Zum Beweiswert elektronischer Dokumente

Eine Entgegnung zu Rüßmann, jur-pc 7/95, S. 3212 ff.

Wolfgang Kilian

Wenn sich alle Richter im Hinblick auf den Beweiswert elektronischer Dokumente so verhalten würden, wie es Rüßmann (jur-pc 7/95, S. 3212 ff.) als EDV-Kundiger beschreibt, wären die praktischen Unterschiede zwischen der rechtlichen Behandlung von Papierurkunden nach der Beweisregel des § 416 ZPO in der Tat "minimal" (S. 3216). Ein solcher Richter müßte allerdings auch Rüßmanns Prämissen akzeptieren, nämlich:

- gesetzliche Beweisregeln als "anachronistisches Restbollwerk gegen den Siegeszug der freien Beweiswürdigung" ansehen (S. 3220)
- die gesetzliche Vermutung des § 416 ZPO stillschweigend für irrelevant halten
- auf die richtige Bewertung eines elektronischen Dokuments im Rahmen der freien Beweiswürdigung vertrauen und Veränderungsmöglichkeiten an elektronischen Dokumenten durch Eingriffe Dritter oder aufgrund von Übermittlungsfehlern vernachlässigen.

Von der Richtigkeit dieser drei Prämissen bin ich nicht überzeugt.

1. Ob man § 416 ZPO als Anachronismus ansieht, mag dahinstehen. Er enthält jedenfalls gültiges Recht und ist deshalb anzuwenden. § 416 ZPO setzt die Verkörperung einer Gedankenerklärung voraus und knüpft die gesetzliche Echtheitsvermutung an die eigenhändige Unterschrift oder eine notarielle Beglaubigung des Handzeichens. Dies ist bei elektronischen Dokumenten im Sinne der einhelligen bisherigen Auslegung (vgl. Kilian/Picot u. a., Electronic Data Interchange, Baden-Baden 1994, S. 139–143) nicht möglich. Also findet § 416 ZPO auf elektronische Dokumente zumindest direkt keine Anwendung. Elektronische Dokumente unterliegen vielmehr der freien Beweiswürdigung nach § 286 ZPO.

2. Der entscheidende Unterschied zwischen beiden Beweisverfahren liegt darin, daß eine unterschriebene Privaturkunde den vollen Beweis für die Abgabe der darin enthaltenen Erklärungen begründet. Die Echtheit der Unterschrift kann freilich von der Gegenseite bestritten werden. Für diese Behauptung trägt die Partei aber auch die Beweislast. Bei einem elektronischen Dokument, das naturgemäß nicht handschriftlich unterzeichnet werden noch notariell beglaubigt werden kann, besteht diese gesetzliche Vermutung nicht. Also muß derjenige, der sich auf die Echtheit beruft, im Falle des Bestreitens die Echtheit beweisen. Somit ist die Beweislast umgekehrt verteilt. Es entsteht ein gravierender Nachteil für den Absender eines elektronischen Dokuments.

3. Dieser Nachteil kann auch nicht auf dem Umweg einer Dokumentation eines abgesandten elektronischen Dokuments beseitigt werden. Die Dokumentation wird in der Regel auch elektronisch vorgenommen und belegt nur mittelbar die Identität der Dokumentation mit dem abgesandten elektronischen Dokument. Ein eventueller Ausdruck der elektronischen Dokumentation auf Papier kann nur die elektronische Dokumentation selbst repräsentieren und deshalb die Beweiskraft nicht verstärken. Fehler, die durch mangelhafte Software oder Eingriffe in die Übertragung des elektronischen Dokumentes auch nach Erstellung des Dokuments leicht möglich sind und in der Praxis häufig vorkommen (Verschlüsselungsfehler; Eingriffe Dritter in das Netz; Fehler eines zwischengeschalteten Dienstleisters, vgl. zur empirischen Häufigkeit solcher Fehler: Kilian/Picot u. a. in: Electronic Data Interchange, Baden-Baden 1994, S. 127–129), können durch die mitlaufende Dokumentation beim Absender des elektronischen Dokuments nicht erfaßt werden. Der Richter muß aber bei seiner Überzeugungsbildung alle diese Faktoren berücksichtigen. Der freie Bewertungsakt des Richters ist für den Absender eines elektronischen Dokuments jedenfalls weit schlechter kalkulierbar als die Anwendung der gesetzlichen Beweisregel des § 416 ZPO. Vorkehrungen zur Reduktion dieser Unsicherheit in der Unternehmenspraxis, etwa durch Parallelversendung schriftlicher Dokumente, erhöhen die Transaktionskosten und schwächen dadurch die Wettbewerbsfähigkeit der Unternehmen.

Indirekt gesteht Rüßmann den höheren Grad an Unsicherheit hinsichtlich der beweisrechtlichen Behandlung elektronischer Dokumente im Vergleich zu Papierdokumenten dadurch ein, daß er ausführlich das Verfahren elektronischer Verschlüsselung solcher Dokumente schildert, mit denen die Fälschungswahrscheinlichkeit verringert werden kann. Dieses Verfahren wird sich in der Praxis wahrscheinlich auch durchsetzen, ist aber nicht notwendig mit der Verwendung eines elektronischen Dokuments verbunden. Der inzwischen weltweit angewandte Standard für elektronische Dokumente UN/EDIFACT (Electronic Data In-

Prof. Dr. jur. Wolfgang Kilian ist Leiter des Instituts für Rechtsinformatik (IRI) der Universität Hannover.

terchange for Administration, Commerce and Trade) der Internationalen Standardorganisation (ISO), auf den ich in meiner von Rüßmann zitierten Veröffentlichung bezug genommen habe, sieht selbst überhaupt keine Verschlüsselung vor. Dennoch arbeiten Unternehmen in der Praxis in allen Bereichen (vor allem in der Automobilindustrie, bei Speditionen, in Banken und demnächst auch im Bereich des Tourismus, der Medizin und in der öffentlichen Verwaltung) zunehmend mit diesem Standard. Das Absicherungsbedürfnis der Praxis ist deshalb sehr wohl nachvollziehbar und beruht keineswegs auf "allfälligen Mißverständnissen" (so Rüßmann, a. a. O., S. 3217).

Da auch eine private Vereinbarung, den elektronischen Dokumenten den gleichen Beweiswert wie Privatkunden nach § 416 ZPO zuzubilligen, den staatlichen Richter nicht bindet, kann die gegenwärtige Ungewißheit über den Ausgang der Bewertung eines Richters im Rahmen der freien Beweiswürdigung nach § 286 ZPO nur durch eine Schiedsklausel erreicht werden. Auf diesem Weg läßt sich nämlich die mit dem Freibeweis verbundene höhere Unsicherheit über das Ergebnis der Bewertung durch den Richter verringern, weil die Zivilprozeßordnung nicht angewandt werden muß. Elektronische Dokumente können dann auch ohne Verschlüsselung wie echte Privaturkunden nach § 416 ZPO behandelt werden. Die Parteien sind auf diesem Wege sogar in der Lage, bindend zu vereinbaren, daß die Echtheit des elektronischen Dokuments nicht angezweifelt werden darf.

Mit Rüßmann bin ich allerdings der Meinung, daß die vorhandenen Verschlüsselungsverfahren für elektronische Dokumente, wie das RSA-Verfahren, sich eignen, den gleichen Grad an Fälschungssicherheit wie Papierdokumente zu garantieren. Diese Verfahren müssen aber zunächst eingeführt und dann zusätzlich vereinbart werden, etwa in einem Rahmenvertrag zwischen den Geschäftspartnern (EDI-Rahmenvertrag). Dies wird in der Praxis auch so gesehen (z. B. bei Banken; im Baugewerbe; bei Speditionen). Die Infrastruktur für eine zuverlässige Verschlüsselung ist in Deutschland bisher noch nicht vorhanden. Nach Einführung der sogenannten Trust Center (Zertifizierungsstellen; Akkreditierungsstellen) steht der Anwendung anerkannter Verschlüsselungsverfahren nichts entgegen. Elektronische Dokumente bilden dann funktionale Äquivalente zu den Privaturkunden. Wenn keine ausdrückliche Gesetzesänderung erfolgt, könnte darauf § 416 ZPO analog angewandt werden, weil alle Funktionen einer eigenhändigen Unterschrift (Echtheits-, Abschluß-, Warn- und Identitätsfunktion) technisch und rechtlich als gesichert gelten.

Ob die funktionale Äquivalenz verschlüsselter elektronischer Urkunden zu Papierurkunden zur analogen Anwendung von § 416 ZPO durch die Gerichte führen wird, ist allerdings offen. Deshalb scheint der Weg vorzugswürdiger zu sein, durch ausdrückliche gesetzliche Regelung der elektronischen Unterschrift auf der Grundlage anerkannter Verschlüsselungsverfahren den gleichen Rang wie einer eigenhändigen Unterschrift zuzubilligen.

Der bereits vorliegende Entwurf des Bundesministers des Innern vom 14.8.1995 zu einer entsprechenden Verordnung (Elektronische Unterschriftsverordnung) über die Anerkennung von Verfahren zur elektronischen Unterschrift durch Schaffung eines Paragraphen 126a Abs. 2 BGB ist daher grundsätzlich zu begrüßen. Eine solche Regelung trägt zur Rechtssicherheit bei und erübrigt spekulative Einschätzungen über den Beweiswert elektronischer Dokumente sowie über die Wahrscheinlichkeit von Bewertungsakten eines Richters im Rahmen des Freibeweises nach § 286 ZPO. Der Verordnungsentwurf weist allerdings andere Mängel auf: Die Organisation der sogenannten Trust-Center (vertrauenswürdige Dritte, die für die Schlüsselvergabe zur Verschlüsselung und Entschlüsselung zuständig sind), erscheint problematisch. Diese Aufgabe dürfen m. E. nur staatsferne Institutionen sowie nicht kommerziell arbeitende Organisationen wahrnehmen (z. B. Notarkammer; Stiftungen des öffentlichen Rechts; branchenspezifische unabhängige Stellen), weil sonst das Vertrauen in die Institutionen fehlt. Die Möglichkeit des Eindringens von Geheimdiensten in die Kommunikationsnetze darf nicht institutionell durch die Organisation der Trust-Center begünstigt werden. Es geht um eine strukturell für die Sicherheit der Datenübertragung und die Vertraulichkeit der elektronischen Kommunikation wichtige Grundsatzentscheidung.