erschien in: NJW (Neue Juristische Wochenschrift) 56/17 (22. April 2003) 1209-1214

Professor Dr. Alexander Roßnagel, Kassel / Professor Dr. Andreas Pfitzmann, Dresden

Der Beweiswert von E-Mail*

Nachdem die ersten Urteile zu bestrittenen E-Mails ergangen sind, die einer ungesicherten E-Mail keinen Beweiswert zumaßen, wird vereinzelt ein Anscheinsbeweis für E-Mails gefordert. Im Beitrag werden die bisherige Rechtsprechung und die Kritik an ihr dargestellt (I), der Beweiswert von E-Mail für ihre Integrität (II) und Authentizität (III) bestimmt und die Argumente für einen Anscheinsbeweis untersucht (IV). Diese erweisen sich als nicht tragfähig. Ein Anscheinsbeweis würde zu einem nicht tragbaren Verlust an Rechtssicherheit führen (V).

I. Verwirrung um den Beweiswert von E-Mail

Der Rechts- und Geschäftsverkehr nutzt zunehmend die Vorteile elektronischer Kommunikation.[1] Neben der papiergestützten rechtlich relevanten Kommunikation entwickelt sich immer stärker ein elektronischer Rechts- und Geschäftsverkehr. In diesem werden Willenserklärungen vor allem in Form von E-Mails oder Web-Formularen ausgetauscht. Rechtsstreitigkeiten im Zusammenhang mit der Verwendung dieser technischen Verfahren sind nicht ausgeblieben und haben inzwischen bereits zu ersten Gerichtsentscheidungen geführt, in denen die Integrität und Authentizität solcher Erklärungen in Frage stand. Wie deren Beweiswert zu beurteilen ist, soll hier am Beispiel von E-Mail erläutert werden. Auf Web-Formulare können die folgenden Erwägungen weitgehend übertragen werden.[2]

Die Instanzgerichte haben einfache ungesicherte E-Mails überwiegend als unzureichend angesehen, um die bestrittene[3] Unverfälschtheit der vorgelegten Erklärung (Integrität)[4] oder die Zurechnung zum angeblichen Aussteller (Authentizität)[5] zu beweisen. Dies gilt auch für die Absicherung der E-Mail-Versendung oder der Teilnahme an einer mailgestützten Internet-Plattform[6] durch Passworte. In ihren Entscheidungen verweisen sie auf die allgemein bekannte Unsicherheit des E-Mail-Verkehrs und die Möglichkeiten, Mails abzufangen und zu manipulieren, unter einer fingierten oder fremden Mail-Adresse Erklärungen abzusenden, Passworte auszuspähen, auszuprobieren oder durch „Trojanische Pferde“ auszuspionieren. Eine Minderheit der Instanzgerichte lässt dagegen die Vorlage der umstrittenen E-Mail oder ihres Ausdrucks als Beweis ausreichen.[7]

---

* Der Autor *Roßnagel* ist Universitätsprofessor für öffentliches Recht an der Universität Kassel, dort Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken. Der Autor *Pfitzmann* ist Professor für Informatik an der Technischen Universität Dresden.

1 S. z.B. BMWi und BMBF, Informationsgesellschaft Deutschland – Fortschrittsbericht zum Aktionsprogramm der Bundesregierung, März 2002.

2 Zur mangelnden Beweiseignung von Web-Formularen s. z.B. *LG Berlin*, CR 2002, 608.

3 Nicht bestrittene Mails sind geeignete Beweismittel für eine behauptete Erklärung – s. z.B. *ArbG Frankfurt*, CR 2002, 615.

4 S. z.B. *AG Bonn*, CR 2002, 301.

5 S. z.B. *LG Bonn*, CR 2002, 293 mit zust. Anm. *Hoeren*; *LG Konstanz*, CR 2002, 609; *AG Erfurt*, MMR 2002, 127.

6 S. z.B. *LG Bonn*, CR 2002, 293 mit zust. Anm. *Hoeren, AG Erfurt*, MMR 2002, 127.

7 S. z.B. *AG Ettlingen*, JurPC Web-Dok. 65/2002; für einen Mail-Ausdruck *AG Hannover*, WuM 2000, 412; in einem obiter dictum *LG Berlin*, CR 2002, 608 für die durch Passwort gesicherte E-Mail; das von *Mankowski*, NJW 2002, 2824 Fn. 34, zitierte *ArbG Frankfurt*, CR 2002, 615, betraf eine unstrittige E-Mail.

erschien in: NJW (Neue Juristische Wochenschrift) 56/17 (22. April 2003) 1209-1214

Die technische[8] und juristische Literatur[9] ging bisher einhellig davon aus, dass ungesicherte Mails ungeeignet sind, eine bestrittene Integrität und Authentizität einer Erklärung zu beweisen. Diese breite Überzeugung war der Grund für die Entwicklung und rechtliche Regelung der elektronischen Signatur. Die europäische Signaturrichtlinie[10] und das SigG[11] sehen elektronische Signaturen als das geeignete Sicherungsmittel, um elektronische Dokumente – und damit auch E-Mails – beweistauglich zu machen.[12]

Nun aber melden sich Stimmen, die – vor allem aus ökonomischen Gründen – die Ablehnung von Mails als geeignetes Beweismittel kritisieren.[13] Sie beschwören die negativen wirtschaftlichen Effekte für die auf ungesichertem E-Mail-Verkehr aufbauenden Geschäftsmodelle, wenn der Nachweis der Integrität und Authentizität einer Erklärung durch einfache E-Mail nicht anerkannt wird. Die bloße Möglichkeit manipulierender Dritteingriffe könne die Ablehnung nicht begründen. Sowohl die Schwierigkeit als auch die Strafbarkeit einer Manipulation führe dazu, dass deren Wahrscheinlichkeit vernachlässigbar sei. Sie plädieren daher sogar für einen Anscheinsbeweis, bei einer ungesicherten E-Mail davon auszugehen, dass sie von dem in der E-Mail-Adresse angegebenen Absender stamme. Dieser sei außerdem durch die Absicht des Gesetzgebers gerechtfertigt, den elektronischen Geschäftsverkehr zu fördern. Allein auf die elektronische Signatur als Problemlösung zu setzen, könne aufgrund ihrer geringen Verbreitung nicht überzeugen.

War also die Entwicklung und Regulierung elektronischer Signaturen nur ein Missverständnis? Kann das Ziel eines rechtssicheren elektronischen Rechts- und Geschäftsverkehrs auch mit ungesicherten E-Mails erreicht werden? Benötigen wir hierfür nur die gerichtliche Anerkennung eines Anscheinsbeweises? Zur Beantwortung dieser Fragen soll im Folgenden der Beweiswert einer ungesicherten E-Mail bestimmt und die technische und rechtliche Begründung für einen Anscheinsbeweis untersucht werden.

II. Beweis der Integrität der Erklärung

Wird eine Willenserklärung bestritten, hat sie derjenige zu beweisen, der sich auf sie beruft.[14] Befindet sich die Willenserklärung in einer E-Mail, wird der Beweis nach § 371 Abs. 2 ZPO „durch Vorlegung oder Übermittlung der Datei angetreten".[15] Ihr sind mögliche Fälschungen aber nicht anzusehen. Sie hat mangels Verkörperung keine Geschichte. Sie enthält einen reinen ASCII-Text, der von jedem, durch dessen Hände oder System sie geht, ohne besonderen Aufwand durch bloßes Eintippen geändert worden sein kann. Zwar ist eine solche Manipulation nach §§ 169 und 303a StGB strafbar. Dennoch können „elektronisch übertragene oder

---

8 S. z.B. *provet/GMD,* Die Simulationsstudie Rechtspflege, 1994, 124 ff.; *Herda*, in: Bundesnotarkammer (Hrsg.), Elektronischer Rechtsverkehr, 1995, 37 ff.; *Damker/Federrath/Schneider*, DuD 1996, 286; *Damker/Müller*, DuD 1997, 24; *Kelm/Kossakowski*. DuD 1997, 192, *Bieser/Kersten*, Elektronisch unterschreiben, 2. Aufl. 1999, 3 ff.; *Fuhrberg*, K&R 1999, 22.

9 S. z.B. *Bizer/Hammer/Pordesch* in: Pohl/Weck (Hrsg.), Beiträge zur Informationssicherheit, 1995, 99 ff.; *Bizer*, in: Haratsch/Kugelmann/Repkewitz (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, 1996, S. 143f.; *Ebbing*, CR 1996, 277; *Mertes*, CR 1996, 770; *Hoeren*, Rechtsfragen des Internet, 1998, 121, *Mense*, DB 1998, 533; *Blaurock/Adam*, ZEuP 2001, 93, *Lüdemann/Adams*, K&R 2002, 8; *Miedbrodt/Mayer*, MDR 2001, 432f.; *Wiebe*, MMR 2002, 128f.

10 S. hierzu Europäische Kommission, Mitteilung „Sicherheit und Vertrauen in elektronischen Kommunikation" vom 6.10.1997, KOM(97)503, 1.

11 S. hierzu die amtliche Begründung, BR-Drs. 966/96, 28; zum SigG s. z.B. *Roßnagel*, NJW 2001, 1817.

12 S. hierzu *Roßnagel*, in: ders. (Hrsg.), Recht der Multimedia-Dienste (RMD), Einl. ins SigG, Rn. 42 m.w.N.

13 S. z.B. *Winter*, JurPC Web-Dok. 109/2002; ihm folgend *Mankowski*, NJW 2002, 2822.

14 S. z.B. *Baumgärtel*, HB der Beweislast im Privatrecht, 2. Auf. 1991, § 145 BGB, Rn. 3.

15 S. z.B. *Ulmer*, CR 2002, 212.

gespeicherte Daten ... verändert werden, ohne dass dies Spuren hinterlässt und nachgewiesen werden kann."[16] Die E-Mail kann nach dem Empfang verändert worden sein, sie kann aber auch bereits „auf ihrem Transport durch offene Netze für den Adressaten unerkennbar gefälscht oder verändert" worden sein.[17] Die Integrität der Datei und damit die Übereinstimmung der zum Beweis vorgelegten mit der ursprünglichen Erklärung kann daher durch die Datei allein[18] nicht bewiesen werden.[19]

III. Beweis der Authentizität

Für die Authentizität des Absenders gilt im Grund das Gleiche. In der als Beweismittel vorliegenden E-Mail-Datei kann jeder – insbesondere der interessierte Beweisführer – ohne Aufwand die gewünschte Absender-Adresse – und bei Bedarf auch alle Header-Einträge, die den Weg der Mail über verschiedene Server dokumentieren – eingetragen oder verändert haben,[20] ohne dass dies erkannt werden könnte.[21] Dieses beliebig manipulierbare elektronische Dokument auszudrucken, kann den Beweiswert nicht erhöhen.[22] Allein aus dem Vorliegen der Datei oder ihres Ausdrucks kann bei einem Bestreiten der Erklärung nicht geschlossen werden, dass der angegebene Absender auch der Erklärende ist.[23] Noch viel weniger darf dies angenommen werden, wenn derjenige, der das elektronische Dokument oder seinen Ausdruck vorlegt, an dem Ausgang des Verfahrens interessiert ist.[24]

Mehr als der bloße Text der E-Mail könnten Logfiles verschiedener Mail-Server über den Versand oder den Weg der E-Mail durch das Internet ergeben. Dies setzt aber voraus, dass Protokollinformationen erhoben wurden, die aussagekräftig, bekannt, noch vorhanden und verfügbar sind. Nicht alle Mail-Server aber erheben die für die Beweisführung notwendigen Informationen. Dem Beweisführer müssten diese außerdem bekannt sein. Die Provider haben allerdings die Nutzungsdaten nach § 6 Abs. 1 TDDSG und die Verbindungsdaten nach § 6 Abs. 2 TDSV[25] sofort nach Ende der Nutzung oder Verbindung zu löschen.[26] Selbst wenn sie dies nicht tun, hat der Beweisführer gegenüber den Betreibern der Mail-Server keinen Anspruch auf Herausgabe der Informationen. Vielmehr verstieße eine Herausgabe gegen die datenschutzrechtliche Zweckbindung der Daten. Eine Vorlage der Informationen könnte allenfalls durch den Richter nach § 142 ZPO angeordnet werden. Dies setzt allerdings voraus, dass der Beweisführer bereits einen Prozess angestrengt hat, bevor er über die Beweismittel

---

16 S. BR-Drs. 966/96, 28.

17 Amtliche Begründung zum FormanpassungsG, BT-Drs. 14/4987, 10, s. z.B. auch *Fuhrberg*, K&R 1999, 22.

18 Im Zusammenhang mit anderen Beweismitteln ist eine Beweisführung möglich.

19 S. hierzu *provet/GMD* (Fn. 8), 124 ff.; *Damker/Müller*, DuD 1997, 24; *Ebbing*, CR 1996, 277; *Mense*, DB 1998, 533; *Fuhrberg*, K&R 1999, 22; *Hoeren*, in Schulze/Schulte-Nölke (Hrsg.), Die Schuldrechtsreform vor dem Hintergrund des Gemeinschaftsrechts, 2001, 320.

20 Diese Möglichkeit übersehen *Winter*, JurPC Web-Dok. 109/2002 und *Mankowski*, NJW 2002, 2822.

21 Der Beweis kann auch nicht dadurch geführt werden, dass im Adressfeld eine namensähnliche Subdomain wie zum Beispiel „Hans@Weissenberg.de" statt einer Provider-Subdomain wie „Hans.Weissenberg@provider.de" angegeben wird – so aber *Mankowski*, NJW 2002, 2822, Fn. 2.

22 S. z.B. *AG Bonn*, CR 2002, 301.

23 S. z.B. *Ebbing*, CR 1996, 277; *Mense*, DB 1998, 533; *Wiebe*, MMR 2002, 128f.

24 Unverständlich daher *AG Hannover*, WuM 2000, 412, das den vom Beweisführer erstellten Ausdruck einer Mail als Beweismittel anerkannte.

25 S. hierzu und zum Streit, ob Mail unter das TDG oder das TKG fallen, s. *Roßnagel/Banzhaf/Grimm*, Datenschutz im Electronic Commerce, 2003, i.E.

26 Ausnahmen gelten für Abrechnungsdaten, die aber nicht zum Beweis einer E-Mail geeignet sind.

verfügt, also bereit ist, ein hohes Prozessrisiko einzugehen. Im Regelfall sind also für die Beweisführung keine aussagekräftigen Protokolldaten verfügbar.

Ein Account für das Versenden von E-Mail ist nicht notwendigerweise durch ein Passwort geschützt. Vielmehr kann eine E-Mail über viele SMTP-Server[27] verschickt werden, die nur prüfen, ob der Sender eine IP-Adresse aus dem passenden Subnetz verwendet. Manche SMTP-Server prüfen sogar nicht einmal das. Um die Identität des Senders bereits beim Versand zu fälschen, ist es nur notwendig, aus einer von ihm empfangenen Mail zu entnehmen, welchen SMTP-Server er benutzt, und zu prüfen, ob dieser für das Versenden ohne Passwort arbeitet. Dann kann jeder – auch ohne größere technische Kenntnisse – im eigenen Mailprogramm eine falsche Absenderangabe und den passenden SMTP-Server eintragen und die Mail abschicken.[28] Wenn der SMTP-Server testet, ob die IP-Adresse des Absenders im Subnetz der Organisation liegt, gelingt dieser Angriff zumindest für Kollegen aus der gleichen Organisation.

Selbst wenn aussagekräftige Protokolldaten vorgelegt werden könnten, aus denen hervorgeht, dass eine Mail vom Account des angegebenen Absenders abgeschickt worden ist, könnte dennoch ein Missbrauch dieses Accounts durch Dritte erfolgt sein, die sich – mit gewissen technischen Kenntnissen – in diesen eingeloggt haben.[29]

Sofern das Versenden der Mail oder die Teilnahme an einer Internetplattform durch ein Passwort abgesichert sein sollte, wird dadurch zwar die Sicherheit erhöht, aber noch kein Beweis für die Authentizität einer Willenserklärung geboten. Zum einen werden immer wieder eklatante Schwachstellen des Schutzes von Passwortdaten beim Systembetreiber bekannt.[30] Zum anderen bieten Passworte nur eine beschränkte Sicherheit gegen ihr Erraten[31] oder Ausspionieren beim Nutzer.[32] Schließlich ist ein Passwortsystem nur so gut wie die vorangegangene Identifizierung des Nutzers. In der Regel aber kann man sich bei einem Mail-Provider oder einer Internetplattform online anmelden – ohne Identifizierung, auch mit übernommenen oder erdachten Namen. Wie soll ein Passwortsystem die Identität eines Erklärenden nachweisen, wenn jeder das Passwort unter falscher Identität erlangen kann?[33]

Ein Passwortschutz muss nicht grundsätzlich ungeeignet sein, den Nachweis über die Identität eines Handelnden zu erbringen. Vielmehr kommt es auf dessen Wirksamkeit an.[34] Diese muss aber vom Beweisführer detailliert nachgewiesen werden, etwa indem dargelegt wird, dass bestimmte Sicherheitskriterien eingehalten wurden[35] und zum Beispiel der Anmeldende persönlich mit Personalausweis identifiziert worden ist, nur Passwörter in ausreichender Länge und mit bestimmten Eigenschaften zugelassen werden, die in bestimmten Zeiträumen geändert werden müssen und nicht umgangen werden können.

---

27 S. hierzu *Schneider/Werner* (Hrsg.), Taschenbuch der Informatik, 4. Aufl. 2001, S. 220, 429, 694.

28 S. hierzu auch *Fuhrberg*, K&R 1999, 23.

29 S. hierzu ausführlich *Damker/Federrath/Schneider*, DuD 1996, 286.

30 S. z.B. zur Sicherheitslücke bei ELSTER im Frühjahr 2001 *Viefhues/Scherf*, K&R 2002, 170f.

31 Im Fall des *LG Bonn*, CR 2002, 293 hatte der Nutzer als sechsstelliges Passwort einer Auktionsplattform sein Geburtsdatum genommen.

32 S. z.B. *LG Bonn*, CR 2002, 294; *AG Erfurt*, MMR 2002, 128; *Fuhrberg*, K&R 1999, 22.

33 Die Beweiseignung verneinen zu recht z.B. *LG Bonn*, CR 2002, 295; *Wiebe*, MMR 2002, 129.

34 Werden mit Snifferprogrammen Passworte abgefangen, ist bei „Replay-Attacken" die Nutzung des Passworts auch dann möglich, wenn es verschlüsselt ist – s. z.B. *Fuhrberg*, K&R 1999, 22.

35 Deren Fehlen kritisiert z.B. *AG Erfurt*, MMR 2002, 128; für Btx *AG Pinneberg*, CR 1998, 693.

erschien in: NJW (Neue Juristische Wochenschrift) 56/17 (22. April 2003) 1209-1214

IV. Anscheinsbeweis für E-Mail?

Weil E-Mail zu unsicher ist, um damit regulär einen Beweis führen zu können, wird vertreten, man müsse die Beweisführung durch einen Anscheinsbeweis ermöglichen.[36] Dieser wird begründet mit der „sehr geringen Wahrscheinlichkeit eines Dritteingriffs", mit der Strafbarkeit solcher Dritteingriffe, mit einem Vergleich zur Ausgestaltung der Beweislast bei schriftlichen Erklärungen, mit einem Wertungswiderspruch zur Einführung der Textform des § 126b BGB und mit der Intention des Gesetzgebers, den elektronischen Geschäftsverkehr zu fördern.

Die von der Rechtsprechung entwickelten Grundsätze gehen davon aus, dass der Anscheinsbeweis für einen ursächlichen Zusammenhang geführt ist, „wenn ein typischer Geschehensablauf feststeht, bei dem nach der Lebenserfahrung aus einem bestimmten unstreitigen oder bewiesenen Sachverhalt auf eine bestimmte Folge oder umgekehrt aus einem feststehenden Erfolg auf eine bestimmte Ursache zu schließen ist".[37]

1. Lebenserfahrung für einen typischen Geschehensablauf?

Eine solche Lebenserfahrung für einen typischen Geschehensablauf reklamieren die Befürworter eines Anscheinsbeweises: Wenn eine ungesicherte E-Mail einen Absender nennt, könne daraus geschlossen werden, dass dieser auch der Autor der E-Mail sei. Manipulationen einer E-Mail seien nur „denklogisch mögliche Geschehensabläufe" mit „absolutem Ausnahmecharakter".[38] Diese Wertung wird neben allgemeinen Erwägungen zur Unmöglichkeit, vollständiger Sicherheit im Wesentlichen mit der persönlichen Erfahrung begründet.[39]

Für die Verwendung einer E-Mail gibt es jedoch weder eine Typizität des Geschehensablaufs, die es zwingend nahelegt, von der Absenderadressangabe auf die Autorenschaft zu schließen, noch gibt es eine Lebenserfahrung, die den „absoluten Ausnahmecharakter" einer Manipulation belegt. Allein persönliche Eindrücke und Erfahrungen aus dem Bekanntenkreis genügen nicht, weil sie durch gegenteilige persönliche Erfahrungen widerlegt werden können.[40] E-Mails werden in so vielen verschiedenen sozialen Kontexten und Prozessen und in so unterschiedlicher Weise technisch realisiert und geschützt, dass kein typischer Geschehensablauf für E-Mail als solche festgestellt werden kann. Erst recht können die dargestellten vielfältigen Möglichkeiten, E-Mails zu fälschen oder zu verfälschen, nicht als „absolute Ausnahme" festgestellt werden.[41] Zum Beispiel beziehen sich die Befürworter eines Anscheinsbeweises allein auf die Gefahr manipulierender Dritteingriffe[42] und blenden das viel größere Risiko einer Manipulation durch den Empfänger vollständig aus.

Doch selbst für das Risiko eines Dritteingriffs kann ein Anscheinsbeweis nicht greifen. Die „Myriade täglich abgesandter E-Mails"[43] hält zwar die statistische Wahrscheinlichkeit eines Dritteingriffs für zufällig herausgegriffene E-Mails gering. Nicht jede große Zahl lässt jedoch Rückschlüsse auf kausale Zusammenhänge zu – wie schon die Millionen täglich erfolgreicher

---

36 S. *Winter*, JurPC Web-Dok. 109/2002, Abs. 11 ff.; *Mankowski*, NJW 2002, 2822 ff.

37 *BGH*, NJW 2001, 1141; *BGH*, NJW 1996, 1828.

38 *Mankowski*, NJW 2002, 2824; *Winter*, JurPC Web-Dok. 109/2002, Abs. 14 ff.

39 Diese führt *Mankowski*, NJW 2002, 2824, als Plausibilitätsargument ein.

40 So war der Autor *Roßnagel* schon zweimal Opfer eines „Identitätsdiebstahls" und streitet mit T-Online über durch Dritte verursachte Gebühren für den Internetzugang.

41 S. Bundeskriminalamt, Notwendigkeiten, Möglichkeiten und Perspektiven der Bekämpfung von Internetkriminalität, 2002; *Fuhrberg*, K&R 1999, 22, ging von mehreren 10.000 Accounts aus, die durch abgefangene Passworte unsicher geworden sind.

42 S. *Mankowski*, NJW 2002, 2823f.; *Winter*, JurPC Web-Dok. 109/2002, Abs. 13 ff.

43 *Mankowski*, NJW 2002, 2823; *ders*., EWiR § 145 BGB 1/01, 1124; *ders*., ZMR 2002, 247.

Vertragsabschlüsse oder die Milliarden unterschriebener Urkunden zeigen, aus denen auch kein Anscheinsbeweis abgeleitet wird. Hinzu kommen muss ein logisch nachvollziehbarer Zusammenhang zwischen einem feststehenden Erfolg (E-Mail) auf eine bestimmten Ursache (Autorenschaft) auf Grund bestimmter Sicherheitsmaßnahmen. Da die beschriebenen Manipulationen mangels Sicherheitsmaßnahmen jederzeit möglich sind, kann aus den – allein auf Grund der großen Zahl – vielen unmanipulierten E-Mails nicht geschlossen werden, dass die umstrittene E-Mail eindeutig oder auch nur mit hoher Wahrscheinlichkeit von dem angegebenen Adressaten stammt.

2. Vergleich mit anderen Anscheinsbeweisen

Daher ist ein Vergleich – selbst wenn nur das Problem des Dritteingriffs gegenüber einer mit Passwort gesicherten Authentifizierung betrachtet wird – mit dem ohnehin umstrittenen Anscheinsbeweis bei Verwendung einer EC-Karte am Geldausgabeautomaten[44] und beim Online-Banking[45] nicht möglich.[46] In beiden Fällen genügt die Kenntnis der PIN für einen Missbrauch nicht. Vielmehr kommen weitergehende Sicherungen zur Anwendung. Bei der Verwendung einer EC-Karte wird die Berechtigung durch die Karte (Haben) und die PIN (Wissen) abgesichert. Außerdem kommuniziert der Nutzer nur direkt mit dem Endgerät, nicht aber über ein offenes Netz. Beim Online-Banking wird die Berechtigung ebenfalls durch zwei Sicherheitsmerkmale abgesichert, durch die PIN und zusätzlich durch eine Transaktionsnummer (TAN), die für jede einzelne Transaktion unterschiedlich ist. Erst diese zusätzliche Sicherungsmaßnahmen, die bei E-Mail fehlen, erlauben zumindest, die Schlussfolgerungen von diesen zum jeweiligen Kausalitätsanschein konkret nachzuvollziehen.[47]

Ähnlich wird auch der – ebenfalls umstrittene – Anscheinsbeweis für Telefonabrechnungen[48] durch zusätzliche Sicherungen gerechtfertigt. Dieser wird nur dann anerkannt, wenn die Einzelgespräche aufgelistet sind und ein nachträgliches Prüfungsverfahren ergeben hat, dass die für Dritte unzugängliche Zähleinrichtung für den jeweiligen Anschluss richtig arbeitet.[49]

Wenn schon ein Vergleich bemüht werden soll, dann entspricht die E-Mail allenfalls einer in Druckbuchstaben mit Bleistift geschriebenen unterschriftslosen Postkarte.[50]

3. Vergleich mit Schrifturkunden?

Für einen Anscheinsbeweis wird geltend gemacht, dass bei einer eigenhändigen Unterschrift eine Vermutung für deren Richtigkeit bestehe und der Beweisgegner deren Fälschung behaupten und beweisen müsse.[51] Dies ist unzutreffend. „Nach §§ 439, 440 ZPO besteht ledig-

---

44 S. z.B. *LG Bonn*, MDR 1995, 277; *LG Frankfurt*, DuD 2000, 109; *LG Stuttgart*, WM 1999, 1934; gegen Anscheinsbeweis z.B. *OLG Hamm*, NJW 1997, 1711; *LG Dortmund,* CR 1999, 556; *LG Frankfurt,* CR 1999, 556.

45 S. z.B. *Werner*, MMR 1998, 232 ff.; *ders.*, MMR 1998, 338.; *Wiesgickl*, WM 2000, 1050; *Pichler*, Rechtsnatur, Rechtsbeziehungen und zivilrechtliche Haftung beim elektronischen Zahlungsverkehr im Internet, 1998, S. 78.

46 Ein Vergleich mit der EC-Karte ist nach *Hoeren* (Fn. 19), 325, nur für die elektronische Signatur zulässig.

47 Ebenso *LG Bonn*, CR 2002, 294, *AG Erfurt*, MMR 2002, 128.

48 Auf ihn berufen sich *Mankowski*, NJW 2002, 2825; *Winter*, JurPC Web-Dok. 109/2002, Abs. 16.

49 S. z.B. *OLG Zweibrücken*, ArchPT 1996, 158; *OLG München*, ArchPT 1997, 54; ; *OLG Schleswig*, ArchPT 1997, 59; *OLG Düsseldorf*, ArchPT 1998, 52; *OLG München*, ArchPT 1997, 54; OLG Koblenz, RTkom 2000, 152, gegen einen Anscheinsbeweis bei deutlich überhöhter Rechnung *LG Landau*, ArchPT 1996, 157; *OLG Celle*, NJW-RR 1997, 568; *LG Oldenburg*, NJW-RR 1998, 1365; *LG Berlin*, NJW-RR 1996, 985; *LG Memmingen*, NJW-RR 2002, 996; *LG Paderborn*, NJW-RR 2002, 998, für SMS; s. hierzu *Allgeier*, RDV 2000, 53; *Reimann*, DuD 2001, 27.

50 S. auch z.B. *Fuhrberg*, K&R 1999, 23.

51 *Mankowski*, NJW 2002, 2824f.

lich eine widerlegliche Vermutung für die Echtheit einer Schrifturkunde, wenn die Unterschrift des Ausstellers unstrittig oder bewiesen ist. Wird die Echtheit der Unterschrift vom Beweisgegner nicht anerkannt, ist sie von der beweisbelasteten Partei zur vollen Überzeugung des Gerichts zu beweisen (§ 440 Abs. 1). Für diesen Beweis sind Erleichterungen nicht vorgesehen. Er unterliegt der freien Beweiswürdigung."[52] Die eingeforderte Gleichbehandlung mit der Schrifturkunde muss also gerade dazu führen, den Anscheinsbeweis abzulehnen. Es wäre ein eklatanter Wertungswiderspruch, der sichereren eigenhändig unterschriebenen Urkunde den Anscheinsbeweis zu versagen, aber der unsicheren E-Mail zuzusprechen. Schließlich unterscheidet sich ein Schriftstück von einer E-Mail durch zwei entscheidende Sicherheitseigenschaften. Der E-Mail fehlt sowohl die Verkörperung, die Manipulationen erkennen lässt, als auch die eigenhändige Unterschrift, die gerade in der Beweisaufnahme eine Identifizierung des Erklärenden an Hand dieses biometrischen Merkmals ermöglicht.[53]

4. Förderung der E-Mail als Textform?

Weiter wird geltend gemacht, mit der Textform nach § 126b BGB, die weder eine Unterschrift noch eine Signatur fordert, hätte der Gesetzgeber E-Mails fördern wollen. Dem müsse auch eine Erleichterung bei der Beweisführung entsprechen, die den Nachweis der Integrität und Authentizität nicht an der bloßen Möglichkeit eines Dritteingriffs scheitern lasse.[54]

Tatsächlich ist die Argumentation des Gesetzgebers genau umgekehrt: Die Textform, durch deren Einführung nur bestehende Ausnahmen von der Schriftform für Massenerklärungen zusammengefasst worden sind, ist nur für Willenserklärungen mit geringem Fälschungsrisiko geeignet. „Entscheidender Beurteilungsmaßstab für die Entscheidung, welche Formtatbestände im Einzelnen für die Textform geöffnet werden sollen, ist die zu gewährleistende Sicherheit im Rechtsverkehr. Die Textform ist nur für solche Formtatbestände vorgesehen, bei denen eine ausreichende Sicherheit auch gegeben ist, wenn ... die Erklärung ... nur mittels telekommunikativer Einrichtungen übermittelt wird. Dies gilt vor allem für die Formtatbestände, bei denen keiner der Beteiligten und auch kein Dritter ein ernsthaftes Interesse an einer Fälschung der Erklärung haben kann."[55] E-Mail ist nur dann akzeptabel, wenn es für die Erklärung kein Fälschungsrisiko gibt. Gibt es aber ein Fälschungsrisiko, ist E-Mail für die Willenserklärung – zumindest als Rechtsform und als Beweismittel – ungeeignet.[56]

5. Förderung des elektronischen Geschäftsverkehrs?

Zwar ist es richtig, dass der Gesetzgeber mit verschiedenen Regelungen versucht, den elektronischen Rechts- und Geschäftsverkehr zu fördern. Aber diese Förderung bezieht sich ausschließlich auf Formen sicherer Kommunikation und gerade nicht auf unsichere E-Mail. „Da elektronische Nachrichten auf ihrem Transport durch offene Netze für den Adressaten unerkennbar gefälscht oder verändert werden könne, bedarf es ... eines sicheren Rahmens zur elektronischen Authentifizierung des Kommunikationspartners und Überprüfung der Integrität der übermittelten Daten."[57] „Diese Forderung erfüllt die gesetzliche digitale Signatur."[58] De-

---

[52] Amtl. Begr. zum Formanpassungesetz, BT-Drs. 14/4987, 25, 23; s. hierzu auch *Nissel*, Neue Formvorschriften bei Rechtsgeschäften, 2001, 88.

[53] Daher hat der Gesetzgeber die Regelungen zur Schrifturkunde nicht auf elektronische Dokumente angewendet– s. Amtl. Begr. zum Formanpassungesetz, BT-Drs. 14/4987, 13, 17, 23, 25.

[54] *Mankowski*, NJW 2002, 2823, 2826.

[55] Amtl. Begr., BT-Drs. 14/4987, 18.

[56] Textform und elektronische Form wurden durch das Formanpassungesetz eingeführt, das aber gezielt nur der elektronischen Form einen Anscheinsbeweis zugebilligt hat.

[57] Amtl. Begr. zum Formanpassungesetz, BT-Drs. 14/4987, 10; ebenso amtl. Begr. zum SigG, BR-Drs. 966/96, 28, und zum 3. VwVfÄG, BT-Drs. 14/9000, 26.

ren Einführung hat der Gesetzgeber durch das SigG und die SigV, durch die elektronische Form im BGB[59] und im VwVfG[60] sowie durch viele weitere gesetzliche Regelungen unterstützt. Der Förderung eines sicheren elektronischen Rechts- und Geschäftsverkehrs würde es widersprechen, die Anerkennung unsicherer E-Mails als Beweismittel zu fördern.

Dementsprechend plant auch die Bundesregierung: Die Bundesverwaltung wird „E-Mails zum Schutz der Integrität und Authentizität nachprüfbar mit einer Absenderkennung versehen ... (und) bei Online-Transaktions-Dienstleistungen Mechanismen zur Authentisierung (und) ... zur sicheren Identifikation ... anbieten".[61] Und das Bundeswirtschaftsministerium empfiehlt mittelständischen Unternehmen, wenn es darauf ankommt, wer ein Dokument verschickt hat und ob der Inhalt während der Übertragung verändert wurde, also beispielsweise bei Bestellungen und rechtsverbindlichen Vertragsabschlüssen, nicht auf E-Mail zu vertrauen, sondern elektronische Signaturen einzusetzen.[62]

Die Mittel, elektronische Signaturen zu erzeugen und zu prüfen, sind noch nicht weit verbreitet, dennoch ist die elektronische Signatur die einzige bewährte Technik, die bei der offenen Kommunikation im Internet Integrität und Authentizität für den elektronischen Rechtsverkehr gewährleisten kann.[63] Sie ist keine „Totgeburt",[64] sondern wird in vielen Bereichen in der Verwaltung, bei Anwälten und Steuerberatern genutzt. Ihr Einsatz entwickelt sich langsamer als erhofft. Dies hat viele Gründe – unter anderem bisher fehlende Rechtsvorschriften, fehlende Anwendungsmöglichkeiten[65] und eine verfehlte Infrastrukturpolitik der Bundesverwaltung.[66] Dies wird aber ihre zunehmende Nutzung nicht aufhalten. Hierzu wird auch die fortschreitende Erkenntnis mangelnder Sicherheit von E-Mails beitragen.

6. Gesetzlicher Anscheinsbeweis nur für qualifizierte elektronische Signaturen

Gegen einen Anscheinsbeweis für E-Mails spricht auch § 292a ZPO, der für die Verwendung elektronischer Dokumente, die mit einer qualifizierten elektronischen Signatur gesichert sind, einen Anscheinsbeweis anordnet.[67] Diese Beweiserleichterung hat der Gesetzgeber allein wegen des „hohen Sicherheitsstandards qualifizierter elektronischer Signaturen" festgelegt, der ihnen einen der eigenhändigen Unterschrift überlegenen Beweiswert gibt.[68] Nur dadurch ist das Abweichen von der Wertung der §§ 439, 440 ZPO gerechtfertigt.[69] Wenn der Anscheinsbeweis für elektronische Dokumente ausdrücklich qualifiziert elektronisch signierten Doku-

---

58 Amtl. Begr. zum SigG, BR-Drs. 966/96, 28.

59 S. z.B. *Müglich*, MMR 2000, 7; *Vehslage*, DB 2000, 1802; *Scheffler/Dressel*, CR 2000, 378; *Oertel*, MMR 2001, 419; *Boente/Riehm*, JURA 2001, 797.

60 S. z.B. *Roßnagel* (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung, 2002; *Storr,* MMR 2002, 579; *Yildirim,* DVBl. 2002, 241; *Schlatmann,* DVBl. 2002, 1005.

61 Beschluss der Bundesregierung vom 16.1.2002 zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung.

62 S. BMWi, Elektronischer Geschäftsverkehr – Ratgeber für kleine und mittlere Unternehmen,2000, S. 21.

63 S. auch *Wiebe*, MMR 2002, 127.

64 So *Hoeren*, CR 2002, 296; a.A. noch *Hoeren* (Fn. 19), S. 324.

65 S. zu den vielen Anwendungen im Test- und Pilotbetrieb z.B. *Viefhues/Scherf*, K&R 2002, 171.

66 Die eine Konkurrenzinfrastruktur zur Infrastruktur der vom SigG vorgesehenen qualifizierten elektronischen Signaturen aufbaut, statt diese zu stützen – s. hierzu kritisch *Roßnagel*, MMR 2002, 221f.; s. auch *Hoeren* (Fn. 19), S. 327.

67 S. hierzu näher auch *Hoeren* (Fn. 19), S. 321 ff.; *Roßnagel*, NJW 2001, 1826; *Fischer-Dieskau/Gitter/Paul/Steidle*, MMR 2003, i.E.

68 Amtl. Begr., BT-Drs. 14/4987, 17, 23, 25.

69 S. *Nissel* (Fn. 52), 90; selbst diese Regelung halten *Roßnagel*, MMR 200, 459f.; *Redeker*, CR 2000, 458; *Hoeren* (Fn. 19), S. 323, für zu weitgehend.

menten vorbehalten ist und dies mit der höheren Fälschungssicherheit begründet wird, kann nicht einfachen, ungesicherten E-Mails der gleiche Anscheinsbeweis zugebilligt werden.[70] Dies würde der Wertung des Gesetzgebers widersprechen.

7. Gegenprobe

Die Anerkennung eines Anscheinsbeweises würde nicht nur die Fälle betreffen, in denen „unwillig gewordene Gegenparteien" „Schutzbehauptungen" vorbringen, die Erklärung stamme nicht von ihnen.[71] Vielmehr wäre auch der umgekehrte Fall betroffen, in dem ein Lehrer, unter dessen E-Mail-Adresse Damenunterwäsche bestellt wurde, ein Politiker, für den Pornohefte geordert wurden, oder ein Arbeitskollege, für den ein Klavier ersteigert wurde, sich gegen die ungerechtfertigte Inanspruchnahme wehren wollen. Da Manipulationen spurenlos erfolgen, hätten sie im Regelfall keine Chance, den Anscheinsbeweis zu erschüttern.

Eine solche Risikoverteilung ist nicht gerechtfertigt. Beide Seiten tragen die Vorteile, aber auch die Risiken der Mail-Kommunikation und ihrer vorhandenen oder unterlassenen Sicherung.[72] In der Regel hat der empfangende Unternehmer sogar den größeren Einfluss auf die Sicherheit der Kommunikation. Es gibt keinen Grund, von der Grundregel der Beweislastverteilung abzurücken.[73]

Schließlich ist zu bedenken, dass die Zahl von E-Mail-Manipulationen deshalb so relativ gering sein könnte, weil der bestrittenen E-Mail gerade kein Beweiswert zukommt. Ein Anscheinsbeweis könnte einen erheblichen Anreiz bieten, die Unsicherheit von E-Mails in Schädigungs- und Bereicherungsabsicht auszunutzen.[74]

V. Ökonomischer Zwang zu geringer Rechtssicherheit?

Die Befürchtung, dass durch die übliche Beweislastverteilung der E-Commerce mit zusätzlichen Kosten belastet und in seiner Entwicklung gefährdet werde, darf nicht dazu führen, für ihn sachlich ungerechtfertigte Sonderregelungen zu erfinden. Eine gerechte Beweislastverteilung, eine hohe Beweissicherheit und die Qualität gerichtlicher Entscheidungen sind Rechtsgüter, die nicht Einzelinteressen geopfert werden dürfen.

Die Anerkennung eines Anscheinsbeweises hätte für den E-Commerce negative ökonomische Effekte. Viele E-Commerce-Systeme und Verkaufsplattformen wurden auf ungesicherter E-Mail-Kommunikation aufgebaut. Dadurch entstehen (Kosten-)Vorteile, aber eben auch (Beweis-)Probleme. Das Recht darf diese ökonomische Kalkulation nicht nachträglich zu Lasten derjenigen korrigieren, die in sichere Systeme investieren. Vielmehr entspricht es dem E-Commerce, den Anbieter zwischen Kosten und Sicherheit – je nach Bedeutung der Transaktionen – wählen zu lassen. Das Recht und auch die Praxis bieten hier eine breite Skala von Möglichkeiten, auf Sicherheitsbedarf und Kostendruck zu reagieren – von der ungesicherten E-Mail, über Passwort- und andere Identifikationsverfahren in geschlossenen Benutzergruppen bis hin zu fortgeschrittenen und qualifizierten Signaturen für den offenen Rechtsverkehr. Unternehmen, die Sicherheitsinvestitionen sparen, verrechnen die Verluste durch mangelnde Beweisbarkeit von Willenserklärungen mit den Gewinnen durch niedrigere Kosten. Dieses Gefüge von rechtlichen und ökonomischen Voraussetzungen und Konsequenzen darf nicht dadurch durcheinandergebracht werden, dass der geringsten Stufe der Sicherheit nun per –

---

70 S. auch *Lüdemann/Adams*, K&R 2002, 12.

71 *Mankowski*, NJW 2002, 2822.

72 S. *LG Bonn*, CR 2002, 294.

73 Ebenso *LG Bonn*, CR 2002, 294.

74 Denkbar sind nicht nur einzelne manuelle Angriffe, sondern auch umfangreiche automatisierte Angriffe insbesondere in Schädigungsabsicht.

willkürlicher – Festlegung eines Anscheinsbeweises die Beweisfolgen zugerechnet werden, die das geltende Recht der höchsten vorbehalten hat.

Schließlich ist zu bedenken, dass ein Anscheinsbeweis für den E-Commerce sogar einen belastenden Effekt haben könnte. Bei einem Anscheinsbeweis könnten Missbrauchsfälle zunehmen und viele potenzielle Teilnehmer sich zurückhalten, Verkaufsplattformen oder gar das Internet als Ganzes meiden und nur noch schriftliche Kommunikation verwenden, weil ihnen das Risiko zu groß ist, durch unsichere E-Mails für nicht abgegebene Willenserklärungen einstehen zu müssen.