

## Thema

Dr. Franz Schmidbauer

■ Zak 2008/151, 83

# Beweis und Anscheinsbeweis bei der Übermittlung einer E-Mail-Erklärung

**Aus Anlass der OGH-E 2 Ob 108/07g = Zak 2008/161,94**

E-Mail ist heute aus der geschäftlichen und privaten Kommunikation nicht mehr wegzudenken. Damit ergeben sich auch neue Rechtsprobleme. Gegenüber älteren Techniken verkehrt man per E-Mail zwar einfacher und schneller, aber gelegentlich auch unsicherer. Es war nur eine Frage der Zeit, bis sich auch die Gerichte mit diesem „Ding“ auseinandersetzen mussten. „Ding“ zunächst deswegen, weil es dazu Einiges zu klären gilt.

## I. Klärungen

### I.1. Artikel und Schreibweise

Zuallererst stellt sich die Frage: Heißt es der, die oder das E-Mail? Jeder Leser wird an dieser Stelle sofort einwenden, dass das ohnedies ganz klar ist. Tatsächlich steht aber nicht einmal das fest. Während nämlich der DUDEN in Deutschland das Geschlecht als weiblich ausweist und sich die Deutschen überwiegend auch daran halten, lässt das Österreichische Wörterbuch (40. Auflage 2007) beide Geschlechter zu und es werden in der Praxis auch beide Formen verwendet, was im Gespräch ziemlich verwirrend klingt und immer wieder für Verunsicherung sorgt. Ich bleibe beim weiblichen Artikel, nicht nur im Sinne einer Vereinheitlichung der deutschen Sprache und der rein zahlenmäßigen deutschen Übermacht, sondern auch weil es mir im Hinblick auf die Übersetzung aus dem Englischen „elektronische Post“ logischer erscheint. Der männliche Artikel wird in der Praxis kaum verwendet, obwohl er in der Übersetzung „elektronischer Brief“ auch ein Argument für sich hätte.

Die Schreibweise mit großem „E“ entspricht DUDEN und Österreichischem Wörterbuch und passt auch zur Schreibweise ähnlicher Wortneuschöpfungen wie E-Gitarre, E-Piano, E-Card, E-Commerce. Nur notorische Kleinschreiber verwenden noch die Form eMail mit oder ohne Bindestrich.

### I.2. E-Mail und Beweismittel

Als Nächstes ist zu prüfen, wie die E-Mail in die Systematik der Beweismittel in der Zivilprozessordnung einzuordnen

ist. Während man in Deutschland die E-Mail zum Augenscheinbeweis rechnet, zählt sie in Österreich zu den Urkunden. Als Urkunden werden Schriftstücke angesehen, die Gedanken in Form der menschlichen Schrift festhalten. Spätestens seit dem Signaturgesetz gilt dies jedenfalls auch für digitale Gedankenaufzeichnungen. Schließlich gibt es heute kaum mehr Urkunden, die keine digitale Herkunft haben. § 294 ZPO idF des BRÄG 2006, BGBl I 2005/164, bezieht in den Begriff der Privaturkunden ausdrücklich auch elektronisch errichtete Urkunden ein.

Allerdings gelten bei digitalen Dokumenten einige Besonderheiten, die es auch bei Gericht zu berücksichtigen gilt. Zunächst muss man sich vor Augen halten, dass das Papierdokument, das bei Gericht vorgelegt wird, bloß eine Ausfertigung der Urkunde ist, nämlich ein Ausdruck auf Papier. Bei E-Mails sind diese Ausdrücke zudem meist unvollständig, weil der Header, der die Übermittlungsdaten enthält, idR nicht mit ausgedruckt wird. Vor allem aber sind Ausdrücke beliebig manipulierbar. Ein bloßer Papierausdruck kann daher niemals einen Anscheinsbeweis liefern. Die Manipulierbarkeit trifft zwar auch auf Papierurkunden in Form von Kopien zu, dort kann aber immerhin bei Bestreitung leicht das Original nachgereicht werden. Was aber soll bei einer E-Mail vorgelegt werden? Letztlich kommt hier nur eine Einsicht in den digitalen E-Mail-Ordner in Betracht, sei es online über einen Webmail-Zugang oder anhand eines mitgebrachten Notebooks. Die Bestellung eines Sachverständigen nur zur Überprüfung, ob sich eine E-Mail im Postordner eines Prozessbeteiligten befindet und ob dessen Wortlaut mit dem Papierausdruck ident ist, kommt wohl nicht in Frage, weil dies eine reine Augenscheinsangelegenheit ist, außer es sind weitere Fragen zu klären, für die technischer Sachverstand erforderlich ist (zB allfällige Manipulationen). Die Aufforderung des Richters „Zeigen Sie mir Ihren E-Mail-Ordner zwecks Inaugenscheinnahme“, mag daher zwar für Verblüffung im Verhandlungssaal sorgen, tatsächlich stellt sie aber die rationellste Echtheitsprüfung dar. Die digitale Vorlage einer einzelnen E-Mail (auf Datenträger) scheitert leider daran, dass die führenden Mailprogramme keine Einzeldateien über gesendete und empfangene E-Mails speichern, sondern alles in einen Sammelordner stecken, und das über Jahre hin, wenn nicht ordnend eingegriffen wird (im Sinne einer über-

Der Autor:

**Dr. Franz  
Schmid-  
bauer**

ist Richter des  
Landesgerichts  
Salzburg und  
Betreiber der Informationsplattform  
[www.internet4jurists.at](http://www.internet4jurists.at).



sichtlichen Postarchivierung empfiehlt sich hier die Anlage von Jahres- oder Monatsordnern; das erleichtert nicht zuletzt die Suche im Streitfall).

Eine solche Überprüfung der Übereinstimmung der digitalen Mail mit dem Ausdruck kann zwar die Echtheit indizieren, muss aber nicht, weil auch die gespeicherten Mails manipuliert sein können. Hier

setzt allerdings bereits die richterliche Beweismwürdigung an. Durch Befragung des Beweisführers könnte geprüft werden, ob eine bewusste Fälschung in Frage kommt. Dazu aber im Rahmen der Problemfälle. Diese liegen beim E-Mail-Verkehr im Zugang, in der Identität des Inhalts und in der des Absenders.

## 2. Der Mail-Zugang

Die Frage, ob eine rechtsgeschäftlich relevante Erklärung dem anderen zugewandt ist, hat die Gerichte schon immer beschäftigt. Das Problem stellte sich beim Briefverkehr und etwas vermindert beim Telefax. Es ist daher nicht weiter verwunderlich, dass um diese Frage auch beim E-Mail-Verkehr gestritten wird. Einen solchen Fall hatte der Oberste Gerichtshof kürzlich zu entscheiden (2 Ob 108/07g = Zak 2008/161, 94):

Die Klägerin erteilte der Beklagten den Auftrag zur Erstellung und Versendung von Werbematerial in drei Etappen. Der erste und der letzte Auftrag wurden von der Beklagten ordnungsgemäß ausgeführt. Dabei wurden die Daten jeweils per E-Mail übermittelt. Bei der zweiten Serie bestritt die Beklagte sowohl den Erhalt einer Mail als auch eine telefonische Vorankündigung und eine nachträgliche telefonische Bestätigung. Das Erstgericht wies die Schadenersatzklage ab, weil es weder den Erhalt der E-Mail noch die beiden Telefonate feststellen konnte. Das E-Mail-Sendeprotokoll liefere weder Beweis noch Anscheinsbeweis für den Zugang der Mail. Das Berufungsgericht gab der Berufung der Klägerin nicht Folge, ließ aber die Revision zu.

Der OGH gab der Revision nicht Folge. Mittels eines E-Mail-Sendeprotokolls könne der Anscheinsbeweis des Zugangs eines E-Mails nicht erbracht werden. Der Anscheinsbeweis sei die Verschiebung des Beweisthemas von der tatbestandsmäßig geforderten Tatsache auf eine leichter erweisliche Tatsache, die mit ihr in einem typischen Erfahrungszusammenhang stehe. Er sei nur zulässig, wenn eine typische formelhafte Verknüpfung zwischen der tatsächlich bewiesenen Tatsache und dem gesetzlich geforderten Tatbestandselement bestehe; er dürfe nicht dazu dienen, Lücken der Beweisführung durch bloße Vermutungen auszufüllen. Auch der sonst für die Zulassung des Anscheinsbeweises geforderte Beweisnot-

stand sei beim Versenden von E-Mails nicht gegeben. So wie beim gewöhnlichen Brief sei es dem Versender möglich, sich den Empfang der E-Mail etwa durch eine Bestätigungsmail oder durch telefonische Rückfrage bestätigen zu lassen.

Das Urteil enthält zahlreiche Literaturhinweise aus Österreich und Deutschland und ist im Ergebnis nicht zu beanstanden. Die Entscheidung ist somit nicht anders ausgefallen als bei Brief und Fax. Es gibt zwar bei allen drei Kommunikationsmitteln keine verfügbaren statistischen Werte, wie hoch die Ausfallrate am Übertragungsweg tatsächlich ist und wie hoch somit die Wahrscheinlichkeit der Zustellung einer ordnungsgemäß abgesandten Nachricht ist; den Gerichten hat aber bereits die vom Sachverständigen aufgezeigte theoretische Möglichkeit von Fehlern bei der Übermittlung genügt, um den Prima-facie-Beweis abzulehnen.

Was in diesem Fall offen geblieben ist, ist die Frage, ob der Anscheinsbeweis bejaht worden wäre, wenn der Kläger eine Übermittlungs- oder Lesebestätigung vorweisen hätte können. Gängige E-Mail-Programme bieten eine Möglichkeit, sich bestimmte Vorgänge bestätigen zu lassen. Die Übermittlungsbestätigung (Delivery Status Notification nach RFC3461, früher RFC1891; RFC oder Requests for Comments legen die technischen Standards im Internet fest) bestätigt den Eingang der Mail in der Mailbox des Empfängers; es handelt sich um eine automatische Antwort des Mailservers. Die Lesebestätigung (Message Disposition Notification nach RFC3798, früher RFC2298) bestätigt das Öffnen und damit Zur-Kennntnis-Nehmen der Mail; es handelt sich um eine automatische Antwort des Mailprogramms. Beides kann beim Absenden eingestellt und damit angefordert werden. In diesem Fall wirken diese Anweisungen im Header der Mail als „Ersuchen“ an den Mailserver bzw. das Mailprogramm des Empfängers, die begehrten Bestätigungen per E-Mail zurückzusenden. Allerdings kann der Empfänger durch generelle oder individuelle Einstellung seines Mailsystems diese Antworten unterdrücken (schließlich muss nicht jeder wissen, um welche Uhrzeit man seine elektronische Post erledigt). Es empfiehlt sich daher zwischen Geschäftspartnern eine ausdrückliche Vereinbarung, dass E-Mails, die eine solche Bestätigung anfordern, auch tatsächlich bestätigt werden müssen (das wäre allenfalls ein neuer Punkt für die AGB). Darüber hinaus sollte bei wichtigen oder zeitkritischen Mails auch eine ausdrückliche Bestätigung verlangt werden. Ein Klick auf die Antwort-Funktion des E-Mail-Programms mit dem Wort „OK“ führt zu keinem spürbaren Mehraufwand. Hingegen ist eine solche Antwortmail, die noch den ursprünglichen Mailtext enthält, ein relativ gutes Beweismittel. Unfälschbar ist aber auch dieses nicht.

Verschiedene Autoren vertreten die Meinung, dass für eine Mail mit (wohl tatsächlich erfolgter) Übermittlungs- oder Lesebestätigung der Anscheinsbeweis zuerkannt werden müsse, weil dies zur Förderung des immer bedeutender werdenden elektronischen Geschäftsverkehrs wichtig sei. Zur Beurteilung dieser Frage sollte man sich zunächst den Ablauf des Mailverkehrs vor Augen

halten und die möglichen Problemstellen ausloten. Eine abgesandte Mail geht vom eigenen Mailprogramm zum Postausgangsserver des Versenders und dann über verschiedene Zwischenrechner im Internet zum Posteingangsserver des Empfängers und wird dort zum Abruf durch das Mailprogramm des Empfängers bereitgehalten. Insofern entspricht der Posteingangsserver dem Briefkasten an der Hauswand, nur dass er irgendwo auf der Welt (zB bei Hotmail in Amerika) platziert sein kann. Die Mailserver werden in der Regel von den Access Providern, also den Diensteanbietern, die den Zugang zum Internet anbieten, betrieben; daneben gibt es aber auch reine Mail-Anbieter wie Hotmail oder GMX. In der Regel hat der Kunde nur ein Postfach auf diesem Mailserver gemietet. Großkunden stellen aber gelegentlich auch ihre eigenen Server bei einem Provider ein (serverhousing) oder betreiben gleich Mailserver im eigenen Unternehmen. Je geringer die Zugriffsmöglichkeit auf den Mailserver ist, desto geringer sind auch die Manipulationsmöglichkeiten und umgekehrt. Einem Mailserver, der im eigenen Betrieb steht, kann man alles „unterjubeln“, und zwar so, dass es nicht nachprüfbar ist, außer es wird auch der zweite beteiligte Mailserver, der in der Regel der Kontrolle der anderen Partei unterliegt, in die Untersuchung einbezogen. Eine solche Auswertung setzt aber voraus, dass die Server-Logdateien genügend lange gespeichert werden, sodass der Vorgang des Übersendens und Empfanges zum Zeitpunkt der Untersuchung noch gespeichert ist.

Übermittlungsprobleme können überall eintreten. Wenn eine Mail im Postausgang „hängen bleibt“, merkt man das spätestens beim Schließen des Programms. Wenn es unterwegs steckenbleibt, etwa weil es zu technischen Problemen bei irgendeinem Mailserver kommt, kann es sein, dass man eine Nachricht über den „Delivery Status“ bekommt. Ganz sicher ist das aber nicht. Man kann daher nie völlig sicher sein, dass eine abgesandte Mail den Empfänger wirklich erreicht. Die erfahrungsgemäß häufigsten Übermittlungsprobleme treten allerdings beim Mailserver des Empfängers auf oder überhaupt auf seinem Computer. Die Hauptfehlerquelle sind dabei Anti-Spam-Programme, die nicht oft, aber doch immer wieder Mails ausfiltern, die sie nicht ausfiltern sollen. Allerdings beeinflusst das nicht mehr den rechtswirksamen Zugang einer Erklärung, weil dabei nur darauf abzustellen ist, dass die Mail in die Einfluss-sphäre des Empfängers gelangt. Das ist jedenfalls mit der Speicherung im Posteingangsserver der Fall.

*Mankowski* (NJW 2004, 1901) und *Herwig* (MMR 2001, 146) befürworten im Falle einer Übermittlungs- oder Lesebestätigung einen Anscheinsbeweis für die erfolgte Zustellung. Tatsächlich handelt es sich aber bei diesen Antwortmails auch nur um – noch dazu automatisch versandte – gewöhnliche E-Mails, die genauso manipulierbar sind wie die ursprüngliche Mail. Sie belegen den Empfang nur, wenn sie ihrerseits echt im Sinne von nicht manipuliert sind. Die Fälschung einer solchen Bestätigung erfordert zwar technisches Wissen, man muss aber davon ausgehen, dass das kein unüberwindliches Hindernis dar-

stellt. Das spricht zunächst gegen die Zulassung eines Anscheinsbeweises.

Es stellt sich dann noch die Frage, ob der Adressat, der behauptet, eine Mail nicht erhalten zu haben, obwohl der Absender eine Lesebestätigung vorweist, eine Möglichkeit hat, den Nicht-Zugang zu beweisen. Dies könnte allenfalls durch sachverständige Untersuchung der Mailserver geschehen, insbesondere durch Auswertung der Server-Logdateien. Dies setzt aber Zugriff auf die Mailserver voraus und dass diese Dateien, die zunehmend aus Datenschutzgründen problematisiert werden, zum Zeitpunkt des Prozesses noch vorhanden sind. Ähnlich wie bei der Telekom-Auskunft hinsichtlich einer Faxübermittlung drängt hier die Zeit. Der Empfänger hätte daher bei Zulassung des Anscheinsbeweises unter Umständen keine Möglichkeit mehr, den Nichtzugang zu beweisen. Streng genommen kann er das sowieso nicht, weil er selbst die Spuren der Mail gelöscht haben könnte; der Umstand, dass eine Mail bei ihm zum Zeitpunkt der Untersuchung nicht vorhanden ist, beweist daher gar nichts.

Aus diesen Gründen plädiere ich dafür, bei der E-Mail gar keinen Anscheinsbeweis zuzulassen und in jedem Fall dem Absender die Beweislast aufzubürden. Es sollte diesem überlassen bleiben, unter Aufbietung aller zur Verfügung stehenden Beweise das Gericht vom Mailzugang zu überzeugen. Sollte der Empfänger dabei die Untersuchung seines Mailservers verweigern, kann dies im Rahmen der Beweiswürdigung angemessen berücksichtigt werden. Ähnlich wie bei den Fällen der qualifizierten Mahnung nach dem VersVG, die auch mit einfachen Briefen verschickt wird, liegt ein Beweis immer im Bereich des Möglichen. Eine Übermittlungs- oder Lesebestätigung ist in diesem Fall zumindest ein günstiges Indiz.

Eine elektronische Signatur ist für die Zugangsproblematik ohne Einfluss, sie hat nur Auswirkungen auf die Identität des Inhalts und des Versenders. Allerdings wäre eine signierte Mailantwort ein gewichtiger Beweis, der einem Rückscheinbrief gleichkäme.

### 3. Der Mail-Inhalt

Es wurde weiter oben schon gesagt, dass sich Ausdrücke von Mails nach Belieben verändern lassen. Bei den digitalen Maildateien ist die Veränderung des Inhalts für einen gewöhnlichen Computeranwender nicht so einfach möglich, wenn auch nicht ausgeschlossen. Dem Inhalt einer Mail kommt daher insbesondere dann keine besondere Glaubwürdigkeit zu, wenn der andere behauptet, dass er die Mail mit anderem Inhalt gesendet bzw empfangen hat. In Fällen, in denen der Inhalt differiert, muss immer auf andere Beweismittel zurückgegriffen werden. Es gibt keine höhere Wahrscheinlichkeit für einen Eingriff beim Sender oder beim Empfänger. Ein Anscheinsbeweis kommt hier auf keinen Fall in Frage.

Die Problematik der Veränderung des Mailinhalts lässt sich durch eine elektronische Signatur ausschalten. Die Signatur ist geradezu prädestiniert zur Lösung des Inhaltsproblems. Bereits eine (einfache) sichere elek-

tronische Signatur entfaltet, von besonderen Rechtsgeschäften abgesehen (§ 4 Abs 2 SigG idF BGBI I 2008/8), die Rechtswirkungen der Schriftlichkeit nach § 886 ABGB. Eine qualifizierte elektronische Signatur ersetzt auch die eigenhändige Unterschrift und der so signierte Inhalt hat die Vermutung der Echtheit nach § 294 ZPO für sich.

#### 4. Der Absender

Die Identität des Absenders wird bei E-Mails milliardenfach gefälscht. Dies trifft natürlich vor allem auf Spam-Mails zu (dort ist es geradezu die Regel, denn kaum ein Spammer gibt seine eigene E-Mail-Adresse preis). Daneben gibt es zunehmend Fälle, in denen jemand mit der E-Mail-Adresse eines anderen Bestellungen tätigt, sei es, um ihn zu ärgern (Stalking), sei es aus Jux. Es ist daher für mich unverständlich, wie etwa *Mankowski* für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei normalen E-Mails plädieren kann (CuR 2003, 44).

Probleme mit der Identität des Kommunikationspartner lassen sich allerdings durch eine elektronische Signatur sehr gut vermeiden.

#### 5. Zusammenfassung

Zusammenfassend ist auszuführen, dass der E-Mail-Beweis einige Besonderheiten aufweist, die im gerichtlichen Verfahren, nach Möglichkeit aber bereits bei der Kommunikation mittels E-Mail, beachtet werden sollten. Ein echter Fortschritt wären elektronisch signierte Mails, die zum Schutz vertraulicher Kommunikation auch noch verschlüsselt werden könnten. Die Zugangsproblematik lässt sich durch ein Bestehen auf einer ausdrücklicher Bestätigung lindern; noch besser wäre eine signierte Antwortmail. Die Zulassung eines Anscheinsbeweises ist auch bei Vorliegen einer (nicht elektronisch signierten) Übermittlungs- oder Lesebestätigung in Anbetracht der Vielzahl den Beweiswert beeinflussender Umstände nicht angebracht. Die Frage des Zugangs sollte vielmehr der umfassenden Beweiswürdigung des Gerichts überlassen werden.

### Hinweise & Anmerkungen

**Lit:** *Herwig*, Zugang und Zustellung in elektronischen Medien, MMR 2001, 145; *Mankowski*, Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails, CuR 2003, 44; *Mankowski*, Zum Nachweis des Zugangs bei elektronischen Erklärungen, NJW 2004, 1901; *Neumayr*, Online-Willenserklärungen – Beweis- und Zurechnungsfragen, in *Plöckinger/Duursma/Mayrhofer* (Hrsg), Internetrecht (2004) 45; *Schuhmacher*, Sichere Signaturen im Beweisrecht, ecolx 2000, 860.