

# Der Vertragsschluss im Internet und die digitale Signatur – einige ungelöste Fragen<sup>1</sup>

von

*Thomas Hoeren*

E-Commerce ist in aller Munde. Es verwundert daher nicht, dass auch Juristen verstärkt der Frage nach dem Vertragsschluss im Internet nachgehen. Allerdings zeigt sich sehr schnell, dass der Vertragsschluss im Internet ähnlich wie im normalen Rechtsverkehr funktioniert (I.). Schwierigkeiten bereitet die Frage des Beweiswertes digitaler Dokumente, sowohl in juristischer (II.) wie in technischer Hinsicht (III.).

## I. Allgemeine Vorüberlegungen

Via Internet können prinzipiell Verträge genauso abgeschlossen werden wie im normalen Geschäftsleben (1.). Ärgerlich sind in diesem Zusammenhang aber die geplanten Neuregelungen im Rahmen des Schuldrechtsmodernisierungsgesetzes, insbesondere § 305b BGB-DiskE (2.).

### 1. Klassisches Zivilrecht

Eine Homepage ist regelmäßig nur als „*invitatio ad offerendum*“ anzusehen.<sup>2</sup> Das Angebot geht demnach vom Besteller aus; der Content-Provider entscheidet nach freiem Ermessen darüber, ob er das Angebot annimmt. Der Besteller kann sein Angebot nach §§ 119, 120 BGB anfechten, wenn seine Willenserklärung via Provider falsch übermittelt worden ist.<sup>3</sup> Macht der Besteller irrtümlich bei der Erstellung seiner Mail falsche Angaben, kann er nach § 119 Abs. 1, 2. Var. anfechten.<sup>4</sup> Eine Anfechtung kommt dagegen nicht bei computergenerierten Erklärungen in Betracht, deren Fehler auf lange zuvor eingegebenem, falschem Datenmaterial be-

---

<sup>1</sup> Der folgende Text enthält lediglich die Überlegungen aus einem 10-minütigen Vortrag. Der Redestil wurde beibehalten; die Belege beschränken sich auf das zum Verständnis Notwendigste. Stand: Januar 2001.

<sup>2</sup> Siehe auch *OLG Oldenburg*, CR 1993, 558; *Eckert*, DB 1994, 717, 718; *Wagner*, WM 1995, 1129.

<sup>3</sup> Siehe *Henn*, CR 1994, 595, 596; *Waldenberger*, BB 1996, 2365, 2366.

<sup>4</sup> *OLG Hamm*; CR 1993, 688; siehe auch *BGH*, DB 1984, 2399.

ruht.<sup>5</sup> Benutzt ein Fremder die Kennung des Users, kommt eine Bindung an elektronische Bestellungen nach den Grundsätzen des Handelns unter fremdem Namen in Betracht.<sup>6</sup> Dem Geschäftspartner geht es um ein Geschäft mit dem Träger des Namens; folglich bindet der Vertrag den Namensträger gem. § 177 Abs. 1 BGB nur bei Genehmigung, nach den Regeln der Duldungsvollmacht oder aufgrund einer Anscheinsvollmacht.<sup>7</sup>

Ferner fragt sich, zu welchem Zeitpunkt ein über das Internet geschlossener Vertrag zustande kommt. Nach deutschem Recht wird zwischen den Willenserklärungen unter An- und Abwesenden unterschieden. Bei einem Vertragsschluss unter Anwesenden geht eine Willenserklärung im Zeitpunkt der akustisch richtigen Vernehmung zu (sog. Vernehmungstheorie). Bei der Abgabe einer Willenserklärung unter Abwesenden ist der Zeitpunkt entscheidend, in dem die Erklärung so in den Machtbereich des Empfängers gelangt ist, dass dieser von der Willenserklärung Kenntnis nehmen kann und unter normalen Umständen auch mit der Kenntnisnahme zu rechnen ist.<sup>8</sup> Bei online-kommunizierenden Computern (etwa im EDI-Bereich) wird teilweise von Willenserklärungen unter Anwesenden ausgegangen.<sup>9</sup> Dies mag für den EDI-Bereich noch vertretbar sein. Im WWW-Sektor ist jedoch die Gegenmeinung überzeugender, wonach der Vertragsschluss im Wege von Willenserklärungen unter Abwesenden erfolgt, zumal § 147 Abs. 1 S. 2 BGB eine Erklärung direkt von Person zu Person voraussetzt.<sup>10</sup> Für den Zugang von Willenserklärungen via E-Mail ist daher maßgeblich, wann mit dem Abruf einer Mail durch den Empfänger üblicherweise gerechnet werden kann. Man wird dabei wahrscheinlich davon ausgehen können, dass Geschäftsleute im Electronic Marketing-Bereich mindestens einmal täglich zu normalen Geschäftszeiten ihre Mails lesen. Schwierig ist die Bestimmung von Zugangszeitpunkten bei Privatleuten, da sich in diesem Bereich nach meiner Erfahrung noch keine Usancen für das Lesen von Mails gebildet haben.

## 2. Das Schuldrechtsmodernisierungsgesetz

Probleme ergeben sich jedoch aufgrund der geplanten Einfügung des § 305b BGB-DiskE im Rahmen des Schuldrechtsmodernisierungsgesetzes, mit der eine entsprechende Vorgabe aus der E-Commerce-Richtlinie umgesetzt werden soll. Hiernach hat der Unternehmer, der sich zum Absatz seiner Waren oder Dienstleistungen eines Dienstes der Informationsgesellschaft bedient, seinem Kunden angemessene, wirksame und zugängliche technische Mittel zur Verfügung zu stellen, mit deren

<sup>5</sup> AG Frankfurt, CR 1990, 469.

<sup>6</sup> Siehe Borsum/Hoffmeister, NJW 1985, 1205.

<sup>7</sup> OLG Oldenburg, CR 1993, 558.

<sup>8</sup> Sog. Empfangs- oder Zugangstheorie; siehe hierzu etwa MünchKommVförschler, § 130 Rn. 3 ff.

<sup>9</sup> So etwa Brinkmann, BB 1981, 1185; Fritzsche/Malzer, DNotZ 1995, 9 ff.

<sup>10</sup> So auch für den EDI-Bereich Bartl, DB 1982, 1100; Fritzmeyer/Henn, CR 1992, 130; Redeker, NJW 1984, 2390, 2391.

Hilfe dieser Eingabefehler vor Abgabe der Bestellung erkennen und berichtigen kann (§ 305b Abs. 1 BGB-DiskE).

### a) Dienst der Informationsgesellschaft

Diese Regelung ist in vielerlei Hinsicht problematisch. Zunächst ist der Begriff des „Dienstes der Informationsgesellschaft“ unklar.<sup>11</sup> Dieser Begriff taucht bereits in der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften<sup>12</sup> sowie in dem Vorschlag für eine Richtlinie über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten<sup>13</sup> auf. Unter den Begriff fallen alle in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachten Dienstleistungen. Diese Definition ist in ihrem Kern brauchbar, enthält aber Unschärfen. So fragt sich, welche Regeln bei nicht-kommerziellen Internetdiensten gelten sollen. Im Bereich des Access-Providing gibt es neben CompuServe und AOL auch Provider wie den DFN-Verein, die nicht gewerblich tätig sind. Ähnliches gilt für universitäre Host-Provider oder für private Content-Provider.

Unklar bleibt auch, wann ein Dienst „in der Regel“ gegen Entgelt erbracht wird; man wird hier auf die Judikatur zum gleich lautenden Art. 60 EGV abstellen müssen. Die Formulierung „Dienstleistung“ sollte man im Übrigen nicht im Sinne des deutschen Dienstvertragsrechts missverstehen. Unter den Begriff dürften folglich auch Dienste zum Verkauf von Waren sowie Teleshopping fallen. Gelohnt hätte sich aber auf jeden Fall eine gesetzgeberische Klarstellung. Diese war – wie die Begründung zu § 305b betont – im Rahmen der Umsetzung der E-Commerce-Richtlinie vorgesehen. Im jetzigen Entwurf eines Elektronischen Geschäftsverkehr-Gesetzes (EGG) fehlt jedoch eine solche Definition. Hier wird stattdessen in Anlehnung an die alte Unterscheidung von Tele- und Mediendiensten an die Begrifflichkeit des Teledienstgesetzes (TDG) angeknüpft. Der Begriff des „Dienstes der Informationsgesellschaft“ geht jedoch weiter über den Begriff der Teledienste hinaus und umfasst zum Beispiel auch Mediendienste. Die E-Commerce-Richtlinie hatte sich über die föderal geprägte Unterscheidung von Medien- und Telediensten hinweggesetzt; dieser innovative Schritt wird nunmehr zugunsten einer traditionellen Differenzierung von Medien-Regelungen der Länder (hier: Mediendienstestaatsvertrag) und Tele-Regelungen (hier: Teledienstgesetz) zurückgenommen. Der Verweis in der Begründung zu § 305b auf eine gesetzliche Definition des Begriffs „Dienst der Informationsgesellschaft“ ist damit obsolet geworden.

<sup>11</sup> Schwierig dürfte auch die Abgrenzung zu dem ähnlichen Terminus „Fernkommunikationsmittel“ sein, der in § 480 Abs. 2 BGB-DiskE legaldefiniert worden ist.

<sup>12</sup> Abl. EG L 204 vom 21. Juli 1998, S. 37.

<sup>13</sup> Gemeinsamer Standpunkt des Rates vom 29. Juni 1998 im Hinblick auf den Erlaß der Richtlinie 98/.../EG des Europäischen Parlaments und des Rates über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, Abl. EG L 262 vom 19. August 1998, S. 34.

### b) Praxisrelevanz der Regelung

Vor allem stellt sich die Frage nach der Praxisrelevanz dieser Regelung. Denn diese Norm hat keinen praktischen Anwendungsfall. Sie gilt ausdrücklich nicht, wenn der Vertrag ausschließlich durch den Austausch von E-Mails geschlossen wird (§ 305b Abs. 4). Nun finden im Internet allerdings viele Vertragsschlüsse – ohne Zwischenschaltung einer Homepage – im direkten Austausch von E-Mails (Angebot des Kunden; Annahme durch Content-Provider) statt (s.o.). Für diesen Fall kommt es daher nicht zur Notwendigkeit, Eingabekorrekturen zu ermöglichen. Aber auch für den Fall, dass der Kunde einseitig – absichts des WWW – eine Bestellung aufgibt, kann die Regelung nicht zum Tragen kommen. Denn der Kunde müsste nach § 305b Abs. 1 ja die Möglichkeit bekommen, „vor“ Abgabe der Bestellung seine Erklärung zu sehen und zu berichtigen. Der Unternehmer weiß aber gar nicht, wer ihm wann eine E-Mail zukommen lässt. Er kann nur retroaktiv – nach Eingang der Bestellung – eine Bestätigung zurückschicken; dies käme aber nach den Vorgaben des Gesetzes zu spät. Daher wird man in einem solchen Fall auf Eingabekorrekturtools verzichten müssen.

Macht der Unternehmer nun aber den Fehler, seine Annahmeerklärung schriftlich zu erklären, wäre er wieder zur Einrichtung einer Korrekturmöglichkeit verpflichtet. Allerdings lässt § 305b Abs. 4 Nr. 1 eine Ausnahme auch dann zu, wenn der Vertrag durch eine dem Austausch von E-Mail vergleichbare individuelle Kommunikation geschlossen wird. Ob der Unternehmer schriftlich oder elektronisch seine Annahmeerklärung abgibt, spielt demnach keine Rolle.

Es bleibt damit eigentlich nur ein Anwendungsfall: Jemand klickt sich durch einen virtuellen Warenkorb im WWW durch und soll am Ende noch einmal seine Bestellung „sehen“ und korrigieren können. Aber auch hier ist Vorsicht geboten. Bei Bestellung über die Homepage wird ebenfalls eine E-Mail – etwa über den Netscape Messenger – generiert. Diese E-Mail des Kunden, individuell adressiert an den Content-Provider, wird dann von diesem individuell – durch E-Mail oder Brief – beantwortet. Auch hier liegt also eine wechselseitige individuelle Kommunikation vor, die zum Ausschluss der Korrekturtoolpflicht führt. Nichts anderes würde für den Fall der elektronischen Bestellung und unmittelbaren Lieferung der bestellten Ware gelten, da auch letztere einen individuellen Aussagegehalt hat.

Ähnliche Probleme bereiten die anderen vorgesehenen Pflichten des Unternehmers. Nach § 305b Abs. 2 soll er vor Abgabe der Bestellung „zumindest“<sup>14</sup> über technische Schritte zum Vertragsschluss oder die für den Vertragsschluss zur Verfügung stehenden Sprachen informieren. Auch dies geht an der Lebenswirklichkeit vorbei. Wenn der Kunde per E-Mail (und sei es auch im Rahmen des WWW-Browsers) bestellt, kommt eine wechselseitige individuelle Kommunikation zustande, die zum Ausschluss nach § 305b Abs. 4 Nr. 1 führt.

<sup>14</sup> Dieses „zumindest“ stammt aus der E-Commerce-Richtlinie. Dort bezog es sich aber auf die Informationspflichten, die der nationale Gesetzgeber „zumindest“, als Minimum, einführen muss. Im Verhältnis zwischen Nutzer und Provider ist dieser Hinweis falsch.

Ineffektiv bleibt aus ähnlichen Gründen die in § 305b Abs. 2 S. 2 vorgesehene Bestätigungspflicht. Hiernach hat der Unternehmer den Eingang der Bestellung dem Nutzer unverzüglich auf elektronischem Weg zu bestätigen. Auch hier kommt die Ausnahmeregelung des § 305b Abs. 4 zum Tragen. Ferner stellt sich die Frage der Sanktionen. Nach § 305b Abs. 5 bleibt die Wirksamkeit des Vertrages von eventuellen Verletzungen der Pflichten unberührt. Schadensersatzansprüche des Kunden sind bei Verletzung der Bestätigungspflicht kaum vorstellbar. Auch für die Geltendmachung eines Rechtsbruches im Rahmen von § 1 UWG fehlt es zumindest an der wesentlichen Beeinträchtigung des Wettbewerbs, die für eine Abmahnbefugnis entsprechender Verbände notwendig wäre. Allenfalls für die fehlende Belehrung hinsichtlich der Korrekturtools (§ 305b Abs. 2 Nr. 3) wäre es denkbar, die Schadensersatzpflicht des Nutzers nach § 122 BGB bei irrtümlicher Bestellung aufzuheben. Hierzu bedürfte es aber einer gesetzgeberischen Klarstellung. Es rächt sich hier allerdings, dass § 305b Abs. 2 Informationspflichten kombiniert, die bedienungsbedingte und sonstige Pflichten unzulässigerweise miteinander kombiniert.<sup>15</sup>

Problematisch ist in diesem Zusammenhang auch die Eingangsregel des § 305b Abs. 2 S. 3. Hiernach gelten Bestellung und Empfangsbestätigung als eingegangen, wenn die Parteien sie abrufen können. Man könnte darin eine neue Regelung des Zugangs sehen. Dies würde bedeuten, dass in Abweichung von § 130 BGB (s.o.) eine elektronische Willenserklärung bereits dann zugeht, wenn sie auf dem Server der Gegenseite abrufbar ist. Doch dies kann nicht gewollt sein. Denn § 305b Abs. 2 S. 3 gilt ausdrücklich nur für Bestellung und Empfangsbestätigung, nicht jedoch für die Annahmeerklärung des Unternehmers. Es würde dann für die Willenserklärung des Kunden § 305b, für die des Unternehmers § 130 gelten. Im Übrigen spricht die Norm auch nicht von „Zugang“, sondern von „Eingang“. Dies ist ein neuer Begriff, den es so im BGB nicht gibt. Auch von der systematischen Stellung her spricht alles dafür, dass § 305b Abs. 2 S. 3 nicht den Zugang regelt, würde man doch in einem solchen Fall eher eine Änderung des § 130 statt der Neueinführung einer Vorschrift im Zweiten Buch des BGB erwarten.

Im Ergebnis handelt es sich bei § 305b um eine überflüssige Regelung, die keinen Lebensbezug hat. Dass das Bundesjustizministerium diese Neuregelung federführend vorbereitet hat, darf man dem Ministerium nicht übel nehmen. Denn durch die E-Commerce-Richtlinie war man in Berlin zur Umsetzung verpflichtet. Dennoch fragt sich, ob eine solche nur symbolisch gen Brüssel gerichtete Gesetzgebung den vielbeschworenen Bedürfnissen der Informationsgesellschaft entspricht.

<sup>15</sup> Siehe hierzu auch die Ausführungen von Hans Christoph Grigoleit in diesem Band.

## II. Die Frage des Beweiswertes

Gerade die Frage des Beweiswertes elektronischer Erklärungen erweist sich als Zünglein an der Waage. Wenn der Kunde bestreitet, überhaupt einen Vertrag via Internet abgeschlossen zu haben, muss das Unternehmen den Abschluss beweisen können. Elektronische Erklärungen haben aber keinen besonderen Beweiswert; sie sind vielmehr manipulationsanfällig und jederzeit veränderbar. In Brüssel macht man sich schon seit einiger Zeit Sorgen um die Beweisfrage im elektronischen Handel. Deshalb wurde eine eigene EU-Signaturrichtlinie eingeführt, die derzeit in das deutsche Recht umgesetzt wird. Diese Regelung sieht einen erhöhten Beweiswert für solche elektronischen Dokumente vor, die mittels digitaler Signatur auf der Grundlage einer besonderen Sicherheitsinfrastruktur authentisch gemacht worden sind. Soweit so gut. Doch die digitale Signatur wirft auch und gerade bei der Neuregelung des Rechtsrahmens eine Reihe schwieriger Rechtsfragen auf. Im weiteren sollen – im Rahmen eines Tagungsbandes und seinem Duktus entsprechend – einige kursorische Überlegungen zur Signatur angestellt werden, insbesondere, was deren Einfluss auf den Beweiswert elektronischer Erklärungen angeht. Grundlage für die Überlegungen ist der Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, dem das Bundeskabinett am 6. September 2000 zugestimmt hat<sup>16</sup>.

Einige Kreise insbesondere innerhalb der Kreditwirtschaft sind der Auffassung, dass die neuen Regelungen der §§ 126a BGB-E und 292a ZPO-E nicht ausreichend seien, um den Schutz der Empfänger einer Erklärung, die mit einer digitalen Signatur unterzeichnet abgegeben wird, zu gewährleisten. Die neue Beweisregel in § 292a ZPO-E sei zwar zu begrüßen, sie reiche aber nicht aus, um das Vertrauen des Empfängers in die Authentizität der Erklärung zu begründen. Verbleibe es bei dieser Regelung, werde sich die digitale Signatur nicht im Geschäftsleben durchsetzen. Nach der geplanten Regelung müssten die Empfänger digital signierter Erklärungen das Risiko des Missbrauchs durch Unberechtigte tragen, ohne dass sie Einfluss auf die ordnungsgemäße und sorgfältige Nutzung des Signaturmediums hätten.

Der Zentrale Kreditausschuss befürwortet deshalb die Einführung einer gesetzlichen Zurechnungsregelung, nach der unter bestimmten Umständen vermutet wird, dass die mit einer digitalen Signatur versehene Erklärung vom Signaturinhaber stammt. In einem früheren Diskussionsentwurf ist eine solche Regelung vorgeschlagen, aber im Nachhinein nicht in den jetzigen Entwurf aufgenommen worden.

Zu klären ist, ob Banken, andere Wirtschaftsunternehmen und Behörden durch die nun geplante Regelung tatsächlich einer solchen Unsicherheit ausgesetzt sind, dass sie durch die Regelung nicht hinnehmbare Nachteile erleiden und die großflächige Nutzung der digitalen Signatur nicht Realität werden wird.

<sup>16</sup> Gesetzesentwurf (Stand: 6. September 2000): [www.bmj-bund.de](http://www.bmj-bund.de)

## 1. Geplante Regelungen

Der neue § 126a Abs. 1 BGB-E regelt die Voraussetzungen, um die gesetzlich vorgeschriebene Schriftform durch eine elektronische Form zu ersetzen. Dazu muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen. Die elektronische Form kann die Schriftform jedoch nur ersetzen, wenn die Beteiligten ausdrücklich oder durch schlüssiges Handeln ihre Anwendung billigen und deshalb mit dem Zugang einer elektronischen Willenserklärung rechnen müssen.<sup>17</sup>

In § 292a ZPO-E wird für die Frage nach der Echtheit einer in elektronischer Form abgegebenen Willenserklärung ein Anscheinsbeweis gesetzlich geregelt. Danach kann der Anschein der Echtheit einer in elektronischer Form abgegebenen Willenserklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, nur durch Tatsachen erschüttert werden, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.

## 2. Beweisführung nach der geplanten Regelung

Die geplante Regelung des § 292a ZPO-E stellt eine gesetzliche Regelung der von der Rechtsprechung entwickelten Grundsätze des Beweis des ersten Anscheins dar. Laut Entwurfsbegründung durch das Bundesjustizministerium werde die Rechtsstellung des Erklärungsempfängers im Prozess wesentlich gestärkt und im Hinblick darauf das Vertrauen in die Rechtssicherheit und die Verkehrsfähigkeit der elektronischen Form in besonderem Maße gewährleistet. Der Nachweis der Echtheit der Signatur werde grundsätzlich schon durch die Prüfung nach dem Signaturgesetz erbracht. Diese bestätige die Signierung mit dem auf der Signaturchipkarte gespeicherten geheimen Schlüssel des Inhabers und dessen Identität. Der Anschein der Echtheit könne dann nur dadurch erschüttert werden, dass der Inhaber des Schlüssels schlüssig Tatsachen vorträgt und beweist, die einen abweichenden Geschehensablauf ernsthaft als möglich erscheinen lassen.<sup>18</sup> Nach den allgemeinen Regeln zum Anscheinsbeweis muss der Signaturinhaber eine ernstliche Möglichkeit eines anderen Geschehensablaufs darlegen. Die vage Möglichkeit entkräftet den Anscheinsbeweis nicht.<sup>19</sup> Die Tatsachen, die diese andere Möglichkeit belegen, müssen konkret sein. Werden diese Tatsachen bestritten, so müssen sie bewiesen werden, womit dem Anschein dann die Grundlage entzogen ist.<sup>20</sup> Falls dieser Beweis gelingt, kann sich der Beweispflichtige, also der Erklärungsempfänger, nicht mehr auf den Ablauf nach der allgemeinen Lebenserfahrung berufen, sondern

<sup>17</sup> Begründung zum Gesetzesentwurf (Stand: 6. September 2000): [www.bmj-bund.de](http://www.bmj-bund.de).

<sup>18</sup> Begründung zum Gesetzesentwurf (Stand: 6. September 2000): [www.bmj-bund.de](http://www.bmj-bund.de).

<sup>19</sup> Baumbach/Lauterbach (Hartmann), Anh. § 286 Rn. 19.

<sup>20</sup> BGHZ 8, 239.

muss seinerseits den vollen Beweis dafür erbringen, dass die Signatur doch vom Schlüsselinhaber abgegeben worden ist.

Bevor allerdings die Regelungen des Anscheinsbeweises eingreifen können, muss die Prüfung nach dem Signaturgesetz stattfinden. Maßgeblich ist dafür zum jetzigen Zeitpunkt der Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen (SigG-E) in der Fassung von April 2000. Das Sicherheitsniveau bezüglich der elektronischen Signaturen entspricht durch diesen Entwurf zum neuen Signaturgesetz den Anforderungen der Richtlinie 1999/93 EG über die gemeinschaftlichen Rahmenbedingungen für elektronische Signaturen. Durch das freiwillige Akkreditierungsverfahren für die Zertifizierungsstellen, das in Art 3 Abs. 2 der Richtlinie 1999/93 EG als Option genannt und in § 15 SigG-E umgesetzt wird, ist eine Steigerung des Niveaus der erbrachten Dienste möglich. Im Rahmen dieses Verfahrens gibt es ein Gütesiegel und damit eine nachgewiesene umfassend geprüfte technische und administrative Sicherheit.<sup>21</sup>

Für die Echtheit der qualifizierten elektronischen Signatur müssen sechs Voraussetzungen erfüllt sein. Die Signatur muss ausschließlich dem Schlüsselinhaber zugeordnet sein, seine Identifizierung ermöglichen, mit Mitteln erzeugt worden sein, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle halten konnte, mit den Daten, auf die sie sich bezieht so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann, auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt worden sein.<sup>22</sup>

Diese Voraussetzungen sind durch den Erklärungsempfänger, also z.B. die Bank, zu beweisen, damit die Tatsachen, an die der Beweis des ersten Anscheins anknüpft, vorliegen.

### 3. Kritikpunkte / Schwächen

Die Neuregelung von § 292a ZPO-E wird nicht nur von der Kreditwirtschaft kritisiert.

Auch andere halten diese Regelung für verfehlt.<sup>23</sup> Die Kritik an der von der Bundesregierung in das Gesetzgebungsverfahren eingebrachten Regelung geht zunächst dahin, dass § 292a ZPO-E überflüssig sei. Es könne den Erklärungsempfängern in der Regel nicht gelingen, die Grundlage für den Anscheinsbeweis, das Vorliegen einer ordnungsgemäßen qualifizierten elektronischen Signatur, nachzuweisen. Es müssten dazu die oben genannten sechs Voraussetzungen der qualifizierten Signatur bewiesen werden. Falls dieser Nachweis dem Erklärungsempfänger allerdings im Einzelfall doch gelinge, sei er nicht mehr auf den Anscheinsbeweis des

§ 292a ZPO-E angewiesen. Gelingt es ihm – erwartungsgemäß – nicht, helfe ihm auch § 292a ZPO-E nichts.<sup>24</sup>

Daneben wird kritisiert, dass § 292a ZPO-E nur auf qualifizierte elektronische Signaturen abstellt und schon an diese die Beweiserleichterung knüpft. Bei Erteilung der Signatur durch akkreditierte Zertifizierungsstellen bestehe nach dem heutigen Stand der Technik kein Zweifel an ihrer Echtheit, so dass die akkreditierten Signaturen als Anknüpfungspunkt für den Beweis des ersten Anscheins dienen können.<sup>25</sup> Für qualifizierte elektronische Signaturen, die in der Rangfolge über der einfachen, aber von den Anforderungen her unter der akkreditierten Signatur stehen, gehe die Vermutung des § 292a ZPO-E zu weit. Es handele sich hierbei um eine Beweisfiktion, die sich auf ein nicht verlässliches Beweismittel stütze. Die gefestigte Lebenserfahrung, die Grundlage des von der Rechtsprechung entwickelten Anscheinsbeweises sei, müsse hier durch rechtlich gesicherte und leicht feststellbare Tatsachen ersetzt werden, da hier für ein neues Technikverfahren eine Beweiserleichterung vorweggenommen werde. Diese Voraussetzung sei aber bei qualifizierten elektronischen Signaturen nicht erfüllt. Erst im Nachhinein, also während des Gerichtsverfahrens, könne festgestellt werden, ob die Signatur im ordnungsgemäßen Verfahren erzeugt worden sei. Der Anscheinsbeweis stütze sich also auf eine Tatsachengrundlage, die nicht hinreichend belastbar sei.<sup>26</sup>

Wenn keine Signatur einer akkreditierten Zertifizierungsstelle genutzt wird, muss jeder Erklärungsempfänger nachweisen, dass der Erklärende eine ordnungsgemäße Signatur benutzt hat, damit er in den Genuss der Beweiserleichterung kommen kann. Er müsste also bei der entsprechenden Zertifizierungsstelle nachfragen, ob die Signatur ordnungsgemäß ist. In der Regel wird diese eventuelle Fehler nicht zugeben, so dass erst im Rahmen eines Gerichtsverfahrens geklärt werden kann, ob die elektronische Signatur die elektronische Form erfüllt hat. Zu seiner eigenen Absicherung könnte der Empfänger sich auch im Vorhinein erkundigen, ob das Zertifizierungsunternehmen, von dem der Erklärende seine Signatur erhalten hat, existent und, wenn ja, auch seriös ist. Im Streitfall kann dieses nachher haftbar gemacht werden. Diese Vorgehensweisen sind aber wenig Erfolg versprechend, weil sie voraussetzen, dass der Empfänger die Zertifizierungsstelle des Erklärenden kennt. An diese Unsicherheit bezüglich der Ordnungsgemäßheit des durchgeführten Signaturerteilungsverfahrens einen Anscheinsbeweis zu knüpfen, geht aus den oben genannten Gründen tatsächlich zu weit.

Rein tatsächlich ist eine große Sicherheit möglich, wenn Signaturen einer akkreditierten Stelle genutzt werden. Die Problematik liegt aber darin, dass die Akkreditierung der Zertifizierungsstellen freiwillig ist, also keine generelle Überprüfung im Vorhinein stattfindet.

Banken, Wirtschaftsunternehmen und alle anderen, die Empfänger einer elektronischen Willenserklärung sind, könnten diese Problematik dadurch umgehen,

<sup>21</sup> Roßnagel, MMR 8/2000 S. 458.

<sup>22</sup> Roßnagel, MMR 8/2000 S. 459.

<sup>23</sup> Roßnagel, MMR 8/2000 S. 459.

<sup>24</sup> Roßnagel, MMR 8/2000 S. 459.

<sup>25</sup> Redeker, CR 7/2000 S. 458.

<sup>26</sup> Roßnagel, MMR 8/2000 S. 459, 460.

dass sie nur Signaturen von akkreditierten Zertifizierungsstellen akzeptieren. Unter Umständen ist in die abzuschließenden Verträge oder als Zusatz zum normalen Girovertrag eine dementsprechende Klausel aufzunehmen. Im Ergebnis werden sich diese akkreditierten Signaturen bzw. Zertifizierungsstellen wohl ohnehin durchsetzen, da sie beiden Vertragsparteien eine größere Sicherheit bieten.

Fraglich ist, ob aus den genannten Gründen die neue Regelung des § 292a ZPO-E aufzuheben und ersatzlos zu streichen ist, wie geplant bestehen bleiben soll, oder ob sie durch eine Zurechnungsregelung, wie sie die Banken fordern, zu ersetzen ist.

#### 4. Bedürfnis nach einer weitergehenden Regelung

Für die Aufnahme einer Zurechnungsregelung, wie sie es sich der Zentrale Kreditausschuss wünscht, könnte ein Bedürfnis bestehen.

Die Kreditwirtschaft befürwortet eine Regelung, wie sie schon in einem früheren Diskussionsentwurf enthalten war. Danach soll vermutet werden, dass eine Erklärung in elektronischer Form vom Schlüsselinhaber abgegeben wurde und dass ein Dritter, der die Erklärung mit dem privaten Schlüssel des Signaturschlüsselinhabers abgegeben hat, von diesem bevollmächtigt wurde. Diese Vermutung würde zu einem stärkeren Schutz des Erklärungsempfängers als es die Vorschriften der ZPO über den Beweis durch Urkunden darstellen führen. Es tritt nicht die Verlagerung der Beweislast ein, sondern der Erklärungsempfänger hat nachzuweisen, dass die nicht anerkannte Namensunterschrift echt ist.<sup>27</sup> Dies wäre eine komplette Änderung der Beweispflicht gegenüber der normalen Regelung, dass derjenige das zu beweisen hat, was für ihn günstig ist. Gefordert ist der Beweis des Gegenteils, der im vollen Nachweis besteht, dass aus dem Indiz, aus dem als Vermutungsgrundlage behandeltes Tatbestand, notwendig ein anderer Schluss zu ziehen ist, dass also jede Möglichkeit des gesetzlichen Schlusses wegfällt.<sup>28</sup> Nicht die Banken müssten bei Bestreiten der Echtheit durch den Erklärenden diese nachweisen, sondern der Erklärende würde als Erzeuger der Signatur gelten und müsste das Gegenteil beweisen.

Diese Regelung geht einigen zu weit. Zu berücksichtigen sei, dass Verfahren, die heute sicher sind, in einigen Jahren unsicher sein können. Durch die Fortentwicklung von Hardware und Software werde es in der Zukunft sicher möglich, Schlüsseln, die man heute nicht entschlüsseln kann, zu entschlüsseln. Sichere Signaturverfahren blieben damit nicht auf die Dauer sicher. Außerdem werde diese Beweisregelung von der Signaturrichtlinie nicht verlangt.<sup>29</sup> Die Unsicherheit bezüglich der Ordnungsgemäßheit der elektronischen Signatur durch die Zertifizierungsstellen trifft beide Parteien. Bei einer Vermutungsregelung würde das Risiko komplett auf den Erklärenden abgewälzt. Fraglich ist, ob dies gerechtfertigt und notwendig ist.

<sup>27</sup> *Brusch*, CR 1999, S. 538.

<sup>28</sup> *Baumbach/Lauterbach* § 292 Rn. 8.

<sup>29</sup> *Redeker* C.R. 7/2000 S. 458.

Eine Antwort könnte sich aus dem Vergleich der Benutzung einer digitalen Signatur und der Benutzung von Euroscheckkarten ergeben.

In beiden Fällen besitzt der Benutzer eine Chipkarte und eine Geheimzahl (PIN).

Zum Schutz der Banken bei der Benutzung von Geldautomaten beinhalten die Sonderbedingungen für EC-Kartenverträge in der Regel die Klausel: „Die Geheimzahl ist geheim zu halten; sie darf insbesondere nicht auf der EC-Karte vermerkt und Dritten nicht mitgeteilt werden, denn jede Person, die im Besitz [...] ist, kann [...] Bargeldauszahlungen zu Lasten des Kontos erlangen, für das die Karte ausgegeben wurde.“

Weiter heißt es: „Der Kontoinhaber trägt alle Folgen und Nachteile des Abhandenkommens, der missbräuchlichen Verwendung, [...] und zwar auch dann, wenn dem Kreditinstitut der Verlust angezeigt worden ist [...] bei einem Verlust ist das Kreditinstitut unverzüglich zu benachrichtigen. Das Gleiche gilt, wenn ein unbefugter Dritter Kenntnis erlangt hat oder der Verdacht besteht.“

Folge dieser Klauseln ist, dass ein Anschein dafür besteht, dass ein Geldautomat unter Benutzung der erforderlichen Codekarte mit der Geheimzahl benutzt worden ist, wenn sich keine anderen Anhaltspunkte ergeben.<sup>30</sup> Auch das *AG Schöneberg* folgt der Ansicht, dass von einem Anscheinsbeweis auszugehen sei. Dieser gehe dahin, dass der Karteninhaber die Karte genutzt hat, wenn eine Verfügung unter Verwendung der Karte und der Geheimnummer ausgelöst wurde. Es stellt die Darlegungs- und Beweislast bei missbräuchlicher Verwendung von EC-Karten der Beweiserleichterung, die für den Nachweis des Diebstahls in den Versicherungsfällen gilt, gleich.<sup>31</sup>

In den EC-Kartenfällen wird also vielfach ein Anscheinsbeweis zugunsten der Bank, dass der Kunde die Karte persönlich benutzt hat, angenommen. Diesen Anscheinsbeweis zu erschüttern und die erforderlichen Tatsachen nachzuweisen, fällt den Kunden zunehmend schwer.<sup>32</sup>

Die Situation bei Benutzung einer digitalen Signatur ist nach der geplanten Regelung mit der gegebenen Situation vergleichbar, da beide Systeme von Chipkarte und PIN-Nummer abhängen. Auf den ersten Blick würden die Banken also nicht schlechter gestellt. Problematisch ist allerdings, dass die Banken keine Möglichkeit haben, Einfluss auf die Nachweisbarkeit einer eventuellen Manipulation zu nehmen. Im EC-Kartenbereich können sie an den Geldautomaten Videokameras aufstellen, die aufnehmen, wer die Karte tatsächlich benutzt. Im Fall der „natürlichen“ Unterschrift bleibt den Banken die Möglichkeit eines graphologischen Gutachtens, wenn sie die Echtheit der Unterschrift nachweisen müssen.

Diese Möglichkeiten haben sie bei der digitalen Signatur nicht. Vor allem fehlt die Kontrollmöglichkeit über Kameras.

<sup>30</sup> *I.G. Saarbrücken*, NJW 1987, 2851.

<sup>31</sup> *AG Schöneberg*, 8 C 258/96, DRsp-ROM Nr. 1997/7005.

<sup>32</sup> *AG Schöneberg*, aaO. (Fn. 31).



Folgt man nicht der Auffassung, dass bei EC-Karten ein Anscheinsbeweis zugunsten der Banken eingreift, sind die Banken im Bereich der digitalen Signatur durch die eindeutige gesetzliche Regelung besser gestellt als bei den EC-Karten.

Ein Grund, die Banken in der Neuregelung besser zu stellen als geplant, wäre gegeben, wenn es für sie unzumutbar schwierig und fast immer erfolglos wäre, eine Manipulation oder Sorgfaltsverletzung durch den Kunden nachzuweisen.

Der Anscheinsbeweis könnte zum Einen dadurch erschüttert werden, dass der Kunde vorträgt, der Fehler liegt entweder bei der Bank oder bei der Zertifizierungsstelle. Dieser abweichende Geschehensablauf dürfte, zumindest im Bankbereich für den Kunden schwer zu beweisen sein. Maximal durch Erkundigungen bei der Zertifizierungsstelle könnte er einen Fehler in deren Verantwortungsbereich beweisen. Dies dürfte aber wegen der Haftung der Zertifizierungsstelle für ihre Fehler nach dem Signaturgesetz erhebliche Schwierigkeiten bereiten.

Als Zweites kann der Karteninhaber vortragen, er habe die Karte verloren, jemand anderes habe sie ihm gestohlen und vorher die PIN-Nummer herausgefunden, jemand aus seiner Familie habe die Karte gegen seinen Willen genommen... Hierbei ist aber zu beachten, dass er den abweichenden Geschehensablauf schlüssig und glaubhaft und auch glaubwürdig darlegen und im Notfall auch beweisen muss. Es findet also eine freie Beweiswürdigung durch das Gericht statt, bei der eine Manipulation schwer zu verbergen sein wird.

Die Hürde für den Kunden, der zunächst diesen abweichenden Geschehensablauf darlegen muss, ist fast genauso hoch, wie wenn er die Vermutung, er habe die Erklärung abgegeben, widerlegen muss.

Ein Bedürfnis für eine weitergehende Regelung besteht für die Banken aus diesen Gründen nicht.

Es ist auch nicht sachgerecht, dem Karteninhaber das komplette Risiko der neuen Technik aufzubürden. Noch sind die Manipulationsmöglichkeiten, wie Entwendung und Verlust, sowie Erspähen und Entlocken der PIN, zu groß.

Durch die Neuregelung sind die Banken besser gestellt als bei der EC-Karte, weil der Anscheinsbeweis gesetzlich geregelt ist und sie sich nicht auf die unterschiedliche Rechtsprechung verlassen müssen. Ein Bedürfnis einer weitergehenden Regelung besteht wegen der schwierigen Widerlegbarkeit des Beweises des ersten Anscheins nicht.

### 5. Änderungen des § 130 BGB

Eine Änderung des § 130 BGB bezüglich des Zugangs elektronischer Willenserklärungen wird von dieser Seite, in Übereinstimmung mit dem Gesetzesentwurf des Bundesjustizministeriums nicht für erforderlich gehalten. Eine Willenserklärung ist zugegangen, wenn sie so in den Bereich des Empfängers gelangt ist, dass dieser unter normalen Verhältnissen die Möglichkeit hat, vom Inhalt Kenntnis zu nehmen.<sup>43</sup> Zum Bereich des Empfängers gehören dabei z.B. Briefkasten, Postfach und

Anrufbeantworter. Empfangsvorrichtung in diesem Sinne ist auch der elektronische Briefkasten. Wie im Einzelnen eine Abgrenzung zwischen dem Bereich des Empfängers und allgemein zugänglichen Datennetzen zu ziehen ist, ist Sache des Einzelfalls und damit der Gerichte. Die technischen Möglichkeiten verändern sich zudem so schnell, dass eine ausdrückliche Regelung bald überholt wäre. Es ist also sinnvoller, sich auf die allgemeine, auslegungsfähige Regelung des jetzigen § 130 BGB zu beschränken.

### III. Ausblick: Spieltheorie und Signatur

Selbst wenn es aber zur Einführung eines adäquaten Rechtsrahmens für die Signatur kommt, stellt sich die Frage nach deren Praktikabilität. Wer gibt dem Kunden eigentlich die Technik für den Einsatz digitaler Signaturen in die Hand? Wie kommen Chipkarten-Lesegeräte und Chipkarten, auf denen die digitale Signatur gespeichert ist, in die Haushalte? Der Kunde selbst wird sich von sich aus solche Gerätschaften nicht kaufen, da für ihn zunächst einmal nur Nachteile mit dieser Technologie verbunden sind; insbesondere kann er dann nicht mehr das Zustandekommen eines Vertrages bestreiten, was eben heute problemlos möglich ist. Also muss die Wirtschaft „ran“. Hier wartet aber eine Branche auf die andere. Niemand ist bereit, zugunsten anderer Industriezweige die notwendigen Investitionen zu tätigen. Insofern droht der digitalen Signatur das Aus, bevor diese Technik überhaupt nennenswert in der Praxis eingesetzt wird. Für E-Commerce ist diese Situation ein Fiasko. Wenn sich der Staat nicht möglichst schnell zusammen mit der Wirtschaft zusammensetzt und in einer konzertierten Aktion die Einführung der digitalen Signatur plant, wird es in Deutschland keinen nennenswerten Handel über das Internet geben.

<sup>43</sup> Palandt/Heinrichs, 60. Aufl. 2001, § 130 Rn. 5.