

- 17) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") Official Journal L 178, 17/07/2000, pp. 0001-0016;
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett
- 18) 1980 Rome Convention on the law applicable to contractual obligations (consolidated version) Official Journal C 027, 26/01/1998, pp. 0034-0046;
[http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=41998Y0126\(03\)&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=41998Y0126(03)&model=guichett)
- 19) Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters Official Journal L 012, 16/01/2001; pp. 0001-0023;
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001R0044&model=guichett
- 20) <http://www.argez.de/>
- 21) <http://www.orgalime.org/publi/pdf/e-commerce.pdf>
- 22) <http://www.bureauveritas.com/>
- 23) <http://www.verisign.com/>
- 24) <http://www.wordandbond.com/>
- 25) <http://europa.eu.int/ISPO/e-commerce/godigital/coordinators.html>
- 26) For papers and proceedings, see <http://europa.eu.int/comm/enterprise/ict/e-marketplace.htm>

Contact

César Santos
 Marianna Perogianni
 European Commission
 DG Enterprise, ICT and E-Business Department
 Rue de la Science 15, 1049 Brussels, Belgium
 Tel.: +322 / 295 16 70 (Santos)
 Tel.: +322 / 295 81 93 (Perogianni)
 Fax: +322 / 296 95 00
 E-Mail: Cesar.Santos@cec.eu.int
 E-Mail: Maria.Perogianni@cec.eu.int
 Internet: <http://europa.eu.int/comm/enterprise>

»

Aktuelle Entwicklungen in der E-Commerce und IT-Politik der USA

von Rufus Pichler, Morrison & Foerster LLP

Der Beitrag befasst sich mit den wichtigsten aktuellen Entwicklungen in der E-Commerce und IT-Politik der USA. Eine kohärente Politik ist von der Bush-Administration in diesen Bereichen bisher nicht vorgelegt worden. Zudem steht zur Zeit die Gesetzgebung eindeutig im Zeichen der Diskussion um die nationale Sicherheit vor dem Hintergrund der Terroranschläge auf das WTC und das Pentagon am 11. September, die für viel und kontrovers diskutierte gesetzgeberische Aktivität gesorgt hat. Beim Datenschutz wird der Kurs der Clinton-Administration, die einen stärkeren Schutz der Verbraucher durch entsprechende gesetzliche Regelungen befürwortete, voraussichtlich nicht fortgesetzt. Weitere Schwerpunkte des Beitrages bilden die Diskussionen um Steuern im Zusammenhang mit dem elektronischen Geschäftsverkehr, Verschlüsselung und Exportbeschränkungen, interaktives Glückspiel sowie der Schutz Minderjähriger. Abschließend wird kurz auf die Position der USA im Hinblick auf einige internationale Entwicklungen und immateriälgüterrechtliche Fragen eingegangen. Eine Lösung der bisher weitgehend offenen Probleme internationaler Gerichtszuständigkeit wird in naher Zukunft nicht erwartet.

1 Einleitung

Die derzeitige E-Commerce und IT-Politik in den USA ist vor allem durch zwei Ereignisse geprägt: den Regierungswechsel zu Beginn des Jahres und die Terroranschläge auf das World Trade Center und das Pentagon am 11. September.

Die Clinton/Gore-Regierung hat der Entwicklung des E-Commerce und des IT-Sektors große Aufmerksamkeit gewidmet. Mit dem Framework for Global Electronic Commerce¹ wurde eine grundlegende Agenda präsentiert, die in jährlichen Berichten der Government Working Group on Electronic Commerce² ergänzt und fortentwickelt und von der Administration insgesamt schrittweise umgesetzt wurde.

Aus der Zeit der Clinton/Gore-Regierung stammen auch einige richtungsweisende Gesetze, die die Schaffung von günstigen Rahmenbedingungen für den elektronischen Geschäftsverkehr zum Ziel haben. Unter diesen Regelungen, die nach wie vor bedeutsam sind, hier aber nicht im Einzelnen erörtert werden sollen, sind vor allem die folgenden hervorzuheben: (i) die Haftungsfreistellungen von Internet Service Providern für die Verbreitung rechtswidriger Drittinhalte im Communications Decency Act von 1996;³ (ii) die vergleichbaren Haftungsprivilegierungen im Hinblick auf Urheberrechtsverletzungen im Digital Millennium Copyright Act (sog. „notice and take down“-Regelung, nach der eine urheberrechtliche Verantwortung eines Internet Service Providers erst in Frage kommt, wenn er einen Inhalt nicht entfernt, nachdem er eine qualifizierte Löschungsaufforderung unter substantiiertes Darlegung der Rechtsverletzung erhalten hat)⁴ und (iii) der bundesrechtliche Electronic Signatures in Global and National Commerce (ESIGN) Act⁵ sowie der in den meisten Einzelstaaten umgesetzte Uniform Electronic Transactions Act (UETA)⁶, die beide die Rechtsgültigkeit elektronischer Signaturen und online geschlossener Verträge bestätigen. Ein weiterer Vorschlag, der Uniform Computer Information Transactions Act (UCITA)⁷, der vor allem die rechtliche Position der Anbieter im Zusammenhang mit elektronischen Transaktionen stärkt (z. B. die Zulässigkeit sog. „click-wrap agreements“ festschreibt und weitgehende Haftungs- und Gewährleistungsausschlüsse, sowie eine elektronische Selbsthilfe erlaubt) ist bisher nur in zwei Staaten (Virginia und Maryland) angenommen worden. Die Unterstützung für UCITA lässt aufgrund starker Proteste aus dem Verbrauchersektor sehr nach, und es wird generell nicht damit gerechnet, dass UCITA in einer nennenswerten Anzahl von Staaten angenommen wird.

Die Bush/Cheney-Regierung hat an den Ansatz ihrer Vorgänger, eine kohärente und nachhaltige E-Commerce und IT-Politik zu entwickeln, bisher nicht angeknüpft. Noch fehlen grundlegende Standortbestimmungen der neuen Regierung. Zu berücksichtigen ist auch, dass mit dem Regierungswechsel personelle Veränderungen in den wichtigen Bundesbehörden wie beispielsweise der Federal Communi-

cations Commission (FCC) und der Federal Trade Commission (FTC) einher gehen, denen eine wichtige Rolle bei der Entwicklung und Umsetzung der E-Commerce und IT-Politik zukommt. Wenn sich bisher eine generelle Tendenz ausmachen lässt, dann ist es die grundsätzliche regulative Zurückhaltung zugunsten einer freien Entwicklung des Marktes, die gelegentlich durchbrochen wird, um in Einzelfällen auf konkrete Bedürfnisse der Wirtschaft und der Politik zu reagieren. Dieser Beitrag geht auf die wichtigsten aktuellen Entwicklungen in der E-Commerce und IT-Politik der USA ein.

Vor diesem Hintergrund hat die Sicherheitsdebatte im Zuge der Terroranschläge vom 11. September für viel und kontrovers diskutierte gesetzgeberische Aktivität gesorgt. Weitere Schwerpunkte bilden die Diskussionen um Steuern im Zusammenhang mit dem elektronischen Geschäftsverkehr, Datenschutz, Verschlüsselung und Exportbeschränkungen, interaktives Glücksspiel sowie der Schutz Minderjähriger vor schädlichen Inhalten. Schließlich ist auf den Standpunkt der USA im Hinblick auf verschiedene Vorhaben auf internationaler Ebene, sowie auf Entwicklungen im Bereich des Immaterialgüterrechts einzugehen.

2 Anti-Terror-Gesetze

Bereits wenige Tage nach den Terroranschlägen vom 11. September brachte Attorney General (dem Generalbundesanwalt vergleichbar) John Ashcroft einen im Justizministerium ausgearbeiteten Vorschlag für einen Anti-Terrorism Act of 2001 im Senat und im Repräsentantenhaus ein. Ziel des Gesetzesvorschlags war es, die Arbeit der Exekutive beim Kampf gegen den Terrorismus zu erleichtern. Der Vorschlag, der insbesondere Erweiterungen und Erleichterungen von Befugnissen enthielt, telefonische und elektronische Kommunikation abzuhören und entsprechende Unterlagen zu beschlagnahmen, wurde von vielen Seiten als zu weit reichend kritisiert.⁸

In der Folge wurden sowohl im Senat, als auch im Repräsentantenhaus unabhängige Kompromissvorschläge erarbeitet. Die Repräsentanten Conyers und Sensenbrenner brachten den Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001⁹ oder

PATRIOT Act ein, der einige der am stärksten kritisierten Bestimmungen des Ashcroft-Vorschlags zurückschnitt, um verfassungsrechtlichen Bedenken Rechnung zu tragen. Das Judiciary Committee des Repräsentantenhauses stimmte dem PATRIOT Act am 3. Oktober einstimmig zu. Im Senat brachten die Senatoren Hatch und Leahy den Uniting and Strengthening America Act of 2001¹⁰ oder USA Act ein, der sich sehr viel mehr am ursprünglichen Ashcroft-Vorschlag orientierte. Am 11. Oktober wurde der USA Act vom Senat mit einer Gegenstimme verabschiedet. Daraufhin wurde im Zuge von Verhandlungen zwischen Führern des Repräsentantenhauses und Mitgliedern der Bush Administration der PATRIOT Act praktisch durch eine leicht veränderte Version des USA Acts ersetzt und in dieser modifizierten Fassung am 12. Oktober – trotz weiterhin bestehender substanzieller Einwände – vom Repräsentantenhaus als USA Act of 2001 verabschiedet.¹¹ Der Senat verabschiedete kurz darauf eine gleichlautende Fassung, und am 26. Oktober wurde das Gesetz als Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)¹² von Präsident Bush unterzeichnet.

Die folgende Darstellung gibt einen kurzen Überblick über die wichtigsten Bestimmungen des USA PATRIOTS Acts und die Hauptkritikpunkte, denen sich der Act ausgesetzt sieht. Das Gesetz erweitert die sogenannten „pen register“ und „trap and trace“ Möglichkeiten der Behörden, die es bisher ohne richterliche Anordnung erlauben, die von einem Telefon gewählten Nummern aufzuzeichnen (nicht jedoch den Kommunikationsinhalt selbst), auf E-Mail und online Kommunikation. Behörden können also, sofern es nach eigener Einschätzung für eine Untersuchung „relevant“ ist, E-Mail Adressen und Internetadressen sowie sonstige technische Parameter der Kommunikation (routing Information etc.) aufzeichnen.

Das Gesetz erlaubt es einem Richter, Abhör- und Durchsuchungsmaßnahmen landesweit anzuordnen. Bisher war die Wirkung solcher Anordnungen auf den jeweiligen Gerichtsbezirk beschränkt. Dasselbe gilt für die Beschlagnahme von „electronic records“, also z. B. den

Inhalt von E-Mail, Voice-Mail oder online Kommunikation.

Die Voraussetzungen für die Anordnung von Abhör-, Durchsuchungs- und Beschlagnahmemaßnahmen und die richterliche Kontrolle derartiger Maßnahmen werden für Terrorismus- und Computerdelikte (deren Definition ihrerseits erweitert wurde) verringert. Gleiches gilt wenn die Ermittlungsmaßnahmen einen Auslandsbezug aufweisen.¹³ Ferner wird der Austausch gewonnener Informationen zwischen verschiedenen Behörden erleichtert.

In zeitlicher Hinsicht sind einige Aspekte der Regelung zunächst auf vier Jahre begrenzt. Diese sogenannte „sunset provision“ ist einer der wenigen Punkte, die aus dem ursprünglichen PATRIOT Act in die neue Regelung übernommen wurden, obgleich dieser eine nur zweijährige Frist vorsah.

Kritiker des USA PATRIOT Acts führen an, dass die Regelungen auf Druck der Regierung überstürzt verabschiedet wurden und eine intensive Diskussion der zum Teil sehr weit reichenden Beschränkungen grundrechtlicher Freiheiten nicht stattgefunden hat. Ferner wird bemängelt, dass das Gesetz generell weit über das Ziel effektiver Terrorismusbekämpfung hinaus schießt und bedenkliche Erweiterungen staatlicher Kontroll- und Abhörmaßnahmen ohne ausreichende richterliche Kontrolle enthält.

3 Steuern

Einen weiteren Schwerpunkt der politischen Debatte in den USA bildet nach wie vor die Besteuerung von E-Commerce-Transaktionen. Hauptsächlich geht es um zwei Bereiche. Dies ist zum einen die an sich wenig umstrittene Verlängerung eines Moratoriums hinsichtlich neuer Steuern auf den Zugang zum Internet oder sonstiger spezifischer Internet-Steuern. Zum anderen geht es um die wesentlich stärker diskutierte Frage, ob einzelne Bundesstaaten ihre bereits bestehende Verkaufssteuer („sales tax“) auch im Zusammenhang mit dem Austausch von Gütern im Rahmen des elektronischen Geschäftsverkehrs erheben können. Kompliziert wird der legislative Prozess vor allem dadurch, dass die beiden Fragen von interessierten Kreisen miteinander verknüpft werden.

3.1 Sales Tax

Aufgrund der negativen Dimension der Commerce Clause der U.S. Verfassung¹⁴, der sogenannten „dormant Commerce Clause“, dürfen bundesstaatliche Steuern nur erhoben werden, wenn ein „substantial nexus“ mit dem besteuerten Staat besteht. In der berühmten Quill Entscheidung¹⁵ bestätigte der U.S. Supreme Court eine frühere Entscheidung¹⁶, wonach ein solcher nexus nicht gegeben ist, wenn ein Unternehmen keinerlei physische Präsenz (z. B. durch Filialen, Vertreter oder sonstige Repräsentanten) im besteuerten Staat hat. Entsprechend wurde die Besteuerung von Unternehmen, die im besteuerten Staat lediglich durch Fernabsatzgeschäfte tätig sind (Versandhandel, mail- und telephone order) als verfassungswidrig bewertet. Auf dieser Grundlage ist es Bundesstaaten nach geltendem Recht nicht möglich, Internet-Transaktionen zu besteuern, wenn der Verkäufer keine physische Präsenz im Staat hat.

Aufgrund der Zunahme des Internet-Fernabsatzes führt dies zu bedeutenden Steuerausfällen auf lokaler und bundesstaatlicher Ebene. Die Schätzungen belaufen sich auf einen Ausfall von 13,3 Milliarden in diesem Jahr und bis zu 54,8 Milliarden US\$ im Jahr 2011.¹⁷

Vor diesem Hintergrund hat sich eine intensive Debatte um die Zulassung bundesstaatlicher Besteuerung von Internet-Transaktionen entzündet. Dies wäre durch ein Bundesgesetz verfassungsrechtlich möglich. Im Senat wurden mehrere Gesetzesvorschläge eingebracht, die den Bundesstaaten eine solche Besteuerung erlauben würden. Unterstützt werden diese Vorschläge von der National Governor's Association¹⁸ vor dem Hintergrund des so genannten „Streamlined Sales Tax Project“, an dem die meisten Bundesstaaten beteiligt sind. Das Projekt strebt eine Vereinheitlichung der verschiedenen sales tax-Systeme an, um die Voraussetzungen für eine Besteuerung von online Transaktionen zu schaffen.¹⁹ Die beiden wichtigsten dieser Vorschläge, der Internet Tax Nondiscrimination Act von Senator Wyden²⁰ und der Internet Tax Moratorium and Equity Act von Senator Dorgan²¹, verknüpften – um die Verhandlungsposition der Staaten zu verbessern – die sales tax-Frage mit der Verlängerung des ablaufenden Internet tax-Moratoriums (dazu sogleich unter 2.1.2). Während die beiden Se-

natoren versuchten, die beiden Vorschläge miteinander in Einklang zu bringen, wurden sie von den Ereignissen des 11. September überholt, in deren Folge das Hauptaugenmerk der beiden Häuser den Anti-Terror-Gesetzen gewidmet war. Aufgrund dessen wurde eine Lösung der sales tax-Frage vor dem Ablauf des Moratoriums unmöglich. Während man sich einig wurde, die Lösung dieser Frage bis 2002 zu verschieben, richtete sich die Aufmerksamkeit nun auf eine nur kurze Verlängerung des Moratoriums, um die notgedrungenermaßen zeitweilig entkoppelten Fragen baldmöglichst wieder miteinander verknüpfen zu können.

3.2 Moratorium hinsichtlich „Internet-Steuer“

Das 1998 beschlossene Internet Tax-Moratorium²², das sowohl die Besteuerung des Internetzugangs an sich (Internet access tax) als auch sonstige spezifische Internet-Steuern (z. B. eine „bit-tax“) vorübergehend unmöglich macht, war zeitlich bis zum 21. Oktober dieses Jahres begrenzt. Grundsätzlich besteht im Kongress Einigkeit, das Moratorium zu verlängern. Ein Vorschlag im Repräsentantenhaus sah eine Verlängerung des Moratoriums für Internet-spezifische Steuern um fünf Jahre und eine dauerhafte Untersagung von Internet access taxes vor.²³ Nur die Verbindung der sales tax-Frage mit der Verlängerung des Moratoriums stand einer zügigen Verabschiedung letzterer entgegen. Mit der Entkopplung der Fragen infolge der Konzentration auf die Anti-Terror-Gesetze stand der isolierten Verlängerung des Moratoriums an sich nichts mehr im Wege – die Frage war nur, wie lang dieses sein würde. Während im Senat konkurrierende Vorschläge von Wyden, Leahy und McCain²⁴ sowie von Dorgan und Breaux²⁵ eingebracht wurden, die eine Verlängerung um zwei Jahre bzw. bis zum 30. Juni 2002 vorsehen, hat das Judiciary Committee des Repräsentantenhauses den ursprünglichen Vorschlag (H.R. 1552) von fünf auf zwei Jahre zurück geschnitten. Dieser Version hat das Repräsentantenhaus am 16. Oktober zugestimmt. Darin war eindeutig ein Kompromissangebot im Hinblick auf die offene sales tax-Frage zu sehen, die damit nicht vom Tisch ist. Dieser Kompromissvorschlag wurde indes im Senat zunächst nicht angenommen. Stattdessen

brachten Enzi und Dorgan noch einen weiteren Vorschlag ein,²⁶ in dem die Verlängerung wiederum mit der sales tax-Frage verknüpft wurde. Über die Diskussion der verschiedenen Vorschläge lief das ursprüngliche Moratorium am 21. Oktober ab, was an sich für die Bundesstaaten das Tor zur Einführung von Internet-Steuern öffnet. In einem erneuten Anlauf wurde nun Mitte November im Senat das 2-Jahres-Moratorium verabschiedet. Mit der Unterschrift des Weißen Hauses wird gerechnet, so dass einer Verlängerung des Moratoriums für „Internet-Steuern“ nun nichts mehr entgegen steht.

4 Datenschutz

Im Gegensatz zur Europäischen Union und ihren Mitgliedsstaaten²⁷, gibt es in den USA weder auf Bundes- noch auf einzelstaatlicher Ebene ein umfassendes Datenschutzrecht, sondern lediglich einige bereichsspezifische Gesetze. Die wichtigsten dieser Gesetze stammen noch aus der Zeit der Clinton-Administration. Zu nennen sind für den Bereich des Gesundheitswesens die Standards for Privacy of Individually Identifiable Health Information²⁸, die auf dem Health Insurance Portability and Accountability Act of 1996 (HIPAA) beruhen²⁹, für den Bereich der Finanzdienstleistungen der Gramm-Leach-Bliley Act³⁰ und für den online-Bereich im engeren Sinne der Children's Online Privacy Protection Act of 1998 (COPPA)³¹. Trotz dieser nur vereinzelt Regulierung ist Datenschutz oder „privacy“ aber in den letzten Jahren auch in den USA zu einem politischen Top-Thema geworden, und die Forderungen von Verbraucherschutzorganisationen nach umfassender Regulierung insbesondere im E-Commerce-Bereich werden lauter. Eine Vielzahl von Gesetzesvorschlägen ist in der jüngeren Vergangenheit im Kongress eingebracht worden, aber bisher ist kein politischer Konsens zustande gekommen. Generell ist unter der Bush-Administration eine Tendenz zurück zur Selbstregulierung der E-Commerce-Industrie zu erwarten, was viele Verbrauchervertreter als Rückschritt gegenüber dem Kurs der Clinton-Administration ansehen, die im Lauf der Zeit verstärkt der Schaffung klarer gesetzlicher Vorgaben zuneigte.

4.1 Gesetzgebung

Obgleich mehrere Gesetzesvorschläge zum Datenschutz im Kongress anhängig sind, wird in absehbarer Zeit nicht mit der Verabschiedung bedeutender Regelungen gerechnet. Ein Grund dafür sind die Auswirkungen der Terroranschläge vom 11. September. In deren Folge wurde Datenschutz im Kongress zunächst eher „unpopulär“, da er dem starken Wunsch nach stärkerer staatlicher Überwachung entgegenzustehen scheint. Überdies wurden viele Gesetzgebungsvorhaben aufgrund der Dringlichkeit der Anti-Terror-Gesetze verschoben. Hinzu kommt, dass die Federal Trade Commission ihren Kurs geändert hat. Technisch erfüllt die FTC zwar lediglich Exekutivaufgaben und hat keinen direkten Einfluss auf den Gesetzgebungsprozess. Aber in tatsächlicher Hinsicht ist die Unterstützung von datenschutzrechtlichen Gesetzgebungsvorhaben durch die FTC von großer Bedeutung für deren Erfolg. Der neue, von Bush eingesetzte FTC Chairman Timothy Muris setzt den Kurs seines Vorgängers Robert Pitofsky nicht fort. Unter Pitofsky befürwortete die Behörde eine umfassendere gesetzliche Regelung des Datenschutzes. Wie Muris in seiner ersten offiziellen Verlautbarung zum Datenschutz kundtat, sieht er derzeit keinen Bedarf für neue gesetzliche Vorgaben.³² Vielmehr wird sich die FTC auf die Durchsetzung bestehender Regelungen konzentrieren (dazu sogleich unter 3.2).

Obwohl die E-Commerce-Branche diesen Richtungswechsel grundsätzlich befürwortet, könnte die Abwesenheit von Regelungen auf Bundesebene zum Bumerang werden, wenn einzelne Bundesstaaten datenschutzrechtliche Regelungen erlassen. Dies könnte im Ergebnis dazu führen, dass die Unternehmen nicht nur unerwartet restriktiven Vorschriften ausgesetzt sein könnten, sondern zusätzlich, dass sie es mit einem regulativen Flickenteppich zu tun hätten. Unter anderem vor diesem Hintergrund ist ein Vorstoß der Vorsitzenden des Committee on Energy and Commerce und des Subcommittee on Commerce, Trade and Consumer Protection, den Repräsentanten Stearns und Tauzin, für eine Regelung zu sehen, die ein datenschutzrechtliches Minimum enthalten und gleichzeitig kollidierende bundesstaatliche Gesetzgebung ausschließen würde. Ein entspre-

chender Gesetzgebungsvorschlag, der vermutlich nächstes Jahr zu erwarten ist, soll unter anderem auch die ausschließliche Verfolgung von Rechtsverstößen durch die FTC vorsehen – sowohl unter Ausschluss eines Klagerechts des betroffenen Individuums, als auch der Verfolgungskompetenz der bundesstaatlichen Attorneys General, die bisher eine wichtige Rolle bei der Durchsetzung von Verbraucherschutzvorschriften spielen. Ein solcher Vorschlag wird mit starkem Widerstand aus dem Konsumentensektor und von bundesstaatlicher Seite aus rechnen müssen.

4.2 FTC Maßnahmen

Wie erwähnt kommt der Federal Trade Commission eine Schlüsselrolle bei der Rechtsdurchsetzung im Bereich des Datenschutzes zu. Chairman Muris hat angekündigt, der Durchsetzung bestehender allgemeiner Regelungen verstärkte Aufmerksamkeit im Online-Kontext zu widmen. Außerhalb der oben genannten bereichsspezifischen Gesetze (COPPA und HIPAA) kann aufgrund der allgemeinen Regelungen gegen ein Unternehmen allerdings nur bei Irreführung von Verbrauchern vorgegangen werden. Dies bedeutet im datenschutzrechtlichen Zusammenhang, dass ein Vorgehen nur in Frage kommt, wenn ein Unternehmen die Einhaltung einer sogenannten „privacy policy“ verspricht und gegen diese (eigene) policy verstößt. Zur Zeit gibt es aber weder eine Pflicht für Unternehmen, überhaupt eine solche privacy policy anzunehmen, noch gibt es diesbezügliche inhaltliche Vorgaben oder Mindeststandards, sollte ein Unternehmen dies freiwillig tun. Aufgrund der allgemeinen Bestimmungen können daher Unternehmen nur belangt werden, wenn sie gegen selbst gesetzte Standards verstoßen, also falsche Versprechungen machen.

4.3 Safe Harbor und Datenexport aus der EU

Im Hinblick auf den Datentransfer aus der Europäischen Union lässt sich feststellen, dass mittlerweile mehrere namhafte Unternehmen wie Intel und Microsoft den sogenannten „Safe Harbor Privacy Principles“ beigetreten sind.³³ Diese sind ein Resultat von Verhandlungen der

USA und der EU im Zusammenhang mit den in der europäischen Datenschutzrichtlinie³⁴ enthaltenen Beschränkungen des Datentransfers in Drittstaaten, die kein angemessenes Schutzniveau gewährleisten.³⁵ Bei Beitritt eines Unternehmens zu den Safe Harbor Privacy Principles, womit es zugleich der Aufsicht der FTC hinsichtlich der Einhaltung dieser Grundsätze unterliegt, geht die Kommission davon aus, dass ein angemessenes Schutzniveau im Sinne der Richtlinie gegeben ist.³⁶

Starker Widerstand wird hingegen in amerikanischen Industriekreisen auch der jüngsten Fassung der Standardvertragsklauseln der EU zur Übermittlung personenbezogener Daten an Verarbeiter in Drittländern³⁷ entgegengebracht. Bei Verbindlichkeit dieser Vertragsklauseln zwischen Datenexporteur und Datenempfänger ist ein Datenexport auch an Empfänger zulässig, die sich nicht den Safe Harbor Privacy Principles verschrieben haben. Hauptkritikpunkt ist, dass diese Standardvertragsklauseln, insbesondere hinsichtlich der Haftung gegenüber dem Datensubjekt, noch rigider seien als die Safe Harbor Prinzipien.

5 Exportbeschränkungen und Verschlüsselung

Ebenfalls im Zuge der Terroranschläge vom 11. September und der in der Folge neu entflammten Sicherheitsdebatte sind die Diskussionen um Exportbeschränkungsregelungen und Datenverschlüsselung wieder aufgelebt.

5.1 Exportbeschränkungen

Die Exportbestimmungen der USA sind komplex und unterliegen der Zuständigkeit verschiedener staatlicher Behörden. Die wichtigste dieser Behörden im Zusammenhang mit E-Commerce ist das Bureau of Export Administration (BXA)³⁸, das für die Anwendung und Durchsetzung der Export Administration Regulations (EAR)³⁹ zuständig ist, die ihrerseits auf dem Export Administration Act of 1979 (EAA)⁴⁰ beruhen. Der EAA wird allgemein als ein Relikt des kalten Krieges angesehen, dessen Revision lange überfällig ist. Das Gesetz ist am 20. August 1994 abgelaufen, wurde jedoch seitdem mehrmals durch präsidiale Verordnung verlängert⁴¹, da im Kongress kein

Konsens für eine neue Regelung gefunden werden konnte. Ein neuer Vorschlag, der Export Administration Act of 2001⁴², der die Exportkontrollbestimmungen insgesamt im Interesse eines freieren Wirtschafts- und Warenverkehrs etwas lockert und aktuellen Bedingungen anpasst, wurde am 6. September vom Senat verabschiedet. Die Zustimmung des Repräsentantenhauses zu diesem Vorschlag ist jedoch unwahrscheinlich. Während schon vor den Terroranschlägen vom 11. September im Repräsentantenhaus eine sehr viel restriktivere Version des Vorschlags befürwortet wurde, die die nationale Sicherheit mehr als den ungehinderten Handel betont, kann nun erwartet werden, dass die Karten im Lichte der neuen Sicherheitsdiskussion neu gemischt werden. Mit einer baldigen Einigung ist daher nicht zu rechnen.

Das geltende Regime der EAR enthält ein komplexes System von Exportverboten, Lizenzanforderungen und Ausnahmen, die je nach Gegenstand und Empfängerstaat variieren und hier nicht im Einzelnen dargestellt werden können.

5.2 Verschlüsselung (Encryption)

Im Hinblick auf Verschlüsselungstechnologien sind zwei Themenkreise von Interesse: die generelle Anwendung der EAR auf solche Technologien zum einen, und die neu aufgeflamnte Diskussion um ein zwingendes „key escrow“ Verfahren zum anderen.

5.2.1 EAR

Verschlüsselungstechnologien unterliegen den EAR. Unter der Clinton-Regierung wurde die Exportkontroll-Politik maßgeblich liberalisiert und die EAR wurden mit Wirkung vom 19. Oktober 2000 entsprechend revidiert.⁴³ Nach den neuen Regeln können Verschlüsselungstechnologien unter anderem nahezu unbeschränkt in die Länder der EU und acht weitere Länder⁴⁴ exportiert werden, nachdem dem BXA eine entsprechende Mitteilung gemacht wurde. Ähnlich vereinfacht wurde das Verfahren für Produkte, die für Endverbraucher bestimmt sind und für sonstige „mass market“ Produkte, abhängig von einer entsprechenden Klassifizierung solcher Produkte durch das BXA.

Obwohl dies vor dem Hintergrund der aktuellen Sicherheitsdebatte nicht auszuschließen ist, scheint eine erneute Verschärfung dieser liberalisierten Regelungen zur Zeit unwahrscheinlich.

5.2.2 Key Escrow

Im Rahmen der aktuellen Sicherheitsdebatte ist allerdings der Vorschlag eines zwingenden „key escrow“ Verfahrens, also einer Schlüssel hinterlegung bei einer Regierungsbehörde, durch Senator Gregg neu zum Leben erweckt worden. Dieser Vorschlag wurde während der Clinton-Administration sehr kontrovers diskutiert und scheiterte schließlich am vehementen Widerstand insbesondere aus dem Lager der Software- und Computerhersteller. Dieser Widerstand hat sich trotz der an sich „guten“ Zeiten für restriktive Sicherheitspolitik schnell erneut geregt, und es wurde generell für unwahrscheinlich gehalten, dass Senator Gregg's Vorschlag nennenswerte Unterstützung finden wird. Mittlerweile rudert der Senator offenbar zurück und hat verlauten lassen, dass er derzeit keinen entsprechenden Gesetzgebungsvorschlag plant.

6 Glücksspiel

Internet-Glücksspiel oder online gambling ist ein weiterhin kontrovers diskutierter Bereich. Glücksspiel im Allgemeinen ist nach dem Recht mancher Bundesstaaten illegal, nach dem Recht anderer Bundesstaaten, wie z. B. Nevada, legal (bei Erteilung einer entsprechenden Lizenz). Ein Problem stellt das sogenannte „offshore“ gambling dar, das von Unternehmen, die meist in der Karibik angesiedelt sind, über das Internet auch Nutzern in den USA angeboten wird.

In einem Fall, der vom Supreme Court von New York, wo Glücksspiel nicht erlaubt ist, entschieden wurde, führte das Gericht aus, dass Glücksspiel auch dort vorgenommen wird, wo die Spieler handeln, also auch in New York. Die Angeklagte war ein in Antigua lizenziertes Kasino, und bot Glücksspiele über das Internet im Einklang mit dem Recht von Antigua an. Das Gericht hielt es indes für irrelevant, dass die Aktivitäten in Antigua legal sind.⁴⁵ Im Sinne dieser Entscheidung erstrecken einige Bundes-

staaten, wie z. B. Kalifornien⁴⁶, das Glücksspielverbot per Gesetz ausdrücklich auf online Angebote, die für Bewohner des jeweiligen Staates zugänglich sind. Andere Staaten hingegen, insbesondere Nevada, haben angesichts geschätzter Einnahmen von bis zu sechs Milliarden Dollar im Jahr 2003 das Angebot von Glücksspielen über das Internet legalisiert, vorausgesetzt der Anbieter erwirbt eine Lizenz und kann garantieren, dass das Angebot nicht von Minderjährigen oder von Personen in Staaten, nach deren Recht Glücksspiel illegal ist, wahrgenommen werden kann.⁴⁷ Insofern setzt die Glücksspiel-Branche unter anderem auf sogenannte „geolocation“, „geotracking“ oder „geotargeting“ Dienste, die anhand der IP-Adresse des Nutzers in Verbindung mit verschiedenen proprietären Technologien den physischen Aufenthalt von Nutzern feststellen können. Die Hauptanbieter dieser Technologien, wie z. B. Quova, NetGeo, InfoSplit, Digital Island, Digital Envoy oder Akamai arbeiten zur Zeit daran, die Genauigkeit ihrer Dienste (die im Hinblick auf das Land des Nutzers zwischen 96 % und 99 %, im Hinblick auf einzelne Staaten innerhalb der USA wegen des proprietären AOL Netzwerkes derzeit aber nur bei ca. 85 % liegt) zu verbessern.

Auf Bundesebene sind mehrere Gesetzesentwürfe, die sich speziell des illegalen Internet-Glücksspiels annahmen, gescheitert. Entsprechende Vorschriften haben allerdings jüngst, zur Überraschung einiger Beobachter, ihren Weg in den Financial Anti-Terrorism Act of 2001⁴⁸ gefunden, der im Zuge der Terroranschläge vom 11. September im Repräsentantenhaus eingebracht wurde, und vor allem die Bekämpfung internationaler Geldwäsche zum Gegenstand hat. Der Vorschlag verbot insbesondere die Annahme von Zahlungen und die Akzeptanz von sonstigen Zahlungsinstrumenten im Zusammenhang mit Internet-Glücksspiel, wenn dieses am Ort, an dem sich der Spieler aufhält, oder am Ort, an dem der Anbieter sitzt, illegal ist.⁴⁹ Der Vorschlag erlaubte ein straf- und zivilrechtliches Vorgehen und sah auch Maßnahmen gegen Finanzinstitute vor, die nach dem Gesetz illegale Zahlungen veranlassen oder bearbeiten. Ziel ist es also insbesondere, den Zahlungsverkehr (vor allem über Kreditkarten) zu den Offshore-Anbietern abzuschneiden. Ähnliche Vorschläge sind bereits bisher

im Kongress gescheitert. Nach intensiven Debatten hinter den Kulissen und auf Druck der Regierung wurden die offenbar zu umstrittenen Glücksspiel-Vorschriften schließlich wieder aus dem Gesetzesentwurf, der möglichst schnell verabschiedet werden sollte, gestrichen. Kurz darauf ist aber die gestrichene Passage als eigenständiger Gesetzesvorschlag wieder im Repräsentantenhaus eingebracht worden.⁵⁰ Zudem hat Repräsentant Goodlatte einige Tage später einen weiteren Vorschlag zum gleichen Thema eingebracht.⁵¹ Die Debatte ist also erst eröffnet.

7 Schutz Minderjähriger

Hinsichtlich des Schutzes Minderjähriger vor schädlichen Inhalten wird momentan auf die Entscheidung des US Supreme Court zum Child Online Protection Act of 1998 (COPA)⁵² gewartet. Etwas vereinfacht ausgedrückt, verbietet es das Gesetz, wissentlich einem Minderjährigen über das Internet näher definierte schädliche (pornographische) Inhalte zugänglich zu machen. Die Haftung kann vermieden werden, wenn der Anbieter Alterskontrollmechanismen (Kreditkarte, adult access codes, etc.) einsetzt. Ein District Court in Pennsylvania hielt das Gesetz, wie die vom U.S. Supreme Court bereits verworfene Vorgängerbestimmung im Communications Decency Act of 1996 (CDA)⁵³, aufgrund übermäßiger Beschränkungen der im ersten Zusatzartikel zur US Verfassung garantierten Redefreiheit für verfassungswidrig.⁵⁴ Das Berufungsgericht bestätigte die Entscheidung der Vorinstanz⁵⁵ und der Supreme Court nahm den Fall zur Entscheidung an.⁵⁶ Die Entscheidung wird mit Spannung erwartet. Wenn auch COPA für verfassungswidrig erklärt wird, kann mit neuen Gesetzesvorschlägen ähnlichen Inhalts gerechnet werden.

8 Internationale Übereinkommen

Im Rahmen der Haager Konferenz für Internationales Privatrecht⁵⁷ wird seit 1992 ein internationales Übereinkommen über gerichtliche Zuständigkeiten und ausländische Urteile in Zivil- und Handelssachen diskutiert. Der Vorschlag für ein solches Übereinkommen ging ursprünglich von den USA aus, die bestrebt waren, die Aussichten der Vollstreckbarkeit amerikanischer Urteile im Ausland zu verbes-

sern. Die Konferenz erarbeitete einen Vorschlag, der 1999 veröffentlicht wurde. Nach Veröffentlichung dieses Vorschlags nahmen die E-Commerce- und IT-Kreise von den Verhandlungen Notiz, was dazu führte, dass die bisher weitgehend ungelösten Probleme internationaler Gerichtszuständigkeit beim globalen elektronischen Geschäftsverkehr mit auf den Verhandlungstisch kamen. Mittlerweile bilden diese Fragen den eindeutigen Schwerpunkt der Diskussionen. Ein Konsens ist im Hinblick auf die meisten kontroversen Fragen, wie der Zuständigkeit in Verbrauchersachen, für Deliktssklagen, im Bereich des Immaterialgüterrechts oder für Sicherungs- und sonstige vorläufige Maßnahmen, derzeit nicht in Sicht.⁵⁸ Die Unterstützung des Vorhabens innerhalb der USA schwindet, da viele Kreise die Einbeziehung der weitgehend ungelösten Fragen der Gerichtszuständigkeit im E-Commerce-Kontext als verfrüht empfinden. Die derzeitige Tendenz in den USA ist es, nur ein Übereinkommen zu befürworten, das sich auf die konsensfähigen Fragen beschränkt, die weitgehend ungelösten Probleme hingegen zunächst ausklammert. Eine Lösung der selbst auf nationaler Ebene noch weitgehend ungelösten E-Commerce-Fragen im Rahmen eines internationalen Übereinkommens wird mittlerweile überwiegend als unrealistisch angesehen. In der nächsten Verhandlungsrunde, die im Jahr 2002 stattfinden soll, wird daher vermutlich zunächst über das Schicksal des Übereinkommens an sich debattiert werden, anstatt über spezifische Zuständigkeitsprobleme im Zusammenhang mit E-Commerce.

9 Immaterialgüterrecht

Im Bereich des Immaterialgüterrechts sind aus europäischer Sicht vor allem die Diskussion um einen Schutz von Datenbanken und ein vielbeachteter Fall im Zusammenhang mit dem Digital Millennium Copyright Act interessant.

9.1 Datenbankschutz

Schon lange ist der rechtliche Schutz von Datenbanken in den USA ein Thema. Seit der berühmten Feist-Entscheidung⁵⁹ steht fest, dass das geltende Urheberrecht keinen solchen Schutz gewährt, wenn die Datenbank, was der Regelfall ist, nicht die generell geltenden Originalitätsan-

forderungen des Copyright Act erfüllt. Mit der Verabschiedung der Datenbankrichtlinie⁶⁰ in der Europäischen Union wuchs der Druck der US Industrie auf den amerikanischen Gesetzgeber, einen vergleichbaren Schutz auch in den USA einzuführen. Bisher hat jedoch keiner der zahlreichen Gesetzesvorschläge die Zustimmung des Kongresses erlangen können.

Im letzten, dem 106. Kongress wurden zwei aussichtsreiche Gesetzgebungsvorschläge eingebracht⁶¹, deren Konsolidierung und Verabschiedung allgemein erwartet wurde, was aber ausblieb. Beide Vorschläge ähnelten im Grundsatz der europäischen Datenbankrichtlinie. Ebenfalls überraschend ist, dass keiner der beiden Vorschläge bisher im 107. Kongress eingebracht wurde. Sprecher des Repräsentantenhauses betonten allerdings, dass die Frage nicht vom Tisch sei. Allerdings sei wegen der Sicherheitsdebatten und der Anti-Terror-Gesetze nicht damit zu rechnen, dass sich der Kongress vor dem nächsten Jahr mit dem Datenbankschutz befasst. Bis dahin erwartet man sich auch eine klare Stellungnahme der Industrie.

9.2 DMCA und der Sklyarov Fall

Noch aus der Zeit der Clinton-Administration stammt der vieldiskutierte Digital Millennium Copyright Act (DMCA)⁶². Der DMCA diene unter anderem der Umsetzung der sog. WIPO-Verträge (World Intellectual Property Organisation) – dem WIPO Copyright Treaty (WCT) sowie dem WIPO Performance and Phonograms Treaty (WPPT) – und enthielt dementsprechend Klarstellungen im Hinblick auf die Anwendung urheberrechtlicher Bestimmungen auf digitale Nutzungshandlungen. Des weiteren enthält der DMCA die in der Einleitung angesprochenen Haftungsprivilegierungen für Internet Service Provider und das häufig als zu weit reichende Einschränkung der Kommunikationsfreiheit und der an sich erlaubten Nutzung („fair-use“) urheberrechtlich geschützter Werke kritisierte⁶³ Verbot der Umgehung technischer Schutzmechanismen, die die Nutzung solcher Werke (wie z. B. das Anfertigen von Kopien) beschränken. Ein aktueller Fall demonstriert, dass es den USA mit der Durchsetzung dieser Bestimmungen ernst ist.

Am 16. Juli wurde der russische Computerprogrammierer Dmitry Sklyarov wegen Versto-

ßes gegen die so genannten „anti-circumvention“ Bestimmungen des DMCA verhaftet und später angeklagt. Sklyarov, ein Programmierer bei der russischen Firma Elcomsoft, hatte ein Computerprogramm (Advanced eBook Processor) entwickelt, das die Umgehung der technologischen Schutzmechanismen des Adobe Acrobat eBook Reader erlaubt. Das Programm wurde von Elcomsoft über das Internet auch in den USA vertrieben. Elcomsoft hat ihren Sitz in Moskau⁶⁴, wo Sklyarov das Programm auch entwickelt hat. Als Sklyarov die USA besuchte, um einen Vortrag bei der DefCon 9 Konferenz in Las Vegas zu halten, wurde er wegen Verstoßes gegen § 1201(b)(1)(A) des Copyright Act⁶⁵ verhaftet, obgleich Vertrieb und Entwicklung der Software offenbar nicht gegen russisches Recht verstößt.

Aus Industriekreisen lässt sich vernehmen, dass eine Erweiterung eines solchen indirekten Schutzes von Urheberrechten angestrebt wird. Angeführt von Disney und mit vorsichtiger Unterstützung der Motion Picture Association of America (MPAA) wollen Rechteinhaber gesetzliche Regelungen durchsetzen, die Gerätehersteller (z. B. Computer, CD-Brenner, etc.) dazu verpflichten würden, ihre Produkte mit Kopierschutzmechanismen zu versehen. Dieser Vorschlag stößt bereits in der Frühphase auf vehementen Widerstand aus dem Technologie-sektor. Intel, IBM, Microsoft und Compaq bilden bereits eine Allianz, die mit allen Mitteln versuchen wird, eine solche gesetzliche Regelung zu verhindern. Als Rechteinhaber und führendes Online-Unternehmen steht AOL Time Warner zwischen den Fronten, hat aber verlauten lassen, dass es den Vorschlag in der derzeitigen Form nicht unterstützt.

10 Ausblick

Die Bush-Administration hat bisher keine klare Agenda für eine kohärente E-Commerce und IT-Politik vorgelegt. Die Gesetzgebung steht eindeutig im Zeichen der Diskussion um die nationale Sicherheit in der Folge der Terroranschläge von New York und Washington. Viele liberale Gesetzesvorschläge wurden im Zuge dieser Debatte verschoben oder gänzlich verworfen. In anderen Bereichen, insbesondere beim Datenschutz, wird der Kurs der Clinton-Administration, die einen stärkeren Schutz der

Verbraucher durch entsprechende gesetzliche Regelungen befürwortete, voraussichtlich nicht fortgesetzt. Die neue Regierung baut hier auf das Modell der Selbstregulierung durch die Industrie. Die Lösung vieler anderer Fragen, wie beispielsweise die sales tax-Problematik, die Exportkontrollgesetzgebung oder der Schutz von Datenbanken ist aufgrund der Anti-Terror-Gesetze ins nächste Jahr verschoben worden. Insgesamt lässt sich eine klare Richtung der E-Commerce und IT-Politik der USA nicht feststellen. Vielmehr wird der Stärke des Einflusses der jeweiligen interessierten Kreise eine entscheidende Bedeutung für die künftige Entwicklung zukommen.

Anmerkungen

Die Nachweise folgen dem Standard für juristische Fachbeiträge. Zum besseren Verständnis seien einige allgemeine Hinweise vorangestellt: Die Abkürzungen „S.“ und „H.R.“ stehen für Gesetzesvorschläge die im amerikanischen Senat bzw. Repräsentantenhaus eingebracht wurden. Die Abkürzung „Pub. L.“ steht für „Public Law“ und bezeichnet verabschiedete Gesetze. Gesetzesvorschläge und verabschiedete Gesetze können unter <http://thomas.loc.gov> abgerufen werden. Der United States Code (U.S.C.) ist unter <http://www4.law.cornell.edu/uscode> abrufbar, und Entscheidungen des US Supreme Court können z. B. unter <http://guide.lp.findlaw.com/casecode/supreme.html> eingesehen werden.

- 1) Clinton/Gore, A Framework for Global Electronic Commerce (1.7.1997); <http://www.ecommerce.gov/framework.htm>
- 2) Vgl. The U.S. Government Working Group on Electronic Commerce, Leadership for the New Millennium, 3rd Annual Report, 2000; <http://www.ecommerce.gov/ecomnews/ecommerce2000annual.pdf>; dies., Towards Digital eQuality, 2nd Annual Report, 1999 <http://www.ecommerce.gov/ecomrce.pdf>; dies., First Annual Report, 1998; <http://www.doc.gov/ecommerce/E-comm.pdf>
- 3) 47 U.S.C. § 230(c)(1) („No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.“)
- 4) 17 U.S.C. § 512
- 5) Pub. L. 106-229
- 6) Abrufbar unter <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>
- 7) Abrufbar unter <http://www.law.upenn.edu/bll/ulc/ucita/ucita1200.htm>

- 8) Am deutlichsten fiel die Kritik der so genannten „civil liberties groups“ aus. Insbesondere sind hier zu nennen die American Civil Liberties Union, <http://www.aclu.org>, das Center for Democracy & Technology, <http://www.cdt.org> und das Electronic Privacy Information Center, <http://www.epic.org>.
- 9) H.R. 2975
- 10) S. 1510
- 11) H.R. 3108 (als Änderung in H.R. 2975 integriert)
- 12) Pub. L. 107-56
- 13) Darin liegt eine Erweiterung der Befugnisse unter dem Foreign Intelligence Surveillance Act (FISA), der generell geringere Anforderungen an Überwachungsmaßnahmen stellt als bei inländischen Ermittlungsmaßnahmen.
- 14) Art. I Abs. 8 S. 3
- 15) Quill Corp. v. Heitkamp, 504 U.S. 298 (1992)
- 16) National Bellas Hess, Inc. v. Dept. of Revenue, 386 U.S. 753 (1967)
- 17) Vgl. Bruce/Fox, State and Local Sales Tax Revenue Losses from E-Commerce: Updated Estimates, 2001; <http://www.statestudies.org/ecomreport.pdf>
- 18) Vgl. <http://www.nga.org>
- 19) Vgl. <http://www.geocities.com/streamlined2000>
- 20) S. 288
- 21) S. 512
- 22) Vgl. Internet Tax Freedom Act, Pub. L. 105-277 (kodifiziert als 47 U.S.C. 151)
- 23) Vgl. Internet Tax Nondiscrimination Act, H.R. 1552
- 24) Internet Tax Moratorium Extension Act, S. 1481
- 25) Internet Tax Moratorium Extension Act, S. 1504
- 26) Internet Tax Moratorium and Equity Act, S. 1567
- 27) Vgl. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABIEG Nr. L 281 v. 23.11.1995, S. 31
- 28) 45 C.F.R. Pt. 160 and 164
- 29) Pub. L. 104-191
- 30) Pub. L. 106-102
- 31) 15 U.S.C. 6501 ff. Vgl. a. Children's Online Privacy Protection Rule, 16 C.F.R. Pt. 312
- 32) Protecting Consumers' Privacy: 2002 and Beyond (4.10.2001); <http://www.ftc.gov/speeches/muris/privisp1002.htm>
- 33) Vgl. U.S. Department of Commerce, Safe Harbor Privacy Principles v. 21.7.2000; <http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm>
- 34) Vgl. oben, Anmerkung 27
- 35) Art. 25 Abs. 1 der Richtlinie
- 36) Vgl. Art. 1 der auf Art. 25 Abs. 1 der Datenschutzrichtlinie gestützten Entscheidung der Kommission vom 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (bekannt gegeben unter Aktenzeichen K(2000) 2441) (2000/520/EG), ABIEG L 215 v. 25.8.2000, S. 7
- 37) Vgl. http://europa.eu.int/comm/internal_market/en/dataprot/news/sccproc.pdf
- 38) Vgl. <http://www.bxa.doc.gov>
- 39) 15 C.F.R. Parts. 730-774
- 40) 50 U.S.C. App. 2401 ff.
- 41) Zuletzt durch Präsident Bush durch Executive Order 13222 v. 17.8.2001. Die Befugnis dazu findet sich im International Emergency Economic Powers Act, 50 U.S.C. § 1702
- 42) S. 149
- 43) Vgl. <http://www.bxa.doc.gov/Encryption/EncryptionRuleOct2K.html>
- 44) Australien, Tschechische Republik, Ungarn, Japan, Neuseeland, Norwegen, Polen, Schweiz
- 45) State v. WIGC, 714 N.Y.S. 2d 844, 850 (Sup. Ct. 1999)
- 46) Vgl. den Gesetzesvorschlag A.B. No. 1229 (23.2.2001)
- 47) A.B. No. 466 (14.6.2001) § 3(2) („The commission may not adopt regulations governing the licensing and operation of interactive gaming until the commission first determines that: [...]; (b) Interactive gaming systems are secure and reliable, and provide reasonable assurance that players will be of lawful age and communicating only from jurisdictions where it is lawful to make such communications; [...].“)
- 48) H.R. 3004
- 49) Vgl. H.R. 3004, § 304
- 50) Unlawful Internet Gambling Funding Prohibition Act, H.R. 556
- 51) H.R. 3215
- 52) Pub. L. 105-227 (1998) (kodifiziert als 47 U.S.C. § 231)
- 53) Der Communications Decency Act of 1996 ist ein Teil, Title V, des Telecommunications Act of 1996, Pub. L. 104-104, kodifiziert als 47 U.S.C. §§ 151 ff.). Für verfassungswidrig wurden 47 U.S.C. §§ 223(a)(1)(B)(ii) und (d) erklärt, und zwar vor allem wegen der „chilling effects“ im Hinblick auf verfassungsrechtlich geschützte Inhalte; Reno v. ACLU, 521

- U.S. 844, 872 (1997) („obvious chilling effects on free speech“).
- 54) *ACLU v. Reno*, 31 F. Supp. 2d 473, 497 (E.D. Pa 1999) („Such a chilling effect could result in the censoring of constitutionally protected speech [...]“).
- 55) 217 F.3d 162 (3d Cir. 2000)
- 56) 121 S. Ct. 1997 (2001)
- 57) Vgl. <http://www.hcch.net>
- 58) Vgl. ausf. Wellbery/Pichler, *Electronic Commerce and the Proposed Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters – Putting the Cart Before the Horse?*, *Computer und Recht International* 2001, 129 ff
- 59) *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991)
- 60) Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABIEG Nr. L 77 v. 27.3.1996, S. 20
- 61) Die sog. Coble Bill, H.R. 354 und die sog. Bliley Bill, H.R. 1858
- 62) Public Law No. 105-304 (kodifiziert als Änderung des Copyright Act of 1976, 17 U.S.C. §§ 101 ff.)
- 63) Vgl. nur Electronic Frontier Foundation, *Digital Millennium Copyright (DMCA) Archive*, <http://www.eff.org/IP/DRM/DMCA>
- 64) *Elcomsoft Co. Ltd.*; <http://www.elcomsoft.com>
- 65) 17 U.S.C. § 1201(b)(1)(A) lautet: „No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof“.

Kontakt

Rufus Pichler, J.S.M.
Rechtsanwalt und Attorney at Law
Technology Transactions Group
Morrison & Foerster, LLP
425 Market Street, San Francisco, CA 94105, USA
Tel.: +1 (415) 268 - 70 00
Fax: +1 (415) 268 - 75 22
E-Mail: rpichler@mof.com
Internet: <http://www.mof.com>

»

Die E-Commerce-Politik der Bundesregierung

von Rolf Hochreiter, Bundesministerium für
Wirtschaft und Technologie

Der Beitrag befasst sich mit den strategischen Programmen der Bundesregierung zur Förderung des E-Commerce. Die Umsetzung der Programme und Initiativen soll durch eine neue „Innovationspartnerschaft“ von Politik, Wirtschaft und Gesellschaft gewährleistet werden. Ein wesentliches Ziel ist es, die Teilhabe aller gesellschaftlicher Gruppen an der umfassenden Nutzung moderner IuK-Techniken sicher zu stellen. Dies setzt eine entsprechende technische Ausstattung, z. B. in Schulen und Hochschulen, in der Aus- und Weiterbildung, vernetzte Infrastruktur sowie Medienkompetenz voraus. Neben diesen allgemein gesellschaftlichen Zielsetzungen ist die Bundesregierung bemüht, günstige rechtliche Rahmenbedingungen für E-Commerce bereit zu stellen. Der Umsetzung einschlägiger EU-Richtlinien wie auch der Eigenverantwortung der Wirtschaft wird hierbei große Bedeutung beigemessen. Ein ganz entscheidender Schwerpunkt der Initiativen der Bundesregierung liegt auf der Nutzung der Potenziale der IuK-Technologien im Bereich der öffentlichen Verwaltung, insbesondere bei der öffentlichen Beschaffung von Gütern und Dienstleistungen. Durch die "E-Government-Initiative" sollen wesentliche Impulse für die Entwicklung von E-Commerce und E-Business ausgelöst werden, denen auch ein strategischer Stellenwert für die Schaffung neuer Arbeitsplätze beigemessen wird.

1 Grundlagen der E-Commerce-Politik der Bundesregierung

Die Politik der Bundesregierung für E-Commerce basiert auf drei strategischen Politikprogrammen, die zusammen das Ziel verfolgen, Deutschland und Europa einen internationalen Spitzenplatz in der Informationsgesellschaft zu sichern:

- das gemeinsam vom Bundesministerium für Wirtschaft und Technologie und Bundesministerium für Bildung und Forschung im September 1999 vorgelegte Aktionsprogramm „Innovation und Arbeitsplätze