsrecht (Aussage: "Wir sind die Besten"), vor dessen Ahndung durch Mitbewerber (Abmahnung, einstweilige Verfügung) er sich durch AGB nicht frei zeichnen kann. Dies stellt aber auch keine Besonderheit der Online-Geschäfte dar.

3.5 Datenschutz

Die Betreiber von Webseiten sammeln regelmäßig Informationen über die Besucher ihrer Seite, sei es in anonymer Form oder durch Abfragen von persönlichen Informationen (z.B. Name, Adresse, Email). Bei der Erhebung und Verwendung von Daten der Besucher stellen sich Fragen der Zulässigkeit nach dem Datenschutzrecht.

(a) Erhebung und Nutzung anonymer Daten (sog. Logfiles)

Die Erhebung und Nutzung von anonymen Informationen über den Besuch der Webseite erfolgt mittels sog. Logfiles, die auf jedem Server standardmäßig erzeugt werden und jeden Zugriff auf eine Webseite protokollieren. Diese Logfiles enthalten die jeweils aufgerufene Seite, die Uhrzeit und die "IP-Nummer" des Besuchers. Bei der IP-Nummer handelt es sich um ein "Nummernschild" des Internet-Sufers, das dieser durch seinen Zugangsvermittler zum Internet (z.B. AOL, T-Online, Germany.net) automatisch erhält. Durch die Auswertung der Logfiles kann der Betreiber einer Webseite erkennen, welche seiner Seiten öfter aufgerufen werden und damit für die Besucher interessanter sind als jene Seiten, die seltener aufgerufen werden. Diese Erkenntnis kann er dann beim Ausbau seiner Webseiten, seines Angebots an Waren und Dienstleistungen sowie beim Marketing berücksichtigen. Da die Datenverarbeitung hier in anonymer Form ohne Zuordnung der Daten zur Person des Besuchers erfolgt, ist sie datenschutzrechtlich unbedenklich.

(b) Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Häufig besteht aber auch ein Bedürfnis, personenbezogene Daten (z.B. Name, Adresse, Email) vom Besucher abzufragen, um zum Beispiel mit ihm direkt einen Vertrag abzuschließen oder weitere Informationen oder ein Vertragsangebot - per Email oder Post - zukommen zu lassen. Die Erhebung, Verarbeitung und Nutzung von Daten, die eine Zuordnung zu einer bestimmten Person erlauben (personenbezogene Daten), ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) sowie § 3 Teledienstschutzgesetz (TDDSG) nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlauben oder der Betroffene eingewilligt hat.

§ 28 Abs. 1 Nr. 1 BDSG erlaubt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bei Abschluß eines Vertrages oder bei einer Vertragsanbahnung im Rahmen der Zweckbestimmung der Datenerhebung. Wer zum Beispiel als Betreiber eines Marktplatzes für den Handel mit Energien (Strom, Wasser, Erdöl) Daten von Kontaktpersonen seiner Online-Geschäftspartner abfragt, darf diesen - seiner Meinung nach finanzkräftigen - Personen nicht nachträglich per Email Werbung über Immobilieninvestments an der Côte d'Azur schicken.

Wenn der Abschluß eines Vertrags zwischen dem Betreiber der Webseite und dem Besucher nicht beabsichtigt ist, zum Beispiel bei der Datenerhebung um diese an Dritte für allgemeine Werbezwecke zur Verfügung zu stellen (CD-ROM "57 Millionen Email-Adressen für 250 US Dollar"), kommt eine datenschutzrechtliche Einwilligung in Betracht. Die Einwilligung nach BDSG hat in der Regel in schriftlicher Papierform zu erfolgen. Allerdings gibt es für die Online-Kommunikation die Möglichkeit der "elektronischen Einwilligung" nach Teledienstschutzgesetz (TDDSG). Dazu ist der Nutzer vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Der Inhalt des Hinweises muß für den Nutzer jederzeit online abrufbar sein.

Eine elektronische Einwilligung des Nutzers ist gemäß § 3 Abs. 7 TDDSG nur wirksam, wenn der Betreiber des Online-Geschäfts sicherstellt, daß (1.) die Einwilligung nur durch eine eindeutige und bewußte Handlung des Nutzers erfolgen kann (Opt-in Klausel), (2.) die Einwilligung nach Abgabe nicht unerkennbar verändert werden kann, (3.) ihr Urheber erkannt werden kann, (4.) die Einwilligung protokolliert wird und (5.) der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann. Die erforderlichen Informationen (Nutzung und Widerruf) sollten auf derselben Seite in unmittelbarem

Zusammenhang mit dem einem eigenen "acceptance"-Button für die datenschutzrechtliche Nutzung stehen.

(c) Verantwortliche Stelle und Server im EU/EWR-Ausland

Bei international operierenden Unternehmen stellt sich häufig die Frage, ob deutsches Datenschutzrecht überhaupt anwendbar ist. Mit der Umsetzung der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ("Datenschutzrichtlinie") wurden einheitliche Regeln für die Frage der Anwendung des nationalen Datenschutzrechts und für den Datentransfer innerhalb und nach außerhalb des Europäischen Wirtschaftsraums (EWR) geschaffen. Die Umsetzung erfolgte in Deutschland im BDSG.

Beispiel: Welches Datenschutzrecht findet Anwendung, wenn ein US-Konzern innerhalb der EG eine Tochtergesellschaft mit Server in London gründet, die mittels des Servers Geschäfte in ganz Europa tätigt?

Innerhalb der Europäischen Gemeinschaft (EG) findet grundsätzlich das Datenschutzrecht des Mitgliedstaates Anwendung, in dem die verantwortliche Stelle ihren Sitz hat. In unserem Fall würde für das Unternehmen in London englisches Datenschutzrecht gelten hinsichtlich der Datenerhebung in allen Mitgliedstaaten der EG. Nach § 1 Abs. 5 Satz 5 BDSG müssen die deutschen Aufsichtsbehörden für den Vollzug des BDSG (Bezirksregierungen) die Einhaltung des englischen Datenschutzrechts überwachen. Dies führt bislang dazu, daß die deutschen Aufsichtsbehörden das Datenschutzrecht aller Mitgliedstaaten der EG kennen müssen. Erstrebenswert wäre hier wohl die Einrichtung zentraler bundesweiter Zuständigkeiten von Aufsichtsbehörde durch Rechtsverordnung des Bundesrates für Unternehmen aus einem Mitgliedstaat.

Hier stellt sich die Frage, ob unser Unternehmen mit Server in London überhaupt personenbezogene Daten in Deutschland erhebt. Findet die Datenerhebung statt (a) zu hause beim Besucher der Webseite, wenn dieser seine Daten in die ihm angebotene Maske eintippt oder (b) auf dem Server des Unternehmens in London? Die Erhebung von Daten findet dort statt, wo die Möglichkeit der Kenntnisnahme der Daten durch das Unternehmen besteht (sog. Briefkastenregel). Aus diesem Grunde findet in unserem Fall die Datenerhebung auf dem Server in London statt; im Ergebnis findet englisches Datenschutzrecht Anwendung ohne daß die deutschen Aufsichtsbehörden involviert sind.

(d) Datentransfer innerhalb des EWR oder in einen Drittstaat : z.B. USA

Die Regelung des Datentransfers ist äußerst kompliziert. Grundsätzlich ist ein "Datentransfer ins Ausland" nur zulässig, wenn die Voraussetzungen für einen Datentransfer vorliegen (z.B. § 11 BDSG Auftragsdatenverarbeitung oder § 28 Abs. 1 Ziffer 1 BDSG im Rahmen der Zweckbestimmung des Vertrages) und der Transfer in ein Zielland mit angemessenem Schutzniveau erfolgt. Nach § 4b Abs. 1 BDSG wird innerhalb des EWR im Anwendungsbereich des EG-Vertrages (Warenfreiheit, Dienstleistungsfreiheit, etc.) ein angemessenes Schutzniveau angenommen. Diese Annahme gilt jedoch nicht für einen Datentransfer im Bereich der zweiten Säule (Gemeinsame Außen- und Sicherheitspolitik, GASP) und dritten Säule (Justiz und Inneres) der Europäischen Union (EU).

Bei US-Konzernen besteht häufig ein Interesse, die in Deutschland oder Europa erhobenen Daten zur Muttergesellschaft in die USA zu schicken. Ein solcher Datentransfer nach außerhalb der EU darf grundsätzlich nach § 4 Abs. 2 Satz 2 BDSG nur erfolgen,

wenn die Voraussetzungen für einen Datentransfer vorliegen (siehe oben) und der Transfer in ein Zielland mit angemessenem Schutzniveau erfolgt. Vom angemessenen Schutzniveau gibt es Ausnahmen nach § 4c BDSG (z.B. zur Erfüllung des Vertrages, Wahrung lebenswichtiger Interessen des Betroffenen), auf die ich hier nicht weiter eingehen will. Für die Auftragsdatenverarbeitung gibt es keine Ausnahme.

Die Europäische Kommission kann nach einer Untersuchung der Situation im Drittstaat für diesen ein angemessenes Schutzniveau durch Entscheidung nach Art. 25 Abs. 6 Datenschutzrichtlinie anerkennen. Bisher sind nur für die Schweiz, Ungarn sowie die Vereinbarung über den sicheren Hafen mit den USA anerkannt worden ("safe harbor principles" : www.export.gov/safeharbor). Voraussetzung für ein angemessenes Schutzniveau im Drittstaat ist eine staatliche Überwachung vergleichbarer Datenschutzgrundsätze. Als staatliche Überwachungsbehörden fungieren in den USA die Federal Trade Commission (FTC) und das Departement of Transportation jeweils innerhalb ihrer Zuständigkeiten. Nur für Unternehmen, die sich diesen Verpflichtungen in den USA unterwerfen, wird ein angemessenes Schutzniveau angenommen. Mittlerweile haben sich über 80 Unternehmen diesem System unterworfen. Eine Unterwerfung ist jedoch nicht in allen Bereichen möglich; Banken und Versicherungen sind zum Beispiel davon ausgeschlossen.

Besteht kein angemessener Schutz im Zielland (oder kann bzw. hat sich das Unternehmen nicht den "safe harbor principles" unterworfen), dann kann das angemessene Schutzniveau durch vertragliche Vereinbarungen zwischen dem Datenexporteur und dem Datenimporteur hergestellt werden. Diese Vereinbarungen unterliegen der Prüfung durch die nationalen Aufsichtsbehörden. Wenn die Standardvertragsklauseln der Europäischen Kommission verwendet werden, besteht ein Anspruch auf Genehmigung des Datentransfers.

4 Fazit

Das Recht des Internet in der deutschen Gesetzgebung besteht aus althergebrachtem Recht aus der Zeit vor dem Internet sowie aus neuem Recht, das speziell für dieses Medium geschaffen wurde : Teledienstegesetz / Mediendienstestaatsvertrag, Signaturgesetz, Änderung des BGB und der ZPO, Fernabsatzgesetz sowie der Änderung des Datenschutzrechts und weiterer Vorschriften. Die neuen Regelungen sind nicht immer besonders übersichtlich und verständlich formuliert. Ziel dieser Regelungen ist die Schaffung eines rechtlichen Rahmens für den elektronischen Handel sowie für einen einheitlichen Verbraucherschutz. Ob dieses Ziel immer erreicht wird, bleibt kritisch zu beobachten. Zum Beispiel stieg im Fernabsatz die Rückgabe von gebrauchten Gegenständen (Smoking, Hochzeitskleid, etc.) merklich. Angesichts der Entwicklung des Internet wird sicherlich in den kommenden Jahren noch Bedarf für Nachregulierungen sowie weitere Rechtsetzung in diesem Bereich bestehen.