Prof. Dr. Helmut Rüssmann

Beweisführung mit elektronischen Dokumenten

Referat an der Tagung für Informatik und Recht, Bern, 26. Oktober 2004

Der Beitrag behandelt das deutsche Recht der Beweisführung mit elektronischen Dokumenten und fragt nach der Zulässigkeit der Beweisführung, der Existenz von Beweisregeln, die den Grundsatz der freien Beweiswürdigung einschränken, den Möglichkeiten, sich ein Urteil über die Wahrheit und Echtheit eines Dokuments zu bilden und den Mitwirkungslasten und Mitwirkungspflichten der Personen, die die Verfügungsgewalt über die elektronischen Dokumente haben.

Inhaltsübersicht

I. Einführung
II. Zulässigkeit der Beweisführung mit elektronischen Dokumenten und Einordnung der elektronischen Dokumente in das Beweismittelrecht der deutschen Zivilprozessordnung (ZPO)
III. Beweiswert elektronischer Dokumente
1. Die elektronische Lüge
2. Unberechtigte Eingriffe Dritter
3. Zwischenergebnis zum Beweiswert elektronischer Dokument
IV. Digitale Signatur, Urkundsbeweis und Anscheinsbeweis
1. Funktionsweise digitaler Signature
2. Zuordnung der Schlüssel zu Personen
3. Beweiswert digital signierter Dokumente
V. Mitwirkungslasten und -pflichten bei der Beweisführung mit Hilfe elektronischer Dokumente
1. Eigene elektronische Dokumente
2. Elektronische Dokumente in der Verfügungsgewalt des Prozessgegners
3. Elektronische Dokumente in der Verfügungsgewalt Dritter
VI. Zusammenfassung

I. Einführung

[Rz 1] Rechtsgeschäfte werden in grossem Umfang elektronisch abgewickelt. Elektronische Dokumentationen lösen in weiten Bereichen die Papierdokumentationen ab. Kommt es zu einem Streit über den Inhalt eines elektronisch geschlossenen Rechtsgeschäfts oder über den Verlauf einer elektronisch dokumentierten medizinischen Behandlung steht man vor der Frage der Beweisführung mit elektronischen Dokumenten. Dem für die Beweisführung an das nationale Recht des Staates gebundenen Juristen, dessen Gerichte den Streit gegebenenfalls zu entscheiden haben, treten mehrere Problemkomplexe entgegen:

1. Erlaubt das Recht die Beweisführung mit elektronischen Dokumenten?
2. Welchem Beweismittel ist das elektronische Dokument zuzuordnen, wenn das Recht Regeln für unterschiedliche Beweismittel kennt?
3. Unterliegt das elektronische Dokument hinsichtlich Echtheit und Inhalt der freien Beweiswürdigung oder ist die Beweiswürdigung des Richters durch Beweisregeln gebunden?
4. Wie kann man sich ein verlässliches Bild von der Echtheit und Wahrheit des elektronisch Dokumentierten machen?
5. Wie erhält man Zugang zu den elektronischen Dokumenten, die nicht in den Händen der beweisführenden Partei liegen?

II. Zulässigkeit der Beweisführung mit elektronischen Dokumenten und Einordnung der elektronischen Dokumente in das Beweismittelrecht der deutschen Zivilprozessordnung (ZPO)

[Rz 2] Im deutschen Recht ist die Zulässigkeit der Beweisführung mittels elektronischer Dokumente unproblematisch zu bejahen. Im Unterschied zum Recht anderer Staaten kennt das deutsche Prozessrecht keine Einschränkungen, die eine Beweisführung mit Hilfe elektronischer Dokumente in irgendeiner Weise behindern [1].

[Rz 3] Beweismittel in der ZPO sind der Augenschein, der Zeugenbeweis, der Beweis durch Sachverständige, der Urkundenbeweis und die Parteivernehmung. In dieser Einteilung kommen zunächst der Urkundenbeweis oder – als Auffangbecken – der Augenscheinsbeweis in Betracht. Urkunden i.S.d. Beweismittelrechts der ZPO sind durch Niederschrift verkörperte Gedankenerklärungen, die geeignet sind, Beweis für streitiges Parteivorbringen zu erbringen.[2] Bei elektronischen Willenserklärungen fehlt es an der notwendigen Verkörperung. [3] Auch Ausdrucke der auf dem Rechner gespeicherten Daten stellen keine Urkunden dar, die die Willenserklärung belegen könnten, denn durch sie wird keine originäre menschliche Gedankenäusserung bekundet, sondern nur die Tatsache der Eingabe und Programmierung von Daten.[4] Der Beweis mit elektronischen Dokumenten unterfällt damit nicht den Regeln über den Urkundenbeweis[5], sondern den Vorschriften über den Beweis durch Augenschein. [6] Um einen Sachverständigenbeweis handelt es sich hingegen, wenn die Visualisierung oder auch die Prüfung der zur Sicherung der Authentizität und Integrität eingesetzten Verfahren besondere Kenntnisse und Fertigkeiten voraussetzen. [7]

III. Beweiswert elektronischer Dokumente

[Rz 4] Mit der Einordnung elektronischer Dokumente in das Beweismittelsystem der ZPO ist aber noch nichts über den Beweiswert der elektronischen Dokumente gesagt. Während für Erklärungen in Privaturkunden die gesetzliche Beweisregel des § 416 ZPO[8]

> § 416 Beweiskraft von Privaturkunden
>
> > Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.

gilt, unterliegen elektronische Erklärungen nach dem bisherigen Recht der freien Beweiswürdigung nach § 286 ZPO:

> § 286 Freie Beweiswürdigung
>
> > (1) Das Gericht hat unter Berücksichtigung des gesamten Inhalts der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme nach freier Überzeugung zu entscheiden, ob eine tatsächliche Behauptung für wahr oder für nicht wahr zu erachten sei. In dem Urteil sind die Gründe anzugeben, die für die richterliche Überzeugung leitend gewesen sind.
> > (2) An gesetzliche Beweisregeln ist das Gericht nur in den durch dieses Gesetz bezeichneten Fällen gebunden.

[Rz 5] Der Richter hat also im Einzelfall unter Berücksichtigung des Ergebnisses der gesamten Beweisaufnahme festzustellen, ob er dem elektronischem Dokument den darin enthaltenen Inhalt «glaubt» oder nicht. Ob er dem elektronischen Dokument «glauben» wird, hängt dabei unter anderem davon ab, in welchem Masse er davon ausgehen kann, dass das, was in der elektronischen Erklärung dokumentiert wird, auch der Wahrheit entspricht. Schon bei einer verkörperten Erklärung in Form einer Urkunde sind verschiedenste Möglichkeiten der Verfälschung gegeben. Bei der elektronischen Erklärung kommen weitere hinzu. Im Folgenden soll auf einige dieser Möglichkeiten hingewiesen werden.

1. Die elektronische Lüge

[Rz 6] Die Gefahren für die Verlässlichkeit der Dokumentation können zunächst von dem ausgehen, der die Dokumentation erstellt. Erstellt er die Dokumentation von vornherein so, dass sie nicht das dokumentiert, was tatsächlich geschehen ist, so enthält die Dokumentation eine Lüge oder auch eine irrtümliche Abweichung von der Wahrheit. Dagegen ist bei elektronischen Dokumentationen so wenig ein Kraut gewachsen wie gegen die schriftliche

Lüge oder den Irrtum in an die Schriftform gebundenen Dokumentationen. Während man nachträgliche Änderungen der schriftlichen Dokumentation unter Umständen ansehen oder durch besondere Analyseverfahren feststellen kann, sind solche Änderungen einer elektronischen Dokumentation prinzipiell spurenlos und der Dokumentation als solcher nicht anzumerken. Hier können Urkunden im Rahmen der freien Beweiswürdigung mehr Sicherheit gewähren als elektronische Dokumente einschliesslich ihrer Ausdrucke. Das sei an einem einfachen Beispiel erläutert.

[Rz 7] Wenn ich auf meinem PC eine Bestellung schreibe und diese Bestellung in einem Beweisverfahren eine Rolle spielen sollte, kann die Bestellung zum Zwecke der Vorlage an das Gericht manipuliert werden, ohne dass das Gericht oder ein gerichtlicher Sachverständiger diese Manipulation nachweisen könnte. Für den Ausdruck versteht sich das von selbst, weil man dem Ausdruck nicht ansehen kann, wann die Bestellung verfasst worden ist und ob in ihr nachträglich Änderungen eingefügt worden sind. Man kann das aber nicht nur dem Ausdruck nicht ansehen, man kann es auch durch eine Untersuchung der Datei auf der Platte, dem elektronischen Speichermedium, nicht feststellen. Obwohl das Betriebssystem des Computers den Zeitpunkt der Speicherung nach Datum und Zeit sekundengenau registriert und die Datei mit einem entsprechenden Zeitstempel versieht, ist diese Information nicht verlässlich für den wirklichen Zeitpunkt der Speicherung, weil ein kleiner Handgriff genügt, um die Systemzeit des Rechners umzustellen und einen Zeitstempel für die Speicherung zu erhalten, der mit dem tatsächlichen Zeitpunkt der Speicherung nichts gemein hat. Niemand kann dem elektronischen Speichermedium diese Manipulation ansehen. Das nur in dieser Form ohne weitere Vorkehrungen Gespeicherte erweist sich im Streitfall als wertlos. Die Situation ändert sich, wenn das Gespeicherte einem nicht änderbaren Datenträger anvertraut oder der änderbare Datenträger einem vertrauenswürdigen Dritten zur Verwahrung übergeben und auf diese Weise sichergestellt wird, dass die unter Umständen an Änderungen interessierte Partei keine Möglichkeit zu Änderungen hatte. Sie ändert sich auch, wenn System-, Programm- und Dateizugriffe lückenlos dokumentiert werden und sich dieser Zusatzdokumentation entnehmen lässt, wann wer mit welchem Programm auf eine Datei zugegriffen hat. [9] Die uns aus dem PC-Bereich vertrauten Betriebssysteme und Programme bieten solche Funktionen jedoch nicht standardmässig an.

2. Unberechtigte Eingriffe Dritter

[Rz 8] Auch Dritte können in vielerlei Hinsicht auf elektronische Erklärungen einwirken oder Erklärungen vortäuschen, die der als Erklärender Genannte nie abgegeben hat.

[Rz 9] So kann beispielsweise bei einer E-Mail sehr leicht ein anderer Absender vorgetäuscht werden, indem die Einstellungen des eigenen Kontos im Mailprogramm geändert und fortan E-Mails unter falschem Namen und falscher Absenderadresse versendet werden. Jeder könnte auf diese Weise E-Mails von «Prof. Rüssmann» versenden. Der tatsächliche Absender einer E-Mail ist nur bedingt vom Empfänger überprüfbar, nämlich nur dann, wenn der Absender in einem Verbund ist, in dem feste IP-Adressen vergeben werden. Wenn sich der Absender per Modem ins Internet einwählt und eine sogenannte dynamische IP-Adresse zugeteilt bekommt (also mit jedem Anruf eine IP-Adresse, die gerade frei ist), wird die Nachverfolgung schwierig: Man muss sich mit dem Provider in Verbindung setzen, über den die Einwahl erfolgte und diesen bitten, die Telefonnummer des Kunden mitzuteilen. Einen Schutz gegen Missbrauch bietet allerdings die unten näher zu erläuternde elektronische Signatur.

[Rz 10] Auch bei Bestellungen über WWW-Formulare ist ein Missbrauch möglich. Niemand ist gehindert, in ein Bestellformular fremde Daten einzugeben.

[Rz 11] Spezialprogramme, die im Bereich des Online Bankings verwendet werden, sind hingegen vor dem Zugriff fremder Personen relativ sicher. Hier wird meist eine Verschlüsselung mit PIN [10] und TAN [11] genutzt. Eine Gefahr liegt in diesem Bereich allenfalls darin, dass Unberechtigte TANs und PIN ausspähen und verwenden. Die Gefahr, dass ein Unbefugter Zugangsdaten nutzt, besteht allerdings bei allen Systemen und führt zur Frage, ob und wie man einen derartigen Missbrauch nachweisen kann. Dazu sind wiederum Logfiles in der Lage, die genau protokollieren, woher ein Anruf kam, wie der Rechnername lautete, von dem die Transaktion ausging, und wie der Benutzer hiess, der eingeloggt war, deren Erstellung aber auf den uns aus dem PC-Bereich vertrauten Betriebssysteme und Programme nicht standardmässig angeboten wird.

3. Zwischenergebnis zum Beweiswert elektronischer Dokumente

[Rz 12] Nach all dem ist im elektronischen Rechtsverkehr eine erhebliche Beweisunsicherheit der Geschäftspartner gegeben. Nach der Auffassung des Bundesgerichtshofs [12] konnten selbst Sendeprotokolle keinen Anscheinsbeweis für den Zugang einer Erklärung bieten, vielmehr stellten auch diese nur Indizien im Rahmen einer Beweiswürdigung nach § 286 ZPO dar.

[Rz 13] Teilweise wurde versucht, diese Beweisprobleme mit Hilfe einer Beweisvereinbarung zu lösen [13]. Diesbezüglich erschien aber zum einen fraglich, ob entsprechende Klauseln – sofern sie in AGB formuliert waren – den rechtlichen Anforderungen für die Geltung von AGB genügten. Zudem kann dem Richter durch die Parteien keine bestimmte Beweiswürdigung vorgeschrieben werden.

[Rz 14] Insgesamt herrscht mithin eine erhebliche Unsicherheit, welchen Beweiswert elektronischen Dokumenten im Einzelfall zugesprochen werden kann. Diese Unsicherheit belastet den elektronischen Handel, der – möchte er «sichergehen» – doch wieder auf die herkömmliche Schriftform zurückgreifen muss.

IV. Digitale Signatur, Urkundsbeweis und Anscheinsbeweis

[Rz 15] Eine Lösung für die genannten Schwierigkeiten wird in der Verwendung digitaler Signaturen gesehen. Digitale Signaturen ermöglichen, dass Manipulationen am Inhalt elektronischer Nachrichten erkannt und Sender und Empfänger einer Nachricht identifiziert werden können. Die digitale Signatur entstand aus dem Bedürfnis heraus, eine sichere elektronische Kommunikation zwischen mehreren Parteien zu gewährleisten. Dieses Bedürfnis nach Sicherheit ist bei jeder Kommunikation über Medien gegeben, also bei jeder Kommunikation, bei welcher nicht zwei persönlich miteinander bekannte Personen direkt miteinander sprechen.

1. Funktionsweise digitaler Signaturen

[Rz 16] Man stelle sich die Situation vor ca. zwei Jahrtausenden vor. Julius Cäsar schickt einen Befehl an seinen Truppenkommandeur irgendwo im römischen Reich. Im Befehl steht «Rückzug». Woher weiss der Kommandant, dass der Befehl «echt» ist? Es gibt die Möglichkeit, die Nachricht zu verschlüsseln, und die, sie zu signieren. Die Signatur ermöglicht die Authentifizierung, jedoch birgt sie die Gefahr, dass der signierte Text auf seinem Weg verändert wurde. Zum Beispiel könnte ein «Niemals» vor dem «Rückzug» kunstvoll aus dem Pergament entfernt worden sein, während der Bote in einer Taverne dem Wein zu heftig zusprach. Die Verschlüsselung bietet die Möglichkeit, den Inhalt der Botschaft für Unbefugte unleserlich zu machen. Die Verschlüsselung hat aber auch eine gewisse Signaturfunktion: Sofern es nur zwei Leute gibt, die den Entschlüsselungscode kennen, weiss der Empfänger einer derart codierten Nachricht, dass die Nachricht vom jeweils anderen stammt, da nur dieser in der Lage ist, die Nachricht anhand des geheimen Codes zu verschlüsseln.

a. Symmetrische Verschlüsselung

[Rz 17] Die Problematik sowohl der digitalen Signatur als auch der Verschlüsselung liegt in der Notwendigkeit der Nutzung eines gemeinsamen Codes und der daraus folgenden Erforderlichkeit, einen solchen Code zu verabreden. Kommt es zwei Parteien darauf an, sich ständig geheime Botschaften zu schicken, so könnten sie sich treffen, um einen geheimen Code zu vereinbaren, den sie fortan immer nutzen. Dies ist soweit unproblematisch – eine ausreichend starke Verschlüsselung vorausgesetzt. Will aber jemand in der heutigen Zeit – im Zeitalter der Rechtsgeschäfte per Internet – über Ländergrenzen und Kontinente hinweg jemandem eine vertrauliche Information zukommen lassen (zum Beispiel die vielzitierte Kreditkartennummer samt Gültigkeitsdatum), dann steht dieser jemand vor dem Problem, nicht *mal schnell* mit dem Gegenüber einen sicheren Code vereinbaren zu können.

b. Asymmetrische Verschlüsselung

[Rz 18] Hier setzt die Public-Key-Verschlüsselung an. Dieses Verfahren arbeitet mit mathematischen Gesetzmässigkeiten. Es wird anhand von Zufallszahlen ein komplexes Zahlenpaar gebildet, bei dem sichergestellt ist, dass man mit Hilfe der einen nicht die andere und mit Hilfe der anderen nicht die eine Zahl errechnen kann. Beide Zahlen passen jedoch «aufeinander».

[Rz 19] Eine dieser Zahlen wird «öffentlicher Schlüssel», die andere «privater Schlüssel» genannt. Der öffentliche Schlüssel wird im Internet auf speziell dafür eingerichteten Computern allen Interessierten zugänglich gemacht, während der private Schlüssel unter strengstem Verschluss beim Inhaber des Schlüsselpaares bleibt (im Idealfall).

c. Sicherung der Vertraulichkeit

[Rz 20] Wenn nun unser jemand (Bob) dem anderen (Tina) eine Mitteilung zukommen lassen will, sucht er auf dem Server den öffentlichen Schlüssel von Tina. Mit diesem verschlüsselt er seine geheime Nachricht und sendet sie ab. Aufgrund der mathematischen Beschaffenheit der Schlüssel kann diese Information jetzt nur noch mit dem privaten Schlüssel von Tina gelesen werden. Selbst die nochmalige Anwendung des öffentlichen Schlüssels bringt die vertrauliche Nachricht nicht wieder zum Vorschein. Sofern man nun davon ausgeht, dass Tina sehr gut auf ihren Schlüssel aufgepasst hat, wird man weiter davon ausgehen können, dass nur noch sie in der Lage ist, die Nachricht zu entziffern. Wenn sie Bob antworten möchte, sucht sie dessen Schlüssel auf dem öffentlichen Server und sendet ihre Nachricht ebenso wie Bob dies eben mit ihrem Schlüssel getan hat.

d. Sicherung der Authentizität (Echtheit)

[Rz 21] Woher aber weiss nun Tina, dass die Nachricht wirklich von Bob kam? Tinas öffentlicher Schlüssel ist ja jedem zugänglich und daher kann auch jedermann diese Nachricht geschickt haben. Die Lösung liegt im *privaten* Schlüssel von Bob: Er signiert die Nachricht. Wie geht das vonstatten? Ganz einfach: Er schreibt seine geheime Nachricht. Dann verschlüsselt er sie mit Tinas öffentlichem Schlüssel. Die Nachricht ist nun sicher vor dem Zugriff anderer (und auch vor ihm selbst). Als dritten Schritt wendet er nun seinen eigenen privaten Schlüssel auf die verschlüsselte Nachricht an. Denn ebenso wie man den öffentlichen Schlüssel nur mit dem privaten Schlüssel wieder öffnen kann, so kann man den privaten Schlüssel nur mit dem öffentlichen öffnen.

[Rz 22] Bob signiert also die verschlüsselte Botschaft mit seinem privaten Schlüssel. Tina bekommt die so signierte und verschlüsselte Botschaft und überprüft, ob die Nachricht von Bob stammt. Dazu wendet sie seinen öffentlichen Schlüssel auf die Botschaft an. Da der private Schlüssel von Bob sich nur von seinem öffentlichen Schlüssel wieder entschlüsseln lassen kann, weiss Tina sicher, dass die Nachricht von Bob ist, sofern ihr die Entschlüsselung mit dessen öffentlichen Schlüssel gelingt. Nun hat sie lediglich noch den Klartext der Botschaft mit ihrem eigenen privaten Schlüssel herzustellen.

e. Digitale Signatur

[Rz 23] Geht es Bob nun aber nicht (primär) darum, seine Nachricht geheim zu halten, sondern möchte er nur ermöglichen, dass Manipulationen seiner Daten durch Dritte erkannt werden können, dann muss er seinen privaten Schlüssel nicht – wie eben geschildert - auf die *gesamte* zu versendende Nachricht anwenden. Da asymmetrische Verschlüsselungsverfahren relativ langsam sind, würde die Erzeugung einer Verschlüsselung des gesamten Textes einige Zeit in Anspruch nehmen. Unter anderem aus diesem Grund wird bei der Erzeugung einer digitalen Signatur – bei der es ja weniger auf die Geheimhaltung als auf die Authentifizierung sowie den Ausschluss von Manipulationsmöglichkeiten ankommt - zunächst auf Grund öffentlich verfügbarer Algorithmen ein sogenanntes Hash-Verfahren auf die unverschlüsselten Daten angewendet. Dabei wird ein Komprimat aus der zu sendenden Nachricht gebildet. Dies ist nichts anderes als eine Prüfsumme (Checksumme). Bob wendet anschliessend seinen privaten Schlüssel nur noch auf die Prüfsumme an. Das Ergebnis dieses Vorgangs bildet dann die digitale Signatur, welche dem unverschlüsselten Text angefügt wird. Erhält Tina von Bob eine mit einer digitalen Signatur versehene Nachricht, so wendet sie hierauf den öffentlichen Schlüssel von Bob an. Dabei geschieht dann zweierlei: Zum einen wird die digitale Signatur (= die verschlüsselte Prüfsumme) entschlüsselt und Tina erhält die von Bob erzeugte Prüfsumme im Klartext. Zum anderen wird aus dem unverschlüsselten Text der Nachricht erneut ein Hash-Komprimat gebildet. Stimmen das durch Tina neu gebildete Komprimat und die in der digitalen Signatur befindliche Prüfsumme überein, so kann Tina sicher sein, dass der Inhalt der von Bob gesendeten Nachricht nicht verändert wurde. Die Überprüfung eines Textes auf Manipulationen beruht also auf einem Prüfsummenvergleich. Wäre beim Transport der Nachricht auch nur ein einzelnes Bit verändert worden, so würden die beiden Prüfsummen bereits nicht mehr übereinstimmen. Das Ganze klingt natürlich nach einem sehr hohen Aufwand. In der Praxis stellt dies aber kein Problem dar, weil alle Vorgänge von der eingesetzten Signiertechnik automatisch erledigt werden.

2. Zuordnung der Schlüssel zu Personen

[Rz 24] Problematisch wird nun, sicherzustellen, dass die auf den Servern «ausgelegten» Schlüssel wirklich ihren vorgeblichen Inhabern gehören. Technisch gesehen ist es kein Problem, einen Schlüssel zu erzeugen, der den Eindruck erweckt, einem anderen zu gehören. Gängige Software erzeugt die Schlüsselpaare und fragt dann nach dem Namen des Anwenders. Wenn «Frieda» den Schlüssel von «Bob» vortäuschen will, wird sie dem Programm einfach als Namen «Bob» eingeben und den öffentlichen Schlüssel so auf einen Server stellen. [14] Befindet sich dort noch kein Schlüssel, wird jeder, der danach sucht, lediglich den «falschen» Schlüssel von «Frieda» sehen, der vorgibt, «Bob» zu gehören. Befindet sich dort schon ein Schlüssel (richtig oder falsch) von «Bob», dann wird der Suchende eben mehrere Schlüssel zur Auswahl haben und sich im Zweifel für den falschen entscheiden.

[Rz 25] Also muss sichergestellt werden, dass die ausgelegten Schlüssel tatsächlich den richtigen Personen gehören. Wie macht man das?

[Rz 26] Es gibt mehrere (unterschiedlich wirksame) Möglichkeiten.

a. Web of trust

[Rz 27] Die Schlüssel sind letztlich selbst nichts anderes als digitale Informationen. Diese kann man natürlich ebenfalls verschlüsselt irgendwo speichern. Dies empfiehlt sich wegen der höheren Sicherheit sogar. Man kann die Schlüssel aber auch signieren. Wenn Bob und Tina sich mal treffen und per Zufall ihre Schlüssel «dabei» haben, kann Tina mit ihrem Privatschlüssel den öffentlichen Schlüssel von Bob signieren. Dies drückt für Peter, der später mit Bob Geschäfte machen will, aus, dass Tina davon überzeugt ist, dass der öffentliche Schlüssel von Bob wirklich zu Bob gehört. Sollten nun zwei Schlüssel auf einem Server sein und einer davon ist von Tina signiert, dann wird Peter (hoffentlich) diesen wählen. Dies wird er umso lieber tun, wenn er Tina persönlich kennt und ihr vertraut. Natürlich kann Tina den Schlüssel von Bob aber auch signieren, ohne Bob jemals gesehen zu haben. Dies wäre aber jedoch fahrlässig, wenn man bedenkt, dass sich andere auf «das Wort» von Tina verlassen, wie dies im obigen Beispiel Peter tat.

b. Trustcenter

[Rz 28] Im heutigen Rechtsverkehr wird es unwahrscheinlich sein, dass sich ein Unternehmen darauf verlässt, dass eine ihm Unbekannte namens Tina den Schlüssel von Bob signiert hat, wenn es Bob eine wichtige Nachricht zustellen will und sichergehen will, dass diese Nachricht auch den Richtigen erreicht. Dem Unternehmen wäre es lieber, wenn eine Institution diese Signatur von Schlüsseln «hoheitlich» durchführen würde. Diese Institution sollte möglichst hohen Sicherheitsanforderungen entsprechen und möglichst einheitliche Standards wahren.

[Rz 29] Im «richtigen Leben» entspräche eine solche Institution der Passbehörde, die einen eindeutigen Nachweis der Identität – nämlich den Pass oder Personalausweis – ausstellt. Im «digitalen Leben» sind solche Institutionen die sogenannten «Trustcenter». Diese Stellen garantieren entweder, dass die zur Verfügung gestellten Schlüssel wirklich zu den richtigen Personen gehören (zum Beispiel dadurch, dass sie einen Mitarbeiter vorbeischicken, der sich den Schlüssel abholt und sich gleichzeitig den Personalausweis der Person zeigen lässt), oder erstellen diese Schlüssel sogar selbst im Auftrag der Personen, nachdem diese sich mit Hilfe eines amtlichen Dokumentes ausgewiesen haben. Natürlich muss man voraussetzen, dass die Mitarbeiter des Trustcenters nicht selbst Interesse am Verfälschen der Schlüssel haben; aber dafür heissen diese Institutionen ja « **Trust**center». Damit ein «Trustcenter» «Trustcenter» sein kann, muss es bestimmte Anforderungen erfüllen; diese sind in Deutschland im Signaturgesetz geregelt. [15]

[Rz 30] Das Signaturgesetz unterscheidet zunächst in § 2 Nrn. 1 bis 3 zwischen verschiedenen Arten elektronischer Signaturen. Gemäss § 2 Nr. 1 SigG sind zunächst «elektronische Signaturen» Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Auf der nächsten Stufe (Nr. 2) stehen «fortgeschrittene elektronische Signaturen». Dies sind elektronische Signaturen, die

- ausschliesslich dem Signaturschlüssel-Inhaber zugeordnet sind,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,

- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
- mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

[Rz 31] Letztlich kennt das Gesetz noch «qualifizierte elektronische Signaturen». Diese elektronische Signaturen müssen die Voraussetzungen der fortgeschrittenen elektronischen Signaturen erfüllen und zusätzlich

- auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
- mit einer sicheren Signaturerstellungseinheit erzeugt werden.

[Rz 32] Diese qualifizierten Signaturen, die auf einem qualifizierten Zertifikat beruhen, bieten die höchste Sicherheit. Qualifizierte Zertifikate können nur sogenannte Zertifizierungsdienstanbieter (=Trustcenter) erteilen. Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei (§ 4 Abs. 1 SigG). Allerdings muss derjenige, der den Betrieb eines Zertifizierungsdienstes aufnimmt, dies der zuständigen Behörde spätestens mit der Betriebsaufnahme anzeigen (§ 4 Abs. 3 S. 1 SigG). Zudem darf nur der einen Zertifizierungsdienst betreiben, der die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde sowie eine Deckungsvorsorge nach § 12 des SigG nachweist und die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 SigG gewährleistet (§ 4 Abs. 2 S. 1 SigG). Die erforderliche Zuverlässigkeit besitzt gemäss § 4 Abs. 2 S. 2 SigG, wer die Gewähr dafür bietet, als Zertifizierungsdiensteanbieter die für den Betrieb massgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt nach § 4 Abs. 2 S. 3 SigG vor, wenn die im Betrieb eines Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes liegen vor, wenn die Massnahmen zur Erfüllung der Sicherheitsanforderungen nach dem Signaturgesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 SigG der zuständigen Behörde in einem Sicherheitskonzept aufgezeigt und geeignet und praktisch umgesetzt sind (§ 4 Abs. 2 S. 4 SigG). Vergabe, Inhalt sowie Sperrung qualifizierter Signaturen ist in den §§ 5 ff. SigG geregelt.

3. Beweiswert digital signierter Dokumente

[Rz 33] Fraglich ist nunmehr, welcher Beweiswert digital signierten Dokumenten zukommt. Dass durch eine digitale Signatur eine sehr hohe Sicherheit dahingehend besteht, dass der in der elektronischen Willenserklärung genannte Absender tatsächlich der Erklärende war und dass die Nachricht nicht verfälscht wurde, steht fest. Damit ist dem Gericht im Rahmen des § 286 ZPO aber noch kein Beweisergebnis vorgeschrieben. [16] Daran ändert auch die geplante Gleichstellung[17] des mit qualifizierter elektronischer Unterschrift versehenen elektronischen Dokuments mit einer Urkunde nichts.

[Rz 34] Denn die Beweisregel des § 416 ZPO

> «Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.»

ist logisch von der Gestalt «Wenn p, dann p». Das aber ist ein logisch wahrer Satz, der in keiner Welt falsch sein kann und diese Tatsache mit der Abwesenheit jeglichen Informationsgehalts bezahlt. Die Voraussetzung für das Eingreifen dieser Beweisregel ist die Tatsache, dass die Urkunde von dem Aussteller stammt. Das ist gleichbedeutend mit der Tatsache, dass die in der Urkunde enthaltenen Erklärungen von dem Aussteller abgegeben worden sind.

[Rz 35] Die Musik und das heisst hier die Bindung des Richters in der Beweiswürdigung steckt in einer anderen, der Schrifturkunde fremden Regel. Seit dem 1. August 2001 gilt in Deutschland § 292a ZPO:

> «Der Anschein der Echtheit einer in elektronischer Form (§ 126a des Bürgerlichen Gesetzbuches) vorliegenden Willenserklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des

Signaturschlüssel-Inhabers abgegeben worden ist.»

[Rz 36] Der Nachweis der Echtheit der in elektronischer Form abgegebenen Willenserklärung wird nach dieser Norm somit grundsätzlich schon durch die Prüfung nach dem Signaturgesetz erbracht, die die Signatur mit dem auf der Signaturchipkarte gespeicherten geheimen Schlüssel des Inhabers und dessen Identität bestätigt. Der Inhaber des Schlüssels kann diesen Nachweis nur erschüttern, wenn er schlüssig Tatsachen vorträgt und beweist, die einen abweichenden Geschehensablauf ernsthaft als möglich erscheinen lassen. Damit wird ein weitergehender Schutz des Erklärungsempfängers erreicht, als es die Vorschriften der Zivilprozessordnung über den Beweis durch Schrifturkunden vermögen, da nach diesen eine entsprechende Beweiserleichterung nicht eintritt, sondern der Erklärungsempfänger den vollen Beweis der Echtheit einer von dem Beweisgegner nicht anerkannten Namensunterschrift erbringen muss (§ 439 Abs. 1 und 2, § 440 Abs. 1 ZPO):

§ 439 Erklärung über Echtheit von Privaturkunden

(1) Über die Echtheit einer Privaturkunde hat sich der Gegner des Beweisführers nach der Vorschrift des § 138 zu erklären.
(2) Befindet sich unter der Urkunde eine Namensunterschrift, so ist die Erklärung auf die Echtheit der Unterschrift zu richten.
(3) Wird die Erklärung nicht abgegeben, so ist die Urkunde als anerkannt anzusehen, wenn nicht die Absicht, die Echtheit bestreiten zu wollen, aus den übrigen Erklärungen der Partei hervorgeht.

§ 440 Beweis der Echtheit von Privaturkunden

(1) Die Echtheit einer nicht anerkannten Privaturkunde ist zu beweisen.
(2) Steht die Echtheit der Namensunterschrift fest oder ist das unter einer Urkunde befindliche Handzeichen notariell beglaubigt, so hat die über der Unterschrift oder dem Handzeichen stehende Schrift die Vermutung der Echtheit für sich.

[Rz 37] Im Hinblick auf den aus diesem Grunde schwächeren Beweiswert der Schrifturkunde und das dem elektronischen Dokument fehlende Wesensmerkmal der Verkörperung auf einem unmittelbar lesbaren Schriftträger, wurde es im Jahre 2001 noch nicht für notwendig gehalten, dem von verschiedener Seite geäusserten Wunsch zu folgen, das elektronische Dokument beweisrechtlich der privaten Schrifturkunde gleichzustellen. Das wird erst durch das Justizkommunikationsgesetz geschehen.[18]

[Rz 38] Die Regelung des § 292a ZPO ist weder Fisch noch Fleisch. Die Aufstellung einer Vermutung im Sinne und mit den Folgen des § 292 ZPO

§ 292 Gesetzliche Vermutungen

Stellt das Gesetz für das Vorhandensein einer Tatsache eine Vermutung auf, so ist der Beweis des Gegenteils zulässig, sofern nicht das Gesetz ein anderes vorschreibt. Dieser Beweis kann auch durch den Antrag auf Parteivernehmung nach § 445 geführt werden.

erschien dem Gesetzgeber offenbar als zu stark. Eingeführt wurde eine Regelung, die sich erstens in der praktischen Handhabung kaum von einer Vermutung unterscheidet und zweitens als ein Fremdkörper im System des Zivilprozessrechts erweist, weil sie eine gesetzliche Beweiswürdigungsregel für einen Einzelfall enthält.

[Rz 39] Mit dem Beweis des ersten Anscheins hat die gerichtliche Praxis ein flexibles Instrument entwickelt, um in bestimmten Situationen dem Beweisbelasteten aus seiner Beweisnot zu helfen. Sie würde dieses Instrument auch im elektronischen Geschäfts- und Rechtsverkehr zu nutzen wissen, ohne die Anweisung des Gesetzgebers zu benötigen. Sie hat es für Geldkarten verwandt, wenn mit der zutreffenden PIN Geld am Automaten abgehoben worden ist.[19] Sie würde auch die Fälle der elektronischen Signatur ohne eine gesetzlich fixierte Beweiswürdigungsregel meistern. Wenn eine gesetzliche Regelung für erforderlich gehalten wird, um Unsicherheiten und Ängsten der am Ausbau des elektronischen Geschäftsverkehrs Interessierten zu begegnen, dann sollte der Gesetzgeber zur Vermutungsregelung greifen und diese daran binden, dass zusätzlich zur elektronischen Signatur der biometrische Zugang zum System

verlangt wird. Der PINgeschützte Zugang zur Chipkarte ist eine ernsthafte Schwachstelle in der Verknüpfung der elektronischen Signatur zu einer Person.

[Rz 40] Ob Anscheinsbeweis oder Vermutungsregel, das grösste Problem stellt die Schnittstelle Nutzer-Schlüssel dar. Hier ist die Möglichkeit gegeben, dass der Schlüssel dem Nutzer abhanden kommt und von Dritten missbraucht wird. Auch eine Sicherung per PIN ist nur solange sicher, wie diese weder ausgespäht werden noch weitergegeben werden kann.[20] Diese Gefahr ist aber nie völlig auszuschliessen. Letzte Sicherheit kann hier wohl nur ein Zugangsverfahren auf Grundlage biometrischer Merkmale bieten.

[Rz 41] Eine weitere denkbare Schwachstelle besteht in der Schnittstelle zwischen Bildschirm und Rechner. Auch wenn häufig ersterer mit letzterem gleichgesetzt (und von manchem Nutzer für die Fehlfunktionen des letzteren auch mit dem einen oder anderen Klaps versehen) wird, ist dies natürlich nicht zutreffend. So gibt das gesehene Bildschirmbild nicht notwendig genau das wieder, was im Rechner geschieht. Auch hier ist es möglich, dem Nutzer einen Inhalt der Erklärung, die er gerade signiert, vorzuspiegeln, den diese gar nicht hat.

[Rz 42] Angesichts der genannten Schwachstellen ist die gesetzliche Normierung des Anscheinsbeweises heftiger Kritik ausgesetzt.[21]

[Rz 43] Es wird geltend gemacht, dass die Voraussetzungen für einen Beweis des ersten Anscheins nicht gegeben seien.[22] In der Ausprägung der Rechtsprechung setzt der Anscheinsbeweis das Feststehen eines typischen Geschehensablaufs voraus. Ein Anscheinsbeweis mit dem vorliegenden Inhalt würde also voraussetzen, dass es der typischen Lebenserfahrung entspricht, dass eine Signatur, soweit sie auf dem Zertifikat einer akkreditierten Zertifizierungsstelle beruht, mit dem Willen des Schlüsselinhabers angebracht wurde. Dies ist angesichts der Tatsache, dass es verfestigte Erfahrungen mit digitalen Signaturen nicht gibt, mehr als zweifelhaft. Andererseits ist zu beachten, dass die genannte Voraussetzung eines Anscheinsbeweises als Selbstbindung der Rechtsprechung unmittelbar nur für die ungeschriebenen Fälle gilt. Der Gesetzgeber dürfte hingegen nicht gehindert sein, Anscheinsbeweiswirkungen auch ohne Beachtung der die Rechtsprechung bindenden Festlegungen für die ungeschriebenen Fälle anzuordnen.

[Rz 44] Ob die Risikoverteilung zulasten des Schlüsselinhabers angemessen ist oder nicht, ist diskussionswürdig. Für die neue Regelung spricht allenfalls, dass die grösste Unsicherheit für die Sicherheit der digitalen Signatur vom Inhaber des Schlüssels ausgeht, der diesen sorgfältig verwahren muss. Kommt er diesen Sorgfaltsobliegenheiten nicht nach, erscheint es auf den ersten Blick gerechtfertigt, ihm die Erschütterung des Anscheinsbeweises aufzuerlegen.[23] Allerdings stellt sich die Frage, ob mit der Zugangssicherung über eine fünfstellige PIN der Schlüsselinhaber nicht überfordert wird. Wer kann sich eine weitere PIN ohne Notierung merken? Der Normalmensch nicht! Dann aber ist es auch nicht gerechtfertigt, ihn mit einer Vermutung oder mit einem Beweis des ersten Anscheins zu belasten, wenn der Schlüsselindustrie andere Zugangsverfahren als die PIN zu Gebote stehen, um die Zuordnung der Signaturkarte zu einer bestimmten Person zu gewährleisten.[24] Diese anderen Verfahren sind Zugangskontrollen durch nicht manipulierbare biometrische Merkmale. Die jetzt getroffene Regelung behindert die Fortentwicklung sicherer Verfahren, statt sie zu fördern. [25] Unter der Geltung der neuen Regelung muss man allein auf die Gesetze des Marktes setzen, um die Unternehmen zu bewegen, weitere sichere Verfahren zu entwickeln, wenn das Anbieten derartiger Verfahren einen Wettbewerbsvorteil gegenüber Mitbewerbern um Kunden darstellt.

V. Mitwirkungslasten und -pflichten bei der Beweisführung mit Hilfe elektronischer Dokumente

[Rz 45] Eine letzte von der Zulässigkeit elektronischer Dokumente als Beweismittel und der Beweiswürdigung zu trennende Frage ist die nach den Mitwirkungslasten und -pflichten der Prozessparteien und ausserhalb des Prozesses stehender Dritter bei der Beweisführung mit Hilfe elektronischer Dokumente. [26] Diese Frage kann sich in den unterschiedlichsten Zusammenhängen stellen. Es ist denkbar, dass die beweisbelastete Partei einen Beweis mit eigenen elektronischen Dokumenten oder mit fremden elektronischen Dokumenten führen will. Die fremden Dokumente können sich in der Verfügungsgewalt des Prozessgegners, der insoweit nicht beweisbelasteten Partei, oder in der Verfügungsgewalt einer dritten Person befinden.

1. Eigene elektronische Dokumente

[Rz 46] Will die beweisbelastete Partei einen Beweis mit eigenen elektronischen Dokumenten führen, muss sie dem Gericht (und dem Gegner) nicht nur den Zugang zu dem fraglichen Dokument (beginnend in der Regel mit der Vorlage eines Computerausdrucks) eröffnen, sondern auch alle Informationen offenbaren, die für die Prüfung der Verlässlichkeit erforderlich sind, und in diesem Rahmen dem Gericht oder einem gerichtlichen Sachverständigen Zugang zu dem System selbst verschaffen. Tut sie das nicht, läuft sie Gefahr, den ihr obliegenden Beweis nicht führen zu können und den Prozess aufgrund der sie treffenden Beweislast zu verlieren. Insoweit regelt die Beweislast das zur Wahrheitsfindung gewünschte Aktivitäts- und Mitwirkungsniveau. Wir haben es mit einem Fall der Mitwirkungslast zu tun.

2. Elektronische Dokumente in der Verfügungsgewalt des Prozessgegners

[Rz 47] Will die beweisbelastete Partei einen Beweis mit elektronischen Dokumenten führen, die sich in der Verfügungsgewalt des Prozessgegners befinden, so versagt das Lastenmodell. Nach dem quasi naturrechtlichen Prozessrechtsgrundsatz «Nemo contra se edere tenetur!» soll niemandem zugemutet werden, gegen sein eigenes Fleisch zu wüten. Der Prozessgegner könnte also trotz der ihm ungünstigen Dokumentationslage die Hände in den Schoss legen, sein Gegenüber beweislos stellen und seine fehlende Mitwirkung mit dem Prozesssieg belohnt finden. Dieses Ergebnis wurde von manchen zumindest in abgemilderter Form akzeptiert. Man beschränkte den Grundsatz lediglich mit Blick auf materiellrechtliche Auskunfts- und Offenbarungsansprüche oder konzedierte minimale Korrekturen im Rahmen des Lastenmodells und auch am Modell selbst durch Herabsetzung der Substantiierungslast der beweisbelasteten Partei unter gleichzeitiger Steigerung der Last zur substantiierten Verteidigung der nicht beweisbelasteten Partei oder durch Heranziehung der Rechtsfigur der Beweisvereitelung [27]. Andere versuchten dagegen dem deutschen Zivilprozess den Weg in die «prozessuale Moderne» [28] zu weisen und eine allgemeine prozessuale Aufklärungs- und Mitwirkungspflicht der nicht beweisbelasteten Partei zu begründen. [29]

[Rz 48] Die traditionelle deutsche Prozessrechtswissenschaft [30] und die Rechtsprechung des Bundesgerichtshofs [31] hielten an dem Grundsatz: «Nemo contra se edere tenetur!» fest und waren darauf angewiesen, auch für elektronische Dokumente in der Verfügungsgewalt des Prozessgegners das Ausnahmepotential auszuschöpfen, das zu diesem Grundsatz entwickelt worden war. Sie mussten nach materiellrechtlichen Ansprüchen fahnden [32], prozessuale Sonderregeln ausfindig machen, [33] Überlegungen zum Umfang der Substantiierungslast für Behauptungen und Gegenbehauptungen anstellen [34] und eventuell zum Instrument der Beweisvereitelung mit seinen prozessualen Sanktionen greifen. [35] Diesen Bemühungen hat erst der Gesetzgeber ein Ende bereitet und Theorie und Praxis den Weg in die prozessuale Moderne gewiesen (dazu unten).

3. Elektronische Dokumente in der Verfügungsgewalt Dritter

[Rz 49] Eine ähnliche Entwicklung hat es bei den elektronischen Dokumenten gegeben, die sich in der Verfügungsgewalt eines nicht am Prozess beteiligten Dritten befinden. Das deutsche Prozessrecht hielt dafür keine Antwort bereit. Beim Urkundenbeweis wie beim Augenscheinsbeweis konnten ausserhalb des Prozesses stehende Dritte nur dann in Pflicht genommen werden, wenn der Beweisführer aufgrund materiellrechtlicher Bestimmungen einen Anspruch auf Urkundenvorlage oder auf Duldung des Augenscheins gegen den Dritten hatte.

[Rz 50] Rechtspolitisch war diese Regelung missglückt. Sie verschloss unnötig Aufklärungsmöglichkeiten und stand in einem unaufgelösten Wertungswiderspruch zu der fast uneingeschränkten Pflicht eines jeden Dritten, als Zeuge oder Sachverständiger zur Aufklärung eines streitigen Sachverhalts beizutragen. Warum man aber nicht sollte zeigen müssen, worüber man unter Zwang (§ 390 ZPO [36]) zum Sprechen angehalten werden konnte, war letztlich nicht begründbar. Die Kommission für das Zivilprozessrecht hatte deshalb im Jahre 1977 mit Recht einen Novellierungsvorschlag unterbreitet, der Dritte in Kongruenz zu ihrer Zeugnispflicht [37] auch verpflichtete, eine Sache vorzulegen oder bereitzuhalten [38]. Dem hat sich 25 Jahre später schliesslich auch der deutsche Gesetzgeber nicht verschlossen. Seit dem 1. Januar 2002 gilt, dass man vorlegen und zeigen muss, worüber man unter Zwang zum Sprechen angehalten werden kann. Und auch die nicht beweisbelastete Partei kann verpflichtet werden, Urkunden vorzulegen und den Augenschein zu dulden:

> § 142 Anordnung der Urkundenvorlegung
>
> (1) Das Gericht kann anordnen, dass eine Partei oder ein Dritter die in ihrem oder seinem Besitz

befindlichen Urkunden und sonstigen Unterlagen, auf die sich eine Partei bezogen hat, vorlegt. Das Gericht kann hierfür eine Frist setzen sowie anordnen, dass die vorgelegten Unterlagen während einer von ihm zu bestimmenden Zeit auf der Geschäftsstelle verbleiben.
(2) Dritte sind zur Vorlegung nicht verpflichtet, soweit ihnen diese nicht zumutbar ist oder sie zur Zeugnisverweigerung gemäss den §§ 383 bis 385 berechtigt sind. Die §§ 386 bis 390 gelten entsprechend.
(3) Das Gericht kann anordnen, dass von in fremder Sprache abgefassten Urkunden eine Übersetzung beigebracht werde, die ein nach den Richtlinien der Landesjustizverwaltung hierzu ermächtigter Übersetzer angefertigt hat. Die Anordnung kann nicht gegenüber dem Dritten ergehen.

§ 144 Augenschein; Sachverständige

(1) Das Gericht kann die Einnahme des Augenscheins sowie die Begutachtung durch Sachverständige anordnen. Es kann zu diesem Zweck einer Partei oder einem Dritten die Vorlegung eines in ihrem oder seinem Besitz befindlichen Gegenstandes aufgeben und hierfür eine Frist setzen. Es kann auch die Duldung der Massnahme nach Satz 1 aufgeben, sofern nicht eine Wohnung betroffen ist.
(2) Dritte sind zur Vorlegung oder Duldung nicht verpflichtet, soweit ihnen diese nicht zumutbar ist oder sie zur Zeugnisverweigerung gemäss den §§ 383 bis 385 berechtigt sind. Die §§ 386 bis 390 gelten entsprechend.
(3) Das Verfahren richtet sich nach den Vorschriften, die eine auf Antrag angeordnete Einnahme des Augenscheins oder Begutachtung durch Sachverständige zum Gegenstand haben.

[Rz 51] Damit hat die Bundesrepublik Deutschland Anschluss an die internationale Entwicklung gefunden. Das Recht auf Information und Beweis war in anderen Rechtsordnungen wesentlich stärker ausgeprägt als im Recht der Bundesrepublik Deutschland. Auch in diesen Rechtsordnungen galt einmal der Grundsatz: «Nemo contra se edere tenetur!» Sie haben den Grundsatz aber in zum Teil dramatischen Kehrtwendungen verabschiedet. [39]

VI. Zusammenfassung

[Rz 52] Der Beweis mit elektronischen Dokumenten ist in Deutschland als Augenscheins- bzw. Sachverständigenbeweis unproblematisch zulässig. Der Beweiswert elektronischer Dokumente ist allerdings durch vielfältige Verfälschungsmöglichkeiten geschmälert. Sicherheit bietet insoweit die digitale Signatur.

[Rz 53] Der Anscheinsbeweis des § 292a ZPO (demnächst § 371a Abs. 1 Satz 2 ZPO) ist eine systematische Fehlentwicklung gegen das Prinzip der freien Beweiswürdigung. Er trägt überdies der Schwachstelle Mensch beim Zugang zu der in einer Chipkarte gespeicherten elektronischen Unterschrift nicht hinreichend Rechnung.

[Rz 54] Deutschland hat im Jahre 2002 das Recht auf Information und Beweis gestärkt und Theorie und Praxis den Weg in die prozessuale Moderne gewiesen. Damit ist garantiert, dass die für die Würdigung elektronischer Dokumente erforderlichen Informationen Eingang in den Prozess finden werden.

Prof. Dr. Helmut Rüssmann, Institut für Rechtsinformatik, Universität des Saarlandes

Résumé français de l’exposé de Helmut Rüssmann aux Journées d’informatique juridique 2004 à Berne: Bassem Zein, Les documents électroniques et l'administration des preuves, in: Jusletter 8. November 2004.

1

Zu den beweisrechtlichen Schwierigkeiten in anderen Ländern s. u.a. *Rüssmann*, Moderne Elektroniktechnologie und Informationsbeschaffung im Zivilprozess, in: Schlosser (Hrsg.), Die Informationsbeschaffung für den Zivilprozess. Die Verfahrensmässige Behandlung von Nachlässen, ausländisches Recht und internationales Zivilprozessrecht, 1997, S. 138 (158 ff.).

[2] Zöller/*Geimer*, ZPO, 24. Aufl. 2004, Vor § 414, Rdnr. 2.

[3] Köhler/Arndt, Recht des Internet, 2. Aufl. 2000, Rdnr. 148; Scherer/Butt, Rechtsprobleme bei Vertragsschluss via Internet, DB 2000 S. 1009 (1016).

[4] Zöller/*Geimer*, Vor § 414, Rdnr. 2 m.N.

[5] Das könnte sich ändern, wenn das Justizkommunikationsgesetz Gesetz wird, das sich gerade im parlamentarischen Verfahren befindet. Es sieht im Rahmen des Augenscheinsbeweises eine Ergänzung vor:
§ 371a Beweiskraft elektronischer Dokumente
(1) Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.
(2) Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 entsprechend.

[6] Zöller/*Geimer*, Vor § 414, Rdnr. 2.

[7] *Rüssmann*, S. 157.

[8] Zu deren Gehalt vgl. *Britz*, Urkundenbeweisrecht und Elektroniktechnologie, 1996, S. 136 ff.

[9] Vgl. zu Protokolldateien allgemein *Runge*, Protokolldateien zwischen Sicherheit und Rechtsmässigkeit, CR 1994, 710.

[10] Personal Identification Number.

[11] Transaction Number.

[12] BGH NJW 1995,665.

[13] Dazu *Köhler/Arndt*, Rdnr. 150.

[14] Dazu: An Introduction to cryptography, Network Associates, Inc., Version 6.5.2, S. 21.

[15] Dazu näher *Köhler/Arndt*, Rdnr. 152 ff.

[16] *Scherer/Butt*, S. 1016.

[17] Siehe oben Fussnote 5.

[18] Siehe oben Fussnote 5.

[19] Dazu *Rüssmann*, Haftungsfragen und Risikoverteilung bei ecKartenmissbrauch, DuD 1998, 395 bis 400.

[20] In einem Pilotversuch zur elektronischen Kommunikation in gerichtlichen Verfahren haben die Rechtsanwälte einfach ihren Sekretärinnen Chipkarte samt PIN zur Zeichnung der Schriftsätze überlassen; vgl. *Rossnagel*, Die Simulationsstudie Rechtspflege, 1994.

[21] AGV, Stellungnahme zum Gesetz vom 11.08.00, S. 10 und Bundesnotarkammer, Stellungnahme vom 27.07.2000, S. 12.

[22] AGV, Stellungnahme zum Gesetz vom 11.08.00, S. 10 und Bundesnotarkammer, Stellungnahme vom 27.07.2000, S. 13.

[23] Dagegen Bundesnotarkammer, Stellungnahme vom 27.07.2000, S. 13.

[24] Das Justizkommunikationsgesetz sieht die Streichung des § 292a ZPO vor, um eine nicht auf Willenserklärungen beschränkte allgemeine Regelung in § 371a Abs. 1 ZPO anzuordnen (siehe oben Fussnote 5).

[25] AGV, Stellungnahme zum Gesetz vom 11.08.00, S. 10 und Bundesnotarkammer, Stellungnahme vom 27.07.2000, S. 14.

[26] Mit dieser Frage rückt die Informationsbeschaffung ins Blickfeld.

[27]

Stein/Jonas/Leipold, § 138 Rdnr. 22; *Lüke, Gerhard*, Der Informationsanspruch im Zivilrecht, JuS 1986, 2 (3); *Greger* in: *Zöller*, 21. Aufl. 2001, § 138 Rdnr. 8a.

[28] *Schlosser*, Die lange deutsche Reise in die prozessuale Moderne, JZ 1991, 599.

[29] Grundlegend *Stürner*, Die Aufklärungspflicht der Parteien des Zivilprozesses, 1976; *ders*., Parteipflichten bei der Sachverhaltsaufklärung im Zivilprozess, ZZP 98 (1985), 237. Der Alternativkommentar zur ZPO hat darin schon immer die bessere Alternative gesehen, AKZPO/*Eike Schmidt*, § 138 Rdnr. 17 ff.

[30] *Arens*, Zur Aufklärungspflicht der nicht beweisbelasteten Partei im Zivilprozess, ZZP 96 (1983), 1; *Lüke*, JuS 1986, 2; *Stein/Jonas/Leipold*, § 138 Rdnr. 22; *Rosenberg/Schwab/Gottwald*, § 117 IV (S. 680); mit Abstrichen auch MünchKommZPO-*Peters*, § 138 Rdnr. 22.

[31] Vgl. BGH, 11. Juni 1990, II ZR 159/89, ZZP 104 (1991), 203 mit dem amtlichen Leitsatz: „Die Zivilprozessordnung kennt keine - über die anerkannten Fälle der Pflicht zum substantiierten Bestreiten hinausgehende - allgemeine Aufklärungspflicht der nicht darlegungs- und beweispflichtigen Partei." Dem BGH stimmt zu *Schreiber*, Zur Frage, inwieweit die Parteien eines Zivilprozesses eine allgemeine Aufklärungspflicht trifft, JR 1991, 415. Eine kritische Anmerkung stammt aus der Feder von *Stürner*, Zur allgemeinen Aufklärungspflicht der nicht beweisbelasteten Partei im Zivilprozess, ZZP 104 (1991), 208.

[32] Etwa für die Offenlegung ärztlicher Dokumentationen.

[33] Wie § 258 Abs. 1 HGB für Handelsbücher.

[34] Das ist die Lösung des Bundesgerichtshofs in Fussnote 31.

[35] Eine geschickte Handhabung des Gesamtinstrumentariums mochte da durchaus zu denselben Ergebnissen führen, die die Anerkennung der prozessualen Aufklärungspflicht der nicht beweisbelasteten Partei mit sich gebracht hätte.

[36] § 390 Folgen der Zeugnisverweigerung
(1) Wird das Zeugnis oder die Eidesleistung ohne Angabe eines Grundes oder aus einem rechtskräftig für unerheblich erklärten Grund verweigert, so werden dem Zeugen, ohne dass es eines Antrages bedarf, die durch die Weigerung verursachten Kosten auferlegt. Zugleich wird gegen ihn ein Ordnungsgeld und für den Fall, dass dieses nicht beigetrieben werden kann, Ordnungshaft festgesetzt.
(2) Im Falle wiederholter Weigerung ist auf Antrag zur Erzwingung des Zeugnisses die Haft anzuordnen, jedoch nicht über den Zeitpunkt der Beendigung des Prozesses in dem Rechtszuge hinaus. Die Vorschriften über die Haft im Zwangsvollstreckungsverfahren gelten entsprechend.
(3) Gegen die Beschlüsse findet die sofortige Beschwerde statt.

[37] Die Bindung an die Zeugnispflicht gibt über die Zeugnisverweigerungsrechte genügend Raum für die Berücksichtigung von legitimen Interessen des Dritten, seine Informationen im Einzelfall nicht preiszugeben.

[38] Vgl. Bundesministerium der Justiz (Hrsg.), Bericht der Kommission für das Zivilprozessrecht, 1977, S. 151 ff.

[39] Siehe den Bericht von *Rüssmann* in: Moderne Elektroniktechnologie und Informationsbeschaffung im Zivilprozess, in: *Schlosser* (Hrsg.), Die Informationsbeschaffung für den Zivilprozess. Die Verfahrensmässige Behandlung von Nachlässen, ausländisches Recht und internationales Zivilprozessrecht, S. 138 (196 ff.).

Rechtsgebiet:	Informatikrecht
Erschienen in:	Jusletter 8. November 2004
Zitiervorschlag:	Helmut Rüssmann, Beweisführung mit elektronischen Dokumenten, in: Jusletter 8. November 2004
Internetadresse:	http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=3466