Neue Juristische Wochenschrift

In Verbindung mit dem Deutschen Anwaltverein

39 1998

und der Bundesrechtsanwaltskammer herausgegeben von *Prof. Dr. Rainer Hamm,* Rechtsanwalt in Frankfurt a. M. – *Prof. Dr. Rudolf Nirk,* Rechtsanwalt beim BGH – *Dr. Fritz Ostler,* Rechtsanwalt in München – *Prof. Dr. Hans-Jürgen Rabe,* Rechtsanwalt in Hamburg – *Prof. Dr. Konrad Redeker,* Rechtsanwalt in Bonn.

Seite 2849–2928
51. Jahrgang
23. September 1998

Schriftleitung: *Prof. Dr. Hermann Weber,* Rechtsanwalt, Palmengartenstraße 14, 60325 Frankfurt a. M.

Aufsätze

Professor Dr. Thomas Hoeren, Münster

Internet und Recht – Neue Paradigmen des Informationsrechts

Das Internet schafft – wider Erwarten – keine neuen Rechtsprobleme. Gerade die jüngst erscheinenden Monographien zum „Cyberlaw" zeigen, daß die Rechtsprobleme des Informationsrechts so neu nicht sind. Und doch tauchen gerade bei der juristischen Auseinandersetzung mit Sachverhalten, die einen Bezug zum Internet haben, eine Reihe interessanter Topoi auf, die zwar schon früher latent vorhanden waren, erst jetzt aber ihre besondere Brisanz und Vielfältigkeit erweisen. Im weiteren soll versucht werden, einige diese Topoi aufzuzeigen, um damit gleichzeitig Facetten eines eigenständigen Informationsrechts zu skizzieren.

I. Das Phänomen der Dematerialisierung und die neuen Property Rights

Als erster Topos des Internet-Rechts[1] fällt die mit dem Netz verbundene Dematerialisierung auf, die dazu führt, daß materielle Wirtschaftsgüter zugunsten neuer, immaterieller Güter an Bedeutung verlieren[2]. Traditionell geht das BGB von der Dichotomie von Waren und Dienstleistungen aus[3]. Schützenswerte Güter, die weder Waren- noch Dienstleistungscharakter haben, werden im geltenden Zivilrecht nicht geschützt. Dieses Phänomen beruht auf der Logik des 19. Jahrhunderts. An der Schwelle von einer Bauern- zu einer Industriegesellschaft mußte das BGB den Primat der Warenproduktion abbilden und konnte selbst im Hinblick auf die Bedürfnisse einer modernen Dienstleistungsgesellschaft nur auf rudimentäre rechtliche Regelungen zum Dienstvertrag verweisen. In einer sogenannten Informationsgesellschaft gibt es jedoch eine ganze Reihe von Rechtsgütern, die sich der Logik Ware gegen Dienstleistung widersetzen. Es handelt sich hierbei um neue Property Rights, schützenswerte Güter, die einer eigenen Sachgesetzlichkeit unterliegen und nicht mit dem klassischen Instrumentarium des Zivilrechts gesichert werden können.

1. Die Information

Zunächst ist hier zu denken an die Information als solche[4]. Der Schutz von Informationen beschränkt sich traditionell auf den Know-how-Schutz, wie er in § 17 UWG verankert ist. Diese Vorschrift erweist sich in mehrerlei Hinsicht als Irrläuferin. Zum einen ist sie als strafrechtliche Regelung im Rahmen des UWG falsch plaziert. Hier äußert sich die Unsicherheit des Gesetzgebers zu Beginn dieses Jahrhunderts hinsichtlich der genauen Ratifizierung von Informationen und ihrem Schutz. Zum anderen sichert die Vorschrift nur den Schutz von Geheimnissen, ohne den Geheimnisbegriff hinreichend absichern zu können.

Dem gleichen Problem unterliegen allerdings auch moderne Versuche einer Zuordnung des Rechtsguts Information. Das Urheberrecht ist auf den Schutz der Werke schöner Literatur und Musik zugeschnitten und ist bis zum heutigen Tag noch nicht auf die Bedürfnisse einer modernen Informationsgesellschaft hin angepaßt worden[5]. Zwar versucht die Europäische Kommission einen solchen Anpassungsprozeß zu initiieren, indem sie etwa in der europäischen Datenbankrichtlinie[6] ein neues Schutzrecht für Informationssammlungen schafft[7]. Die Konturen dieses neu-

1) Zu den jüngst erschienenen Monographien s. etwa *Hilty* (Hrsg.), Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, 1996; *Hoeren/Sieber* (Hrsg.), Hdb. MultimediaR (erscheint demnächst); *Lehmann* (Hrsg.), Internet- und MultimediaR (Cyberlaw), 1997; *Schwarz* (Hrsg.), Rechtsfragen des Internet, Loseblatt (Stand: 1998); *Strömer*, OnlineR, 1997; zum österreichischen Recht: *Mayer-Schönberger*, Das Recht am Info-Highway, 1997. Im weiteren werden die Belege aus Platzgründen auf das Notwendigste beschränkt.

2) S. hierzu *Bercovitz*, GRURInt 1996, 1010 (1011).

3) Vgl. hierzu die Überlegungen in *Hoeren*, GRUR 1997, 866 ff.

4) Vgl. hierzu *Hoeren*, Information als Gegenstand des Rechts, Beil. zu MMR H. 9/1998, 6*.

5) Berechtigt insoweit die grundlegende Kritik von *Barlow*, The Economy of Ideas: A Framework for Rethinking Patents and Copyrights, in: WIRED 2.03, 1994, 84 ff.; zu Reformvorschlägen s. den Zweiten Zwischenbericht der Enquete-Kommission Zukunft der Medien, Neue Medien und UrheberR, 1997, und *Schricker* (Hrsg.), UrheberR auf dem Weg zur Informationsgesellschaft, 1997.

6) Richtlinie 96/9/EG v. 11. 3. 1996, ABlEG Nr. L 77 v. 27. 3. 1996, 20 = EWS 1996, 199. S. hierzu die Aufsätze von *Gaster*, der seitens der Europäischen Kommission die Entstehung der Datenbankrichtlinie maßgeblich beeinflußt hat, z. B. *Gaster*, Ent. LR. 1995, 258 ff.; *ders.*, ÖSGRUM 19 (1996), 15 ff.; *ders.*, Revue du Marché Unique Européen 4/1996, 55 ff.

7) S. aus der vielfältigen Literatur zu diesem Themenkomplex *Bechtold*, ZUM 1997, 427 ff.; *Berger*, GRUR 1997, 169 ff.; *Dreier*, GRURInt 1992, 739 ff.; *Flechsig*, ZUM 1997, 577 ff.; *Gaster*, CR 1997, 660 ff. (Teil I) und 717 ff. (Teil II); *Lehmann*, NJW-CoR 1996, 249 ff.; *Wiebe*, CR 1996, 198 ff.

en Schutzsystems sind jedoch nicht klar definiert. Niemand weiß beispielsweise, was unter einer qualitativ oder quantitativ wesentlichen Investition zu verstehen ist, wie es § 87 a UrhG als Voraussetzung für den Schutz von Datenbanken vorsieht. Hierin zeigt sich symbolisch das Grundproblem des Informationsrechts: Sichere Kriterien für die Verteilung von Informationszugangs- und Informationsausschließlichkeitsrechten gibt es nicht[8]. Der Traum von einer Wissensordnung[9] bleibt ein Traum[10].

2. Die Domain

Aber abseits der Information selbst gibt es eine Reihe anderer neuer Property Rights, deren juristisches Schicksal im unklaren bleibt. Hierzu zählt z. B. die Domain, die Kennzeichnung von Identität eines Providers im Internet[11]. Die Domain stellt solange ein vermögenswertes Gut dar, wie sie die virtuelle Identität des Providers und seiner Produkte kennzeichnet. Derzeit ist eine Person hauptsächlich über die ihr eindeutig zugewiesene Domain im Internet präsent. Die Domain ist die conditio sine qua non für einen Internetauftritt und tauscht dementsprechend auch als Teil der Unternehmenskennzeichnung auf Visitenkarten, Broschüren und Werbetexten auf. Typischerweise werden Property Rights über staatliche Verteilungsorganisationen vergeben; diese stehen sozusagen als Garanten für die distributive Gerechtigkeit. Im Falle der Domains wird der Staat nur repressiv tätig, was als Novum angesehen werden kann. Domains werden von privatrechtlich organisierten Einrichtungen nach dem Prinzip „first come first served" vergeben. Ein Dritter kann stets erst nachträglich gegen die Vergabe einer Domain unter Hinweis darauf vorgehen, daß die zugewiesene Kennzeichnung in sein Recht am eigenen Namen eingreift. Der Staat untersagt dem Domain-Inhaber dann die weitere Nutzung der Domain[12]. Allerdings weigert er sich, positiv zugunsten des Dritten in das Verteilungssystem der Vergabestellen einzugreifen[13]. Der Verletzer muß nämlich nicht die Domain an den Berechtigten übertragen; ihm soll bloß die Pflicht obliegen, die weitere Nutzung der streitgegenständlichen Domain zu unterlassen.

Die Kennzeichnungskraft einer Domain könnte sich allerdings reduzieren. Denn zu beachten ist zunächst die wachsende Bedeutung von Suchmaschinen, gerade für die virtuelle Identität eines Providers[14]. Bei der enormen Geschwindigkeit, mit der das world wide web (www) wächst, ist die Frage der Informationsrecherche drängend. Lost in cyberspace – das Gefühl, im www auf der Suche nach einer bestimmten Homepage verloren zu gehen, kann man nicht mehr durch Hinweis auf die bestehende Domain eines Providers in den Griff bekommen. Vielmehr gewährleisten zunehmend Suchmaschinen eine effiziente Informationsbeschaffung. Künftig werden sogar Intelligent Robots dem Nutzer jedwede Mühe bei der Suche nehmen; der Nutzer gibt nur noch allgemein an, zu welchen Themenbereichen er Informationen haben will und bekommt diese periodisch mundgerecht vom www-Roboter serviert. Diese Umwälzungen führen dazu, daß auch über die Kennzeichnungskraft einer Domain neu nachgedacht werden muß. Der Nutzer wird sich eventuell kaum noch einer Domain bedienen, um einen Provider zu finden. Er wird häufiger über Suchmaschinen und Roboter agieren, ohne daß die Domain dabei noch eine Rolle spielt.

II. Das Internet und die Deterritorialisierung des Rechts

Im Internet verlaufen sich alle Normen ins Nichts, die auf den Raum, das Territorium, den Sitz Bezug nehmen. Die elektronische Geschwindigkeit deterritorialisiert das Recht[15].

1. Problemfelder

Hier fallen zunächst die Vorschriften des internationalen Zivilprozeßrechts und des Kollisionsrechts auf. Diese verweisen, bedingt durch ihre Herkunft aus der Idee der Nationalstaatlichkeit im 19. Jahrhundert, sehr häufig auf lokale Bezüge. Dies ist z. B. bei der Anknüpfung an den Wohnsitz des Beklagten der Fall. Ähnliches gilt für Anknüpfungspunkte wie den Handlungs- und Erfolgsort bei Fragen des Deliktsrechts oder den Ort des Vertragsschlusses bei Verbrauchergeschäften. Aber auch andere Rechtsgebiete sind durch die Anknüpfung an territoriale Vorgegebenheiten geprägt. Zu verweisen ist hier auf den Betriebsstättenbegriff im Steuerrecht[16], der gerade in bezug auf das Internet zu kaum lösbaren Problemen führt.

Aber auch im Vertragsrecht führen räumliche Beziehungen in bezug auf das Internet häufig in die Irre. Zu denken ist vor allem an Verträge, die eine räumliche Beschränkung von Nutzungsrechten vorsehen, wie dies etwa bei Fernsehlizenzen oder Warenvertriebsverträgen typischerweise der Fall ist. Solche Vertragstypen bereiten unvorhergesehene Schwierigkeiten, wenn es um die Frage der Verwendung von Filmmaterial oder die Werbung für Produkte über das Internet geht.

Zum Problem wird die territoriale Anknüpfung ferner bei der Geltendmachung von Unterlassungsansprüchen. Diese sind traditionell darauf beschränkt, eine bestimmte Handlung auf dem Gebiet eines bestimmten Staates zu verbieten; ein Handlungsverbot, das über die Grenzen eines Staatsgebietes hinaus Wirksamkeit entfalten soll, wäre bereits aus völkerrechtlichen Gründen nicht durchsetzbar[17]. Dies würde allerdings für Rechtsverletzungen im Internet darauf hinauslaufen, daß die Geltendmachung von Unterlassungsansprüchen aus technischen Gründen unmöglich wird. Denn es ist derzeit für einen Provider unmöglich, den Abruf seines Angebotes für User aus einem bestimmten Staatsgebiet auszuschließen. Bezogen auf bestimmte Domains läßt sich zwar an eine Sperrung des Abrufs denken. Die Vielfalt gängiger Kennzeichnungssysteme macht jedoch eine Selektion unmöglich. Es lassen sich im Internet nicht Benutzergruppen auf territorialer Basis definieren; niemand weiß, ob sich hinter der Adresse hoeren@aol.com ein User aus Deutschland, den USA oder Malaysia verbirgt. Dies zwingt deutsche Gerichte dazu, Unterlassungsgebote weiter zu stecken als rechtlich zulässig. Verboten wird nicht nur die Abrufmöglichkeit in Deutschland, sondern das gesamte www-Angebot, selbst wenn dieses nach der Rechtsordnung anderer Staaten rechtlich zulässig sein sollte. Das *KG* hat als erstes deutsches Gericht

---

8) Vgl. hierzu auch die Thesen von *Druey*, Information als Gegenstand des Rechts, 1995, 441 ff.

9) Grdl. *Spinner*, Die Wissensordnung, 1994, insb. S. 111 ff.

10) Insofern sind auch die sehr innovativen Überlegungen von *Kloepfer* zur Reform der Datenschutzrechts nicht überzeugend. *Kloepfer* fordert in seinem Gutachten für den nächsten DJT die Verabschiedung eines Bundesdatengesetzes bzw. eines Informationsgesetzbuches, ohne daß die Eckdaten einer solchen Informationsordnung konkretisierbar wären.

11) Vgl. aus der neueren Literatur *Bettinger*, GRURInt 1997, 402 ff.; *Omsels*, GRUR 1997, 328 ff.; *Stratmann*, BB 1997, 689 ff.; *Ubber*, WRP 1997, 497 ff.; *Völker/Weidert*, WRP 1997, 652 ff.; *Wilmer*, CR 1997, 562 ff.

12) Die damit verbundenen kennzeichnungsrechtlichen Fragen werden sich nicht dadurch reduzieren lassen, daß künftig eine Reihe weiterer Top-Level-Domains genutzt werden können; diese neue Vergabepraxis führt nur zu einer Vervielfachung des Problems der genauen Zuordnung von Domain-Names. S. hierzu *Bettinger*, GRURInt 1997, 404 (420 f.), *Kur*, CR 1997, 325 ff.

13) So jedenfalls in der Krupp-Entscheidung *OLG Hamm*, MMR 1998, 214 m. Anm. *Berlit*, NJW-RR 1998, 909 = NJW-CoR 1998, 175 = CR 1998, 241 m. Anm. *Bettinger*. A. A. etwa *LG München I*, NJW-RR 1998, 973, CR 1997, 479; *LG Frankfurt a. M.*, MMR 1998, 151; *LG Düsseldorf*, CR 1998, 174.

14) S. hierzu auch *Wilmer*, CR 1997, 562 ff.

15) S. *Vief*, Digitales Geld, in: *Rötzer* (Hrsg.), Digitaler Schein, 1991, S. 117, 130.

16) Allg. hierzu *Vink*, in: *Albarda u. a.*, Caught in the Web, 1998, S. 58 ff.; *Lejeune u. a.*, European Taxation 1998, S. 2 ff.

17) Anders sieht dies allerdings die niederländische Rechtsprechung im Rahmen von De Corte Geding-Entscheidungen; s. hierzu *Brinkhof*, EIPR 1994, 360; *Gielen/Ebbink*, EIPR 1994, 243. Diese Rechtsprechung ist jedoch aktuell revidiert worden in der nicht veröffentlichten Entscheidung des *Berufungsgerichts Den Haag* vom 23. 4. 1998, Az: 97/1296 – Boston Scientific.

auf diese Problematik und auf das Dilemma der Justiz bei der Tenorierung von Unterlassungsansprüchen hingewiesen. Es sah sich gezwungen, eine weite Tenorierung vorzunehmen und www-Angebote weltweit zu untersagen[18].

2. Lösungsmöglichkeiten

Die Frage ist allerdings, wie das Recht auf die internetspezifische Deterritorialisierung reagieren soll. Das Territorialitätsproblem läßt sich vielleicht durch die Schaffung eines virtuellen Raums lösen. In diesem „Cyberspace" haben alle Beteiligten ihre eigene Netzidentität, die nur noch wenig mit dem Wohnsitz oder der Betriebsstätte zu tun hat[19]. Innerhalb dieses Raumes haben die Provider ihre Identität offenzulegen, wie dies in § 6 I MedienStV und § 6 TDG auch vorgesehen ist[20]. Dieser Offenbarungseid ist lediglich für die gerichtliche Geltendmachung von Ansprüchen notwendig. Denn auch im nächsten Jahrtausend werden wir nicht vermeiden können, daß Ansprüche mittels staatlicher Entscheidungs- und Vollstreckungsorgane durchgesetzt werden.

Ansonsten zählt aber das virtuelle Handeln der User. Insofern sollte auf alle Rechtsregeln verzichtet werden, die auf den Sitz, die Betriebsstätte oder den Wohnort eines Betroffenen abstellen. Dieser Verzicht wird sich vor allem im Kollisionsrecht und im Internationalen Zivilverfahrensrecht auswirken, wo immer schon territoriale Akzente bevorzugt worden sind. In diesen Bereichen würde den Gegebenheiten des Cyberspace am besten dadurch Rechnung getragen, daß auf das Marktortprinzip als einheitliche Anknüpfungsregel abgestellt wird. Das Marktortprinzip stammt aus dem Wettbewerbsrecht[21] und bemißt die Reichweite staatlicher Regeln danach, wo final in das Marktgeschehen eingegriffen wird. Wer sich für seine Werbung des Internets bedient, muß dies nur dann an deutschem Recht messen lassen, sofern sein Angebot auf den deutschen Markt gerichtet ist. Diese Regel wird inzwischen auch für das Strafrecht diskutiert[22]; sie ähnelt darüber hinaus dem amerikanischen Minimum-Contacts-Prinzip. Eine Anwendung des Prinzips im Immaterialgüterrecht ist bislang immer von der h. M. mit dem Hinweis abgelehnt worden, die Rechtsordnung könne ein Urheber- oder Markenrecht immer nur territorial, limitiert auf ein Staatsgebiet, zuweisen. Unausweichlich ist dann jedoch das Dilemma, daß der Provider wegen der weltweiten Abrufmöglichkeiten das Immaterialgüterrecht aller Rechtsordnungen kennen und beachten müßte[23].

III. Das Internet und die Extemporalisierung des Rechts

Aber auch zeitliche Bezüge werden durch das Internet ad absurdum geführt.

1. Problemfelder

Zu denken ist hier vor allem an § 130 BGB, der ein Widerrufsrecht bei zumindest gleichzeitigem Zugang der Widerrufserklärung vorsieht. Im Internet werden Bestellungen so schnell ausgeführt, daß dieses Widerrufsrecht insbesondere im Falle automatisierter Bestellsysteme de facto totläuft. Bei solchen Systemen dürfte kaum jemand in der Lage sein, einen Widerruf so schnell zu formulieren, daß er vor oder gleichzeitig mit der angegriffenen Willenserklärung zugeht.

Auch im Urheberrecht finden sich Ansätze einer Detemporalisierung durch das Internet. So versucht die deutschen Immaterialgüterrechtslandschaft schon seit langem, das mit Online-Diensten verbundene Phänomen der „sukzessiven Öffentlichkeit" dogmatisch in den Griff zu bekommen. Das Urheberrecht kennt unkörperliche Formen der Werknutzung nur in der Weise, daß dieses an eine Mehrzahl von Personen gleichzeitig wiedergegeben wird[24]. Typisch ist insoweit der Vorgang der Fernseh- und Radiosendung. Das Internet führt jedoch das Merkmal der Gleichzeitigkeit des Zugriffs ad absurdum. Abrufe erfolgen nicht mehr simultan, sondern sukzessiv. Überhaupt geht es beim Internet seltener um Verteil- als um Abrufdienste[25]. Man kann in dieser Situation versuchen, die traditionellen Regeln zur öffentlichen Wiedergabe analog auf Abrufdienste zu übertragen. Diese in Deutschland gängige Vorgehensweise ist jedoch durch die Entscheidung der internationalen Staatengemeinschaft obsolet geworden, ein eigenes Recht des „Making available to the public" in das Urheberrecht einzuführen[26]. Dadurch wird das Problem der Kategorisierung von Abrufdiensten gelöst; schon das Bereithalten von Informationen zum Abruf konstitutiert einen Eingriff in Verwertungsbefugnisse der Urheber und Leistungsschutzberechtigter[27]. Es werden aber Folgeprobleme auftauchen, etwa hinsichtlich der Abgrenzung von Öffentlichkeit und Nicht-Öffentlichkeit im sogenannten *Intra*net und der Integration des neuen Schutzrechts in das System urheberrechtlicher Schranken.

Das Phänomen der verlorenen Zeit macht auch vor dem Verbraucherschutzrecht nicht halt. Ein wichtiges Instrument des Verbraucherschutzes besteht im Zeitgewinn zugunsten des Verbrauchers. Dieser Übereilungsschutz wird vor allem durch die Einführung von Widerrufsrechten und den Zwang zur Beachtung der Schriftform gewährleistet (s. etwa § 766 BGB; § 4 VerbrKrG)[28]. Es hat sich allerdings sehr schnell gezeigt, daß das klassische Gespann Verbraucherkreditgesetz und Haustürgeschäftewiderrufsgesetz im wesentlichen nicht auf den elektronischen Handel Anwendung findet[29]. Die auftretenden Schutzlücken könnten allerdings ab dem Jahr 2000 durch die Umsetzung der Fernabsatzrichtlinie[30] geschlossen sein[31]. Genau diese Richtlinie zeigt jedoch das verbraucherschutzrechtliche Dilemma des Electronic Commerce. Zwar wird infolge der Richtlinie europaweit ein Widerrufsrecht für elektronische Bestellungen eingeführt (Art. 6 I 1 und 2), worüber der Verbraucher auch zu informieren ist (Art. 4 I lit. f). Für eine Reihe von Dienstleistungen werden jedoch Widerrufsrechte versagt, ohne daß Substitute entwickelt werden (Art. 3 I und II). Insofern ergeben sich aus der

---

18) *KG*, NJW 1997, 3321 – Concert Concept.

19) S. hierzu *Turkle*, Leben im Netz 1998, S. 9.

20) Vgl. zum MedienStV und zum TDG allg. *Bröhl*, CR 1997, 74 ff.; *Engel-Flechsig*, ZUM 1997, 234 ff.; *Hoeren*, Jahrb. f. Telekommunikation und Gesellschaft 1997, S. 133 ff.; *Koch*, NJW-CoR 1997, 302 ff.; *Roßnagel*, NVwZ 1998, 1 ff.

21) S. dazu *BGHZ* 113, 11 (15) = NJW 1991, 1054 – Kauf im Ausland; *OLG Karlsruhe*, GRUR 1985, 556 (557); *Kotthoff*, CR 1997, 676 ff.

22) *Hilgendorf*, NJW 1997, 1873 ff.

23) Die verschiedenen Lösungsansätze sind diskutiert bei *Hoeren/Thum*, ÖSGRUM 20 (1997), 78 ff. S. dazu auch *BGH*, MMR 1998, 35 m. Anm. *Schricker* – Spielbankaffäre.

24) S. *Schricker/v. Ungern-Sternberg*, UrhG, § 15 Rdnr. 30 m. w. Nachw. A. A. nur *LG Berlin*, Schulze LGZ 98, 5 zu § 11 II LUG, und *öst. OGH* in der Arpanet-Entscheidung.

25) Zu Differenzierungen s. *Hoeren*, CR 1996, 517 ff.

26) S. Art. 8 WIPO Copyright Treaty und darauf basierend Art. 3 I des Entwurfs zur Richtlinie für eine Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft vom 10. 12. 1997, KOM (97) 628 endg.

27) Hierzu auch von *Lewinski*, MMR 1998, 115 ff.

28) *Kemper*, Verbraucherschutzinstrumente, 1994, S. 220 ff.

29) Ausf. *Meents*, Verbraucherschutz und Internet, Diss. Münster 1998; *Waldenberger*, BB 1996, 2365 ff.

30) Richtlinie 97/7/EG des Europäischen Parlaments und des Rates v. 20. 5. 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABlEG Nr. L 144/19 v. 4. 6. 1997.

31) S. allg. zu dieser Richtlinie *Bodewig*, DZWiR 1997, 447 ff.; *Gößmann*, MMR 1998, 88 ff.; *Kröger*, in: *Albarda u. a.*, Caught in the Web, 1998, S. 29 ff.; *Martinek*, NJW 1998, 207; *Reich*, EuZW 1997, 581 ff.

Richtlinie eine Reihe von Schutzlücken für weite Bereiche des www.

Noch laxer wird mit dem Zeitproblem in der Diskussion um die elektronische Form umgegangen[32]. Es gehört schon fast zum Credo der Signaturszenerie, daß die durch das Signaturgesetz[33] eingeführten Anforderungen an die digitale Signatur elektronische Unterschriften zum funktionellen Äquivalent für die Handschrift machen[34]. In der Tat erfüllt eine digitale Signatur bei Beachtung der (allerdings sehr hoch angesetzten) Sicherheitsanforderungen die meisten Funktionen der Unterschrift, von der Abschluß- bis hin zur Echtheitsfunktion. Großzügig hinweggegangen wird dabei jedoch über den Verlust der Warnfunktion. Wer etwas handschriftlich zu unterzeichnen hat, wird durch diesen Vorgang deutlich darauf hingewiesen, daß er dabei ist, etwas Rechtserhebliches zu tun. Diese Warnung entfällt, wenn digitale Signaturen binnen Sekundenbruchteilen automatisiert generiert und verschickt werden. Asymmetrische Verschlüsselungstechniken dekonstruieren den zeitlichen Kontext; das Zeitmoment wird nur noch nachträglich im Absendeprotokoll vermerkt.

2. Lösungsansätze

Es zeigt sich, daß mit zunehmender Übertragungsgeschwindigkeit Rechtsregeln, die auf zeitliche Verzögerungen abstellen, ihre Basis verlieren. Dieser Verlust muß kompensiert werden; es bedarf in größerem Umfang der juristischen (Wieder-)Entdeckung der Langsamkeit. So ist z. B. bei der Substituierung der Schriftform durch elektronische Formäquivalente zu sichern, daß dem User eine Denkpause zuzubilligen ist, innerhalb derer er darüber reflektieren kann, ob er überhaupt eine Willenserklärung diesen Inhalts abgeben will. § 130 BGB ist durch ein Widerrufsrecht eigener Prägung zu ersetzen, das es dem Erklärenden gestattet, elektronische Bestellungen auch nach Zugang seiner Erklärung rückgängig zu machen. Die Fernabsatzrichtlinie sieht ein solches Widerrufsrecht für Verbraucher vor. Man müßte dies auf alle Erklärenden, unabhängig von ihrer Verbrauchereigenschaft, ausdehnen, um jedermann angesichts der Schnelligkeit des Nachrichtenübertragung im Netz eine Bedenkpause zu sichern.

IV. Selbstregulierung statt staatlicher Regulierung

Die verschiedenen Probleme bei der Rechtsdurchsetzung führen dazu, daß der Ruf nach Selbstkontrolle und Selbstregulierung im Internet sehr laut wird. Diese Diskussion verbindet sich auf eigentümliche Weise mit einer älteren Fragestellung, der von *Teubner* aufgerührten Frage nach der Selbstregulierung[35]. Diese Diskussion hatte sich eigentlich erledigt, da die verschiedenen Ansätze *Teubners* in der Literatur heftig kritisiert worden waren. Doch durch das Internet wittern die Vertreter der *Teubner*'schen Linie wieder Morgenluft. Sie sehen in den verschiedenen Formen der Verhaltensregulierung im Internet eine Bestätigung ihrer Theorie, daß staatliche Intervention durch Selbstregulierung ersetzt werden könne. Sie verweisen in diesem Zusammenhang auf die sogenannte Netiquette, die Benimmregeln im Internet, sowie auf die verschiedenen Ansätze zu einer freiwilligen Selbstkontrolle der Provider.

Allerdings wird dabei wenig beachtet, daß es „die" Netiquette gar nicht gibt[36]. Die einzelnen Diensten verfügen über eigene Verhaltensregeln, die je nach Gruppe unterschiedlich definiert sind. Texte reichen in ihrer Lage von zehn Zeilen bis zu 40 Seiten. Gleiches gilt für die Idee der freiwilligen Selbstkontrolle. Die unterschiedlichen Selbstkontrolleinrichtungen benutzen verschiedenste Regelwerke mit spezifischen Inhalten. Ungeklärt ist weiterhin auch die Effektivität der Selbstkontrolle, deren Sanktionsmechanismen nicht an staatliche Durchsetzungsregeln anknüpfen können. Der Versuch, sie als Ausdruck einer besonderen Berufsstandesvergessenheit über § 1 UWG zu qualifizieren, dürfte gescheitert sein, da es eine den freien Berufen vergleichbare Homogenität der Internetnutzer nicht gibt. Abseits vertraglicher Bindungen scheitert damit eine staatliche Durchsetzung von Internet-Selbstkontrolle. Erst wenn Verhaltensregeln vertraglich, etwa durch Vereinbarung zwischen Access Provider und User, verbindlich gemacht werden, kommt eine Sanktionierung in Betracht.

In diesem Falle ist aber die Frage nach der Rechtskonformität solcher Selbstverpflichtungen zu klären. Diese stellt sich vor allem hinsichtlich der Inhaltskontrolle nach dem AGB-Gesetz. Wenn zum Beispiel über die AGB dem User der Erhalt von Werbung untersagt wird, stellt sich sofort die Frage nach der Vereinbarkeit mit § 3 AGB-Gesetz[37]. Die Nutzung von Maildiensten für das Anfordern von Werbung ist – anders als der Fall unerwünschter Werbemails[38] – legal; jeder Nutzer kann sich über das Netz, die Werbung zuschicken lassen, die er will und wünscht. Es dürfte daher für den Internet-Nutzer höchst überraschend sein, mit einem Access-Provider „freie Fahrt" im Internet zu vereinbaren, um dann aber festzustellen, daß ihm der Provider den Zugriff auf erwünschte Werbemails verweigern will.

Auch kartellrechtlich ist die Legitimität der Selbstkontrolle ungeklärt. Das Legitimationsdefizit ist am eklatantesten bei der Verteilung von Domains über die NIC-Organisationen[39]. Eine staatliche Legitimation fehlt und soll auch zukünftig nicht geschaffen werden. Vielmehr agieren diese Verteilungsorganisationen im luftleeren Raum, in dem sich dementsprechend auch die vergebenen Namen bewegen. Auch für die Frage der Verhaltenskodices – etwa im Jugendschutzbereich – stellt sich die Frage, wieso gerade private Provider in größerem Umfang Verhaltensbeschränkungen vorsehen und regulieren können. GWB und Art. 85 EGV lassen Verhaltenskodices mit wettbewerbsbeschränkendem Inhalt nur zu, sofern diese geltendes, EU-konformes Lauterkeitsrecht wiederholen und konkretisieren. Verhaltenskodices, die den Marktauftritt eines Providers einschränken, stehen daher mit einem Bein im kartellrechtlichen Grab. Sofern sie ein Verhalten unterbinden wollen, das sich nachträglich als lauterkeitsrechtlich irrelevant und neutral erweist, verstoßen sie gegen § 1 GWB bzw. Art. 85 EGV.

Aber auch die Frage der Sanktionierbarkeit schafft Probleme. Zunächst fragt sich, wie ein Verstoß gegen die Netiquette geahndet werden kann. Sofern deutsche Gerichte die Einhaltung etwa über § 1 UWG sichern, ist eine Durchsetzung auf nationaler Ebene gewährleistet. Die internetimmanente Deterritorialisierung führt jedoch zu Vollstreckungsproblemen im Verhältnis zum Ausland. Setzt sich ein Provider ins Ausland ab, kann er geschickt Vollstrek-

---

32) Vgl. *Bizer/Hammer*, DuD 1993, 619 ff.; *Ebbing*, CR 1996, 271 ff.; *Heun*, CR 1995, 2 f.; *Kilian*, DuD 1993, 607 ff.; *Pordesch/Nissen*, CR 1995, 562 ff.

33) Das Signaturgesetz ist Teil des IuKDG, s. BGBl I, 1870. S. dazu auch *Roßnagel*, NVwZ 1998, 1 (5 ff.); *ders.*, DuD 1997, 77 ff.; *ders.*, MMR 1998, 75 ff.

34) A. A. *Erber-Faller*, CR 1996, 375 (378 f.). Gescheitert ist der Versuch des Bundesjustizministeriums, das Problem der Schriftform durch Einführung einer elektronischen Textform zu lösen: s. den Entwurf eines Gesetzes zur Änderung des Bürgerlichen Gesetzbuches und anderer Gesetze vom 31. 1. 1997 – BMJ 3414/2 (unveröff.).

35) *Teubner*, Recht als autopoietisches System, 1989; *ders.*, ARSP 1982, 13 ff. Zur Kritik an *Teubners* Ansatz s. *Habermas*, Faktizität und Geltung, 1992, S. 69 f.; *Tonner*, KritJ 18 (1983), 107 ff.

36) Diese These ist ausführlicher begründet worden bei *Hoeren*, in: *Bekker* (Hrsg.), Rechtsprobleme internationaler Datennetze, 1996, S. 35 ff.

37) S. hierzu auch *US District Court for the Eastern District of Pennsylvania*, D. C. Epa, CA No. 96 CV-2486, 9/4/96, Cyper Promotions v. AOL; s. hierzu BNA Electronic Information Policy Report 1 (1996), 519.

38) So auch *LG Traunstein*, MMR 1998, 53 = NJW-CoR 1997, 497. Ähnl. inzwischen *Ernst*, BB 1997, 1057 (1060); *Schmittmann*, DuD 1997, 636 (639); *Schrey/Westerwelle*, BB 1997, Beil. 18, S. 17; *Ultsch*, DZWiR 1997, 466 (470); a. A. nur *Reichelsdorfer*, GRUR 1997, 191 ff.

39) Zu den damit verbundenen kartellrechtlichen Problemen s. *Nordemann*, NJW 1997, 1891 ff.

kungsoasen benutzen, um sich jedweder Rechtsdurchsetzung zu entziehen. Mit dem Scheitern staatlicher Rechtsdurchsetzung erhöht sich auch der Ruf nach einer privaten Rechtsdurchsetzung über eigene Verfahrensregeln. Zu denken ist hier an die alte amerikanische Diskussion um Alternative Dispute Resolutions (ADR). In den USA wird parallel auch über die Einführung einer Internetsgerichtsbarkeit und eines Schiedsverfahrens im Internet nachgedacht. Allerdings ist die Diskussion nie über das Nachdenken hinaus gekommen. Ernsthafte Ansätze zur Etablierung solcher virtueller Entscheidungsgremien sind nicht bekannt. In der Tat dürfte die Einrichtung von Internet Courts auch nichts an der Vollstreckungsproblematik ändern. Denn anders als staatliche Gerichte, die zumindest eine Vollstreckung im nationalen Kontext und im Rahmen internationaler Abkommen gewährleisten, sind Entscheidungen der Internet-Courts nicht vollstreckungsfähig. Insbesondere handelt es sich regelmäßig nicht um Schiedsgerichte i. S. von §§ 1041 ff. ZPO. Hinzu kommt, daß die Beachtung von Entscheidungen eines Internetgerichts nicht (mehr) auf dem Common Sense der Web Community beruht. Die Gemeinschaft der Internetbenutzer hat sich verändert, ist zunehmend inhomogen, löst sich von den alten Zeiten universitärer Forschung. Im Zeitalter des Elektronic Commerce ist der elegante ADR-Weg für das Internet indiskutabel.

Vorbei ist damit aber auch die Durchsetzung über technische Mittel. Am bekanntesten dürfte das Beispiel des Mail-Bombing sein, das insbesondere häufig im Kampf gegen unerwünschte E-Mail-Werbung verwendet wird. Der Nutzer überschüttet den Provider mit einer Flut elektronischer Schmähbriefe. Dieser Vorgang kann dazu führen, daß der Provider wegen Überlastung seinen Internetzugang nicht mehr nutzen kann. Allerdings muß sich die Vereinbarkeit eines solchen virtuellen Faustrechts mit geltendem Recht erst noch zeigen. So erweist es sich als besonders schwierig, die Sanktionen in einer rechtskonformen Weise zu gestalten. Boykottaufrufe, etwa in der Form des Mail-Bombing, wecken Erinnerungen an die Rechtsprechung des *BGH* zur Boykottfrage, in der der *BGH* Aktionsaufrufe als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb qualifiziert hat[40].

V. Technik statt Recht

Die soeben erwähnte Facette der Diskussion führt zu einer grundlegenderen Beobachtung: Vielleicht liegt die Antwort auf die Maschine ja in der Maschine[41]. Eine Reihe schwieriger juristischer Fragestellungen könnten im Internet vielleicht durch Einsatz bestimmter technischer Verfahren obsolet werden. Zu denken ist hier an Digital Watermarking Techniques und Digital Fingerprints[42]. Diese Verfahren gewährleisten, daß der Inhaber von Rechten eindeutig festgestellt werden kann und Pirateriefälle ebenso einfach verfolgt werden können. Ähnliches gilt für kryptographische Verfahren, die gerade im Zusammenhang mit der Diskussion über die digitale Signatur einen enormen Boom erleben[43].

Allerdings stellt sich die Frage, wie solche technischen Verfahren selbst wiederum innerhalb der Rechtsordnung anzusiedeln sind. Die Technik als solche ist nur ein Faktum, das als solches aus sich heraus noch keine Legitimität beanspruchen kann. So wäre es gefährlich, wenn man die Umgehung jedweden Kopierschutzes als illegal qualifizieren würde. Denn der Kopierschutz kann ja durchaus von jemandem angebracht worden sein, dem seinerseits die Rechtsstellung eines Berechtigten fehlt; die Umgehung von Sicherungsmaßnahmen, die ein Softwarepirat vorgenommen hat, kann nicht verboten sein. Das Legitimationsdefizit technizistischer Modelle wird besonders eklatant bei der digitalen Signatur[44]. Das Signaturgesetz wird allerorts vielgepriesen, kombiniert es doch sehr extensive technische Zertifizierungsanforderungen mit einem marktwirtschaftlich orientierten Institutionenmodell[45]. Diese Verknüpfung läuft allerdings zweifach fehl. Zum einen sind die technischen Sicherheitsanforderungen für die Zertifizierung so hoch angesiedelt, daß fast kein Unternehmen diese auch nur ansatzweise erfüllen kann. Dies mag man innerhalb Deutschlands noch hinnehmen. Im internationalen Kontext wird diese Ansatzweise als diskriminierendes Zugangshindernis abgelehnt werden, zumal Deutschland mit seinen hohen Anforderungen weltweit alleine steht. Die Europäische Kommission wird dieser Umstand jedoch nicht ruhen lassen. Solange nicht ein europaweit akzeptables Marktmodell für Zertifizierungsstellen vorliegt, wird die Zukunft des deutschen Signaturgesetzes ungewiß sein.

Als noch problematischer erweist sich jedoch das Institutionenmodell des Signaturgesetzes. Schon für den Bereich des Electronic Commerce ist die Zuweisung von Zertifizierungsaufgaben an privatrechtlich organisierte Einrichtungen kritisiert worden; fast wäre das Signaturgesetz im Bundesrat daran gescheitert[46]. Losgelöst von dieser Frage ist bislang aber die Anwendbarkeit des Signaturgesetzes im Bereich der öffentlichen Verwaltung nicht bedacht worden. Es wird künftig möglich sein, daß ein privates Unternehmen die Ausstellung eines Führerscheins zertifiziert oder die Ausstellung eines Strafbefehls durch eine Behörde bestätigt. Dies ist meines Erachtens problematisch. Bislang bezog die Hoheitsverwaltung ihre Legitimität immer aus sich selbst; die Identität des Ausstellers eines Verwaltungsaktes wurde immer nur innerhalb des Systems des Verwaltungsorganisationsrechts verifiziert. Doch im digitalen Kontext bestätigen Private (partiell) die Wirksamkeit von hoheitlichen Verfügungen; quelle surprise.

VI. Electronic Commerce und das Problem des Trust

Die zentrale Weichenstellung hinsichtlich des Electronic Commerce wird die Frage des Trust sein[47].

1. Vertrauen im „analogen" Bereich

Verträge schließt nur derjenige, der darauf vertrauen kann, daß der Vertrag auch von der anderen Seite erfüllt wird. Ein solches Vertrauen besteht, wenn beide Parteien schon in einer längerfristigen Geschäftsbeziehung stehen und von daher keine Bedenken hinsichtlich der Vertragserfüllung bestehen. Schwierigkeiten bestehen jedoch bei neuen Geschäftsbeziehungen. Abseits des allgemeinen Problems der Zahlungsfähigkeit und -bereitschaft muß sich jede Vertragspartei erst einmal darüber vergewissern, wer die andere Seite ist und wie die Erklärung der anderen Seite zu verstehen ist. Die Gewährleistung der Identität und Authenzität erfolgt im „analogen" Leben über den persönlichen Kontakt oder durch Beachtung der Schriftform. Bei Vertragsverhandlungen unter Anwesenden weiß jede Seite, mit wem sie es zu tun hat und welchen Inhalt die Willenser-

40) Vgl. *BGH*, DB 1965, 889; NJW 1998, 377.

41) S. hierzu *Hoeren*, Law, Computers and Artificial Intelligence 4 (1995), 175 ff.

42) Dazu *De Selby*, ACM Management Review 1997, 467 ff.

43) S. dazu Imprimatur, The Law and Practice of Digital Encryption, Amsterdam 1998.

44) *Roßnagel*, NJW-CoR 1994, 96 ff.; *Bieser*, CR 1996, 566 ff.

45) Vgl. *Timm*, DuD 1997, 525 (528); *Rieß*, DuD 1997, 284 (285); *Hohenegg/Tauschek*, BB 1997, 1541 ff.

46) S. BT-Dr 13/7385, S. 57 ff. und BR-Dr 420/97.

47) S. hierzu *Khare/Rifkin*, Weaving a Web of Trust, in: World Wide Web Journal, Summer 1997, 77 ff.

klärungen ausgetauscht worden sind (s. § 147 I BGB). Die Schriftform gewährleistet zumindest eine gewisse Authenzität der Nachricht; hinsichtlich der Person des Erklärenden kann sich Gewißheit mittels Einschaltung eines Notars verschafft werden (§§ 128, 129 BGB).

2. Trust und digitale Signatur

Diese vertrauensbildenden Maßnahmen entfallen auf lange Sicht im Internet. Die Parteien kennen einander nicht, begegnen sich nur digital. Es fehlen persönliche Kontakte ebenso wie die Möglichkeiten zur Absicherung über die Schriftform (s. o.). Von daher weiß bei elektronischen Bestellungen niemand, ob wirklich derjenige bestellt hat, der sich als Besteller ausgibt. Auch der Inhalt einer Bestellung kann auf dem langen Internet-Weg zum Erklärungsempfänger aufgefangen und umgestaltet worden sein. In dieser Notlage sollen asymmetrische Verschlüsselungstechniken Abhilfe schaffen, die in Form der digitalen Signatur die Identität und Richtigkeit des Erklärenden sichert, bei Verschlüsselung mittels des öffentlichen Schlüssels gegen unbefugte Einsicht schützt.

Doch wer gewährleistet, daß eine verschlüsselte Nachricht wirklich von demjenigen stammt, der den Text unter einem bestimmten Namen erstellt hat? Hier verweist das Signaturgesetz darauf, daß die Identität des Absenders von der Zertifizierungsstelle gewährleistet wird (§ 5 I SigG). Die Zertifizierungsstelle soll insoweit die Rolle des Notars übernehmen. Doch die Zertifizierungsstellen sind privatrechtlich organisiert. Jedermann kann eine solche Stelle aufbauen, nach künftigen Plänen der Europäischen Kommission sogar ohne gesonderte Zulassung. Es stellt sich daher die Frage nach den hinreichenden Bedingungen für „Trust" im Hinblick auf Zertifizierungsstelle. Oben wurde bereits darauf hingewiesen, daß ein solches Vertrauen dort an Grenzen stößt, wo hoheitliches Handeln durch private Stellen zertifiziert werden soll. Für den Bereich der Privatwirtschaft wird die Vertrauensfrage über die von der Zertifizierungsstelle zur Verfügung zu stellende Sicherheitsinfrastruktur gelöst. Ein möglichst hohes Niveau an Sicherheitstechnik soll vertrauensbildend wirken und gewährleisten, daß die Schlüssel stets eindeutig einer bestimmten Person zugewiesen und Daten für Zertifikate nicht unbemerkt verändert werden können.

Doch diese Vorgehensweise hat ihre Tücken: Zum einen wird der hohe Sicherheitsstandard von anderen europäischen Staaten als übertrieben angesehen und von der Europäischen Kommission als wettbewerbsfeindlich abgelehnt. Insofern wird es europäisch zu einer Absenkung des Schutzniveaus kommen, die die Frage nach „Trust" wieder aufleben läßt. Zum andern kann schon methodologisch Vertrauen in Technik nicht durch Technik selbst begründet werden. Sobald sich die Technik weiterentwickelt, wird das Vertrauen in bestehende Verschlüsselungstechniken hinfällig. Jetzt als sicher erachtete Kryptographieverfahren können sehr schnell obsolet werden; dann fragt sich, was mit den bisher vergebenen Schlüsseln geschieht. Meines Erachtens hat der Gesetzgeber deshalb gut daran getan, den Beweiswert digitaler Signaturen nicht festzuschreiben. Denn eine digitale Signatur hat keinen feststehenden Beweiswert; dieser variiert intertemporal[48].

Von daher sollte durch Augenscheins- und Sachverständigenbeweis im Einzelfall geklärt werden, welchen Einfluß die jeweils verwendeten Verfahren auf die Beurteilung des Beweiswerts eines digital generierten und übermittelten Dokuments haben[49]. Daneben ist zu beachten, daß sich für die Zertifizierungsstellen ihrerseits die Frage nach der Identität stellt. Hier kann nur auf das Wurzel-Zertifikat der Regulierungsbehörde verwiesen werden, die sozusagen über den „Meta-Schlüssel" verfügt (§ 4 V SigG). Der öffentliche Schlüssel der Regulierungsbehörde wird wiederum zur Gewährleistung seiner Integrität im Bundesanzeiger veröffentlicht. Dies zeigt, daß am Ende der Zertifizierungskette doch wieder das gute, alte Papier steht. Doch dieser nostalgische Blick trügt. Denn die Europäische Kommission plant den völligen Verzicht auf jedwede Schlüsselhierarchie[50]. Jedermann soll ohne Zulassung eine Zertifizierungsstelle errichten können und nur repressiv über die Haftung bei Mängeln in die Verantwortung gezogen werden. Es fragt sich, wie auf diese Weise „Trust" vermittelt werden soll, zumal eine Zertifizierungsstelle jederzeit durch Wahl einer geeigneten Rechtsform das Haftungsrisiko minimieren kann.

VII. Zusammenfassung

Die bisherigen Überlegungen lassen sich wie folgt zusammenfassen:

1. Das Internet wirft keine spezifischen, nur auf das Netz selbst beschränkten Rechtsprobleme auf. Vielmehr steht das Internet selbst nur als Spitze des Eisbergs für die allgemeine Frage nach einer Wissensordnung und den Spezifika einer Informationsgerechtigkeit. Hinter dem Internet wölbt sich der Zenit des Informationsrechts.
2. In der vielbeschworenen Informationsgesellschaft entstehen eine Reihe neuer Vermögensgüter, die sich einer rechtlichen Beurteilung nach Maßgabe bisheriger Klassifizierungsversuche entziehen. Zu diesen Property Rights zählen u. a. die Information und (noch) die Domain.
3. Das Internet führt zu einer Dematerialisierung, Deterritorialisierung und Extemporalisierung des Rechts, das damit seine aus dem römischen Recht ererbten Substrate (Sache, Raum, Zeit) verliert. An deren Stelle tritt der virtuelle „Raum" und die Entdeckung der Langsamkeit.
4. Selbstkontrolle kann im Internet das Recht ergänzen, jedoch niemals ersetzen. Gerade die kartellrechtlichen Fragen rund um die Durchsetzung privater Verhaltensregeln bedürfen genauerer Klärung.
5. Technik kann niemals Technik legitimieren. Deshalb erweist sich die Frage nach „Trust", dem Vertrauen in die Integrität und Authenzität elektronischer Texte, als fast unlösbar.

---

48) S. dazu §§ 17 II, 18 der am 1. 11. 1997 in Kraft getretenen Signaturverordnung (SigV), wonach die Sicherheitsanforderungen jährlich sowie bei Bedarf neu zu bestimmen und bei Nichteignung neue digitale Signaturen zu erteilen sind.

49) Um so erstaunlicher ist es, daß nach dem italienischen Signaturgesetz jedwede digitale Signatur privat- und verwaltungsrechtlich als vollwertiges Äquivalent zu Unterschriften unter Papierdokumenten angesehen wird.

50) S. den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen vom 13. 5. 1998, KOM (1998) 297 endg. Eine zusammenfassende Darstellung des Entwurfs findet sich in MMR 6/1998, S. V, m. Anm. *Roßnagel* und *Geis*.