E-mail im Geschäftsverkehr – Beweisfragen

Sonja Janisch[1]

Fachbereich Privatrecht, Universität Salzburg
Churfürststraße 1, 5020 Salzburg
sonja.janisch@sbg.ac.at

Schlagworte: **e-mail, Beweisprobleme, Identitätsbeweis, Anscheinsbeweis, Beweis der Authentizität und Integrität, Zugangsbeweis, sichere digitale Signaturen**

Abstract: E-mails sind aus dem Geschäftsverkehr nicht mehr wegzudenken. Ihre Verwendung für rechtsgeschäftliche Erklärungen birgt aber durchaus auch Risiken. So können sich in einem Streitfall schwerwiegende Beweisschwierigkeiten ergeben. Dieser Beitrag untersucht, wer den Beweis bezüglich der Identität des Absenders, der Authentizität und Integrität der Nachricht sowie deren (rechtzeitigen) Zugang führen muss und welche Probleme sich diesbezüglich in der Praxis stellen. Abschließend wird aufgezeigt, wie derartigen Beweisschwierigkeiten vorgebeugt werden kann.

1. Einführung

Die rechtliche Problematik rund um e-mails ist bereits seit geraumer Zeit Gegenstand juristischer Diskussion. Dabei sind die durch e-mails aufgeworfenen Rechtsfragen vielfältig und betreffen unterschiedlichste Rechtsgebiete.[2] Dieser Beitrag beschränkt sich auf den zivilrechtlichen Bereich, in dem sich im Wesentlichen vier Themenkreise bilden lassen: Dies sind zunächst Fragestellungen rund um den Vertragsabschluss per e-mail, der Bereich der e-mail-Werbung, die Frage der Haftung für mittels e-mail übertragene Viren sowie schließlich beweisrechtliche Aspekte des e-mail-Verkehrs. Während insbesondere die beiden zuerst genannten Thematiken in der Literatur bereits ausführlich diskutiert wurden,[3] haben

---

[1] Ich möchte mich herzlich bei Prof. Dr. *Peter Mader* für seine Anregung zu diesem Thema und seine wertvolle Unterstützung und Diskussionsbereitschaft bedanken.

[2] S zu einer umfassenden Untersuchung verschiedenster Problemfelder *IT-LAW.AT* (Hrsg), e-Mail – elektronische Post im Recht (2003).

[3] S nur *Mottl*, Zur Praxis des Vertragsabschlusses im Internet, in *Gruber/Mader* (Hrsg), Privatrechtsfragen des e-commerce (2003) 1 ff; *Gruber*, E-mail-Werbung, in FS-*Koppensteiner* (2001) 381 ff; *Janisch*, Online-Werbung (2004) 183 ff.

Beweisfragen bislang noch wenig Beachtung gefunden. Da ihnen aber insbesondere im Bereich des Geschäftsverkehrs eine immanente praktische Bedeutung zukommt, sollen diese hier erörtert werden.

Das Grundproblem der Internetnutzung liegt – wie allgemein bekannt – in der Unsicherheit der Kommunikation. Dabei bestehen vier zentrale Problemfelder, die den Parteien bewusst sein müssen, wenn sie rechtsgeschäftliche Erklärungen (Vertragsangebote, Mahnungen, Kündigungen etc) per e-mail übermitteln. Dies sind Unsicherheiten bezüglich

- **der Person des Absenders:**
  - Identität: Ist der Kommunikationspartner tatsächlich die Person, die er zu sein vorgibt?
  - Authentizität (Echtheit): Stammt die vom Empfänger erhaltene Nachricht tatsächlich vom darin genannten Absender?
- **des Inhalts:** Unverfälschtheit der Nachricht (Integrität): Wurde die Erklärung nachträglich (zB am Übertragungsweg) verändert?
- **des Zugangs:** Wie ist die Situation, wenn der Empfänger behauptet, die e-mail nie bzw nicht rechtzeitig erhalten zu haben?
- **der Vertraulichkeit:** Wurde die Erklärung auf dem Weg zum Empfänger mitgelesen?[4]

Trotz dieser Unsicherheiten hat sich die Kommunikation per e-mail mittlerweile zu einem fixen Bestandteil des Geschäftsverkehrs entwickelt. Dieser Beitrag zeigt anhand von drei Szenarien auf, welche Beweisschwierigkeiten sich durch die Verwendung von e-mails für rechtsgeschäftliche Erklärungen in einem Streitfall ergeben können, inwieweit diesen vorgebeugt werden kann und wann es – zumindest derzeit noch – anzuraten ist, auf ein anderes Medium auszuweichen.

2. Szenario I: „Ich habe nie eine e-mail an den Empfänger versandt“

Diese Konstellation betrifft die Frage der Identität des Absenders sowie der Authentizität der Nachricht. Der scheinbare Absender bestreitet, jemals eine e-mail (zB eine Bestellung) an den Empfänger gesandt zu haben. Aus zivilprozessualer Sicht stellt sich daher die Frage, wer beweisen muss, dass eine e-mail wirklich von dem in ihr angegebenen Absender stammt und nicht etwa eine unbefugte dritte Person unter dessen Namen gehandelt hat.

---

[4] Eine Abhilfe gegen die unbefugte Einsichtnahme in elektronische Dokumente bietet eine Verschlüsselung. S dazu etwa *Janisch/Mader*, E-Business[2] (2002) 72 f.

Nach allgemeinen Grundsätzen liegt die Behauptungs- und Beweislast, dass eine bestimmte Person eine konkrete Erklärung abgegeben hat (oder ihr diese zumindest zurechenbar ist), beim Erklärungsempfänger, der sich darauf berufen will.[5] Dieser Beweis ist in der Praxis allerdings schwer zu führen. Denn im Rahmen der freien Beweiswürdigung ist alleine die Vorlage einer (ungesicherten) e-mail oder ihres Ausdrucks nach überwiegender Ansicht[6] unzureichend, um zu beweisen, dass der darin angegebene Absender, der die Erklärungsabgabe bestreitet, tatsächlich der Erklärende ist. Der Inhalt einer e-mail und damit auch der darin angegebene Absendername kann nämlich sowohl vom Empfänger als auch von einem Dritten auf dem Übertragungsweg leicht gefälscht oder verändert werden.

Auch der in der Kopfzeile der e-mail aufscheinende Name bzw die Mailadresse geben keine sichere Auskunft über den tatsächlichen Versender. Es ist nämlich jedermann ohne besondere Schwierigkeiten möglich, die Absenderkennung zu manipulieren, ohne dass dies erkannt werden kann.[7] Der Empfänger der e-mail kann zunächst nur die IP-Adresse des Absender-PC sowie des vom Sender benutzten Mailservers herausfinden. Über letztere lässt sich idR der Betreiber des Servers feststellen, der uU Auskunft darüber geben kann, welchem Nutzer die jeweilige IP-Adresse zum in Frage stehenden Zeitpunkt zugeordnet war.[8] Fraglich ist allerdings, ob der Provider diese Auskunft erteilen darf. IP-Adressen zählen nach der Definition des TKG zu den Zugangsdaten, die – wie alle Verkehrsdaten – dem Kommunikationsgeheimnis nach § 93 Abs 1 TKG unterliegen. Die Auskunftserteilung an Dritte ohne Anordnung des Gerichts aufgrund besonderer Ermächtigung in einzelnen Materiengesetzen oder ausdrücklicher Zustimmung des Betroffenen ist damit unzulässig. Zudem besteht nach § 99 TKG die grundsätzliche Verpflichtung, dass der Betreiber diese Daten nach Beendigung der Verbindung unverzüglich löscht oder anonymisiert.

---

[5] S nur *Rechberger/Simotta*, Zivilprozessrecht[6] (2003) Rz 583, 585. ZPO.

[6] Statt vieler *Rossnagel/Pfitzmann*, Der Beweiswert von E-Mail, NJW 2003, 1209 f; so auch *Neumayr*, Online-Willenserklärungen – Beweis- und Zurechnungsfragen in *Plöckinger/Duursma/Mayrhofer* (Hrsg) Internet-Recht (2004) 54.

[7] S nur *Mankowski*, Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?, NJW 2002, 2823.

[8] S etwa *Mosing*, Spamming: Werbung bzw Massensendung per elektronischer Post, in IT-LAW.AT, e-Mail (2003) 110; *Neumayr*, aaO 46.

Entgegen der in der Literatur vielfach propagierten Ansicht[9] kommt mE § 18 Abs 4 ECG hier nicht zur Anwendung. Diese Regelung bezieht sich auf Host-Provider, die Speicherplätze für fremde Inhalte bereit stellen, indem sie etwa einem Nutzer die erforderliche Infrastruktur für eine Website zur Verfügung stellen oder die Möglichkeit einräumen, Kommentare online zu publizieren. Die Bestimmung soll dann zB einer in ihren Marken- oder Urheberrechten verletzten Person eine Möglichkeit zur Verfolgung ihrer Rechte bieten. Sie bezieht sich damit auf Publikations- und nicht auf Kommunikationsvorgänge. Zudem verpflichtet die Bestimmung nur zur Bekanntgabe von Name und Adresse des jeweiligen Nutzers und nicht zur Auskunft über Verkehrsdaten. Eine derart weite Auslegung des § 18 Abs 4 ECG wäre aus verfassungsrechtlicher Sicht bedenklich, da das Fernmeldegeheimnis auch in Art 10a StGG abgesichert ist und der grundrechtliche Schutz der Daten nur durch einen richterlichen Befehl aufgrund einer Ermächtigung in einem Materiengesetz durchbrochen werden kann.

Im Regelfall sind damit für die Beweisführung neben der e-mail selbst keine aussagekräftigen Daten vorhanden.[10] In Hinblick auf die somit schwierige Beweislastsituation wurde insbesondere in der deutschen Literatur[11] vorgeschlagen, einen Anscheinsbeweis zuzulassen, dass eine e-mail von der Person stammt, unter deren e-mail-Adresse sie versandt wurde.[12]

Diese Ansicht ist abzulehnen.[13] Zum einen ist die Absenderadresse leicht zu fälschen, weshalb es unzulässig ist, davon auszugehen, dass von der Absenderadresse typischerweise auf den Erklärenden geschlossen werden kann.[14] Zudem gibt es keine Lebenserfahrung, die darauf hinweist, dass eine Manipulation nur eine

---

[9] S nur *Mosing* in IT-LAW.AT, e-Mail (2003) 110; *Neumayr* in *Plöckinger/Duursma/Mayrhofer* (Hrsg) Internet-Recht (2004) 46.

[10] Selbst dann, wenn der Empfänger durch eine entsprechende Auskunftserteilung des Providers nachweisen könnte, dass die e-mail von einem bestimmten PC versandt worden ist, bedeutet das immer noch nicht, dass sie auch tatsächlich vom konkreten Nutzer stammt. Schließlich könnte diese auch eine andere Person von dort aus versandt haben. Vgl *Neumayr*, aaO 54.

[11] S etwa *Mankowski*, NJW 2002, 2824 ff, der dies ua mit der geringen Wahrscheinlichkeit einer Manipulation durch Dritte begründet. Zudem würde die Belastung des Erklärungsempfängers mit einem kaum zu erbringenden Beweis dazu führen, dass Schutzbehauptungen des e-mail-Adressinhabers, die e-mail stamme gar nicht von ihm, vorschnell Tor und Tür geöffnet werden.

[12] Oder sie stammt zumindest von einer vom Adressinhaber ermächtigten Person.

[13] S ausführlich *Roßnagel/Pfitzmann*, NJW 2003, 1211 ff; *Neumayr*, aaO 53.

[14] Vgl *Neumayr*, aaO 53.

sehr seltene Ausnahme darstellt.[15] Dagegen lässt sich auch nicht einwenden, dass dieses Risiko in der Praxis gering ist. Zum anderen wäre der vermeintliche Sender damit gezwungen, seine gesamte elektronische Kommunikation offen zu legen (sofern die Verkehrsdaten überhaupt noch verfügbar sind), um einen atypischen Geschehensablauf darzutun und damit den Anschein zu erschüttern, dass eine bestimmte e-mail von ihm stammt. Dies würde zu einer gravierenden Beeinträchtigung seiner Geheimhaltungsinteressen führen.[16]

Auch die deutschen Gerichte[17] haben bisher einen Anscheinsbeweis im durchaus vergleichbaren Fall einer Internet-Auktion abgelehnt. Die Angabe einer e-mail-Adresse in Verbindung mit einem Passwort sei – aufgrund der unzureichenden Sicherheitsstandards im Internet – kein ausreichendes Indiz dafür, dass tatsächlich der angebliche Bieter an der Versteigerung teilgenommen hat. Diese Grundsätze müssen daher erst recht für e-mails gelten, bei denen nicht einmal die Absicherung durch ein zusätzliches Passwort besteht.

3. Szenario II: „Ich habe diese e-mail zwar versandt, aber mit einem anderen Inhalt“

Diese Konstellation betrifft die Frage nach der Integrität einer Nachricht. Was gilt, wenn die per e-mail übermittelte Erklärung während der Übertragung oder beim Empfänger verändert wurde (zB der Preis eines Anbots) oder der Versender dies zumindest im Nachhinein behauptet?

Nach allgemeinen Grundsätzen gilt, dass eine Willenserklärung auf Gefahr des Erklärenden reist.[18] Sie gilt so, wie sie in den Herrschaftsbereich des Empfängers (zB den Mailserver seines Providers) eingeht, und bindet damit den Versender.

Nachdem sich der Empfänger auf den – möglicherweise verfälschten – Inhalt der erhaltenen Erklärung berufen will, obliegt ihm auch der Beweis, dass ihm die Erklärung so zugegangen ist. Da elektronische Dokumente nach hA[19] keine Urkunden iSd ZPO darstellen, für die gemäß § 294 ZPO – unter der Voraussetzung, dass

---

[15] *Roßnagel/Pfitzmann*, NJW 2003, 1211.
[16] *Neumayr*, aaO 53.
[17] S etwa OLG Köln 19 U 16/02, K&R 2003, 83; jüngst OLG Naumburg 9 U 145/03.
[18] S nur *Koziol/Welser*, Bürgerliches Recht I[12] (2002) 102.
[19] *Rechberger/Simotta*, Zivilprozessrecht[6], Rz 617.

sie unterschrieben sind – eine qualifizierte Echtheitsvermutung bezüglich ihres Inhalts gilt,[20] sondern nur Augenscheinsobjekte darstellen, die der richterlichen Beweiswürdigung unterliegen, ist fraglich, ob ein derartiger Beweis gelingt. Denn auch hier sind Fälschungen ohne besondere Schwierigkeiten möglich.

4. Szenario III: „Ich habe diese e-mail nie/zu spät erhalten“

Im elektronischen Geschäftsverkehr kann aus verschiedensten Gründen auch der Frage der Beweisbarkeit des Zugangs bzw Zugangszeitpunkts einer e-mail besondere Bedeutung zukommen. Dies ist – hier für den Absender – zum einen etwa wegen der Frage der Rechtzeitigkeit einer Erklärung (zB Kündigung) wichtig. Ebenso aber etwa auch im Bereich der downloadable goods, also der kostenpflichtigen digitalen Güter, deren Bezahlung vielfach mittels Kreditkarte erfolgt (zB eine Datenbankauskunft).[21] So wäre es denkbar, dass der Käufer den Erhalt des Contents abstreitet und die Belastung seiner Kreditkarte storniert.

Der Versender hat in diesen Fällen somit ein eminentes Interesse daran, den Zugang seiner Nachricht beim Empfänger nachweisen zu können, wenn dieser bestreitet, eine e-mail überhaupt oder bis zu einem bestimmten Zeitpunkt erhalten zu haben.[22]

In der Praxis wird die Nachweisbarkeit der Zustellung einer e-mail derzeit allerdings kaum zu erbringen sein, da sich Verfahren, die eine dokumentierte Zustellung ermöglichen – wie etwa ein eingeschriebener Brief im herkömmlichen Geschäftsverkehr – im e-mail-Verkehr noch nicht durchgesetzt haben. Selbst wenn der Empfänger den Zugang einer e-mail, etwa durch eine Antwort-e-mail bestätigt hat, kann – bei späterem Bestreiten des Empfängers – nicht bewiesen werden, ob die entsprechende Bestätigungs-e-mail tatsächlich vom (dies bestreitenden) Empfänger stammte und nicht etwa vom ursprünglichen Versender selbst erstellt wurde.[23]

---

[20] S *Rechberger/Simotta*, aaO, Rz 622.

[21] Vgl *Diening*, Beweisbarer Versand und Zustellung von eMails, 2, http://www.irecht.fh-darmstadt.de/fileadmin/dokumente/vortragslite.pdf.

[22] Erst wenn die e-mail unbestritten beim Empfänger angekommen ist, kann die Bestimmung des § 12 ECG, die regelt, unter welchen Umständen darin enthaltene Erklärungen als zugegangen gelten, zur Anwendung gelangen.

[23] S oben Pkt 2; dies übersehend *Neumayr*, aaO 55.

Auch Lesebestätigungen, deren Anforderungsmöglichkeit viele e-mail-Programme vorsehen, können vom ursprünglichen Absender mit geringem Aufwand selbst erstellt bzw – wenn diese tatsächlich vom Empfänger stammen – zu seinen Gunsten (zB Datum und Uhrzeit) verändert werden.[24] Ebenso leicht manipulierbar sind automatische Übermittlungsbestätigungen, die darüber hinaus kaum aussagekräftige Daten enthalten. Solchen Bestätigungen kann deshalb nur eine minimale Beweiskraft als Indiz für den Zugang(szeitpunkt) beim Empfänger zukommen.[25]

5. Welche Möglichkeiten bestehen, um diese Aspekte beweisen zu können?

Abhilfe für die Beweisschwierigkeiten in Szenario I und II bietet eine sichere digitale Signatur[26], die derzeit aber noch vergleichsweise selten Verwendung findet. Ihre Bedeutung im elektronischen Geschäftsverkehr besteht in der Schaffung von Kommunikationssicherheit. Dabei ist ihre Verwendung für beide Parteien vorteilhaft:

Der Empfänger hat sowohl Sicherheit über die Identität seines Kommunikationspartners als auch hinsichtlich der Authentizität und Integrität der Erklärung. Sicher elektronisch signierte Dokumente sind gemäß § 4 Abs 3 SigG eigenhändig unterschriebenen Privaturkunden gleichgestellt. Dies bedeutet, dass bei einem Prozess bis zum Beweis des Gegenteils von der Echtheit des Dokuments auszugehen ist.

Der Erklärende kann sein Risiko (eventuelle Bindung an einen verfälschten Erklärungsinhalt) durch Verwendung einer sicheren elektronischen Signatur ausschließen, wenn er das Vertrauen des Empfängers in den Inhalt seiner Erklärung (zB Bestellung) unter den Vorbehalt stellt, dass die Signatur verifiziert wurde. Unterlässt der Empfänger die Signaturprüfung, kann er sich im Konfliktfall nicht mehr auf das Vertrauen in den Erklärungsinhalt berufen.

Keine Lösung bietet die digitale Signatur zunächst für Szenario III. Der Zugang(szeitpunkt) kann zwar etwa dann bewiesen werden, wenn ihn der Empfänger durch eine entsprechende, mit einer sicheren digitalen Signatur versehene Antwort-e-mail bestätigt. Im Streitfall wird

---

[24] *Diening*, Beweisbarer Versand und Zustellung von eMails, 2 f, http://www.irecht.fh-darmstadt.de/fileadmin/dokumente/vortragslite.pdf.

[25] S *Neumayr*, aaO 55.

[26] S dazu etwa *Janisch/Mader*, E-Business[2] (2002) 66 ff; Forgó, e-mail und elektronische Signatur in *IT-LAW.AT* (Hrsg), e-Mail – elektronische Post im Recht (2003) 13 ff.

der Empfänger, der behauptet, eine e-mail nicht (rechtzeitig) erhalten zu haben, aber gerade keine derartige Antwort-e-mail versenden. Es bestehen aus technischer Sicht dennoch mögliche Verfahren, deren Einsatz in Verbindung mit digitalen Signaturen zumindest sehr starke Indizien für die Zustellung einer e-mail erzeugen können.[27] So etwa ein Treuhandverfahren, bei dem die Entgegennahme und Zustellung von e-mails mit einer digital signierten Bestätigungs-e-mail des Treuhänders dokumentiert wird.[28] Derartige Verfahren sind derzeit allerdings noch kaum verbreitet.

Insgesamt ist noch festzuhalten, dass für die meisten Zwecke des Geschäftsverkehrs auch eine Erklärung, die nur mit einer einfachen digitalen Signatur versehen ist, ausreichend sein wird. Diese hat zwar nicht die besonderen Rechtswirkungen der sicheren digitalen Signatur, sie gilt aber als allgemeines Beweismittel (§ 3 Abs 2 SigG) und ihre Verwendung erhöht – je nach Ausgestaltung – die Kommunikationssicherheit. Im Rahmen der richterlichen Beweiswürdigung wird auch ihr Beweiswert ungleich höher bewertet werden als der von unsignierten Dateien.

6. Fazit

- Der Empfänger kann nur dann beweisen, dass er eine e-mail mit einem bestimmten Inhalt von einem konkreten Absender erhalten hat, wenn dieser eine sichere digitale Signatur verwendet hat. Die Beweissituation wird aber bereits durch den Einsatz einer einfachen digitalen Signatur verbessert. Der Empfänger sollte sich damit bemühen, seinen Kommunikationspartner dazu anzuregen, zumal dies auch für diesen eine erhöhte Sicherheit bringt.
- Kommt es für den Erklärenden in concreto besonders darauf an, dass er den Zugang bzw Zugangszeitpunkt seiner Erklärung beweisen kann, sollte er sich derzeit nicht unbedingt einer e-mail bedienen, da diese Aspekte (noch) nicht bewiesen werden können. Da dies ein großes Hemmnis für den elektronischen Geschäftsverkehr darstellt, ist die Wirtschaft gefordert, sich für die Verbreitung von bereits existenten Verfahren für einen dokumentierten Zugang einzusetzen.

---

[27] S ausführlich *Diening*, Beweisbarer Versand und Zustellung von eMails, 2 ff, http://www.irecht.fh-darmstadt.de/fileadmin/dokumente/vortragslite.pdf.

[28] S dazu *Diening*, aaO 4.