HANS-BREDOW-INSTITUT
für Medienforschung an der Universität Hamburg

Lutz Schreiber

Digitale Signaturen im Rechtsverkehr

Dezember 1999

Arbeitspapiere des Hans-Bredow-Instituts Nr. 4

Arbeitspapiere des Hans-Bredow-Instituts Nr. 4

Schreiber: Lutz: Digitale Signaturen im Rechtsverkehr, Hamburg: Verlag Hans-Bredow-Institut 1999

ISSN 1435-9413

ISBN 3-87296-089-X

Schutzgebühr: 10,- DM

Die Hefte der Schriftenreihe "Arbeitspapiere des Hans-Bredow-Institut" finden sich zum Download auf der Website des Instituts unter der Adresse

www.hans-bredow-institut.de/service/abpapiere/

Hans-Bredow-Institut für Medienforschung an der Universität Hamburg

Verlag

Heimhuder Str. 21

D-20148 Hamburg

Tel.: (+49 40) 450 217-12

Fax: (+49 40) 450 217-77

E-Mail: verlag@hans-bredow-institut.de

Inhalt

A) Einleitung

Die immer rascher fortschreitende Entwicklung der Informations- und Kommunikationsdienste eröffnet neue Möglichkeiten des Informationsaustauschs und der wirtschaftlichen Betätigung. Dabei genießt insbesondere der Electronic Commerce die Aufmerksamkeit von privatwirtschaftlichen Unternehmen, welche darin einen neuen Absatzmarkt für ihre Produkte und Dienstleistungen zu finden suchen. Aber auch Verwaltungen versuchen, ihre Behördenstruktur im World-Wide-Web abzubilden, um eine zusätzliche Schnittstelle zum Bürger durch ein virtuelles Rathaus zu etablieren. Dabei soll neben Kommunikation auch Partizipation entscheidendes Element bürgernaher Online-Verwaltung sein. Schließlich eröffnen sich Möglichkeiten zu einer internen Verwaltungsbeschleunigung und Straffung und Vereinfachung von Ablaufprozessen.

Rechtlich relevante Vorgänge wie Warenbestellungen, Zahlungsanweisungen, Anträge oder Einsprüche bei Behörden, die in der Vergangenheit über Papier abgewickelt wurden, können bereits vielfach auch elektronisch durchgeführt werden, oder erfahren gerade ihre Integration in ein solches Online-Angebot. Elektronisch übertragene oder gespeicherte Daten sind jedoch in besonderem Maße anfällig für Manipulationen durch Dritte oder Fehler im Dokumentenmanagement. In diesem Zusammenhang sichert die digitale Signatur die Integrität und Authentizität elektronischer Nachrichten. Diese entscheidenden Faktoren für eine sichere und vertrauensvolle Kommunikation werden durch das Signaturgesetz des deutschen Gesetzgebers rechtlich abgesichert. Als Ziel wurde ein administrativer Rahmen definiert, bei dessen Einhaltung digitale Daten als sicher vor Verfälschung gelten können (Integrität) und einer bestimmten Person eindeutig zuzuordnen sind (Authentizität).

Das Signaturgesetz wurde als Art. 3 des Informations- und Kommunikationsdienstegesetzes (IuKDG) am 22.7.1997 verkündet und trat am 1.8.1997 in Kraft.[1] Die Signaturverordnung (SigV), welche das SigG konkretisiert, wurde am 8.10.1997 von der Bundesregierung beschlossen und trat am 1.11.1997 in Kraft. Durch das Signaturgesetz wurden jedoch keine Regelungen hinsichtlich der rechtlichen Behandlung elektronischer Dokumente getroffen. Es enthält keine Aussagen über ihre rechtlichen Wirkungen. Zweck des Signaturgesetzes ist es, eine Sicherheitsinfrastruktur zu etablieren, unter deren Voraussetzungen die Sicherheit in der Verwendung digitaler Signaturen gewährleistet werden kann, um in einem nächsten Schritt die Umsetzung digitaler Signaturen in die Rechtsordnung zu ermöglichen.[2]

Daher bedarf es einer grundsätzlichen Auseinandersetzung elektronischer Dokumente unter Berücksichtigung digitaler Signaturen, um eine Einordnung digitaler Daten im Rechtsverkehr vornehmen zu können. Dabei sind aber nicht nur nationale Regelungen zu berücksichtigen, sondern aufgrund des globalen Charakters auch auf internationaler

---

1 Zur Entstehungsgeschichte des Signaturgesetzes, vgl. Roßnagel/Roßnagel, Einleitung SigG, Rn. 41 ff.

2 BT-DrS 13/7385, S. 26.

Ebene entstehende Regelwerke zu beachten. Namentlich sind hierbei die EU-Richtlinie über elektronische Signaturen und den Electronic Commerce in die Untersuchung einzubeziehen.

Die nun folgende Darstellung setzt sich mit der digitalen Signatur im Rechtsverkehr auseinander. Dabei werden die verschiedenen Auffassungen von Literatur und Rechtsprechung berücksichtigt. Die zunehmende Verbreitung der Telematik führt zu einer Anwendung der neuen Techniken in Bereichen, die vom Gesetzgeber bisher nicht hinreichend berücksichtigt werden konnten. Es ergeben sich daher Reibungspunkte zwischen virtueller Realität und rechtlicher Wirklichkeit.

B) Digitale Signatur

Zur Verständlichkeit der Problematik hinsichtlich des Einsatzes digitaler Signaturen im Rechtsverkehr ist es hilfreich, die Funktionsweise zu verstehen und die Einsatzmöglichkeiten digitaler Signaturen zu kennen.[3] Gleichzeitig sollen mögliche Sicherheitsrisiken und Angriffspunkte berücksichtigt werden.

I. Funktionsweise

1) Asymmetrisches Signaturverfahren

Unter einem digitalen Signatursystem versteht man ein algorithmisches Verfahren, welches mit Hilfe eines „privaten Signierschlüssels“ dem Autor einer Nachricht erlaubt, diese digital zu unterzeichnen und dem Empfänger dieser Nachricht gestattet, mit einem „öffentlichen Signierschlüssel“ die Unterschrift zu verifizieren. Aufgrund der Verknüpfung von geheimem privaten und öffentlichem Signierschlüssel wird es als asymmetrisches Verfahren bezeichnet.

Eine digitale Signatur ist ein Kryptogramm[4], welches einer elektronischen Nachricht beigefügt wird, um die Authentizität, Integrität und Beweisfähigkeit dieser Nachricht sicherstellen zu können. Der Autor berechnet mit Hilfe seines privaten Signierschlüssels einen digitalen Authentikator seiner Nachricht. Dabei ist der Begriff des Schlüssels nicht wörtlich zu verstehen, sondern lediglich Bezeichnung eines mathematischen Algorithmus. Vor einer Versendung oder Archivierung werden mit Hilfe einer sog. „Hashfunktion“ (einem mathematischen Verfahren) aus einer Nachricht ihre unverwechselbaren Bestandteile extrahiert und ein sog. Hashwert H (T) (vergleichbar einer Quersumme) ermittelt.[5] Dieser ist eine Art „Fingerabdruck“ des digitalen Dokuments (auch „Faltung“ genannt).

---

3 Siehe hierzu auch Bieser/Kersten, Elektronisch unterschreiben; zu den Begriffsbestimmungen des Signaturgesetzes siehe Schlechter, K&R 1998, S. 147, 148f; Schindler, K&R 1998, S. 433 ff.

4 Zu den Unstimmigkeiten der Bezeichnung der digitalen Signatur als Siegel im Signaturgesetz vgl. Roßnagel, Jahrbuch Telekommunikation und Gesellschaft 1999, S. 212 ff.

5 Zur Sicherheit von Hashfunktionen vgl. Dobbertin, Digitale Fingerabdrücke, DuD 1997, 82 ff.

Er wird danach mit einem einzigartigen unfälschbaren Signaturalgorithmus verschlüsselt und der Nachricht beigefügt. Verschlüsselt wird demnach nicht die Nachricht selbst, sondern nur ihr Hashwert. Dies hat praktische Gründe zur Einsparung von Speicherplatz, Rechen- und Übertragungszeit. Die Nachricht bleibt in unveränderter Form bestehen und mithin bei einer Übertragung für jedermann lesbar. Zwar kann diese Nachricht auch noch verschlüsselt werden, die gängigen Systeme zur Signierung elektronischer Nachrichten bieten solche Möglichkeiten an, Kryptosysteme werden aber nicht durch das SigG geregelt und sollen nach Ansicht der Bundesregierung auch in absehbarer Zeit nicht reguliert werden.[6]

Zur Nachprüfung einer digitalen Signatur wird das Kryptogramm mit einem dem privaten Schlüssel zugeordneten öffentlichen Prüfschlüssel entschlüsselt und dieser Hashwert S (H(T)) damit wieder „sichtbar" gemacht. Nur mit dem öffentlichen Schlüssel ist eine Entschlüsselung des Kryptogrammes möglich. Die Zuordnung des öffentlichen Schlüssels an eine bestimmte Person und damit die Sicherung der Authentizität des Dokumentes wird durch eine Zertifizierungsinstanz sichergestellt, welche private Schlüssel u.a. auch selbst herstellt und sich die Identität vom Signierenden im Zuge dieses Verfahrens bestätigen lässt. Danach bestätigt sie diese Zuordnung mit einem Zertifikat, welches mit einer Signatur der Zertifizierungsinstanz versehen wird. Aufgrund der Zuordnung kann auf den Inhaber des privaten Schlüssels und mithin auf den Autor geschlossen werden.

Der öffentliche Schlüssel zur Prüfung der Signatur wird mit dem Dokument mitgeschickt oder kann von einem Schlüsselverzeichnis einer Zertifizierungsinstanz heruntergeladen werden. Danach wird auf Seiten des Prüfenden ebenfalls ein Hashwert H (T) mit derselben Funktion erzeugt. Dieser Fingerabdruck H (T) wird mit dem gesendeten und mittlerweile entschlüsselten Hashwert S (H(T)) verglichen und die Integrität des Dokumentes ermittelt. Nur bei Übereinstimmung der beiden Werte kann von ein und demselben Dokumententext ausgegangen werden.[7] Sollten die Werte nicht übereinstimmen, ist die Prüfung fehlgeschlagen und die Integrität bzw. Authentizität des Dokumentes nicht sichergestellt.

Dies kann verschiedene Ursachen haben. Der öffentliche Schlüssel könnte der falsche, das Dokument nach dem Signiervorgang verändert oder die Übermittlung fehlerhaft gewesen sein. Eine Identifikation des Fehlers kann durch den Prüfvorgang nicht vorgenommen werden.

---

6 Eckpunkte deutscher Kryptopolitik, Pressemitteilung des Bundesministeriums des Innern und des Bundesministeriums für Wirtschaft und Technologie vom 2. Juni 1999.

7 Zu den Ausnahmen und Fehlerquellen, die eine Authentifizierung und Überprüfung positiv ausfallen lassen, obwohl die Dokumente verändert wurden oder aber im Nachhinein etwas anderes anzeigen, als der Aussteller auf seinem Bildschirm visualisiert hatte, vgl. Fox, DuD 1998, S. 386ff; Pordesch, DuD 1993, S. 561 ff; Bizer/Hammer, DuD 1993, S. 689 ff; zum Interpretationsproblem verschiedener Dateiformate vgl. auch Roßnagel/Pordesch, § 14 SigG, Rn. 184.

Für die Sicherung der Identität sind verschiedene Faktoren unumgänglich - die Einzigartigkeit und Fälschungssicherheit des privaten Schlüssels[8], eine gesicherte Zugangskontrolle zum privaten Signierschlüssel und die Richtigkeit der Zuordnung von Schlüssel und Person. Erst wenn diese Faktoren als sicher eingestuft werden können, kann die Richtigkeit der Identität unterstellt werden.

Digitale Signaturen im Rechtsverkehr

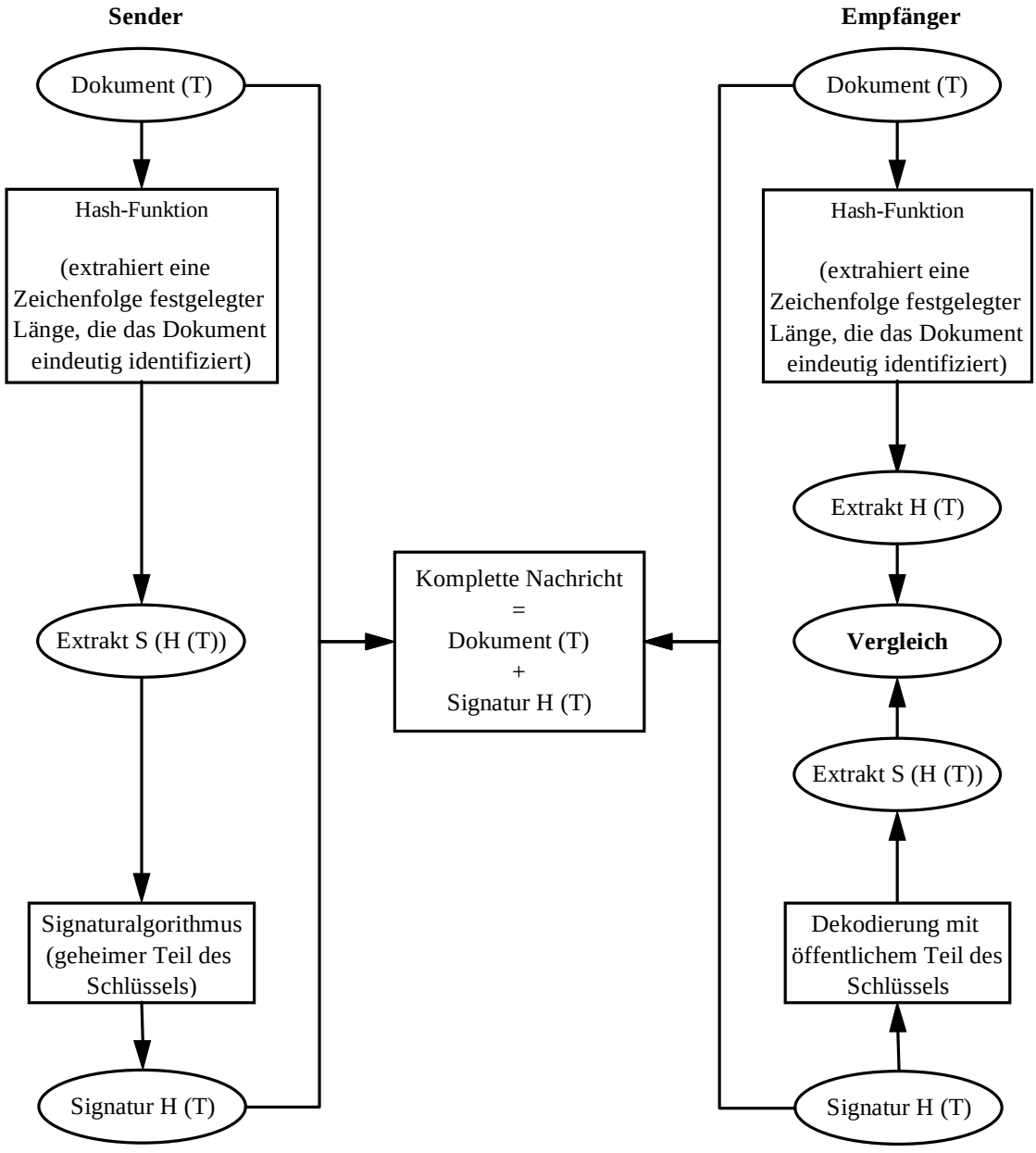

Abbildung: Skizze der Wirkungsweise einer digitalen Signatur; aus Rüßmann, Jur-PC, S. 3212, 3218

8 Vgl. hierzu D. Fox, Fälschungssicherheit digitaler Signaturen, DuD 1997, 69 ff.

2) Zeitstempel

Bei der Versendung elektronischer Dokumente bekommt der Versender in der Regel keine Rückmeldung, wann seine Nachricht bei dem Empfänger eingegangen ist bzw., ob dieser die Nachricht überhaupt erhalten hat. Umgekehrt bekommt der Empfänger durch die Nachricht keine Auskunft darüber, wann diese abgeschickt worden ist. Gleichzeitig fehlt ihm auch der sichere Beweis des Empfanges zu einem bestimmten Zeitpunkt. Zwar sind diese Auskünfte zum Teil durch den Quelltext einer E-Mail in Erfahrung zu bringen. Die Entschlüsselung des Quelltextes ist aber nicht von jedermann vorzunehmen und kann in einfacher Weise verändert werden, um eine beliebige Zeit als Absende- oder Empfangszeitpunkt festzulegen. Auch sind Manipulationen der Systemzeit des Mailservers möglich, die eine Feststellung des Versendezeitpunktes verhindern würden.

Gleichzeitig ist es aber für Beteiligte von entscheidender Bedeutung, festzustellen, wann eine Datei signiert worden ist, da sich die Gültigkeit des Zertifikates durch Sperrung oder Ablauf ändern kann. Daher ist es für den Signierenden wichtig, beweiserheblich festzulegen, dass seine Signatur zu einem bestimmten Zeitpunkt geleistet worden ist, zu dem sein Zertifikat noch gültig war.

Daher bestimmt das Signaturgesetz in § 9 SigG, dass ein so genannter Zeitstempeldienst („time-stamping“) zu den Pflichtdienstleistungen von Zertifizierungsstellen gehört. Dabei kann jeder, der einen Bedarf für einen solchen Zeitstempel sieht, beliebige Daten an den Zeitstempel-Server der Zertifizierungsstelle übermitteln und erhält von dort eine digital signierte Datei zurück, die neben dem übermittelten Datensatz auch die gültige gesetzliche Zeit enthält. Dies wird durch eine Signatur der Zertifizierungsstelle gesichert. Für einen Nachweis des Signaturzeitpunktes ist der Zeitstempeldienst ein geeignetes Instrument. Der entscheidende Zeitpunkt der Signatur wird festgehalten und vor Manipulationen geschützt. Dies führt zu einer Rechtssicherheit hinsichtlich der Verifizierung der Signatur.

Problematisch ist aber, dass die zeitgestempelte Datei an denjenigen zurückgesendet wird, der die Daten selbst übermitteln möchte. Wann er dies tut, wird durch den Zeitstempel nicht festgehalten. Zum Beweis des Absendens einer elektronischen Nachricht ist der Zeitstempeldienst somit ungeeignet. Anders ist dies jedoch beim Empfang einer E-Mail. Der Empfänger kann diese elektronische Nachricht an den Zeitstempel-Server der Zertifizierungsstelle übermitteln, um das Vorliegen der Nachricht zu einem bestimmten Zeitpunkt nachweisbar zu machen.

Das Problem des Zugangs bzw. Empfangs einer Nachricht könnte aber evtl. dadurch gelöst werden, dass eine Zertifizierungsstelle nicht nur einen Zeitstempel der Nachricht hinzufügt, sondern auch die Weiterleitung an den Empfänger übernimmt. Dadurch wäre sowohl die Gültigkeit des Zertifikates zu einem bestimmten Zeitpunkt gesichert als auch die Möglichkeit des Nachweises von Empfang und Zugang zu bestimmten Zeiten geschaffen.

II. Sicherheit

Die Sicherheit digitaler Signaturen ist sehr voraussetzungsvoll. Dabei geht es nicht bloß um kryptologische oder physische Sicherheit, sondern ebenso um Verwendungs-, Zugriffs-, Anwendungs- und Organisationssicherheit.[9] So geht es beispielsweise nicht lediglich um die Frage der Sicherheit des Verschlüsselungsmechanismus (kryptologische Sicherheit), sondern auch um Fragen einer sicheren Zertifizierungsstruktur[10] und Organisation (Organisationssicherheit). Diese Fragen der Sicherheit sind vielfältig und können hier nur oberflächlich dargestellt werden.[11]

1) Entschlüsselung

Aufgrund des technischen Fortschritts sind heutzutage Verschlüsselungsalgorithmen möglich, die eine Entschlüsselung durch Unbefugte praktisch nicht mehr zulassen. Eine theoretische Entschlüsselung ist jedoch immer noch denkbar, mit Hilfe heutiger Rechenleistung aber nicht in einem akzeptablen Zeitrahmen zu erreichen. Um diese praktische Unfälschbarkeit gewährleisten zu können, ist daher zu beachten, dass der verwendete Signaturschlüssel eine ausreichende Bit-Länge erreicht, da andernfalls das Risiko einer Entschlüsselung gegeben sein kann.[12] Ebenfalls sieht das SigG ein „Verfallsdatum“ für digitale Signaturen vor, nach dem ein Dokument erneut digital signiert werden muss.

2) Mangelndes Sicherheitsbewusstsein

Probleme des Umgangs mit digitalen Signaturen sind ebenso zu bedenken. In einer Simulationsstudie „Rechtspflege“ wurden von „provet e.V. - Projektgruppe verfassungsverträgliche Technikgestaltung e.V.“ Studien angestellt, wie die Rechtspflege mit den neuen Möglichkeiten der elektronischen Signatur umgehen würden.[13] Dabei wurden erhebliche Sicherheitsmängel durch den Umgang mit den neuen Techniken aufgedeckt. So gingen Rechtsanwälte recht sorglos mit ihren Chipkarten um, auf denen der private Signierschlüssel gespeichert war. Sie händigten diese Karte ihrer Sekretärin aus, nannten ihnen die PIN und baten darum, anstelle ihrer zu unterschreiben. Eine solche Vorgehensweise wäre bei einer eigenhändigen Unterzeichnung nicht möglich und von den betroffenen Personen mit Sicherheit auch nicht in Betracht gezogen worden.

Dieser Gefahr kann dadurch begegnet werden, dass man die Verwendung einer Chipkarte zusätzlich zu einer PIN mit einem biometrischen Merkmal sichert. Ein solches Vorgehen wird durch § 16 Abs. 2 S. 3 SigV ausdrücklich ermöglicht. Dies kann u.a.

---

9 Diese Aufzählung entnommen bei Roßnagel, NJW 1998, S. 3312, 3314.

10 Zu der Aufsicht der Zertifizierungsstellen durch Prüf- und Bestätigungsstellen nach dem SigG vgl. Roßnagel, MMR 1999, S. 342 ff.

11 Für weitere Ausführungen vgl. Roßnagel, NJW 1998, S. 3312 ff m.w.N.

12 Zu den Möglichkeiten des Entschlüsselns von Verschlüsselungscodes vgl. statt vieler Fox, c’t 10/1995, S. 278ff.

13 Vgl. hierzu provet e.V., Die Simulationsstudie Rechtspflege.

durch die manuelle Unterschrift auf einem Notepad erfolgen. Diese Technik ist mittlerweile derart verbessert worden, dass nicht nur das Schriftbild als solches untersucht wird, sondern auch der Anpressdruck, der Winkel des Stiftes zur Schreibunterlage und auch die Flüssigkeit der Bewegungen des Schreibenden. Andererseits werden auch Methoden der Iris-Erfassung, Gesichtsidentifikation oder der Fingerabdruckanalyse weiterentwickelt. Dabei scheinen insbesondere die Fingerabdruckgeräte für digitale Signaturverfahren geeignet zu sein[14], da diese relativ preisgünstig herzustellen sind und ihrerseits durch die kulturelle Akzeptanz des Fingerabdrucks als Identifikationsmerkmal bereits ein gewisses Vertrauen von der Allgemeinheit in Anspruch nehmen dürfen. Zwar gibt es noch Probleme mit der Erkennungsrate bzw. der noch auftretenden Fehlerhäufigkeit, aber als zusätzliche Sicherung neben der PIN ist der Fingerabdruckscanner eine mögliche Variante.

3) Angriff auf das Sicherheitssystem

Die Möglichkeiten eines Angriffs auf Signatursysteme sind vielfältig[15] - die Risiken ihrer Verwendung damit auch. Dabei können am Prüfprogramm Manipulationen derart vorgenommen werden, dass ein Prüfergebnis als korrekt angezeigt wird, obwohl die Prüfung negativ ausgefallen ist. Es kann vorkommen, dass durch Fehler in der Software Text in eine elektronische Nachricht eingeschoben wird, dieses aber durch das Prüfprogramm nicht und stattdessen ein „korrektes“ Ergebnis angezeigt wird. Auch können Signaturen so verändert werden, dass diese nicht mehr als solche zu erkennen sind. Eine Veränderung des Textes und ein neuer Signiervorgang sind damit möglich.[16]

III. Verwendungsmöglichkeiten

Die Einsatzmöglichkeiten digitaler Signaturen sind vielfältig. Sie reichen von der Unterzeichnung digitaler Post, über die Authentifizierung von Online-Transaktionen bis hin zur Sicherung der Integrität von Archivdateien und dem Nachweis der Identität bei digitalen Behördengängen.

Der Einsatz ist nicht auf die Versendung elektronischer Nachrichten beschränkt, sondern auch im Offline-Bereich möglich und wegen der einfachen Sicherung des Bestandes von Daten auf wiederbeschreibbaren Datenträgern von Interesse.[17]

Durch die sich immer weiter verbreitende Technisierung der Gesellschaft und der Ausrüstung von öffentlichen Stellen, Gerichten und Behörden mit Computertechnologie wird die Identifikation in offenen Netzen ein entscheidender Faktor zur Akzeptanz di-

---

14 Vgl. hierzu die Ausführungen zu biometrischen Fingerabdruckscanner bei Scheuermann, Smart-Cards und Biometrie; Scheuermann/Struif, GMD-Spiegel 1999, S. 59; vgl. auch Oliver Diedrich in c’t 10/99, S. 74.

15 Vgl. zu den verschiedenen Angriffsformen statt vieler Pordesch/Nissen, CR 1995, S. 562 ff.

16 Für eine Auflistung potenzieller Gefährdungen vgl. Schindler, K&R 1998, S. 433, 437 ff.

17 Dies übersieht Ebbing in CR 1996, S. 271, S. 275, der scheinbar von der Möglichkeit einer digitalen Signierung lediglich bei der *Versendung* von elektronischen Nachrichten ausgeht.

gitaler Kommunikation und die Sicherheit ein entscheidender Faktor ihrer Verbreitung sein.[18]

C) Rechtliche Einordnung digital signierter elektronischer Dokumente

Im nun folgenden Teil werden die rechtlichen Aspekte digital signierter elektronischer Dokumente erörtert und die hierzu vertretenen Ansichten einander gegenübergestellt. Dabei werden die Probleme nach Rechtsgebieten getrennt. Zunächst werden die besonderen Formvorschriften und Normen über Willenserklärungen untersucht (I.). Danach werden Beweiseignung und Beweiskraft im Zivilprozessrecht behandelt (II.). Abschließend werden die Möglichkeiten des Einsatzes elektronischer Dokumente unter Berücksichtigung der digitalen Signatur bei der Kommunikation mit Gerichten und Behörden erörtert (III.) und ein Ausblick darüber gegeben, welche Veränderungen die EU-Richtlinien zu elektronischen Signaturen und Electronic Commerce bringen werden (IV-V.).

I. Materielles Zivilrecht

Im Rahmen des materiellen Zivilrechts bestehen vor allem rechtliche Probleme hinsichtlich der Einordnung in die Formvorschriften des BGB. Des Weiteren bedürfen die Besonderheiten der digitalen Dokumente einer Erörterung hinsichtlich Zugang, Zurechnung und Anfechtbarkeit elektronischer Nachrichten. Auch müssen Verbraucherschutzregeln ebenso untersucht werden, wie Haftungsfragen der digitalen Kommunikation.

Das Signaturgesetz führt in diesen Punkten nicht weiter. Es regelt keine rechtlichen Wirkungen digitaler Unterschriften, sondern lediglich die Voraussetzungen sicherer Infrastrukturen. Der rechtskonforme Einsatz digitaler Signaturen mit besonderen rechtlichen Wirkungen muss demnach an sonstigen Vorschriften beispielsweise des BGB oder der ZPO gemessen werden. Zusätzliche Vorschriften zur ausdrücklichen Anerkennung digitaler Unterschriften sind erst vereinzelt zu finden. So wurde in die Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung in § 41 Abs. 1 folgende Bestimmung aufgenommen: „Soweit nach dieser Verwaltungsvorschrift eine Unterschrift verlangt wird, kann diese durch digitale Signatur nach dem Signaturgesetz geleistet werden.“ Dadurch wird es ermöglicht, anstelle der körperlichen Unterschrift die digitale Signatur zu verwenden.[19]

1) Gesetzliche Schriftform, § 126 BGB

Nach § 126 BGB muss eine Urkunde vom Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden, um einer

18 Vgl. hierzu Hammer, CR 1992, S. 435 ff.

19 Vgl. hierzu die Darstellung dieser Vorschrift bei Bieser, in: Geis, Rechtsaspekte des elektronischen Geschäftsverkehrs, S. 49, 57 ff.

durch Gesetz vorgeschriebenen schriftlichen Form zu entsprechen. Die entscheidenden Merkmale sind die Urkundeneigenschaft und die Eigenhändigkeit der Unterzeichnung.

a) Funktionen der Schriftform

Diese Voraussetzungen dienen verschiedenen Funktionen im Rechtsverkehr.[20] Grundsätzlich ist eine Form zum Abschluss wirksamer Rechtsgeschäfte nicht vorgesehen. Es gilt das Prinzip der Formfreiheit. Die gesetzliche Schriftform wird aber in den Fällen notwendig, in denen besondere juristische Besonnenheit von den Vertragsschließenden vonnöten ist.[21]

aa) Echtheitsfunktion

Die Echtheitsfunktion soll den Nachweis für die Urheberschaft einer Erklärung vom Aussteller erbringen.

bb) Abschlussfunktion

Die Abschlussfunktion, auch Garantiefunktion genannt, besagt, dass die Unterschrift den unterzeichneten Text räumlich und zeitlich abzuschließen hat. Damit wird gewährleistet, dass der Text als inhaltlich richtig und vollständig vom Willen des Unterzeichners erfasst ist.

cc) Warnfunktion

Die Warnfunktion dient dem Übereilungsschutz vor gefährlichen und unbedachten Rechtsfolgen einer geleisteten Unterschrift im Rechtsverkehr. Die Unterschrift weist den Unterzeichner auf die rechtliche Rechtserheblichkeit seines Tuns hin.

dd) Identitätsfunktion

Die Identitätsfunktion ist bei der eigenhändigen Unterschrift im Wesentlichen durch die stets gleichartige Gestaltung des Namenszuges gewährleistet und dient der Identifizierung des Autors.

ee) Beweisfunktion

Vereinzelt wird bei der gesetzlichen Schriftform noch auf eine Beweisfunktion abgestellt.[22] Diese dient dem Beweiswert des Schriftstückes im Zivilprozess.

ff) Transportfunktion

Schließlich soll die Schriftlichkeit eine Transportfunktion gewährleisten. Diese sichert ein Recht durch Verkörperung desselben in einem Schriftdokument. Mit dieser Trans-

---

20 Vgl. hierzu die Ausführungen von Seidel, GMD-Studie, S. 29 ff.

21 Vgl. Motive bei Mugdan, S. 451.

22 Vgl. Bizer, DuD 1992, S. 169, 173.

portfunktion soll erreicht werden, dass die Zahl der Urkunden über ein bestimmtes Recht nicht vermehrt werden kann, wie dies beim Scheck oder Wechsel der Fall ist. Auf diese Weise wird die Originalität des Dokumentes sichergestellt.

b) Anwendbarkeit der Vorschrift

Die Anwendbarkeit des § 126 BGB hängt entscheidend von der Frage der Funktionserfüllung ab. Dabei ist dies ein grundsätzliches Problem elektronischer Dokumente, welches unter Berücksichtigung der digitalen Signatur zu einer anderen Beurteilung führen kann.

aa) De lege lata

Die überwiegende Literatur vertritt die Ansicht, dass elektronische Dokumente, auch digital signierte, die Anforderungen des §126 BGB an ein Schriftdokument nicht erfüllen können. Vereinzelt werden aber auch Stimmen geäußert, die § 126 BGB de lege lata auf elektronische Dokumente erstrecken möchten.

Ernst weist darauf hin, dass eine nach der Vorschrift des § 126 BGB wirksame Erklärung durch die Einführung des Signaturgesetzes nun auch elektronisch abgegeben werden könne.[23] Seine Ausführungen deuten darauf hin, dass er die geltende Gesetzeslage für ausreichend erachtet.

Bachofer führt in diesem Zusammenhang die Aufgeschlossenheit der Rechtsprechung für moderne Übermittlungsmethoden und die Berücksichtigung der Ausführungen zur gesetzlichen Schriftform an. Dadurch bestehe die Möglichkeit, auch moderne Kommunikationsmittel als Schriftformersatz wirksam einzusetzen.[24] Damit deutet er auf eine analoge Anwendung der Vorschriften zu Schriftformerfordernissen hin. Allerdings ist bei den Ausführungen Bachofers zu beachten, dass dieser bei digital unterschriebenen Dokumenten von einer Unterschrift mittels Notepad ausgeht, also einer biometrischen Aufzeichnung der Handsignatur in digitaler Form.[25]

Auch Hohenegg/Tauschek verweisen darauf, dass die Gerichte nach Inkrafttreten des Signaturgesetzes die gesetzlichen Schriftformzwecke durch digital signierte Dokumente als erfüllt ansehen könnten, bevor der Gesetzgeber diese Fragen explizit regelt. Eine Klarstellung zum wirksamen Abschluss solcher Rechtsgeschäfte, für die das Gesetz die Schriftform anordnet, wäre somit entbehrlich. [26] Sie identifizieren zwar gewisse Risiken durch die Gleichstellung mit Schrifturkunden, meinen aber, dass eine absolute Sicherheit nicht gefordert werden könne, da dies eine Voraussetzung wäre, die durch die eigenhändige Unterschrift heute schon nicht mehr erreicht würde. Einschränkend fügen sie jedoch hinzu, dass dies nur für digital signierte Dokumente gelte, welche den Anfor-

---

23 Ernst, NJW-CoR 1997, S. 165, 166.

24 Bachofer, NJW-CoR 1993, S. 25, 26.

25 Bachofer, NJW-CoR 1993, S. 25 ff.

26 Hohenegg/Tauschek, BB 1997, S. 1541, 1547.

derungen des Signaturgesetzes entsprechen. Sonstige elektronische Dokumente können nicht alle Funktionen der eigenhändigen Unterschrift erbringen und somit nicht die Voraussetzungen des § 126 BGB erfüllen.[27]

bb) De lege ferenda

Die Mehrheit der Literatur verneint eine Anwendung des § 126 BGB de lege lata. Entweder können die Funktionen der Schriftform nicht erfüllt oder aber es könne eine Analogie nicht gebildet werden. Die Begrifflichkeit der Schriftform sei nicht so dehnbar, dass elektronische Dokumente hierunter subsumiert werden könnten. Eine Anpassung der bestehenden Gesetzeslage sei daher erforderlich.

Seidel war einer der ersten Vertreter der Anpassung der Formvorschriften bei formgebundenen elektronischen Dokumenten. Er war jedoch nicht für eine generelle Gleichstellung elektronischer und konventioneller Dokumente, sondern für eine kritische Auseinandersetzung mit den Grenzen funktionsäquivalenter Abbildung.[28] Er ist nicht der Auffassung, dass elektronische Dokumente per se die Funktionserfordernisse erfüllen würden. Es sei jeweils kritisch zu hinterfragen, welche Funktionen erfüllt werden müssten und, ob diese auch durch ein elektronisches Dokument gewährleistet werden könnten.[29] Erst dann sei eine partielle Angleichung möglich.

Auch die digitale Signatur könne seiner Ansicht nach nicht die eigenhändige Unterzeichnung ersetzen. Die manuelle Unterschrift sei ein Sicherheitskennzeichen, welches sich als biometrisches Identifikationsmerkmal kulturell eingebürgert habe und von nahezu allen Rechtsordnungen rezipiert worden sei. Die digitale Signatur würde einen derartigen Vertrauenstatbestand nicht funktionsäquivalent ausfüllen. Sie habe lediglich eine reduzierte Identitätsfunktion.[30]

Den Ausführungen Seidels stimmt auch Ebbing zu. Er hält digital signierte Dokumente nicht mit § 126 BGB vereinbar, da diese weder die Identitäts- noch die Abschluss-/Beweisfunktion erfüllen.[31] Allerdings vertritt er die Auffassung, dass grundsätzlich auch elektronische Dokumente das Schriftformerfordernis des § 126 BGB erfüllen könnten.[32] Dazu sei lediglich eine zeitgemäße Auslegung des § 126 BGB notwendig. Es sollte nicht pauschal aufgrund fehlender eigenhändiger Unterschrift auf eine fehlende Form nach § 126 BGB geschlossen werden, sondern die Formvorschrift anhand ihres Zweckes untersucht und dabei die Erfordernisse eines modernen Geschäftsverkehrs

---

27 Hohenegg/Tauschek, BB 1997, S. 1541, 1543.

28 Seidel, Jahrbuch Telekommunikation und Gesellschaft 1994, S. 148, 150.

29 Seidel, Jahrbuch Telekommunikation und Gesellschaft 1994, S. 148, 154.

30 Seidel, CR 1993, S. 484, 486; ders. in GMD-Studie, S. 31f.

31 Ebbing, CR 1996, S. 271, 275.

32 Ebbing, CR 1996, S. 271, 273.

beachtet werden.[33] Dabei erfüllten elektronische Dokumente, welche durch das Einfügen einer Unterschriftsdatei erstellt wurden, die Formerfordernisse des § 126 BGB.[34]

An eine Anpassung bestehender Gesetze dachte bereits die Bundesnotarkammer 1995 und legte ihrerseits einen Entwurf vor, der im Jahre 1997 an das Signaturgesetz angepasst wurde. Es waren Regelungen über elektronische Willenserklärungen und Vertragsabschlüsse vorgesehen und gründeten sich dabei auf die digitale Signatur, deren Verwendung eine der Schriftform vergleichbare - allerdings nicht dieselbe - Wirkung haben sollte.[35] Insbesondere ging es um die Einführung einer elektronischen Form in einem § 126 a BGB.[36]

Diese Vorgehensweise befürwortet auch Schippel, der einen § 126 a BGB in Anlehnung an § 126 BGB formuliert wissen möchte. Gleichzeitig fordert er aber auch, dass die Gefahren elektronischer Manipulation ausgeräumt bzw. erheblich minimiert werden müssten.[37] Aufgrund dieser Gefahren sollte eine Belehrung über die weit reichenden Folgen der Verwendung elektronischer Signaturen durch Notare erfolgen.[38] Eine weiter gehende Untersuchung hinsichtlich eines Schriftformersatzes sei außerdem dort angebracht, wo die Unterschrift vorwiegend Warnfunktion besitze.[39]

Auch Deville/Kalthegener schlossen sich der Forderung der Bundesnotarkammer nach der Einführung eines § 126 a BGB an. Die elektronische Unterschrift sei mindestens ebenso zuverlässig und genau wie die herkömmliche Unterschrift.[40] Dabei könne aber, anders als Schippel dies fordert, auf eine Absicherung durch einen Notar verzichtet werden. Von leichtfertigen Willenserklärungen durch einen übereilten Druck einer Taste könne keine Rede sein. Die Warnfunktion werde durch geeignete Abläufe des Signiervorganges sichergestellt. Gleichzeitig ziehen Deville/Kalthegener einen Vergleich zur Kreditkarte, bei der auch niemand bei der Aushändigung durch einen Notar aufgeklärt werden müsse, wie weit reichend die Folgen der Verwendung seien. Wer die Voraussetzungen zur Teilnahme am Rechtsverkehr im Internet für sich selbst schaffe, sei über die Möglichkeiten und Risiken im Bilde.[41]

Erber-Faller sieht bis zu einer gesetzlichen Regelung keinen Anreiz, die Methoden des elektronischen Rechtsverkehrs einzusetzen. Die Rechtsprechung könne kein zufrieden stellendes Äquivalent schaffen, da für Grundsatzentscheidungen nach dem Gewalten-

---

33 Ebbing, CR 1996, S. 271, 274.

34 Ebbing, CR 1996, S. 271, 277.

35 Vgl. hierzu Erber-Faller, CR 1996, S. 375, 379.

36 Vgl. hierzu auch die Beschreibung des Vorschlages der Bundesnotarkammer von Erber-Faller, in: Geis, Rechtsaspekte des elektronischen Geschäftsverkehrs, S. 85, 92 ff.

37 Schippel, FS Odersky, S. 657, 659.

38 Schippel, FS Odersky, S. 657, 664.

39 Schippel, FS Odersky, S. 657, 665; diesem stimmen grundlegend auch Fritzsche/Malzer, DNotZ 1995, S. 3, 19 zu, sehen die Warnfunktion aber als erfüllt an.

40 Deville/Kalthegener, NJW-CoR 1997, S. 168, 171.

41 Deville/Kalthegener, NJW-CoR 1997, S. 168, 172.

teilungsprinzip der Gesetzgeber verantwortlich sei. Aus der Sicht des potenziellen Anwenders hält sich demnach der rechtliche Nutzen mangels materiellrechtlicher Formwirksamkeit in engen Grenzen.[42]

Diesen Ausführungen schließt sich auch Geis an, der die gesamten Rechtsgeschäfte, welche der gesetzlichen Schriftform unterliegen, dem elektronischen Rechtsverkehr als entzogen ansieht.[43] Auch Schumacher stimmt diesem zu und macht auf eine massive Behinderung des elektronischen Handels aufmerksam.[44] Schließlich merken Herget/Reimer an, dass die virtuelle Realität die Gegenwart eingeholt habe und daher dringender Gesetzgebungsbedarf bestehe.[45]

Grundsätzlich schließen sich auch Graf Fringuelli/Wallhäuser diesen Ansichten an. Elektronische Dokumente können nicht die Anforderungen einer Urkunde und somit der gesetzlichen Schriftform erfüllen, da ihnen zwar nicht die Perpetuierung, aber die Wahrnehmbarkeit aus sich heraus fehle.[46] Es sei im Hinblick auf die Möglichkeiten der neuen Medien eine sinnvolle rechtliche Neuregelung zu schaffen, wolle man den reibungslosen Umgang für die Zukunft sichern. Bei den gesetzlichen Formerfordernissen wäre aber die Grenze erreicht, an der der Ruf nach dem Gesetzgeber gerechtfertigt sei.[47]

Gräve/Lukies gehen davon aus, dass der Gesetzgeber in Zukunft eine Vielzahl von Gesetzen an die Anforderungen des SigG anpassen werde. Dies könne u.a. bei den §§ 126, 127 BGB oder auch den Regeln der ZPO geschehen. Im Rahmen einer solchen Anpassung halten sie aber auch eine Verschärfung des § 690 Abs. 3 ZPO für denkbar. Dabei könne es Ziel sein, das DFÜ-Mahnverfahren signaturgesetzkonform zu gestalten. Insbesondere sei dabei an eine Verlängerung der bisher verwendeten Schlüssel auf mindestens 1024 Bit sowie eine Ausgabe der Chipkarten durch ein zugelassenes Trust-Center zu denken.[48]

Etwas zurückhaltender äußern sich dagegen Rott und Roßnagel. Rott differenziert die Möglichkeiten der Gleichstellung elektronischer Dokumente mit der Schriftform nach § 126 BGB aufgrund der verschiedenen Funktionen, welche durch die Schriftform erfüllt werden sollen. Er sieht mit Ausnahme der Warn- und Transportfunktion sämtliche übrigen Funktionen durch ein elektronisches Dokument mit digitaler Signatur nach dem SigG funktionsäquivalent abgebildet.[49] Durch einen bloßen Mausklick oder das Aufrufen eines Signaturprogramms sei eine Warnfunktion jedoch nicht ausreichend zu erfüllen. Auch könne auf eine ausreichende Warnung nicht mit dem Argument verzichtet werden, der Schriftform käme ohnehin kein ausreichender Schutz vor Übereilung mehr

---

42 Erber-Faller, MittBayNot 1995, S. 182, 190.

43 Geis, NJW 1997, S. 3000, 3000.

44 Schumacher, CR 1998, S. 758, 761.

45 Herget/Reimer, DStR 1996, S. 1288, 1291.

46 Graf Fringuelli/Wallhäuser, CR 1999, S. 93, 95.

47 Graf Fringuelli/Wallhäuser, CR 1999, S. 93, 97.

48 Gräve/Lukies, NJW-CoR 1998, S. 228, 232.

49 Rott, NJW-CoR 1998, S. 420, 427.

zu. Dies würde den Schutz des Verbrauchers in bestimmten Fällen außer Kraft setzen und somit der Tendenz der Rechtsprechung zuwider laufen, den Bürger stärker zu schützen, als dies nach der jetzigen Gesetzeslage der Fall sei. Eine gänzliche Gleichstellung von elektronischen Dokumenten und der Schriftform nach § 126 BGB sei daher ein inakzeptables Ergebnis.[50]

Die Erfüllung einer Transportfunktion könne nach der Ansicht von Rott weder herbeigeführt werden, noch sei hierfür überhaupt ein Bedürfnis zu entdecken. Daher sei eine Anpassung gesetzlicher Regelungen in diesen beiden Bereichen nicht nötig oder möglich.[51]

Roßnagel dagegen sieht die Erfüllung beinahe aller Funktionserfordernisse als gegeben an. Gleichzeitig weist er aber auch darauf hin, dass in Bezug auf die Warnfunktion Prozeduren festgeschrieben werden müssten, die über einen einfachen „Klick mit der Maus“ hinausgingen. Lediglich die Transportfunktion könne nicht durch ein elektronisches Dokument ausgefüllt werden.[52] Zurückhaltung sei hinsichtlich einer Gesetzesanpassung jedoch unabdinglich, da die notwendigen Erfahrungssätze noch nicht zur Verfügung stünden.[53]

Die Regelungslücken hat das Bundesjustizministerium ebenfalls erkannt und bereits im Jahre 1997 einen Entwurf zur Einführung einer elektronischen „Textform“ vorgelegt. Dabei sollte diese Form lediglich für solche Rechtsgeschäfte ein wirksames Formäquivalent sein, in denen ein nennenswertes Fälschungsrisiko nicht bestünde. Es sollten u.a. bestimmte Regelungen in HWiG[54], VerbrKrG und auch im VVG angepasst werden, um beispielsweise den elektronischen Widerruf eines Geschäftes nach dem HWiG oder dem VerbrKrG zu ermöglichen. Im Oktober 1997 nahm das Bundesjustizministerium von diesem Vorschlag jedoch Abstand und erklärte, vorerst keine weiteren Gesetzesvorschläge zu unterbreiten, sondern sich zunächst weiter dem Studium dieser Materie zu widmen. Dabei sollten insbesondere die Möglichkeiten des Einsatzes einer digitalen Signatur im Rahmen einer elektronischen Form untersucht werden.[55]

Diese Untersuchungen mündeten in einen neuen Entwurf, der im Mai 1999 veröffentlicht worden ist.[56] In diesem ist insbesondere eine weit gehende Gleichsetzung der digitalen Signatur mit der gesetzlich Schriftform vorgesehen. Zu diesem Zweck soll eine neue „elektronische Form“ als Option zur Schriftform in das BGB eingeführt werden. Dabei nimmt die elektronische Form Bezug auf die Anforderungen des Signaturgeset-

---

50 Rott, NJW-CoR 1998, S. 420, 428.

51 Rott, NJW-CoR 1998, S. 420, 428.

52 Roßnagel, NJW-CoR 1994, S. 96, 98f.

53 Roßnagel, NJW-CoR 1994, S. 96, 100.

54 Ob das HWiG auf Geschäfte im Internet überhaupt angewendet werden kann, ist umstritten. Vgl. hierzu die Ausführungen von Ernst, VuR 1997, S. 259, 262 (ablehnend); Meents, K&R 1999, S. 53 ff (zustimmend).

55 Vgl. hierzu Hoeren/Sieber/Waldenberger, Teil 13.4, Rn. 86ff m.w.N.

56 Verfügbar unter: http://www.dud.de/dud/files/bgbe0599.zip.

zes. Gleichzeitig soll auch an den ursprünglichen Entwurf angeknüpft und die Textform eingeführt werden. Diese unterhalb der gesetzlichen Schriftform angesiedelte Form brauche lediglich in Schriftzeichen lesbar zu sein und den Aussteller erkennen lassen. Eine irgendwie geartete Absicherung der Authentizität findet nicht statt. Diese Form soll überall dort Anwendung finden können, wo die Informationsfunktion gegenüber einer Beweisfunktion überwiegt.[57] So brauchen beispielsweise die Vertragsbedingungen eines Überziehungskredites gem. § 5 Abs. 1 S. 3 VerbrKrG nicht mehr schriftlich, sondern lediglich in Textform bestätigt zu werden. In § 7 Abs. 1 VerbrKrG wird von der Schriftlichkeit dagegen gänzlich Abstand genommen und jede Form des Widerrufes akzeptiert.

cc) Gegner der Anwendung de lege lata oder de lege ferenda

Die Anwendung des § 126 BGB wird von Malzer weder de lege lata, noch de lege ferenda befürwortet. Elektronische Dokumente könnten nicht die Schriftform im Sinne des § 126 BGB erfüllen, da ihnen die Verstofflichung in Schriftzeichen fehle. Sie seien lediglich in Form eines digitalen Codes auf dem Datenträger niedergelegt.[58] Auch eine digitale Signatur ändere an dieser Einschätzung nichts.[59] Eine analoge Anwendung scheide schließlich aufgrund der besonderen Stellung des § 126 BGB als Ausnahmevorschrift aus.[60]

Die Anpassung oder Erweiterung der Vorschrift verneint Malzer aber auch und vor allem aufgrund der seiner Ansicht nach bestehenden Regelungen des Signaturgesetzes. Durch diese würde Rechtsunsicherheit geschaffen.[61] Dabei kritisiert er vor allen Dingen die privatwirtschaftlich organisierte Zertifizierungsstruktur und Lücken in der Sicherung der Integrität digital signierter Nachrichten.[62] Er wendet sich auch gegen die u.a. von ihm früher vertretene Auffassung, dass die Einführung eines § 126 a BGB das Problem der elektronischen Form lösen könnte.[63] Auch eine sog. „Textform“ hält Malzer für nicht sinnvoll. Seiner Ansicht nach vermag diese nicht annähernd die durch die Schriftform gewährleisteten Funktionen zu erfüllen.[64]

Vor ihm hat auch schon Bizer eine Anpassung bestehender Formvorschriften verneint. Seiner Ansicht nach sei eine Erfüllung der gesetzlichen Schriftform nur durch eine Gesetzesänderung zu erreichen. Jedoch sieht er verfassungsrechtliche Bedenken, das Recht den technischen Anforderungen und Zwängen anzupassen.[65] Auch hänge die Funktions-

---

57 Vgl. die Begründung zum Entwurf S. 21; abzurufen unter http://www.dud.de/dud/files/bgbebegr.zip.

58 Malzer, DNotZ 1998, S. 96, 103.

59 Malzer, DNotZ 1998, S. 96, 107.

60 Malzer, DNotZ 1998, S. 96, 108; so auch Heun, CR 1995, S. 2 ff.

61 Malzer, DNotZ 1998, S. 96, 121.

62 Malzer, DNotZ 1998, S. 96, 108.

63 Fritzsche/Malzer, DNotZ 1995, S. 3 ff.

64 Malzer, DNotZ 1998, S. 96, 116.

65 Bizer, DuD 1992, S. 169, 173, jedoch ohne nähere Begründung.

äquivalenz entscheidend vom Beweiswert des Dokumentes ab. Da er aber eine Anpassung der Urkundenbeweisregeln im Ergebnis ablehnt, könne die Beweisfunktion derzeit nicht in ausreichender Weise erfüllt werden.[66] Damit wendet er sich im Ergebnis auch gegen eine Änderung gesetzlicher Formvorschriften.[67]

dd) Standardkommentare

Soweit die Standardkommentare sich überhaupt zu elektronischen Dokumenten äußern, wird eine Einhaltung des Schriftformerfordernisses einhellig abgelehnt. Auch eine digitale Signatur genüge den Anforderungen nicht. Das Signaturgesetz wolle zwar Fälschungssicherheit elektronischer Dokumente sicherstellen, der Gesetzgeber habe aber davon abgesehen, die digitale Signatur der eigenhändigen Unterschrift rechtlich gleichzustellen. Daher sei § 126 BGB durch elektronische Dokumente in jedem Falle nicht erfüllt.[68] Dabei wird auch die Rechtssicherheit digitaler Signaturen im Sinne des Signaturgesetzes und die Notwendigkeit einer neuen Form angezweifelt.[69]

2) Gewillkürte Schriftform, § 127 BGB

Wird die Schriftform nach § 127 BGB vereinbart, ist entsprechend der gesetzlichen Schriftform im Zweifel grundsätzlich eine eigenhändige Unterzeichnung erforderlich.

Daher meint Schippel in diesem Zusammenhang, wie auch schon bei § 126 BGB, dass die Vorschrift des § 127 BGB auf die elektronische Unterschrift anwendbar gemacht werden müsse.[70]

Diesem schließt sich Malzer an und meint, dass die Vorschrift restriktiv auszulegen sei. Durch den elektronischen Rechtsverkehr lägen nun neuartige Sachverhalte vor, die erst de lege ferenda in § 127 BGB einbezogen werden müssten. Eine erweiternde Auslegung des § 127 S. 2 BGB scheide aus.[71]

Anders hingegen Hohenegg/Tauschek, die bei der Vereinbarung der Schriftform nach § 127 BGB nicht prinzipiell die gleichen Probleme wie bei der gesetzlichen Schriftform nach § 126 BGB sehen. Durch die einfache Vereinbarung einer gewillkürten Schriftform könne eine elektronische Erklärung als wirksam angesehen werden, wenn aus dem Verhalten der Parteien entnehmbar wäre, dass elektronische Dokumente zur Erfüllung der gewillkürten Form ausreichen sollen.[72]

---

66 Bizer, DuD 1992, S. 169, 173.

67 Vgl. unten C II 2.

68 Palandt/Heinrichs, § 126, Rn. 7.

69 Jauernig/Jauernig, § 126, Rn. 12, unter Hinweis auf Malzer, DnotZ 1998, S. 96 ff.

70 Schippel, FS Odersky, S. 657, 665.

71 Malzer, DNotZ 1998, S. 96, 109.

72 Hohenegg/Tauschek, BB 1997, S. 1541, 1547.

3) Notarielle Beurkundung, § 128 BGB, Öffentliche Beglaubigung, § 129 BGB

Bezüglich einer notariellen Beurkundung nach § 128 BGB und der öffentlichen Beglaubigung nach § 129 BGB ist es einhellige Meinung, dass digitale Signaturen diese nicht ersetzen können.[73]

4) Zugang, §§ 130 ff BGB, § 147 BGB

Bei der Frage nach dem Zugang von elektronischen Dokumenten ist entscheidend, ob es sich bei der Übermittlung um Willenserklärungen unter Anwesenden oder Abwesenden handelt.

Herget/Reimer ziehen einen Vergleich zur telefonischen Kommunikation und schließen daraus, dass die Vorschrift des § 147 Abs. 1 S. 2 BGB analog angewendet werden könne, da die beiden Situationen vergleichbar seien. Daher seien Erklärungen via Online-Kommunikation als Willenserklärungen unter Anwesenden anzusehen. [74]

Graf Fringuelli/Wallhäuser halten die analoge Anwendung des § 147 Abs. 1 S. 2 BGB für ausgeschlossen, da keine Vergleichbarkeit zwischen telefonischer Kommunikation und Internet-Dialog bestehe. Es liege gerade nicht die für ein mündliches Gespräch typische Situation des unkörperlichen Dialogs vor, da die Erklärungen via Internet im Arbeitsspeicher perpetuiert und somit gespeichert abrufbar seien, auch wenn die Reaktionszeiten der Teilnehmer in einer Online-Unterhaltung äußerst kurz wären.[75]

Auch Fritzsche/Malzer halten den Rechtsgedanken des § 147 Abs. 1 S. 2 BGB wegen einer weit gehenden Annäherung an den telefonischen Dialog für anwendbar, wenn Computer im Online-Verfahren verbunden seien und unmittelbar miteinander kommunizierten. Anders sei es jedoch bei einer Übermittlung in den elektronischen Briefkasten des Empfängers. Dort handelte es sich mangels unmittelbarer Übertragung um eine Erklärung unter Abwesenden.[76] Dadurch, dass die Nachricht in der Regel unter Abwesenden erfolge, könne der Zugang nur während der üblichen Geschäftszeiten eintreten. Anders sei dies jedoch dann, wenn die Anlage des Empfängers, eine eingehende Nachricht eigenständig bearbeitet und beantwortet. Dann sei unabhängig vom Zeitpunkt des Eingangs von sofortiger Wirksamkeit auszugehen. Ein Widerruf erscheine aufgrund der kurzen Laufzeiten der elektronischen Nachrichten in diesem Zusammenhang weder möglich noch sinnvoll.[77]

Demgegenüber sind die übrigen Vertreter der Literatur der Auffassung, dass es sich bei der elektronischen Übertragung von Willenserklärungen insgesamt um Erklärungen unter Abwesenden handelt, so dass die Vorschriften über den Widerruf von Willenser-

---

73 Vgl. statt vieler Hohenegg/Tauschek, BB 1997, S. 1541, 1547.

74 Herget/Reimer, DStR 1996, S. 1288, 1291.

75 Graf Fringuelli/Wallhäuser, CR 1999, S. 93, 98.

76 Fritzsche/Malzer, DNotZ 1995, S. 3, 11.

77 Fritzsche/Malzer, DNotZ 1995, S. 3, 13.

klärungen, § 130 Abs. 1 S. 2 BGB, und zur Annahmefrist für Angebote unter Abwesenden, § 147 Abs. 2 BGB, zur Anwendung kommen.[78]

Heun ist dabei der Auffassung, beim Dialog Computer-Mensch oder Computer-Computer liege ein Vertragsschluss unter Abwesenden vor, weil anders als bei der Kommunikation Mensch-Mensch eine individuelle Nachfragemöglichkeit nicht vorhanden und eine sofortige Überprüfung des materiellen Erklärungsinhaltes nicht möglich sei.[79]

Auch Ernst unterstützt die Auffassung, dass eine elektronische Nachricht als Willenserklärung unter Abwesenden anzusehen ist, da dies den besonderen Anforderungen der Kommunikation in offenen Netzen entspreche. Eine Nachricht sei bereits als zugegangen anzusehen, wenn das Dokument auf dem Server, in welchem sich der elektronische Briefkasten befinde, angekommen ist. Wer mit der Einrichtung eines elektronischen Briefkastens und Veröffentlichung seiner Adresse den digitalen Briefverkehr eröffne, müsse auch der Obliegenheit genügen, die sich aus der resultierenden Erwartung des Absenders ergebe, dass die Nachricht alsbald eingehe. Daher gehe eine Nachricht im Geschäftsverkehr zu normalen Geschäftszeiten ein, bei Privatleuten jeweils am nächsten Tage.[80]

Dem schließen sich auch Fritzemeyer/Heun an, die rechtlich keinen Unterschied zwischen herkömmlichem und elektronischem Briefkasten ausmachen können.[81] Sie verneinen jedoch die Einschränkung des Zugangs auf bestimmte Zeiten wie den üblichen Geschäftszeiten. Sinn einer elektronischen Kommunikation sei gerade die Informationsübermittlung unabhängig von bestimmten Geschäftszeiten. Eine Beschränkung könne daher nicht angenommen werden. Wollten die Parteien dies jedoch vereinbaren, sei es im Rahmen eines entsprechenden Vertrages durchaus möglich.[82]

Einen Widerruf sehen Fritzemeyer/Heun als praktisch bedeutungslos an, da die Übertragung ohne Zeitverlust vonstatten gehe und somit die Widerrufszeit auf Null schrumpfe.[83]

Auf die mangelnde Möglichkeit eines Zugangsnachweises machen Deville/Kalthegener aufmerksam. Auch ein Zeitstempel sei nicht ausreichend, wenn lediglich der Zeitpunkt des Eingangs beim Server und nicht der entscheidende Zeitpunkt des Eingangs beim Empfänger dokumentiert werde. Als Ausweg käme eine Vereinbarung zwischen den

---

78 Hoeren/Sieber/Mehrings, Teil 13.1, Rn. 73, m. w. N.

79 Heun, CR 1994, S. 595, 597; weitere Nachweise bei Hoeren/Sieber/Mehrings, Teil 13.1, Rn. 70; so auch Graf Fringuelli/Wallhäuser, CR 1999, S. 93, 97.

80 Ernst, NJW-CoR 1997, S. 165, 166; so auch Geis, NJW 1997, S. 3000, 3000; Hoeren/Sieber/Mehrings, Teil 13.1, Rn. 73, 80, 85; Graf Fringuelli/Wallhäuser, CR 1999, S. 93, 99; schließlich auch Kaiser/Voigt, K&R 1999, S. 445, 447, unter Hinweis auf die Grundsätze bezüglich des Zugangs von Fax-Sendungen.

81 Fritzemeyer/Heun, CR 1992, S. 129, 130.

82 Fritzemeyer/Heun, CR 1992, S. 129, 130.

83 Fritzemeyer/Heun, CR 1992, S. 129, 131; so auch Graf Fringuelli/Wallhäuser, CR 1999, S. 93, 99.

Parteien in Betracht, welche den Server als Ort wählen würde, bei dem die Willenserklärungen zusammenlaufen.[84]

5) Zurechnung

Sollte eine Signatur ohne Wissen des Inhabers erfolgt sein, oder aber streitet er die Vornahme einer elektronischen Unterschrift ab, ist fraglich, ob dennoch eine Zurechnung erfolgen kann. Der private Schlüssel eines digitalen Signatursystems muss nach dem Signaturgesetz auf einer SmartCard gespeichert und zusätzlich durch eine PIN gesichert werden. Aufgrund dessen wird eine Anwendung der bisherigen Rechtsprechung zu sonstigen Kartenanwendungen mit ähnlicher technischer Sicherung wie beispielsweise EC-Karten erwogen.

Bizer/Hammer vertreten hierbei die Ansicht, dass die Regeln der Anscheinsvollmacht nach den §§ 164 ff BGB analog angewendet werden könnten. Habe der Anspruchsgegner seine Chipkarte einem Dritten überlassen, dann müsse er demnach die Folgen des missbräuchlichen Handelns unter seinem Namen tragen.[85] Nicht anders sei es bei einer gestohlenen Chipkarte. Dabei komme es darauf an, ob der Erklärungsempfänger wusste oder hätte wissen müssen, dass der Anspruchsgegner nicht mehr über seine Chipkarte verfügte.[86]

Fritzsche/Malzer dagegen plädieren für die Ausweitung der Rechtsscheinhaftung auf die Zurechnung elektronischer Erklärungen. Dabei halten sie eine gesetzliche Regelung de lege ferenda für möglich, welche in den §§ 170 ff BGB eine Vertretungsmacht bei nachweisbarem Handeln unter Schlüssel- und Zertifikatsverwendung fingiere. Die Regelung könnte inhaltlich an die Rechtsprechung zu BTX orientiert sein, bei der die Nutzung eines durch Geheimzahl gesicherten BTX-Anschlusses dem Anschlussinhaber zugerechnet werde.[87]

6) Anfechtbarkeit

Obwohl elektronisch übersandte Nachrichten „normale“ Willenserklärungen darstellen, bringt die Verwendung der neuen Technologien auch neue Risiken hinsichtlich inhaltlicher Mängel durch Fehlübertragungen oder Fehlbedienung mit sich. Es ist jedoch fraglich, wie diese in die Regelungen der §§ 119 ff BGB eingeordnet werden können.

Nach der Ansicht von Ernst könne eine elektronische Willenserklärung, welche durch eine fehlerhafte Übermittlung falsch versendet worden sei, nach den Vorschriften der §§ 119 Abs. 2, 120 BGB angefochten werden.[88]

---

84 Deville/Kalthegener, NJW-CoR 1997, S. 168, 171.

85 Bizer/Hammer, DuD 1993, S. 689, 694.

86 Bizer/Hammer, DuD 1993, S. 689, 694.

87 Fritzsche/Malzer, DNotZ 1995, S. 3, 15; zur BTX-Rechtsprechung vgl. BVerwG, NJW 1995, S. 2121, 2121.

88 Ernst, NJW-CoR 1997, S. 165, 167.

Fritzsche/Malzer konkretisieren diese Ansicht und halten § 120 BGB für anwendbar, wenn eine Erklärung durch den Transport Übermittlungsfehler aufweise.[89] Zugangsmängel durch falsche Aufnahme bzw. Verarbeitung durch das Empfangsgerät seien dagegen entsprechend der Wertung bei Empfangsboten und -vertretern zu Lasten des Empfängers zu werten.[90]

Mehrings unterscheidet die Frage der Anfechtung danach, wann der zum Irrtum führende Fehler aufgetreten sei. Lediglich Fehler bei Abgabe der Erklärung kommen in Betracht. Diese fallen unter § 120 BGB. Fehler durch Verwendung eines fehlerhaften Datenmaterials scheiden ähnlich einem Kalkulationsirrtum als unbeachtlicher Motivirrtum aus.[91]

Schippel plädiert abschließend für eine Ausdehnung des § 120 BGB auf elektronische Dokumente de lege ferenda, da die Gefahren der Übermittlung durch elektronische Medien ebenso groß seien wie durch Übermittlungsboten bei herkömmlichen Schriftdokumenten. Eine Anwendung de lege lata sei seiner Ansicht nach jedoch nicht möglich.[92]

7) Verbraucherschutz

Durch die Möglichkeit des elektronischen Rechtsschlusses ergeben sich neue Probleme bei der Umsetzung vorhandener Verbraucherschutzregeln. Dabei sind insbesondere das HWiG und das VerbrKrG zu beachten und in ihrem Anwendungsbereich mit elektronischen Dokumenten zu untersuchen.[93]

Nach einer Entscheidung des LG München sei auch bei einem Vertrieb über das Internet das Erfordernis der drucktechnisch deutlich gestalteten Widerrufsbelehrung nach § 7 Abs. 2 S. 2 VerbrKrG zu erfüllen. Ein Vertrag, der unter das Verbraucherkreditgesetz fiele, bedürfe zu seiner Wirksamkeit der Schriftform, d. h. der eigenhändigen Unterzeichnung im Sinne des § 126 BGB. Die strengen Inhalts- und Formvorschriften würden nicht dadurch entbehrlich, dass die elektronische Form des Vertragsschlusses gewählt wurde.[94] Die Anforderungen des Verbraucherkreditgesetzes und damit auch des Haustürwiderrufgesetzes[95] könnten im Internet nicht ohne Medienbruch erfüllt werden.[96]

---

89 Fritzsche/Malzer, DNotZ 1995, S. 3, 13.

90 Fritzsche/Malzer, DNotZ 1995, S. 3, 14.

91 Hoeren/Sieber/Mehrings, Teil 13.1, Rn. 110.

92 Schippel, FS Odersky, S. 657, 666.

93 Ebenfalls ist die Frage der wirksamen Einbeziehung von AGB in Internet-Geschäften zu beachten, spielt jedoch in diesem Kontext keine Rolle, vgl. hierzu Mehrings, BB 1998, S. 2373 ff; Ernst, NJW-CoR 1997, S. 165, 167.

94 LG München, NJW 1999, S. 2127, 2128.

95 Ob das Haustürwiderrufgesetz überhaupt auf Online-Geschäfte Anwendung findet, ist umstritten. Die wohl überwiegende Meinung bejaht ein Umgehungsgeschäft i.S.d. § 5 HWiG und wendet somit das Gesetz auch auf Verträge im WWW an; vgl. hierzu Meents, K&R 1999, S. 53 ff; a.A. Borges, ZIP 1999, S. 130 ff; differenzierend Waldenberger, BB 1996, S: 2365, 2367; jeweils mit weiteren Nachweisen.

96 So auch MüKo/Ulmer, § 4 VerbrKrG, Rn. 12.

Auch Waldenberger vertritt die Ansicht, dass manche Internet-Geschäfte, auf die das HWiG anwendbar sei, de facto unmöglich wären. Allerdings sieht er eine Lösung in der analogen Anwendung des § 5 Abs. 3 S. 2 HWiG. Das Widerrufsrecht könne dabei durch ein einwöchiges Rückgaberecht im Sinne dieser Vorschrift zum Nutzen aller Beteiligten ersetzt werden. Es könne nicht Sinn des HWiG sein, im Internet abgeschlossene Rechtsgeschäfte zu verhindern. Das Gesetz bedürfe daher einer teleologischen Reduktion auf dasjenige Maß, das für einen wirksamen Verbraucherschutz erforderlich erscheine.[97] Ein Widerruf nach VerbrKrG oder HWiG sei aber auf jeden Fall nach derzeitiger Rechtslage ausgeschlossen.[98]

Hoeren tritt in diesem Zusammenhang für ein gänzliches Widerrufsrecht unabhängig von der Verbrauchereigenschaft ein. § 130 BGB sei durch ein solches Recht eigener Prägung zu ersetzen, da aufgrund zunehmender Übertragungsgeschwindigkeit eine Reflektion über Inhalt und Wirkung der eigenen Willenserklärung immer seltener möglich wäre. Dieser Verlust sei durch eine (Wieder-)Entdeckung der Langsamkeit durch Sicherung einer Bedenkpause zu kompensieren.[99]

Deville/Kalthegener schlagen zur Sicherheit des Verbrauchers eine Ergänzung des § 1 Abs. 1 HWiG vor. In einer neuen Ziffer 4 könnte die Anwendbarkeit des Haustürwiderrufgesetzes auf mit elektronischer Unterschrift getätigte Rechtsgeschäfte geregelt werden. Ferner wären auch §§ 5, 7, 8 VerbrKrG anzupassen. Als Gründe werden vor allem die notwendige Erhöhung des Verbraucherschutzes im Internet-Rechtsverkehr und die Vermeidung streitiger Rechtsfälle genannt. Wenn ein Widerruf eines Rechtsgeschäftes bereits nach HWiG oder VerbrKrG möglich sei, erübrige sich in der Regel ein Rechtsstreit über die missbräuchliche Verwendung einer elektronischen Unterschrift durch Dritte oder Minderjährige.[100]

Zum Schutz des Verbrauchers tritt Melullis dagegen für eine Anpassung durch die Einführung einer summenmäßigen Begrenzung der Verpflichtungsmöglichkeiten in Abhängigkeit von der Zeit und den wirtschaftlichen Verhältnissen des Kunden ein.[101]

Anders dagegen Ernst, welcher der Auffassung ist, dass auch Verträge, die unter das Verbraucherkreditgesetz fielen, elektronisch abgeschlossen werden könnten.[102] Lediglich die deutliche Kenntlichmachung der Belehrung über das Widerrufsrecht nach § 7 Abs. 2 S. 1 VerbrKrG und der zweiten Unterschrift sei erforderlich. Das Merkmal der „drucktechnischen Abgesetztheit“ sei teleologisch dahingehend zu erweitern, dass

97 Hoeren/Sieber/Waldenberger, Teil 13.4, Rn. 19.

98 Hoeren/Sieber/Waldenberger, Teil 13.4, Rn. 20, 62.

99 Hoeren, NJW 1998, S. 2849, 2852.

100 Deville/Kalthegener, NJW-CoR 1997, S. 168, 172.

101 Melullis, MDR 1994, S. 109, 114.

102 Ernst, NJW-CoR 1997, S. 165, 166.

auch eine visuelle Absetzung des Hinweises vom übrigen Text auf einem Bildschirm ausreichend sei.[103]

Derselben Ansicht hinsichtlich der Anforderungen des Verbraucherkreditgesetzes ist auch Köhler, sieht den Ausweg aus dem Schriftformerfordernis jedoch im Versandhandelsprivileg des § 8 VerbrKrG. Seiner Ansicht nach wäre § 4 VerbrKrG nicht anwendbar, da er als „Verkaufsprospekt" auch eine Verkaufsinformation versteht, die dem Verbraucher im Wege der Telekommunikation übermittelt wird und die er auf dem Bildschirm sichtbar machen und sich ausdrucken lassen kann.[104] Daher sei auch ein Internetangebot in „Verkaufsprospekt" im dargelegten Sinne.

Hiergegen wenden Kaiser/Voigt ein, dass das Versandhandelsprivileg des § 8 VerbrKrG nicht auf Internetgeschäfte Anwendung finden könne, da einerseits die Voraussetzung des Verkaufsprospektes dem Wortsinn nach nicht auf das Internet übertragbar sei und außerdem der Gesetzgeber zu Zeiten des BTX, als also bereits elektronische Abwicklung von Geschäften bekannt war, den Begriff des Verkaufsprospektes gewählt hätte. Eine Verwendung des § 8 VerbrKrG widerspräche somit dem Willen des Gesetzgebers.[105]

8) Selbstbeschränkung

Selbstbeschränkung bedeutet die inhaltliche oder summenmäßige Begrenzung der rechtswirksamen Signaturerstellung durch Zusatz im Zertifikat. Der Inhaber eines Signaturschlüssels kann gem. § 7 Abs. 1 Nr. 7 SigG bereits bei der Antragstellung in das Zertifikat aufnehmen lassen, dass nur bestimmte Arten von Rechtsgeschäften oder diese nur bis zu einer bestimmten Höhe mit seiner Signatur möglich sein sollen. Andere als die im Zertifikat enthaltenen Rechtsgeschäfte werden nach den allgemeinen Grundsätzen, insbesondere wegen der Perplexität von Willenserklärungen, dem Schlüsselinhaber nicht zugerechnet. Auf diese Weise kann sich ein Zertifikatsinhaber vor allzu unachtsamer Verwendung oder unübersehbaren Folgen seiner digitalen Signatur schützen.

Diese Art der Selbstbeschränkung wird von Deville/Kaltehegener als unnötig und unsinnig angesehen. Es widerspreche dem Wesen des Internet und führe nur zu einer Verlagerung des Geschehens außerhalb der deutschen Rechtsordnung.[106]

Dagegen sieht Erber-Faller in der Selbstbeschränkung im digitalen Zertifikat eine neue dogmatische Figur, die den Verbraucherschutz stärken könne. Sie vergleicht diese Form der „Selbstermächtigung" mit der Beschränkung der Vertretungsmacht im Außenverhältnis und legt insoweit eine Anwendung der entsprechenden Vorschriften nahe.[107]

---

103 Ernst, NJW-CoR 1997, S. 165, 166.

104 Köhler, NJW 1998, S. 185, 188.

105 Kaiser/Voigt, K&R 1999, S. 445, 449; ebenfalls Borges, ZIP 1999, S. 130, 134.

106 Deville/Kalthegener, NJW-CoR 1997, S. 168, 172.

107 Erber-Faller, CR 1996, S. 375, 379.

9) Pflichtverletzungen und Haftungstatbestände

Durch die Verwendung einer elektronischen Signatur soll die Identität des Autors einer Nachricht nachgewiesen werden. Wenn dieser Nachweis zwar geführt, die Angabe der Zertifizierungsstelle jedoch fehlerhaft ist, stellt sich die Frage nach der Haftung sowohl für den auf das Zertifikat vertrauenden Dritten als auch für den Signaturinhaber bei eventuellen eigenen Schäden. Das Signaturgesetz selbst stellt keine besonderen Haftungsvoraussetzungen oder -vorschriften bei der Verwendung digitaler Signaturen auf. Nach dem Willen des Gesetzgebers soll eine Haftung nach den allgemeinen Regeln erfolgen.[108]

Gounalakis/Rhode setzen sich mit der Haftung der Zertifizierungsstellen gegenüber den Vertragspartnern und Dritten auseinander, die in keinerlei vertraglicher Beziehung zu dem Trust Center stehen. Dabei sehen sie den Vertragspartner ausreichend durch die §§ 633 ff BGB sowie den Rechtsinstituten der positiven Forderungsverletzung und der culpa in contrahendo geschützt.[109] Anders sehe es hingegen bei einem Dritten aus, der auf vertragliche oder vertragsähnliche Haftungsnormen und -institute nicht zurückgreifen könne. Mangels personenrechtlichen Einschlags der Vertragsverbindung von Zertifizierungsstelle und Zertifikatsinhaber, d.h. mangels Fürsorge- und Obhutspflicht des Gläubigers, komme auch ein Vertrag mit Schutzwirkung zugunsten Dritter nicht in Betracht.[110] Die Anwendung des Instituts der Drittschadensliquidation dagegen könne nicht gänzlich ausgeschlossen werden, hänge aber von eigenen „Anspruchshülsen“ des Vertragspartners der Zertifizierungsstelle ab.[111] Das Deliktsrecht in Form des § 823 Abs. 1 BGB helfe hier nur bedingt weiter, da diese Vorschrift keine Vermögensschäden ersetze, welche aber die typischen Schäden fehlerhafter Zertifikate sein dürften. Daher entstünden Schutzlücken, die einzig durch eine Einordnung des Signaturgesetzes als Schutzgesetz nach § 823 Abs. 2 BGB geschlossen werden könnten. Dies könne jedoch nicht pauschal erfolgen, sondern erfordere die Untersuchung der einzelnen Regelungen.[112] Dabei seien vereinzelte Vorschriften durchaus als Schutzgesetz zu werten. Andererseits sei trotz dieser Schutzgesetzlösung die Aufnahme eigenständiger Haftungsnormen in das SigG wünschenswert. Es würde Rechtsklarheit und Rechtsgerechtigkeit geschaffen, wenn dem Geschädigten die Möglichkeit eröffnet würde, direkt gegen die Zertifizierungsstelle und nicht deren Personal vorgehen zu müssen.[113]

---

108 BT-DrS 13/7385, S. 27; demgegenüber forderte der Bundesrat in seiner Stellungnahme zum IuKDG, eine angemessene Haftungsregel in das Signaturgesetz einzufügen, BT-DrS 13/7385, S. 58f; ebenso die Fraktion Bündnis 90/Die Grünen in einem Änderungsantrag im Ausschussverfahren, Ausschußdrucksache 13-654.

109 Gounalakis/Rhode, K&R 1998, S. 225, 227.

110 So auch Timm, welche jedoch dieses Rechtsinstitut an der fehlenden Erkennbarkeit des Personenkreises scheitern lässt, DuD 1997, S. 525, 526.

111 Gounalakis/Rhode, K&R 1998, S. 225, 227.

112 Gounalakis/Rhode, K&R 1998, S. 225, 229.

113 Gounalakis/Rhode, K&R 1998, S. 225, 234.

Emmert schließt sich grundsätzlich den Ausführungen von Gounalakis/Rhode an, meint aber erweiternd, dass einem Zertifikatsinhaber die Beweiserleichterungen entsprechend § 282 BGB zugute kommen, wenn sich ein Schaden aus dem Gefahrenkreis der Zertifizierungsstelle ergebe.[114] Auch bei der Bestimmung der Schutzgesetznormen stimmen diese mit den genannten Autoren weitgehend überein.[115] Anderer Ansicht ist Emmert bezüglich der Haftung über den Vertrag mit Schutzwirkung zugunsten Dritter. Eine Haftung komme grundsätzlich in Betracht.[116]

Aber auch Emmert sieht Regelungslücken, die durch eine in das SigG einzuführende Gefährdungshaftung der Zertifizierungsstellen geschlossen werden können.[117] Dies würde auch Sicherheit gegenüber denjenigen Zertifizierungsstellen bedeuten, die Zertifikate ausgeben, aber nicht den Anforderungen des Signaturgesetzes entsprechen.[118]

Zu einer völlig anderen Einschätzung kommt Timm, welche die Einführung einer Haftungsregelung in das Signaturgesetz nicht für erforderlich und mit dem Konzept des Signaturgesetzes auch für unvereinbar hält. Es bestehe kein Bedürfnis hinsichtlich einer gesonderten Haftungsregelung, da sich die Haftungsfragen, welche sich im Zusammenhang mit der digitalen Signatur ergeben, weitgehend problemlos in das bestehende System des Haftungsrechts einordnen ließen.[119] In der Regel hafte die Zertifizierungsstelle nach Organisationsverschulden gem. § 823 Abs. 1 BGB. Allerdings erkennt Timm auch, dass Vermögensschäden nach ihrer Auffassung nicht ersatzfähig wären.[120]

Außerdem sei es die Zielsetzung des Gesetzes, zunächst die Erprobung der digitalen Signatur unter rechtlich geregelten Rahmenbedingungen zu ermöglichen. Dabei solle Vertrauensschutz durch die faktische Sicherheit des Verfahrens erreicht werden, nicht durch die Androhung finanzieller Restitution.[121] Daher verneint sie auch die Schutzgesetzeigenschaft des Signaturgesetzes, da eben die Zielrichtung eine generell-abstrakte Regelung von Verfahrensweisen, nicht jedoch der Individualschutz sei.[122]

Umgekehrt sehen Fritzsche/Malzer für die Haftung des Schlüsselinhabers gegenüber der Zertifizierungsstelle als seinem Vertragspartner die c.i.c. oder pVV als einschlägige Haftungsinstitute an. Der Schlüsselinhaber hafte dabei grundsätzlich nach § 278 BGB für das Verschulden seiner Erfüllungsgehilfen, also insbesondere Angestellten, sollte der private Schlüssel missbräuchlich verwendet werden.[123]

---

114 Emmert, CR 1999, S. 244, 245.

115 Emmert, CR 1999, S. 244, 246; Gounalakis/Rhode, K&R 1998, S. 225, 229ff.

116 Emmert, CR 1999, S. 244, 246.

117 Emmert, CR 1999, S. 244, 247.

118 Emmert, CR 1999, S. 244, 250.

119 Timm, DuD 1997, S: 525, 528.

120 Timm, DuD 1997, S. 525, 527.

121 Timm, DuD 1997, S: 525, 528.

122 Timm, DuD 1997, S. 525, 527.

123 Fritzsche/Malzer, DNotZ 1995, S. 3, 16.

II. Zivilprozessrecht

Mit der stetigen Zunahme elektronischer Dokumente steigt zwangsläufig auch die Bedeutung, die diesen als Beweismittel vor Gericht zukommen können. Im Rahmen der Beweisaufnahme stehen die Gerichte mithin vor der Aufgabe, anstelle der üblichen Schriftstücke, elektronische Dokumente einer richterlichen Würdigung zu unterziehen. Hierzu sind bislang keine Entscheidungen bekannt, welche auf die Regeln des Urkundenbeweises zurückgreifen oder die Anwendung derselben überhaupt erwägen würden. Elektronische Dokumente werden durch die Gerichte wie beinahe selbstverständlich unter die Vorschriften des Augenscheinsbeweises nach § 371 ZPO subsumiert und im Rahmen der freien richterlichen Beweiswürdigung nach § 286 ZPO beurteilt.

Soweit sich die Standardkommentare zur Zivilprozessordnung mit dieser Technik auseinander setzen, gehen auch diese von einer Anwendung des Augenscheinsbeweises im Rahmen freier richterlicher Beweiswürdigung aus.[124]

Das Signaturgesetz führt insoweit auch zu keiner anderen Einschätzung der Rechtslage, als es lediglich die Sicherheitsinfrastruktur von Zertifizierungsdienstleistungen regelt. Änderungen im Beweisrecht sollten erst in einem weiteren Schritt geprüft werden.[125] Jedoch enthält es in § 1 Abs. 1 SigG eine Vermutung, dass digitale Signaturen nach dem SigG als sicher gelten.

In dieser Vorschrift sieht Abel eine Beweisregel für die Integrität elektronischer Dokumente mit digitaler Signatur.[126]

Auch Roßnagel bezeichnet diese Vorschrift als „Beweiserleichterung". Durch die Sicherheitsvermutung zugunsten von Signaturverfahren nach dem Signaturgesetz werde „eine ausreichende und technikadäquate Beweisregelung geschaffen". Die Sicherheitsvermutung beziehe sich auf die digitale Signatur und das Prüfverfahren und könne als „vorgezogener Anscheinsbeweis" bezeichnet werden. Eine willentliche Signaturerzeugung werde jedoch nicht vermutet, da die Autorisierung digitaler Signaturen nicht unter die Formulierung subsumiert werden könne. [127]

Die Sicherheitsvermutung ist im Rahmen der freien Beweiswürdigung zu verwenden und erleichtert dem Beweisführer den Nachweis seiner Behauptungen, lässt aber dem Gegner die Möglichkeit der Widerlegung und dem Gericht die Würdigung der vorgelegten Beweise.[128] Daher gewährleiste diese Regelung ein höheres Maß an Einzelfallgerechtigkeit als eine von den Umständen des zu entscheidenden Falles losgelöste feste Beweisregel.[129]

---

124 Vgl. Baumbach/Lauterbach/Albers/Hartmann/Hartmann § 416 Rn. 4; Thomas/Putzo, Vor § 371, Rn. 6; MüKo-ZPO/-Schreiber, § 415, Rn. 6; Zöller/Geimer, Vor § 415, Rn. 2.

125 BT-DrS 13/7385, S. 26.

126 Abel, MMR 1998, S. 644, 647.

127 Roßnagel, NJW 1998, S. 3312, 3316.

128 Roßnagel, NJW 1998, S. 3312, 3318.

129 Roßnagel/Roßnagel, § 1 SigG, Rn. 57; Roßnagel, NJW 1998, S. 3312, 3318.

Die übrige Literatur ist recht uneinheitlich hinsichtlich der beweisrechtlichen Einordnung elektronischer Dokumente und führt zu unterschiedlichen Ergebnissen bei der Auseinandersetzung. Einhelligkeit besteht jedoch darüber, dass elektronische Dokumente keine Urkunden im Sinne des Beweisrechts seien und mithin einer direkter Anwendung der Urkundenbeweisregeln de lege lata nicht zugänglich seien. Eine analoge Anwendung der Urkundenbeweisregeln wird hingegen vereinzelt befürwortet, ebenso wie eine gesetzliche Gleichstellung de lege ferenda. Andere Autoren treten für eine Anwendung des Augenscheinsbeweises ein und lehnen die Gleichstellung digitaler Dokumente de lege lata oder de lege ferenda generell ab.

1) Befürworter der Anwendung von Beweisregeln des Urkundenbeweisrechts

a) De lege lata

Bereits Lampe befasste sich in seinen Ausführungen zum strafrechtlichen Schutz technischer Aufzeichnungen mit dem Beweiswert im Zivilprozess. Er war der Ansicht, dass die Urkundenbeweisregeln in analoger Form unproblematisch auch auf technische Aufzeichnungen angewendet werden könnten, da diese den schriftlichen Nachrichten in nichts nachstünden.[130] Technische Aufzeichnungen seien unter anderem durch Daten verarbeitende Maschinen (Computer) hergestellte Aufzeichnungen[131] und besäßen im Wesentlichen dieselbe gesetzliche Beweiskraft wie Schrifturkunden.[132]

Lampe bezog sich dabei jedoch nur auf die §§ 416 ff ZPO, eine Anwendung des § 415 ZPO käme nicht in Betracht, da die vor einer Behörde abgegebenen Erklärungen nicht technisch, sondern in einem schriftlichen Protokoll aufgezeichnet würden.[133]

Anders wäre es jedoch zu beurteilen, wenn einer privaten technischen Aufzeichnung die Angabe fehle, welchem Herstellungsvorgang sie entstamme. Dann würde der Nachweis ihrer Herkunft auf dem Zeugnis des Beweisführers beruhen müssen. Allerdings könnte sich ein Anschein herausbilden, dass der Nachweis gemäß freier Beweiswürdigung als urkundlich erbracht angesehen werden könne.[134]

Im gleichen Sinne äußerte sich auch Jöstlein, die Beweisvorschriften der ZPO auf elektronische Dokumente zu erstrecken. Würden technische Aufnahmen im Rechtsleben dazu hergestellt, um rechtlich erhebliche Tatsachen zu beweisen, so stünden sie in ihrem Beweiswert den Urkunden nicht nach. Die Form der Aufzeichnung spiele dabei keine Rolle.[135]

---

130 Lampe, NJW 1970, S. 1097, 1100.
131 Lampe, NJW 1970, S. 1097, 1097.
132 Lampe, NJW 1970, S. 1097, 1101.
133 Lampe, NJW 1970, S. 1097, 1100.
134 Lampe, NJW 1970, S. 1097, 1101.
135 Jöstlein, DRiZ 1973, S. 409, 412.

Abel hat sich bereits mit den Auswirkungen des Signaturgesetzes auf den Beweiswert elektronischer Dokumente befasst und plädiert für eine differenziertere Wertung unter Berücksichtigung der Regelungen des neuen Gesetzes.[136] Eine analoge Anwendung der §§ 415 ff ZPO komme seiner Ansicht nach grundsätzlich in Frage, sei jedoch unterschiedlich hinsichtlich der Erscheinungsform des elektronischen Dokumentes zu beurteilen. Dabei kommt Abel zu dem Ergebnis, dass digital nach dem SigG signierte Dokumente, welche in Form einer 3,5"-Diskette oder einer CD-ROM vorlägen, aufgrund der weiten Verbreitung entsprechender Lesemedien die Verkehrsfähigkeit erfüllen, den Anforderungen an eine Urkunde genügen und eine analoge Anwendung der Beweisregeln ermöglichen würden. Im Übrigen gelten die Regeln des Augenscheinsbeweises. [137]

Auch Hohenegg/Tauschek scheinen ähnlich der Ansicht von Abel die Verkehrsfähigkeit elektronischer Dokumente und somit auch die Anwendung der Beweisregeln grundsätzlich für möglich zu halten. Sie überlassen die abschließende Bewertung aber der Rechtsprechung.[138]

Von Sponeck hält die Vorschriften über das Urkundenbeweisrecht nicht auf elektronische Urkunden ohne Signatur für anwendbar. Diese könnten den Zusammenhang zwischen Aussteller und dem durch seine Unterschrift gedeckten Text nicht in hinreichender Weise erbringen. Es reiche nicht aus, dass eine technische Aufzeichnung eine automatisch angefertigte Herkunftsbezeichnung enthalte.[139] Anders sei dies jedoch bei elektronisch signierten Dokumenten, bei denen der Echtheitsbeweis als erbracht gelten könne und eine analoge Anwendung der Beweisregeln der §§ 415 ff ZPO nahe liege.[140] Gleichwohl sieht von Sponeck es als dienlicher an, eine gesetzliche Regelung zu etablieren, anstatt sich der „Krücke der Analogie" zu bedienen. Die Zulässigkeit einer Analogie müsse bei förmlichen Beweisregeln schon vom Prinzip her in Frage gestellt werden.[141]

b) De lege ferenda

Bergmann/Streitz sehen in ihrer Auseinandersetzung mit dem Beweiswert elektronischer Aufzeichnungen den Druck auf den Gesetzgeber wachsen. Elektronische Dokumente seien mangels Schriftform keine Urkunden im Sinne der ZPO und unterlägen damit der freien Beweiswürdigung durch den Richter.[142] Diese geringere Beweiskraft verglichen zu den sonstigen schriftlichen Urkunden sei nur durch eine Änderung des Gesetzgebers zu korrigieren, wie dies bereits durch Einfügung entsprechender Vorschriften in die Abgabenordnung und in das Handelsgesetzbuch geschehen sei. Eine

---

136 Abel, MMR 1998, S. 644 , 645.

137 Abel, MMR 1998, S. 644 , 649.

138 Hohenegg/Tauschek, BB 1997, S. 1541, 1543.

139 Von Sponeck, CR 1991, S. 269, 272.

140 Von Sponeck, CR 1991, S. 269, 272f.

141 Von Sponeck, CR 1991, S. 269, 273.

142 Bergmann/Streitz, CR 1994, S. 77, 78.

Anpassung des Urkunds- und Originalbegriffs allein sei jedoch ungeeignet, zur Lösung des Problems beizutragen. Es müssten Voraussetzungen definiert werden, unter denen elektronischen Dokumenten förmliche Beweiskraft zuerkannt werden könne.[143]

Seidel kann als einer der Hauptvertreter der Einführung gesetzlicher Beweisregeln für elektronische Dokumente gelten. Auch Seidel möchte die Ungeeignetheit des geltenden Beweisrechts für elektronische Dokumentations- und Kommunikationsformen unter qualifizierenden Voraussetzungen durch die Gleichstellung mit Schrifturkunden beseitigen.[144] Der gesetzgeberische Handlungsbedarf sei deshalb so besonders groß, weil beträchtliche Investitionen im Bereich der Privatwirtschaft zurückgestellt würden, da die rechtlichen Rahmenbedingungen fehlten und die geltende Rechtslage unklar sei.[145] Die Anwendung eines funktionierenden Zertifizierungssystems sei dabei eine entscheidende Voraussetzung zur Funktionsäquivalenz elektronischer Dokumente.[146] Eine urkundenrechtliche Anerkennung elektronischer Dokumente sei schließlich nur dann möglich, wenn die Gedankenerklärung auf einem urkundensicheren Speicher geleistet und mit einer jederzeitigen schriftlichen Ausdruckbereitschaft versehen worden sei.[147]

Auch Fritzemeyer/Heun erkennen die Mängel des Beweisrechts im Sinne Seidels an und empfehlen daher den Abschluss einer EDI-Vereinbarung[148] über den Beweiswert elektronischer Urkunden. Dabei weisen sie aber auch darauf hin, dass eine solche Vereinbarung nicht die Beweismittel der ZPO erweitern könne und die freie richterliche Beweiswürdigung nicht beschränken dürfe.[149]

Raubenheimer rät ebenso zu einer Vereinbarung im Rahmen eines EDI-Vertrages. Er weist jedoch darauf hin, dass die Regelungen nur inter partes wirken und es daher im Hinblick auf unbeteiligte Dritte beim Beweis durch Augenschein gem. §§ 371 ff ZPO bleibe.[150] Daher empfiehlt er einerseits, vor Beginn jeder Geschäftsbeziehung eine entsprechende vertragliche Vereinbarung zu treffen, und fordert andererseits den Gesetzgeber auf, die Hindernisse des elektronischen Geschäftsverkehrs zu beseitigen. Vorzugswürdig sei seiner Ansicht nach eine Lösung auf EU-Ebene.[151]

---

143 Bergmann/Streitz, CR 1994, S. 77, 79.

144 Seidel, GMD-Studie, S. 80.

145 Seidel, Jahrbuch Telekommunikation und Gesellschaft 1994, S. 148, 153.

146 Seidel, Jahrbuch Telekommunikation und Gesellschaft 1994, S. 148, 154.

147 Seidel, GMD-Studie, S. 81.

148 EDI = Electronic Data Interchange, Elektronische Datenfernübertragung; diese Form des elektronischen Geschäftsverkehrs ist mittlerweile im Business-to-Business Bereich sehr verbreitet und durch einen internationalen Standard ISO IS 9735 als EDIFACT (EDI for Administration, Commerce and Transport) normiert. In Deutschland ist dieser Standard als DIN Norm 16556 umgesetzt worden; vgl. zu EDI und EDIFACT, Bruns, in: Geis, Rechtsaspekte des elektronischen Geschäftsverkehrs, S. 127, 134 ff; Fritzemeyer/Heun, CR 1992, S. 129 ff; Kilian, DuD 1993, S. 606 ff.

149 Fritzemeyer/Heun, CR 1992, S. 129, 131 f.

150 Raubenheimer, CR 1993, S. 19, 23 f.

151 Raubenheimer, CR 1993, S. 19, 26.

Bis zu einer solchen Gesetzesänderung rät auch Kilian dazu, im Rahmen eines EDI-Vertrages die funktionale Äquivalenz von EDI-Nachrichten und papiernen Dokumenten herzustellen. Dabei könnten Klauseln verwendet werden, welche die Vornahme bzw. Nichtvornahme von Prozesshandlungen oder die Beweislast regeln.[152] Er geht aber noch einen Schritt weiter als die vorher genannten Autoren und rät, auf den ordentlichen Rechtsweg in Gänze zu verzichten. Zur Sicherung des Beweiswertes empfiehlt er daher den Parteien, eine Schiedsklausel zu vereinbaren, um den Beweiswert elektronischer Dokumente zu stärken, da der Richter an den ordentlichen Gerichten im Rahmen freier Beweiswürdigung an eine solche Vereinbarung nicht gebunden wäre. Er fügt aber noch hinzu, dass eine analoge Anwendung des § 416 ZPO bei mit digitaler Signatur unterzeichneten Dokumenten dann zu erwägen wäre, wenn eine ausdrückliche Gesetzesänderung nicht erfolgen sollte.[153]

Nach der Ansicht von Geis sei die derzeitige gesetzliche Lage unbefriedigend. Zwar mag eine Urkunde eine Gedankenerklärung enthalten, diese ermangele aber der Schriftform. Gleichfalls sei die Unterschrift als biometrisches Merkmal eine Sicherheitstechnik, die sich nicht auf digitale Dokumente übertragen lasse.[154] Damit sei das Dokument nicht Urkunde, sondern Objekt des Augenscheins.[155] Dies gelte auch für digital oder durch WORM-Technologie[156] gesicherte Dokumente.[157] Selbst ausgedruckte elektronische Dokumente seien keine Urkunden. Lediglich Ausdrucke, die ihrerseits durch den Aussteller handschriftlich unterschrieben werden, seien der Anwendung der Urkundenbeweisregeln zugänglich. Das mache aber nicht das elektronische Dokument, sondern eben nur den Ausdruck zur Urkunde.[158] Hierin sieht Geis ein großes Problem der Rechtssicherheit. Diesem Problem könnte die Rechtsprechung durch Entwicklung eines Anscheinsbeweises entgegentreten, wenn sich die Ansicht durchsetzt, dass im Unterschied zur Telefaxtechnologie der Transport und der Zugang der digital signierten Erklärung hochgradig gesichert und dies ein Indiz für die Fälschungssicherheit der Erklärung und die Authentizität des Urhebers sei. Der Richter käme im Rahmen der freien Beweiswürdigung zu demselben Ergebnis wie die Beweisregeln.[159] Doch an anderer Stelle setzt sich auch Geis für die Einführung einer gesetzlichen Regelung ein.[160]

Eine mögliche Gesetzesänderung sieht die AWV-Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. in der Gleichstellung elektronischer Dokumente mit Privaturkunden im Sinne von § 416 ZPO. Die nicht absehbare technische Entwicklung und neuarti-

---

152 Kilian, DuD 1993, S. 606, 609.

153 Kilian, Jur-PC 1996, S. 62, 63.

154 Hoeren/Sieber/Geis, Teil 13.2, Rn. 3.

155 Geis, CR 1993, S. 653, 653; ders. in: Hoeren/Sieber/Geis, Teil 13.2, Rn. 5.

156 WORM = Write once - read many.

157 Geis, CR 1993, S. 653, 654.

158 Geis, CR 1993, S. 653, 654.

159 Geis, NJW 1997, S. 3000, 3002.

160 Geis, CR 1993, S. 653, 655.

ge technologische Innovationen könnten durch Verwendung unbestimmter Rechtsbegriffe berücksichtigt werden.[161] Es sollte ein § 416 a ZPO eingefügt werden, der die Beweiskraft von auf Datenträgern gespeicherten Dokumenten denjenigen von Schrifturkunden gleichstellt, wenn nach dem Stand der Technik ein geeignetes Verfahren der Datenauthentizität und die Identität des Ausstellers zu erkennen und das elektronische Dokument durch geeignete Techniken und organisatorische Maßnahmen vor Verfälschung gesichert seien.[162]

Bis zur Einführung einer gesetzlichen Regelung empfiehlt die AWV die Verabredung von Beweisvereinbarungen über den Austausch digitaler Erklärungen. Dabei könne für Schiedsverfahren die Beweisqualität elektronischer Urkunden derjenigen von Schrifturkunden gleichgestellt und im „normalen" Gerichtsverfahren den Parteien durch Anerkennungsvertrag untersagt werden, die Beweiskraft von elektronischen Dokumenten zu bestreiten.[163] Im normalen Verfahren könne nicht wie im schiedsgerichtlichen Verfahren die Beweisqualität inter partes bestimmt werden, da dies in die richterliche Prärogative der freien Beweiswürdigung eingreifen würde.[164] Problematisch sei außerdem eine Beweislastvereinbarung mittels AGB, da dies der Vereinbarung eines Anscheinsbeweises gleichstehen würde und somit nach § 11 Nr. 15 AGBG unzulässig wäre.[165]

Schuppenhauer schlägt ebenfalls eine Formulierung zur Ergänzung des § 416 ZPO vor, welche einerseits das elektronische Medium in seinem Beweiswert dem Papierdokument gleichstellt, aber offen genug für künftige technische Entwicklungen sei.[166] Gleichzeitig erwägt er aber die Beschränkung einer solchen Regelung auf den Geschäftsverkehr unter Kaufleuten, da unter Privaten die nötigen technischen Voraussetzungen evtl. noch nicht vorliegen würden. Dies wäre auch eine ideale Möglichkeit zur Sammlung von Erfahrungswerten, um später an eine generelle Gleichstellung von elektronischem und papiernem Dokument zu denken.[167]

Auch Rihaczek sieht dringenden Handlungsbedarf zur Gleichstellung des elektronischen Mediums mit dem Papier. Andernfalls wäre mangels Anwendbarkeit der Beweisregeln die Zukunft des elektronischen Beweissicherungsverfahrens wenig Erfolg versprechend. Zwar mag die flexible Handhabung der digitalen Signatur im Rahmen des Freibeweises eine gute Möglichkeit zur Erfahrungssammlung sein. Es komme aber nicht darauf an, wie eine neue Technik eines Tages bewertet werden könne, sondern wie diese zum Einführungszeitpunkt zu bewerten sei.[168] Daher sollte zur Gewährleistung der Rechtssicherheit de lege ferenda eine Regelung eingeführt werden, die aber nicht notwendigerweise

---

161 Geis, CR 1993, S. 653, 657.

162 AWV-Schrift 06 531, S. 17f - Nachweis bei Britz, S. 30; ähnlich Geis, CR 1993, S. 653, 657.

163 Hoeren/Sieber/Geis, Teil 13.2, Rn. 47.

164 Hoeren/Sieber/Geis, Teil 13.2, Rn. 48.

165 Hoeren/Sieber/Geis, Teil 13.2, Rn. 61.

166 Schuppenhauer, DB 1994, S. 2041, 2045f; so auch Melullis, MDR 1994, S. 109, 112f.

167 Schuppenhauer, DB 1994, S. 2041, 2046.

168 Rihaczek, DuD 1994, S. 127, 132.

den schriftlichen Urkundenbeweis in allen seinen Facetten auf das elektronische Medium übertragen müsse.[169]

Schippel plädiert für die vollständige Gleichstellung der Beweisqualität elektronischer Dokumente mit Schriftstücken herkömmlicher Form. Gleichzeitig seien auch Ergänzungen in §§ 439 Abs. 2 und 440 Abs. 2 ZPO vorzunehmen, wenn und soweit die elektronische Unterschrift der eigenhändigen Unterschrift i.S.d. §§ 126, 127 BGB gleichgestellt werden sollte.[170]

Auch Rott setzt sich für die Einführung einer gesetzlichen Regel zur Behandlung elektronisch signierter Dokumente in die ZPO ein. Dabei plädiert er jedoch für eine zurückhaltende Gestaltung, um den Möglichkeiten des technischen Wandels und der fortschreitenden Entwicklung digitaler Verschlüsselungssysteme Rechnung tragen zu können. Ebenso wie die AWV hält er eine offene Formulierung, die auf den jeweiligen Stand der Technik abstellt oder im Wege der Rechtsverordnung ausgefüllt werden könnte, für vorzugswürdig.[171] Bis dahin seien elektronische Dokumente im Rahmen des Augenscheinsbeweises richterlich zu würdigen. Dabei erwartet Rott die Übertragung der Maßstäbe des Missbrauchs von mit PIN gesicherten Karten in geschlossenen Systemen auf die Verwendung digitaler Signaturen.[172] Er geht davon aus, dass bei der Erstellung einer Datei mit Hilfe des geheimen Schlüssels der Beweis des ersten Anscheins dafür sprechen werde, dass die Erklärung vom Inhaber des Schlüssels stamme und nicht verändert wurde.[173]

2) Gegner der Anwendung von Beweisregeln des Urkundenbeweisrechts

Baltzer war einer der Ersten, der sich gegen die Anwendbarkeit von Urkundenbeweisregeln auf elektronische Dokumente ausgesprochen hat. Die Beweisführung durch elektronische Handelsbücher sei von einem sonstigen Urkundenbeweis derart weit entfernt, dass eine Gleichstellung von technischer Aufzeichnung und konventioneller Urkunde nicht zu einer Harmonisierung führen werde. Gleichzeitig hielt er aber eine gesetzliche Regelung für wünschenswert, setzte den Schwerpunkt dieser Änderung jedoch nicht im Urkundenbeweisrecht, sondern im Bereich des Augenscheinsbeweises.[174]

Auch Reithmann und Redeker halten eine Gleichstellung des Urkundenbeweises für andere Arten der Datenspeicherung für nicht sinnvoll. Das Urkundenwesen basiere auf dem Prinzip der unmittelbaren Erfassbarkeit des Inhaltes durch optische Wahrnehmung. Dies könne aber nicht durch elektronische Dokumente gewährleistet werden.[175] Redeker

---

169 Rihaczek, DuD 1994, S. 127, 132.

170 Schippel, FS Odersky, S. 657, 666.

171 Rott, NJW-CoR 1998, S. 420, 428.

172 Vgl. zu den Auswirkungen der Rechtsprechung zum ec-Kartensystem, Werner, MMR 1998, S. 338 ff.

173 Rott, NJW-CoR 1998, S. 420, 428.

174 Baltzer, FS Bruns, S. 73, 91.

175 Reithmann, S. 2.

sieht auch keinen Anlass zur Gleichstellung des Inhaltes eines Computerspeichers mit einer Urkunde. Elektronischen Speichern fehle sowohl die Verkehrsfähigkeit als auch seien diese nicht fälschungssicher genug, um den Grund der Privilegierung des Urkundsbeweises für sich in Anspruch nehmen zu dürfen.[176] Allerdings erwähnt Redeker auch, dass Beweisverbesserungen durch Verschlüsselungssysteme erbracht werden könnten, die in Bezug auf digitale Signaturen eine andere Bewertung erlauben könnten.[177]

Hammer und Bizer ordnen elektronische Dokumente ebenfalls unter den Augenscheinsbeweis ein, folgern daraus aber eine rechtliche Unsicherheit hinsichtlich ihres Beweiswertes. Sie lehnen jedoch eine Anwendung von Urkundenbeweisregeln auch de lege ferenda ab.[178] Allenfalls für öffentliche Urkunden könnten nach § 415 ZPO andere Anforderungen gelten, wenn das Gesetz, wie in § 37 Abs. 3 VwVfG, andere Voraussetzungen zur Identifizierung des Ausstellers gelten ließe.[179] Durch die Anwendung des Augenscheinsbeweises eröffneten sich außerdem Erfahrungsräume für eine rechts- und verfassungsverträgliche Technikgestaltung.[180]

Aber auch Bizer und Hammer erkennen, dass für die zukünftige Entwicklung ein dem Papierdokument entsprechender Beweiswert erforderlich sei.[181] Elektronische Signaturverfahren könnten die Abschluss- und Echtheitsfunktion besser als herkömmliche Urkunden gewährleisten. Sofern Zertifizierungsstrukturen die Identität einer Person belegen könnten, wäre auch die Identitätsfunktion erfüllt.[182] Eine Anpassung der Beweisregeln sei allerdings erst dann zu empfehlen, wenn ausreichendes Erfahrungswissen für die Beurteilung des Beweiswertes elektronisch signierter Dokumente vorhanden sei.[183] Bis dahin könnten Dokumente lediglich im Rahmen des Augenscheinsbeweises und der freien Beweiswürdigung durch das Gericht beachtet werden.[184] Die Gerichte könnten die Prüfung eines elektronisch signierten Dokumentes durch einen Sachverständigen bzw. einen sachverständigen Zeugen vornehmen lassen und auf seine Erkenntnisse ihre Beweiswürdigung stützen.[185] Im Laufe der Zeit wäre ein Anscheinsbeweis zugunsten desjenigen herauszubilden, der mit elektronischen Dokumenten seinen Standpunkt zu beweisen versucht, an dessen Ende ein eigenständiger „elektronischer Urkundenbeweis“ stehen könnte.[186]

---

176 Redeker, NJW 1984, S. 2390, 2394.

177 Redeker, NJW 1984, S. 2390, 2394.

178 Bizer/Hammer, DuD 1993, S. 619, 622.

179 Bizer/Hammer, DuD 1993, S. 619, 624.

180 Bizer/Hammer, DuD 1993, S. 619, 625; Bizer, Jahrbuch Telekommunikation und Gesellschaft 1994, S. 157, 163.

181 Bizer/Hammer, DuD 1993, S. 689, 696.

182 Hammer, CR 1992, S. 435, 439.

183 Bizer/Hammer, DuD 1993, S. 689, 697.

184 Bizer/Hammer, DuD 1993, S. 689, 689.

185 Bizer/Hammer, DuD 1993, S. 689, 690.

186 Bizer, Jahrbuch Telekommunikation und Gesellschaft 1994, S. 157, 163.

Rüßmann sieht keine Notwendigkeit zur Gleichstellung elektronischer Dokumente mit Schriftdokumenten. Die Faktoren der Echtheit, Unverfälschtheit und Vertrauenswürdigkeit, welche die entscheidenden Vorteile der elektronischen Dokumente seien, unterlägen auch bei Schriftdokumenten der freien Beweiswürdigung und würden von keiner Beweisregel erfasst. Da elektronische Dokumente ohnehin im Rahmen der freien Beweiswürdigung gewertet würden, sei eine Anpassung nicht notwendig.[187]

Auch Deville/Kalthegener halten eine Ausweitung des Urkundsbegriffs auf elektronische Unterschriftsverfahren für nicht erforderlich. Aufgrund vielfältiger Sicherungsmechanismen bei digital signierten Dokumenten lasse der Beweis durch Augenschein zusammen mit der freien Beweiswürdigung nach § 286 ZPO der elektronischen sogar einen höheren Beweiswert zukommen als der gewöhnlichen Urkunde.[188] Allerdings sollten die Vorschriften zum Urkundsprozess erweitert werden, um vom Gericht selbst überprüfbare Fälle elektronischer Unterschriften durch die §§ 592 ff ZPO zu erfassen. Diese seien jedoch so flexibel zu gestalten, dass eine Anpassung an Veränderungen technischer Gegebenheiten ermöglicht werde.[189]

Roßnagel hält eine Anwendung der Beweisregeln für Urkunden aufgrund der noch vorhandenen Unsicherheiten betreffend digitaler Signaturen für nicht möglich. Zwar deutet er die Gleichstellung de lege ferenda an, rät aber von der Einführung aufgrund fehlender praktischer Erfahrungen ab. Statt technische Unsicherheiten durch rechtliche Fiktionen zu überspielen, sollten lieber erst einige Jahre lang Erfahrungen im Umgang mit elektronischen Dokumenten gesammelt werden, da das Beweisrecht kein geeignetes Instrument zur Forcierung innovativer Techniken sei.[190]

Dies führe aber auch andererseits nicht dazu, dass der Richter technische Sachverhalte willkürlich beurteilen dürfe. Es sei insgesamt damit zu rechnen, dass sich für digitale Signaturen bald Regeln des Anscheinsbeweises herausbilden, die den Nutzern digitaler Signaturen ausreichende Beweissicherheit bieten würden.[191] Der Beweiswert eines digitalen Dokumentes sei zudem demjenigen eines Papierdokuments ebenbürtig, wenn nicht sogar überlegen.[192] Die Vermutung des § 1 Abs. 1 SigG spräche für die Unverfälschtheit des digitalen Dokumentes, wenn die Echtheit erst einmal nachgewiesen sei.

---

187 Rüßmann, Jur-PC 1995, S. 3212, 3220.

188 Deville/Kalthegener, NJW-CoR 1997, S. 168, 172; so auch Graf Fringuelli/Wallhäuser, CR 1999, S. 93, 100.

189 Deville/Kalthegener, NJW-CoR 1997, S. 168, 172.

190 Roßnagel, NJW-CoR 1994, S. 96, 100; so auch Pordesch/Nissen, CR 1995, S. 562, 564f, die für eine behutsame rechtliche Anerkennung dieser neuen Techniken unter Definition klarer technischer und organisatorischer Sicherheitsanforderungen eintreten, S. 569.

191 Roßnagel, RDV 1998, S. 5, 14f.

192 So auch Bieser, in: Geis, Rechtsaspekte des elektronischen Geschäftsverkehrs, S. 49, 56.

Das Signaturgesetz sei eine „geglückte Regelung“[193], welche durch die Sicherheitsvermutung sogar mehr Beweissicherheit als die Papierurkunde biete.[194]

Zwar mag der Nachweis (lediglich) im Rahmen eines Augenscheinsbeweises erfolgen, die Vermutung des § 1 Abs. 1 SigG dürfte aber praktisch den Richter nicht an der Echtheit und Integrität zweifeln lassen. Schlechter gestellt sei der Verwender einer elektronischen Nachricht im Beweisverfahren allerdings, wenn die Sicherheitsvermutung widerlegt würde, da dann die Echtheit der Unterschrift im Rahmen der freien Beweiswürdigung nachgewiesen werden müsste. Eine solche Beweiserfahrung dürfte sich nach der Ansicht Roßnagels mit der Zeit jedoch herausbilden und somit die Schlechterstellung nach und nach relativieren.[195] Eine Änderung des Beweisrechtes sei daher, zumindest solange keine gegenteilige Erfahrung vorliege, nicht erforderlich.[196]

Den Ausführungen Roßnagels schließt sich auch Britz in seiner umfangreichen Untersuchung zum Beweiswert der Elektroniktechnologie an. Gesetzesänderungen, wie die von manchen Autoren vorgeschlagenen, würden ungeeignet sein, die gewünschte Beweiskraft überhaupt sicherzustellen.[197] Neu einzuführende Beweisregeln für elektronische Dokumente seien aber auch gar nicht notwendig, da mittels tatsächlicher Vermutungen und anderer Beweiserleichterungen ebenso angemessene Ergebnisse zu erzielen wären.[198]

Auch Malzer wendet sich gegen die Einführung einer Regelung zur Gleichstellung von elektronischer und Schrifturkunde. Die in einem Computer niedergelegten Dateien bekundeten keine originären menschlichen Gedanken, sondern lediglich die Tatsache der Eingabe und Programmierung von Daten. Dies könne einer schriftlichen Urkunde nicht gleichgestellt werden.[199] Auch der Tatbestand eines Anscheinsbeweises liege aufgrund noch bestehender Unsicherheiten nicht vor.[200]

III. Digitale Signaturen in der öffentlichen Verwaltung

Auch und insbesondere die öffentliche Verwaltung kann die digitale Signatur in elektronischen Dokumenten wirksam zum Einsatz bringen. Die Verwaltung kann zum Vor-

193 Roßnagel/Roßnagel, Einl. SigG, Rn. 143; Roßnagel, NJW 1998, S. 3312, 3320.

194 Roßnagel/Roßnagel, Einl. SigG, Rn. 141; ähnlich Graf Fringuelli/Wallhäuser, die grundsätzlich von der hohen Beweissicherheit digitaler Signatursysteme ausgehen, dies aber nicht allein auf signaturgesetzkonforme Verfahren beschränken wollen, CR 1999, S. 93, 100.

195 Roßnagel/Roßnagel, Einl. SigG, Rn. 143.

196 Roßnagel, in: Jahrbuch Telekommunikation und Gesellschaft 1999, S. 158, 163f.

197 Britz, S. 248 ff.

198 Britz, S. 254 ff.

199 Malzer, DNotZ 1998, S. 96, 106.

200 Malzer, DNotZ 1998, S. 96, 121.

reiter dieser modernen Technologie werden und entscheidend die Diffusion der Telekooperation und der digitalen Signatur vorantreiben.[201]

Die Telekooperation kann hierbei die Kommunikation zwischen Bürgern und Behörden vereinfachen und die Bearbeitungsdauer verkürzen oder zwischen verschiedenen Behörden eine Vereinfachung der Zusammenarbeit ermöglichen. Aber auch innerhalb einer Behördeneinheit kann ein elektronisches Dokument ein wichtiges Hilfsmittel sein, wenn beispielsweise die Archivierung von Verwaltungsdokumenten elektronisch erfolgt und die Integrität durch Signaturen gesichert wird. Die Bandbreite der möglichen Anwendungen reicht von verschiedenen Meldeverfahren über Informationsangebote mit direktem Beamtenkontakt per E-Mail, bis hin zu der Möglichkeit des elektronischen Einvernehmens zwischen Behörden und der elektronischen Aktenführung bzw. -archivierung. Der Rechtswirksamkeit elektronisch ausgetauschter und signierter Erklärungen stehen dabei aber noch über 3.800 Verordnungen entgegen, welche die Schriftform zwingend voraussetzen.

Mit der Möglichkeit des Einsatzes digitaler Signaturen in der öffentlichen Verwaltung hat sich Roßnagel in einem Beitrag beschäftigt.[202] Dabei macht er auf verschiedene Aspekte der Nutzung von digitalen Signaturen und den Besonderheiten der Anforderungen der öffentlichen Verwaltung aufmerksam. Dabei setzt er sich u.a. mit der Führung elektronischer Akten, digitalen Verwaltungshandelns und der elektronischen Archivierung von Verwaltungsunterlagen auseinander.

Die Akte, die Technik der Aktenführung und die Organisation der Aktenverwaltung sind an dem Informationsträger Papier orientiert. Die Führung einer elektronischen Akte muss sich an diesen Vorgaben messen lassen. Eine solche elektronische Akte biete viele Vorteile - rascher Zugriff zentral gelagerter Daten, gleichzeitige Bearbeitung verschiedener Mitarbeiter an verschiedenen Orten, leichtere Kontrolle durch vorgesetzte Stellen. Die „Pflicht zur Führung wahrheitsgetreuer und vollständiger Akten“[203] müsse aber auch durch die elektronische Form der Aktenführung gewährleistet sein. Die Integrität und Identität könne dabei durch digitale Signaturen und Zeitstempel, die Vollständigkeit durch einen signierten Index nachgewiesen werden. Schließlich könnten Verschlüsselungsverfahren das Aktengeheimnis wahren. Grundsätzlich bestünden keine rechtlichen Bedenken, diese Vorgehensweise zu verfolgen. Roßnagel macht aber auch darauf aufmerksam, dass in vielen Vorschriften die Schriftform gefordert würde, so dass dort eine elektronische Akte ohne Rechtsänderung nicht eingerichtet werden könne. [204]

Für den sonstigen Einsatz digitaler Signaturen bei der Verwaltungskommunikation seien zwar nicht in allen, aber in manchen Fällen Rechtsänderungen erforderlich. So könne nach § 37 Abs. 2 S. 1 VwVfG ein Verwaltungsakt in beliebiger Weise erlassen werden.

---

201 Zu möglichen Konzepten des Einsatzes digitaler Signaturverfahren in der öffentlichen Verwaltung vgl. Bieser, in: Geis, Rechtsaspekte des elektronischen Geschäftsverkehrs, S. 49, 61 ff.

202 Roßnagel, in: Jahrbuch Telekommunikation und Gesellschaft 1999, S. 158 ff.

203 BverwG NVwZ 1988, 622.

204 Roßnagel, in: Jahrbuch Telekommunikation und Gesellschaft 1999, S. 158, 162.

Auch könne bei einem schriftlichen Verwaltungsakt nach § 37 Abs. 3, 4 VwVfG auf die eigenhändige Unterschrift verzichtet werden. Da aber auch gleichzeitig in derselben Vorschrift die Schriftform gefordert werde, für die eine Verkörperung der Willenserklärung in Form von Schriftzeichen auf einer Urkunde erforderlich sei, könne ohne Gesetzesänderung ein solcher elektronischer Verwaltungsakt nicht den schriftlichen ersetzen.[205] Aufgrund des Ausnahmecharakters dieser Vorschrift könne auch nicht der Anwendungsbereich auf elektronische Dokumente ausgedehnt werden.[206] Im Übrigen bestünden bei der Erfüllung der Schriftform im Verwaltungsverfahren dieselben Bedenken wie bei der gesetzlichen Schriftform nach § 126 BGB.

Gleichzeitig macht Roßnagel auch darauf aufmerksam, dass diese Form der Kommunikation immer nur als Ergänzung verstanden werden sollte, um eine Akzeptanz auf freiwilliger Basis zu erreichen. Ein exklusiver Einsatz digitaler Dokumente würde in vielen Fällen an durch die Grundrechte gezogene Schranken scheitern.[207]

Nach Abschluss eines Aktenvorgangs seien alle papiernen Unterlagen eine bestimmte gesetzliche Frist, in der Regel zehn bis dreißig Jahre, aufzubewahren. Zur Einsparung von Speicherraum könne wie bei der elektronischen Aktenführung auch eine elektronische Dokumentation und Archivierung realisiert werden. Der möglichen Gefahr der technischen Überholung des Signierverfahrens werde durch § 18 SigV ausreichend Rechnung getragen. Zusätzliche Regelungen zum Archivmanagement wären aber hilfreich.[208]

In diesen Anwendungsfeldern bestehe auch ein Problem des Geheimnis- und Datenschutzes in der Einhaltung rechtlicher Anforderungen bei jeder Neuorganisation von Verwaltungshandeln durch geeignete technisch-organisatorische Sicherungen.[209]

Ebenfalls könnte beispielsweise eine Online-Veröffentlichung zur Erfüllung auf kommunaler Ebene bestehender Publikationspflichten dienen. Hierzu wären aber Gesetzesänderungen notwendig, da in der Regel eine verkörperte Publikation vorgeschrieben ist. Zu einer ausschließlichen Online-Bereitstellung von Termin- oder Regelungsbekanntmachungen werde es jedoch in absehbarer Zeit nicht kommen bzw. kommen können, da mangels ausreichender Verbreitung von Internet-Zugängen die notwendige Bekanntmachung nicht gewährleistet wäre.[210]

Ein Feldversuch Elektronischer Rechtsverkehr soll nun am Hamburger Finanzgericht in Zusammenarbeit mit den Berufskammern der Steuerberater, Wirtschaftsprüfer, Rechts-

---

205 Roßnagel, in: Jahrbuch Telekommunikation und Gesellschaft 1999, S. 158, 163; so auch Stelkens/Bonk/Sachs/Stelkens, § 41, Rn. 32.

206 Vgl. Staatskanzlei NRW, S. 10f.

207 Roßnagel, in: Jahrbuch Telekommunikation und Gesellschaft 1999, S. 158, 163, 166.

208 Roßnagel, in: Jahrbuch Telekommunikation und Gesellschaft 1999, S. 158, 163.

209 Roßnagel, in: Jahrbuch Telekommunikation und Gesellschaft 1999, S. 158, 164.

210 Krahn/Stenner/Werthmann, S. 58.

anwälte, Notare und der Patentanwälte zusammen mit der Datev eG durchgeführt werden.

Vom 2. August 1999 an will das Finanzgericht Hamburg u.a. die Einreichung von Klagen und den Austausch juristischer Schriftsätze per E-Mail erproben.[211] Dabei werden Schriftsätze der Anwälte von den Richtern oder Geschäftsstellen am Bildschirm bearbeitet und als E-Mail an die Finanzämter weitergeleitet. Diese schreiben ihre Klageerwiderung und schicken alles über das Netz zurück ans Gericht.[212] Durch dieses Pilotprojekt verspricht man sich neue Perspektiven in der Praxis der rechts- und steuerberatenden Berufe. Es wird auch erwartet, rechtzeitig praktische Erfahrungen für die Möglichkeiten des elektronischen Rechtsverkehrs bei den einzelnen Berufsgruppen zu sammeln, um mit diesen Erfahrungen umso wirkungsvoller die technischen und rechtlichen Entwicklungen begleiten und fördern zu können.[213]

In diesem Zusammenhang bleibt noch zu erwähnen, dass das OLG Karlsruhe in einem obiter dictum zu einer Entscheidung, in der es um die Übermittlung eines Schriftsatzes per DFÜ ging, erwog, die gesetzliche Schriftform als erfüllt anzusehen, wenn bei der Übermittlung elektronische Signaturen zum Einsatz kommen würden.[214] Dies deutet auf eine mögliche Aufweichung der Rechtsprechung zu elektronischen Dokumenten hin und könnte zu einer Erweiterung der Möglichkeiten der Gerichtskommunikation führen. Es ist aber abzuwarten, ob die Aussagen des OLG Karlsruhe ein Einzelfall bleiben werden.

IV. Die EU-Richtlinie zu elektronischen Signaturen

Auf europäischer Ebene wurde im Mai 1998 eine erste Fassung einer EU-Richtlinie zu elektronischen Signaturen von der Kommission ausgearbeitet und im Juni dem Rat und dem Europäischen Parlament vorgelegt. Das Europäische Parlament hat im Januar seinerseits eine Stellungnahme abgegeben, während der Wirtschafts- und Sozialausschuss sowie der Ausschuss der Regionen ebenfalls Stellung genommen haben. Am 22. April 1999 hat die Kommission einige Änderungsvorschläge des Parlamentes aufgegriffen und einen geänderten Vorschlag über eine Signaturrichtlinie vorgelegt. Auf Grundlage des angepassten Entwurfs der Kommission und den Änderungsvorschlägen des Parlamentes hat schließlich am 28. Juni 1999 der Rat seinen Gemeinsamen Standpunkt fest-

---

211 Vgl. Mitteilung von heise Online vom 28. Juli 1999 unter: http://www.heise.de/newsticker/data/mbb-28.07.99-000/.

212 Vgl. auch die Mitteilungen von Focus Online unter http://www.focus.de/D/DC/DCM/dcm.htm?snr=56461&streamsnr=3 und Web.de unter http://seite1.web.de/show/37A6C67F.AP1/?id=990804-08914-00.

213 So eine Übersicht über den Feldversuch, zusammengestellt von K.-A. Höwel, DATEV eG; auf Anfrage dem Verfasser zugesandt.

214 OLG Karlsruhe, NJW 1998, S. 1650, 1651; vgl. auch das VG Karlsruhe, NJW 1998, S. 2693, 2693, welches bereits eine per Telefax online vom PC übermittelte Klageschrift akzeptierte, obwohl eine eigenhändige Unterschrift nicht vorlag; die Rechtsfrage, ob ein Schriftsatz auch mit eingescannter Unterschrift formwirksam sein kann, ist mittlerweile dem Gemeinsamen Senat der obersten Gerichtshöfe des Bundes zur Entscheidung vorgelegt worden, vgl. RDV 1999, S. 165 f.

gelegt. Dabei hat der ursprüngliche Entwurf der Signaturrichtlinie erhebliche Änderungen durchlaufen. Insbesondere sind noch im Gemeinsamen Standpunkt Regelungen eingeführt, gestrichen bzw. umformuliert worden, die durch die Kommission erst ein- und umgearbeitet worden waren. Die Richtlinie zu elektronischen Signaturen (RLeS) wurde am 30. November vom Rat verabschiedet und muss innerhalb von 18 Monaten in nationales Recht umgesetzt werden.

Die Richtlinie zu elektronischen Signaturen sieht Regelungen vor, die über den Gehalt des deutschen Signaturgesetzes hinausgehen und auf materiellrechtlicher bzw. prozessrechtlicher Ebene die Umsetzung elektronischer Signaturen in die Rechtsordnung anstreben.[215] Wichtige Regelungen sind hierbei insbesondere die Erweiterung der Signiermethoden auch auf andere als asymmetrische Systeme. Zwar wurden von der Kommission im Zuge des Arbeitsprozesses die asymmetrischen Kryptoverfahren als derzeit bekannteste bezeichnet[216], aber durch die bewusst offene Formulierung auch andere Signiersysteme zugelassen. Die im deutschen Signaturgesetz geregelte auf einem asymmetrischen Kryptoverfahren basierende digitale Signatur kann in diesem Zusammenhang als ein Unterbegriff der elektronischen Signatur nach der RLeS verstanden werden.[217]

Die RLeS sieht verschiedene elektronische Signaturen als Authentifikationssysteme vor. Zum einen werden einfache elektronische Signaturen definiert, welche lediglich der Authentifizierung in einfacher Form dienen sollen, Art. 2 Nr. 1 RLeS. Zum anderen werden fortgeschrittene elektronische Signaturen eingeführt, Art. 2 Nr. 1 lit. a RLeS, welche strengeren Sicherheitsanforderungen entsprechen müssen. Sowohl die einfachen als auch die fortgeschrittenen Signaturen bringen als solche noch keine weiter gehenden Rechtsfolgen hervor.

Beruhen fortgeschrittene elektronische Signaturen jedoch auf einem qualifizierten Zertifikat und sind diese von einer sicheren Signaturerstellungseinheit erstellt worden, werden gem. Art. 5 Abs. 1 RLeS weitere rechtliche Folgen an deren Verwendung geknüpft. Nach Art. 5 Abs. 1 lit. b RLeS sind dann die fortgeschrittenen elektronischen Signaturen als Beweismittel in Gerichtsverfahren zuzulassen und nach Art. 5 Abs. 1 lit. a RLeS die Gleichstellung mit handschriftlichen Unterschriften in Bezug auf Daten, die auf Papier vorliegen, sicherzustellen.

Das bedeutet aber nicht gleichzeitig, dass damit auch zwangsnotwendig die gesetzliche Schriftform erfüllt wird. Dies kann in manchen Staaten der Fall sein, in denen die gesetzliche Schriftform lediglich das Erfordernis der handschriftlichen Unterzeichnung besitzt. Anders ist dies jedoch in Deutschland, wo die gesetzliche Schriftform eben zusätzlich noch das Erfordernis der perpetuierten Schriftform auf einem Nachrichtenträger, das Papier, kennt.

---

215 Für eine Übersicht zu Unterschieden zwischen deutscher und europäischer Regelung vgl. Hillebrand/Büllingen, S. 56.

216 In den Erwägungsgründen zu KOM (1998) 297 endg.

217 Brisch, CR 1998, S. 492, 494.

Insoweit ist der jeweilige deutsche Gesetzgeber bei der Umsetzung der Richtlinie nicht gezwungen, ein digital signiertes Dokument grundsätzlich der gesetzlichen Schriftform gleichzustellen, sondern kann dort digitale Signaturen in das Zivilrecht einführen, wo er sie für sinnvoll hält.[218] Dies führt zu einer nahezu freien einzelstaatlichen Kompetenz zur sektorspezifischen Rechtswirkung.[219]

Im Übrigen darf einer elektronischen Signatur die rechtliche Wirksamkeit und Zulassung als Beweismittel vor Gericht nicht allein deshalb abgesprochen werden, weil diese in elektronischer Form vorliegt, nicht auf einem qualifizierten Zertifikat beruht, ein qualifiziertes Zertifikat nicht von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellt oder die Signatur nicht von einer sicheren Signiererstellungseinheit erstellt wurde, Art. 5 Abs. 2 RLeS.

Dieser Zusatz wurde eingeführt, um für die übrigen elektronischen Signaturen einen Grundsatz der Nichtdiskriminierung festzuschreiben. Damit sollen elektronische Signaturen, die nicht den besonderen Anforderungen des Absatzes 1 entsprechen, nicht allein deshalb rechtlich wirkungslos bleiben, weil sie in elektronischer Form vorliegen. Aus anderen Gründen als den in Absatz 2 genannten, scheint eine Ablehnung der rechtlichen Wirkung möglich zu sein.

Roßnagel sieht die von Art. 5 RLeS geforderten Rechtsfolgen der Rechtsgültigkeit und Zulassung als Beweismittel durch die deutsche Prozessordnung als gewährleistet an. Durch die Zulassung elektronischer Dokumente als Augenscheinsobjekte im Rahmen eines gerichtlichen Verfahrens werde der Anforderung entsprochen.[220] Anders sei dies jedoch bei den Regelungen zur Schriftform. Digitale und „fortgeschrittene“ elektronische Signaturen seien der handschriftlichen Unterschrift weitgehend gleichzustellen. Allerdings würden in Art. 3 Abs. 2 RLeS und Art. 3 Abs. 7 RLeS Ausnahmen geregelt, die im Rahmen der Kommunikation mit öffentlichen Stellen andere Regelungen zuließen und daher nicht eine homogene Regelung im deutschen Recht erzwingen würden.[221]

Daran anknüpfend prophezeit Roßnagel für Signaturen zukünftig kein einheitliches Sicherheitsniveau auf europäischer Ebene, sondern mindestens drei rechtlich zu unterscheidende Sicherheitsstufen. Zum einen sei ein hohes Sicherheitsniveau zu erwarten, welches den digitalen Signaturen nach dem SigG entsprechen werde. Ein mittleres Sicherheitsniveau werde durch die fortschrittlichen elektronischen Signaturen mit qualifiziertem Zertifikat nach der RLeS erfüllt. Außerdem sei mit einem weiteren einfachen Sicherheitsniveau zu rechnen, welches aus sonstigen Signaturen besteht, die den Voraussetzungen des Art. 2 Nr. 1 RLeS entsprechen. Dies könnten die bereits im Internet

---

218 Vgl. hgierzu auch Schlechter, K&R 1998, S. 147, 150.

219 Gravesen/Dumortier/Van Eecke, MMR 1999, S. 577, 580.

220 Roßnagel, MMR 1998, S. 331, 335f.

221 Roßnagel, MMR 1999, S. 261, 263f.

etablierten Verfahren wie SSL und von Kreditkartenzahlungen bekannten SET-Verfahren[222] sein.[223]

Dabei leitet er die Zulassung verschiedener Systeme aus den Regelungen des Marktzuganges für Zertifizierungssysteme nach Art. 3 RLeS ab. Nach Art. 3 Abs. 2 RLeS dürfen Mitgliedsstaaten „freiwillige Akkreditierungssysteme einführen oder bereithalten, die auf höherwertige Zertifizierungsdienste abzielen".[224] Außerdem ist es nach Art. 3 Abs. 7 RLeS den Mitgliedstaaten gestattet, im öffentlichen Bereich die Verwendung elektronischer Signaturen von weiteren Anforderungen abhängig zu machen. Damit könne nach Ansicht von Roßnagel das Signaturgesetz als freiwilliges Akkreditierungssystem beibehalten und im öffentlichen Bereich die Verwendung gesetzeskonformer digitaler Signaturen vorgeschrieben werden.[225]

Bedauern äußert Roßnagel in diesem Zusammenhang, dass ungeprüfte Signaturverfahren, die der Richtlinie entsprechen, erst im Nachhinein an ihren Voraussetzungen gemessen werden. Erst im Streitfall wird festgestellt werden, ob die Verfahren auch wirklich die notwendigen Voraussetzungen erfüllen und einen Beweiswert erbringen. Der Nachweis wird mangels Vorabkontrolle auf die Stellen übertragen, die am wenigsten hierfür geeignet sind: die Gerichte und die Internetnutzer. Dieser Nachweis wird in jedem einzelnen Fall von überforderten Gerichten und inkompetenten Nutzern geführt werden müssen. Durch die mangelnde Sicherheitsvermutung, wie noch für Signaturen nach dem Signaturgesetz in § 1 Abs. 1 SigG vorgesehen, wären sie mit einem großen Aufwand für Beweisverfahren verbunden.[226]

Den Regelungsansatz des deutschen Signaturgesetzes hält Roßnagel mit den Zielen der Richtlinie für vereinbar. Nach § 1 Abs. 2 SigG kann jeder ungehindert Zertifizierungsdienste anbieten, ohne vorher eine Genehmigung einholen zu müssen. Das Signaturgesetz muss als freiwilliges Akkreditierungssystem lediglich geringfügig angepasst werden. § 1 Abs. 2 SigG sei so auszulegen, dass alle nicht SigG-konformen Dienste als freiwillige Zertifizierungsdienste in diesem Sinne zu verstehen seien.[227]

Brisch sieht dagegen als Folge der Zulassung auch anderer als asymmetrischer Systeme eine Notwendigkeit zur Öffnung und Anpassung des Signaturgesetzes für weitere Formen der Verschlüsselung.[228]

Andererseits ist Brisch ebenso wie Roßnagel der Ansicht, dass im Rahmen einer Anpassung der Formvorschriften der Gesetzgeber aufgerufen wäre, diese den Anforderungen

---

222 Zum SET-Verfahren vgl. Pichler, NJW 1998, S. 3234, 3237 ff.

223 Roßnagel, MMR 1999, S. 261, 265f.

224 So jedenfalls noch der Wortlaut im ersten Richtlinienentwurf der Kommission [KOM (1998) 297 endg.]. In der geänderten Fassung [KOM (1999) 195 endg.] wurde auf eine Ausrichtung auf höherwertige Dienste verzichtet, im Gemeinsamen Standpunkt aber wieder eingeführt.

225 Vgl. hierzu Roßnagel, NJW 1999, S. 1591, 1593.

226 Roßnagel, DIN-Mitteilungen 1999, S. 712, 714.

227 Roßnagel, DIN-Mitteilungen 1999, S. 712, 715.

228 Brisch, CR 1998, S. 492, 495; jedoch ohne hierzu näherer Ausführungen zu machen.

der RLeS anzupassen. Bei den Beweiswirkungen seien aber weder in der ZPO noch im SigG Änderungen notwendig.[229]

Nach Art. 6 RLeS haftet im Bereich der Identitätsprüfung der Diensteanbieter gegenüber „jeder Person", also nicht bloß gegenüber dem Nutzer seiner elektronischen Signatur, sondern auch gegenüber Personen, zu denen er in keinerlei vertraglicher Beziehung steht. Damit unterwirft die Richtlinie die Zertifizierungsstellen einer vertragsunabhängigen Verschuldenshaftung mit Beweislastumkehr bei Organisationsverschulden gegenüber Dritten. Die Einführung dieser Haftungsregelung nähert sich den Forderungen vieler Autoren an, die eine ähnliche Regelung bereits für das SigG gefordert hatten[230].

Zu erwähnen ist noch, dass im Gemeinsamen Standpunkt keine Regelung zur Aufdeckung der Identität einer Person enthalten ist, welche mit einem Pseudonymzertifikat eine elektronische Signatur erzeugt hat. In dem geänderten Vorschlag der Kommission vom April 1999 [KOM (1999) 195 endg.] war noch in Art. 8 Abs. 4 RLeS eine Regelung hinsichtlich einer Aufdeckung zur Aufklärung von Straftaten bzw. für Rechtsansprüche in Gerichtsverfahren enthalten. Insbesondere die zweite Alternative wurde bereits für das Signaturgesetz als notwendig erachtet und aufgrund des bisherigen Fehlens von der wissenschaftlichen Literatur eingefordert.[231] Die Streichung dieser Passage aus Art. 8 RLeS wurde mit dem Hinweis begründet, dass eine solche Regelung zu restriktiv wäre und einen Anreiz für eine illegale Verwendung elektronischer Kommunikation bedeuten könnte. Umso erstaunlicher und bedauerlicher ist die Streichung des zwischenzeitlich eingefügten Artikels, da nunmehr eine solche Regelung gänzlich durch einzelstaatliche Initiative im Rahmen der Umsetzung in die nationale Gesetzgebung eingeführt werden müsste, ohne dass ein entsprechender Regelungsdruck auf die Mitgliedstaaten vorhanden wäre.[232]

In den Erwägungsgründen zur RLeS wird außerdem eine Revision der Signaturrichtlinie durch die Kommission zwei Jahre nach ihrer Umsetzung festgeschrieben. Dabei soll diese Überprüfung unter anderem sicherstellen, dass der technologische Fortschritt oder Änderungen des rechtlichen Umfelds keine Hindernisse für die Realisierung der erklärten Ziele mit sich gebracht haben. Ein zusammenfassender Bericht soll dann dem Parlament und dem Rat vorgelegt werden.

Die Evaluierung bietet dabei genügend Raum für eine Begutachtung der sich durch die rasche technologische Entwicklung und den globalen Charakter des Internet abzeichnenden Änderungen und Strömungen und lässt eine Anpassung an die dann vorliegen-

---

229 Brisch, CR 1998, S. 492, 497.

230 Für das Signaturgesetz wurde jedoch in der Regel die Einführung einer Gefährdungshaftung gefordert, Brisch, CR 1998, S. 492, 497; zur Gefährdungshaftung und dem SigG vgl. statt vieler Emmert, CR 1999, S. 244, 248.

231 Vgl. statt vieler: Börner, ZUM 1997, 245ff; Roßnagel, NVwZ 1998, S. 1ff.

232 Dies geht jedenfalls aus dem Fehlen der entsprechenden Vorschrift im Gemeinsamen Standpunkt des Rates hervor.

den Gegebenheiten aufgrund des wandelnden technologischen, kulturellen und sozialen Umfeldes erhoffen.

V. Die EU-Richtlinie zu E-Commerce

Mit einem Vorschlag zur Regelung rechtlicher Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt[233] veröffentlichte die Europäische Kommission im November 1998 ihren ersten Entwurf für eine Electronic-Commerce-Richtlinie (EC-RL). Innerhalb dieser Richtlinie werden unter anderem auch das Verhältnis elektronischer Verträge zu Formvorschriften und Aspekte des Vertragsschlusses im Internet geregelt. Im September 1999 wurde eine erneute Fassung der Richtlinie vorgestellt, die sich in einigen Punkten von der bisherigen Version unterscheidet.[234]

In Art. 9 EC-RL wird von den Mitgliedstaaten gefordert, in ihren jeweiligen nationalen Rechtsordnungen einen Vertragsschluss auch „online", also auf elektronischem Wege zu ermöglichen. Dabei müsse ein solcher Vertrag grundsätzlich die gleiche Gültigkeit und Rechtskraft haben wie ein „konventioneller" Vertrag.

In Art. 11 EC-RL werden die Voraussetzungen eines wirksamen Vertragsschlusses im Internet geregelt. Dabei geht es nicht um die Klärung des Streites, ob Offerten auf einer Homepage im Internet ein Angebot oder eine invitatio ad offerendum darstellen. Geregelt sind ausdrücklich nur diejenigen Verträge, die auf einem Angebot des Offerierenden beruhen.

Interessant ist in diesem Zusammenhang, dass die Richtlinie des Europäischen Parlamentes über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz[235] im Entwurfstadium noch eine Regelung über eine „Bestellaufforderung" vorgesehen hatte. Diese wurde allerdings bis zur endgültigen Verabschiedung wieder gestrichen, um das Zusammenspiel von Angebot und Annahme gerade den mitgliedschaftlichen Rechtsordnungen überlassen.[236] Diese Verantwortung ist den Staaten durch die Richtlinie zum E-Commerce bei Angeboten im Internet nun wieder genommen worden.

Nach der alten Fassung der Richtlinie musste derjenige, der ein Angebot im Internet annehmen möchte, die Annahme gegenüber dem Anbieter erklären. Der Empfang der Annahmeerklärung musste dann durch diesen bestätigt und diese Bestätigung wiederum durch den Annehmenden seinerseits noch einmal bestätigt werden. Diese Vorgehensweise zum Abschluss eines Vertrages wurde in der Literatur aufgrund der Umständlichkeit und rechtlichen Unsicherheit kritisiert. Insbesondere sei unklar, was eigentlich passiere, wenn ein Kunde die Bestätigung nicht erstelle, selbst aber von einem wirksamen Vertragsschluss ausgehe, der in Wahrheit noch gar nicht vorliege. Insoweit hat sich zur

233 KOM (1998) 586.

234 KOM(1999) 427 endg.

235 Richtlinie 97/7/EG, ABIEG Nr. L 144 vom 4. Juni 1997, S. 19.

236 Vgl. hierzu die Mitteilungen über die internationale Konferenz in Trier über die Auswirkungen der Fernabsatzrichtlinie vom Oktober 1997, in NJW 1998, S. 210, 211.

neueren Fassung die Prophezeiung Tettenborns bewahrheitet, der dieser Vorschrift keinen langen Bestand voraussagte [237], da die Bestätigung der Empfangsbestätigung ersatzlos gestrichen wurde. Als geschlossen gilt ein Vertrag nun bereits dann, sobald der Nutzer vom Diensteanbieter auf elektronischem Wege die Bestätigung des Empfangs seiner Annahme erhalten hat.

Maennel hat in seinen Äußerungen zu Art. 9 EC-RL einen engen Zusammenhang zur Signaturrichtlinie herausgestellt. In der E-Commerce-Richtlinie werden grundsätzliche Probleme des Vertragsschlusses angesprochen, während mit der RLeS ein europäischer Rechtsrahmen für die Werkzeuge geschaffen würde, die für eine sichere und vertrauensvolle Kommunikation in den Datennetzen benötigt werde. Beide Regelungswerke ergänzen sich gegenseitig und seien aufeinander abgestimmt.[238]

Hoeren und Tettenborn bewerten das Zusammenspiel von EC-RL und RLeS jedoch nicht so harmonisch wie Maennel. Nach der Ansicht Hoerens würde sich der Streit zwischen Deutschland und dem Rest der EU über die Formfrage bei digitalen Dokumenten durch die EC-RL erledigt haben. Jeder elektronische Text erfülle demnach die Schriftform unabhängig davon, wie er zustande gekommen sei. Wie die Formvorschrift der RLeS dazu passe, ließ er jedoch offen.[239]

Tettenborn greift diese Frage von der anderen Seite auf und meint, dass die Vorschrift des Art. 9 Abs. 1 EC-RL weitgehend obsolet werden dürfte, wenn die Signaturrichtlinie in Kraft treten werde. Dass die Mitgliedstaaten den Abschluss elektronischer Verträge nach der EC-RL ermöglichen müssten, dürfte durch die Signaturrichtlinie überflüssig werden. [240]

Die Kommission wollte jedoch ausdrücklich, dass elektronische Unterschriften durch die E-Commerce-Richtlinie unberührt und ungeregelt bleiben. Gerade dies sei Aufgabe der RLeS. Das Erfordernis der Unterschrift falle demnach nicht unter die Formvorschriften des Art. 9 EC-RL, es sei lediglich eine Regelung in Bezug auf den Träger eines Vertrages als Medium oder auch um Erfordernisse hinsichtlich der Mitwirkung von Dritten.[241] Auf die deutsche Rechtsordnung übertragen bedeutet dies, dass die gesetzliche Schriftform in Bezug auf die Unterschrift von der RLeS und in Bezug auf das Papier von der EC-RL erfasst würde.

Weitere Probleme sahen Tettenborn und Hoeren bei der Regelung des Art. 9 Abs. 3 EC-RL. Bedenklich fand Tettenborn dabei, dass es der Kommission möglich sein sollte, die Liste der Ausnahmen nach Art. 9 Abs. 2 EC-RL allein im Wege des Komitologieverfahrens ändern zu können.[242] Hoeren sah eine Gefahr darin, dass die meisten Mitgliedstaa-

---

237 Tettenborn, K&R 1999, S. 252, 258.

238 Maennel, MMR 1999, S. 187, 190.

239 Hoeren, MMR 1999, S. 192, 198.

240 Tettenborn, K&R 1999, S. 252, 257.

241 KOM (1998), 586 endg., S. 28.

242 Tettenborn, K&R 1999, S. 252, 257.

ten jedweden Impetus verlieren würden, dem Gedanken von Art. 9 Abs. 1 EC-RL in ihrem nationalen Recht Rechnung zu tragen. Diese würden erst versuchen, ihre nationalen Bestimmungen durch Anrufung der Kommission zu retten.[243] In der nun veröffentlichen Fassung vom September 1999[244] wurde diese Vorschrift ersatzlos gestrichen. Daher besteht nun der angemahnte Anpassungsdruck an die nationalen Vorschriften. Zu beachten sind jedoch die Ausnahmen in Art. 22 und den Anhängen der EC-RL.

Hinsichtlich des Art. 11 EC-RL ist Tettenborn der Ansicht, dass diese Norm für Deutschland nicht von größerer Bedeutung sein werde. In der Regel dürften Offerten via Internet als invitatio ad offerendum zu qualifizieren sein, welche nicht erfasst wären.[245]

Hoeren sieht darin die Verkennung der tatsächlichen Gegebenheiten des E-Commerce. Auch er ist der Ansicht, dass bei einer Offerte im Internet regelmäßig eine invitatio ad offerendum vorliege, so dass ein Angebot vom Kunden und nicht vom Anbieter ausgehe. [246]

Hierzu merkt Mehrings an, dass nicht bloß pauschal von einer invitatio ad offerendum ausgegangen werden dürfe, sondern vielmehr im Einzelfall zu entscheiden sei, wie eine Offerte im Internet auszulegen wäre. Dabei könne es sich durchaus um ein verbindliches Angebot im Sinne des § 145 BGB handeln.[247]

Der grundsätzlichen Annahme einer invitatio ad offerendum stimmen auch Kaiser/Voigt zu, machen jedoch dort eine Ausnahme, wo die weitere Vertragsabwicklung vollautomatisch abläuft und der Kunde sofort bezahlen muss. Dann seien die Grundsätze, die für Warenautomaten entwickelt wurden, auch auf das Internet anwendbar, und führten dazu, die Web-Site als Angebot „ad incertas personas“ anzusehen. Der Vertrag komme dann durch Inanspruchnahme der Leistung durch den Kunden zustande. [248]

Die EU-Richtlinie wurde mittlerweile am 7. Dezember 1999 vom Ministerrat verabschiedet und muss binnen 12 Monaten von den Mitgliedstaaten in nationales Recht umgesetzt werden.

---

243 Hoeren, MMR 1999, S. 192, 198.

244 KOM(1999) 427 endg.

245 Tettenborn, K&R 1999, S. 252, 257.

246 Hoeren, MMR 1999, S. 192, 198f.

247 Hoeren/Sieber/Mehrings, Teil 13.1, Rn. 63.

248 Kaiser/Voigt, K&R 1999, S. 445, 446f; a.A. Mehrings, BB 1998, S. 2373, 2375, der jegliche Angebote mit Verkaufsabsicht als Angebote „ad incertras personas“ verstanden wissen will, solange der Anbieter keine klarstellenden Hinweise oder sonstige Vorbehalte anbringt, mit denen er seinen Vorbehalt hinsichtlich des rechtlichen Bindungswillens kenntlich macht.

Literaturverzeichnis

Abel, Stefan: Urkundenbeweis durch digitale Dokumente, MMR 1998, S. 644 ff.

Bachofer, Thomas: Die Rechtsgültigkeit der elektronischen Unterschrift, NJW-CoR 1993, S. 25 ff.

Baltzer, Johannes: Elektronische Datenverarbeitung in der kaufmännischen Buchführung und Prozeßrecht, in: Gedächtnisschrift für Rudolf Bruns, S. 73 ff, München: 1980.

Baumbach, Adolf / Lauterbach, Wolfgang / Albers, Jan / Hartmann, Peter: Zivilprozeßordnung mit Gerichtsverfassungsgesetz und anderen Nebengesetzen, 57. Auflage, München: 1999 (zit.: Baumbach/Lauterbach/Albers/Hartmann/Bearbeiter).

Bergmann, Margarethe / Streitz, Siegfried: Beweisführung durch EDV-gestützte Dokumentation, CR 1994, S. 77 ff.

Bieser, Wendelin: Digitale Signatur: Vom Papierdokument zum beweissicheren digitalen Dokument, in: Rechtsaspekte des elektronischen Geschäftsverkehrs, herausgegeben von Ivo Geis, Eschborn: 1999, S. 49 ff.

Bieser, Wendelin / Kersten, Heinrich: Elektronisch unterschreiben – Die digitale Signatur in der Praxis, 2. Auflage, Heidelberg: 1999.

Bizer, Johann: Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD 1992, S. 169 ff.

Bizer, Johann: Rechtliche Probleme der elektronischen Signatur, in: Jahrbuch Telekommunikation und Gesellschaft 1994, herausgegeben von Herbert Kubicek u.a., S. 157 ff.

Bizer, Johann / Hammer, Volker: Elektronisch signierte Dokumente als Beweismittel, DuD 1993, S. 619 ff.

Bizer, Johann / Hammer, Volker: Beweiswert elektronisch signierter Dokumente, DuD 1993, S. 689 ff.

Borges, Georg: Verbraucherschutz beim Internet-Shopping, in ZIP 1999, S. 130 ff.

Brisch, Klaus M.: Gemeinsame Rahmenbedingungen für elektronische Signaturen, CR 1998, S. 492 ff.

Britz, Jörg: Urkundenbeweisrecht und Elektroniktechnologie: eine Studie zur Tauglichkeit gesetzlicher Beweisregeln für elektronische Dokumente und ihre Reproduktionen im Zivilprozeß, München: 1996.

Bruns, Werner F. C.: EDI und Electronic Commerce: Definitionen, informationstechnologische Grundlagen und Normen, in: Rechtsaspekte des elektronischen Geschäftsverkehrs, herausgegeben von Ivo Geis, Eschborn: 1999, S. 127 ff.

Daumke, Michael: Rechtsprobleme der Telefaxübermittlung, ZIP 1995, S. 722 ff.

Deville, Rainer / Kalthegener, Regina: Wege zum Handelsverkehr mit elektronischer Unterschrift, NJW-CoR 1997, S. 168 ff.

Diedrich, Oliver: Erkennungsdienstliches Login - Fingerabdruck-Scanner von Compaq, c't 10/99, S. 74.

Dobbertin, Hans: Digitale Fingerabdrücke - sichere Hashfunktionen für digitale Signaturen, DuD 1997, S. 82 ff.

Ebbing, Frank: Schriftform und E-Mail, CR 1996, S. 271 ff.

Emmert, Ulrich: Haftung der Zertifizierungsstellen, CR 1999, S. 244 ff.

Engel-Flechsig, Stefan: Rechtliche Grundlagen für die Informationsgesellschaft: TKG, IuKDG und MDStV, in: Rechtsaspekte des elektronischen Geschäftsverkehrs, herausgegeben von Ivo Geis, Eschborn: 1999, S. 15 ff.

Erber-Faller, Sigrun: Perspektiven des elektronischen Rechtsverkehrs, MittBayNot 1995, S. 182 ff.

Erber-Faller, Sigrun: Gesetzgebungsvorschläge der Bundesnotarkammer zur Einführung elektronischer Unterschriften, CR 1996, S. 375 ff.

Erber-Faller, Sigrun: Elektronischer Rechtsverkehr und digitale Signaturen in Deutschland – Bisherige Entwicklungen, internationale Bezüge und Zukunftsperspektiven aus notarieller Sicht, in: Rechtsaspekte des elektronischen Geschäftsverkehrs, herausgegeben von Ivo Geis, Eschborn: 1999, S. 85 ff.

Ernst, Stefan: Der Mausklick als Rechtsproblem - Willenserklärungen im Internet, NJW-CoR 1997, S. 165 ff.

Fox, Dirk: Automatische Autogramme - mit digitalen Signaturen von der Datei zur Urkunde, c't 10/1995, S. 278 ff.

Fox, Dirk: Fälschungssicherheit und digitale Signaturen, DuD 1997, S. 69 ff.

Fox, Dirk: Zu einem prinzipiellen Problem digitaler Signaturen, DuD 1998, S. 386 ff.

Fringuelli, Graf Pietro / Wallhäuser, Matthias: Formerfordernisse beim Vertragsschluß im Internet, CR 1999, S. 93 ff.

Fritzemeyer, Wolfgang / Heun, Sven-Erik: Rechtsfragen der EDI-Vertragsgestaltung: Rahmenbedingungen im Zivil-, Wirtschafts- und Telekommunikationsrechts, CR 1992, S. 129 ff.

Fritzsche, Jörg / Malzer, Hans M.: Ausgewählte zivilrechtlicher Probleme elektronisch signierter Willenserklärungen, DNotZ 1995, S. 3 ff.

Geis, Ivo: Zivilprozeßrechtliche Aspekte des elektronischen Datenmanagements, CR 1993, S. 653 ff.

Geis, Ivo: Die digitale Signatur, NJW 1997, S. 3000 ff.

Gounalakis, Georgios / Rhode, Lars: Haftung der Zertifizierungsstellen, K&R 1998, S. 225 ff.

Gräve, Karsten / Lukies, Dietmar: Der Königsweg - Das gerichtliche Mahnverfahren per Datenfernübertragung, NJW-CoR 1998, S. 228 ff.

Gravesen, Gavan G. / Dumortier, Jos / Van Eecke, Patrick: Die europäische Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung, MMR 1999, S. 577 ff.

Hammer, Volker: Rechtsverbindliche Telekooperation - Sicherungsanforderungen der Rechtspflege, CR 1992, S. 435 ff.

von Herget, Harald / Reimer, Mathias: Rechtsform und Inhalte von Verträgen im Online-Bereich, DStR 1996, S. 1288 ff.

Heun, Sven-Erik: Die elektronische Willenserklärung - Rechtliche Einordnung, Anfechtung und Zugang, CR 1994, S. 595 ff.

Heun, Sven-Erik: Elektronisch erstellte oder übermittelte Dokumente und Schriftform, CR 1995, S. 2 ff.

Hoeren, Thomas: Internet und Recht – Neue Paradigmen des Informationsrechts, NJW 1998, S. 2849 ff.

Hoeren, Thomas: Vorschlag für eine EU-Richtlinie über E-Commerce, MMR 1999, S. 192 ff.

Hoeren, Thomas / Sieber, Ulrich: Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, Grundwerk, München: 1999 (zit.: Hoeren/Sieber/Bearbeiter).

Hohenegg, Christoph / Tauschek, Stefan: Rechtliche Problematik digitaler Signaturverfahren, BB 1997, S. 1541 ff.

Jauernig, Othman: Bürgerliches Gesetzbuch. Mit Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, 9. Auflage, München: 1999 (zit.: Jauernig/Bearbeiter).

Jöstlein, Hans: Technische Aufzeichnungen als Beweismittel im Zivilprozeß, DRiZ 1973, S. 409 ff.

Kaiser, Andreas / Voigt, Dennis: Vertragsschluß und Abwicklung des Electronic Commerce im Internet – Chancen und Risiken, K&R 1999, S. 445 ff.

Kilian, Wolfgang: Möglichkeiten und zivilrechtliche Probleme eines rechtswirksamen elektronischen Datenaustausches (EDI), DuD 1993, S. 606 ff.

Kilian, Wolfgang: Zum Beweiswert elektronischer Dokumente, eine Entgegnung zu Rüßmann, Jur-PC 7/95, S. 3212 ff, Jur-PC 1996, S. 62 f.

Köhler, Helmut: Die Rechte des Verbrauchers beim Teleshopping (TV-Shopping, Internet-Shopping), in NJW 1998, S. 185 ff.

Krahn, Christoph / Stenner, Daniel / Werthmann, Christoph: Kommunen und Multimedia, herausgegeben von Thomas Hoeren und Bernd Holznagel, Münster 1999.

Lampe, Ernst-Joachim: Fälschung technischer Aufzeichnungen, NJW 1970, S. 1097 ff.

Maennel, Frithjof A.: Elektronischer Geschäftsverkehr ohne Grenzen - der Richtlinienvorschlag der Europäischen Kommission, MMR 1999, S. 187 ff.

Malzer, Hans Michael: Zivilrechtliche Form und prozessuale Qualität der digitalen Signatur nach dem Signaturgesetz, DNotZ 1998, S. 96 ff.

Meents, Jan Geerts: Verbraucherschutz bei Haustürgeschäften im Internet, K&R 1999, S. 53 ff.

Mehrings, Josef: Verbraucherschutz im Cyberlaw: Zur Einbeziehung von AGB im Internet, in BB 1998, S. 2373 ff.

Melullis, Kalus-J.: Zum Regelungsbedarf bei der elektronischen Willenserklärung, MDR 1994, S. 109 ff.

Münchener Kommentar zum Bürgerlichen Gesetzbuch: Bd. 3, Schuldrecht - Besonderer Teil, 3. Auflage, München: 1995 (zit.: MüKo/Bearbeiter).

Münchener Kommentar zur Zivilprozeßordnung: herausgegeben von Gerhard Lüke und Alfred Walchshöfer, Bd. 2, §§ 355-802, München: 1992 (zit.: MüKo-ZPO/Bearbeiter).

Mugdan, Benno: Die gesamten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich, Band 1, Einführungsgesetz und Allgemeiner Teil, Neudruck der Ausgabe Berlin 1899, Aalen. 1979.

Palandt, Otto: Bürgerliches Gesetzbuch, 58. Auflage, München: 1999 (zit.: Palandt/Bearbeiter).

Pichler, Rufus: Kreditkartenzahlung im Internet, in NJW 1998, S. 3234 ff.

Pordesch, Ulrich: Risiken elektronischer Signaturverfahren, DuD 1993, S. 561 ff.

Pordesch, Ulrich / Nissen, Kai: Fälschungsrisiken elektronisch signierter Dokumente, CR 1995, S. 562 ff.

Provet e.V.: Die Simulationsstudie Rechtspflege: eine neue Methode zur Technikgestaltung für Telekooperation, Berlin: 1994.

Raubenheimer, Andreas: EDI im Bereich von Steuer und Buchführung, CR 1993, S. 19 ff.

Reithmann, Christoph: Allgemeines Urkundenrecht, Begriffe und Beweisregeln, Köln: 1972.

Rihaczek, Karl: Der elektronische Beweis - die Lücke bei der Umsetzung von Technik zum Rechtsgebrauch, DuD 1994, S 127 ff

Roßnagel, Alexander: Digitale Signaturen im Rechtsverkehr, NJW-CoR 1994, S. 96 ff.

Roßnagel, Alexander: Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, S. 3312 ff.

Roßnagel, Alexander: Das Gesetz und die Verordnung zur digitalen Signatur - Entstehung und Regelungsgehalt, RDV 1998, S. 5 ff.

Roßnagel, Alexander: Offene Rechtsfragen des Signaturgesetzes, MMR 1998, S. 75 ff.

Roßnagel, Alexander: Elektronische Signaturen in Europa – Der Richtlinienvorschlag der Europäischen Kommission, MMR 1998, S. 331 ff.

Roßnagel, Alexander: Die digitale Signatur in der Verwaltung, in: Jahrbuch Telekommunikation und Gesellschaft 1999, herausgegeben von Herbert Kubicek u.a., S. 158 ff.

Roßnagel, Alexander: Zur Evaluierung des Signaturgesetzes, in: Jahrbuch Telekommunikation und Gesellschaft 1999, herausgegeben von Herbert Kubicek u.a., S. 212 ff.

Roßnagel, Alexander: Sicherheitspolitiken; qualifizierte Zertifikate – Einführung in die Thematik; DIN-Mitteilungen 1999, S. 712 ff.

Roßnagel, Alexander: Recht der Multimedia-Dienste, Kommentar zum IuKDG und MDStV, herausgegeben von Alexander Roßnagel, München: 1999. (zitiert: Roßnagel/Bearbeiter)

Roßnagel, Alexander: Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung, MMR 1999, S. 261 ff.

Roßnagel, Alexander: Anerkennung von Prüf- und Bestätigungsstellen nach dem Signaturgesetz, MMR 1999, S. 342 ff.

Rott, Peter: Die Auswirkungen des Signaturgesetzes auf die rechtliche Behandlung von elektronischem Datenmanagement und Datenaustausch - eine Prognose, NJW-CoR 1998, S. 420 ff.

Rüßmann, Helmut: Das Beweisrecht elektronischer Dokumente, Jur-PC 1995, S. 3212 ff.

Scheuermann, Dirk: SmartCards und Biometrie - Kodierung biometrischer Referenzdaten am Beispiel der Fingerabdruck-Erkennung, GMD Forschungszentrum Informationstechnik GmbH, 1999.

Scheuermann, Dirk / Struif, Bruno: Biometrische Benutzer-Authentisierung zur Freischaltung digitaler Signaturen, GMD-Spiegel 1999, S. 59 ff.

Schindler, Werner: Sicherheitsaspekte der elektronischen Unterschrift, K&R 1998, S. 433 ff.

Schippel, Helmut: Die elektronische Form, neue Formvorschriften für den elektronischen Rechtsverkehr, Festschrift für Walter Odersky zum 65. Geburtstag am 17. Juli 1996, hrg. von Reinhard Böttcher, Götz Hueck, Burkhard Jähnke, S. 567 ff, Berlin: 1996.

Schlechter, Richard: Sicherheit im Internet – Grundzüge einer europäischen Rechtspolitik, K&R 1998, S. 147 ff.

Schumacher, Stephan: Digitale Signaturen in Deutschland, Europa und den USA, ein Problem, zwei Kontinente, drei Lösungen?, CR 1998, S. 758 ff.

Schuppenhauer, Rainer: Beleg und Urkunde - ganz ohne Papier? - Welche Beweiskraft bietet das elektronische Dokument an sich?, DB 1994, S. 2041 ff.

Seidel, Ulrich: Bestandsaufnahme über die elektronischen Signaturverfahren; Studie des GMD im Auftrag des BSI, 1992.

Seidel, Ulrich: Dokumentenschutz im elektronischen Rechtsverkehr (II), CR 1993, S. 484 ff.

Seidel, Ulrich: Rechtliche Probleme von elektronischen Dokumenten und elektronischer Signatur, in: Jahrbuch Telekommunikation und Gesellschaft 1994, herausgegeben von Herbert Kubicek u.a., S. 148 ff.

von Sponeck, Henning: Beweiswert von Computerausdrücken, CR 1991, S. 269 ff.

Stelkens, Paul / Bonk, Heinz Joachim / Sachs, Michael: Verwaltungsverfahrensgesetz: Kommentar, 5. Auflage, München: 1998 (zit.: Stelkens/Bonk/Sachs/Bearbeiter).

Tettenborn, Alexander: Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr, K&R 1999, S. 252 ff.

Thomas, Heinz / Putzo, Hans: Zivilprozeßordnung: mit Gerichtsverfassungsgesetz und den Einführungsgesetzen, 22. Auflage, München: 1999.

Timm, Birte: Signaturgesetz und Haftungsrecht, DuD 1997, S. 525 ff.

Tschentscher, Axel: Beweis und Schriftform bei Telefaxdokumenten, CR 1991, S. 141 ff.

Waldenberger, Arthur: Grenzen des Verbraucherschutzes beim Abschluß von Verträgen im Internet, BB 1999, S. 2365 ff.

Werner, Stefan: Elektronischer Zahlungsverkehr – Auswirkungen der Rechtsprechung zum ec-Kartensystem, in MMR 1998, S. 338 ff.

Zöller: Zivilprozeßordnung: mit Gerichtsverfassungsgesetz und den Einführungsgesetzen, mit internationalem Zivilprozeßrecht, Kostenanmerkungen, 21. Auflage, Köln: 1999 (zit.: Zöller/Bearbeiter).