MODERNE TECHNOLOGIEN IM ZIVILVERFAHREN

HELMUT RÜßMANN

Universität des Saarlandes, Saarbrücken

Es mag Menschen geben, die von einem komplett digitalisierten Gerichtsverfahren träumen, in dem es kein Papier mehr gibt. In einem solchen Verfahren würde schon das verfahrenseinleitende Dokument in elektronischer Form eingereicht und so vorbereitet werden, dass die Gerichtsverwaltung die Stammdaten des Verfahrens unmittelbar in das eigene EDV-System übernehmen könnte und die eigene Erfassung der Daten sparen würde. Auch das Gericht würde mit den Verfahrensbeteiligten lediglich elektronisch kommunizieren und selbst die Verhandlung könnte virtuell erfolgen ohne gleichzeitige Anwesenheit der Verfahrensbeteiligten in einem realen Gerichtssaal. Ich möchte in meinem Beitrag zwei Teilaspekte eines digitalisierten Gerichtsverfahrens ansprechen, die mit elektronischen Dokumenten und Dokumentationen zu tun haben.

Bei dem einen geht es um die elektronische Gerichtsakte und um elektronische gerichtliche Register. Hier stellt sich die Frage nach Sicherheit, Authentizität und Echtheit einer elektronischen Dokumentation. Bei dem anderen geht es um die Beweisführung mit elektronischen Dokumenten. Hier wird nach dem Beweisrecht elektronischer Dokumente gefragt.

A. Elektronische Akten und Register

In einer elektronischen Akte wird das gesamte Gerichtsverfahren von seiner Einleitung mit dem verfahrenseinleitenden Dokument bis zu seinem Abschluss mit der gerichtlichen Entscheidung in elektronischer Form dokumentiert. Die elektronische Akte wird entweder parallel zu einer Papierakte geführt und erleichtert so den Umgang mit den für das Verfahren relevanten Informationen, ohne die Papierakte zu ersetzen. In diesem Fall bleibt die maßgebliche Akte die Papierakte. Fragen der Sicherheit und Echtheit können leicht mit einem Vergleich der beiden Akten beantwortet

werden. Neue Probleme stellen sich nicht. Das ändert sich, wenn die elektronische Akte die Papierakte ersetzt. Jetzt stellen sich die Fragen der Sicherheit und Echtheit der elektronischen Dokumentation. Es muss nach Antworten gesucht werden, wie in der neuen Welt der elektronischen Akte die Sicherheitsstandards der alten Welt der Papierakte realisiert werden können.

Bei den elektronischen Registern geht es um das Grundbuch, das Handelsregister, das Vereinsregister und andere Register. Die Informationen in diesen Registern sind in unterschiedlichem Ausmaß mit öffentlichem Glauben verbunden. Einmal wird das positive Vertrauen in die Richtigkeit der Dokumentation geschützt (Grundbuch, guter Glaube), zum anderen wird das negative Vertrauen in die Abwesenheit einer nicht dokumentierten, aber eintragungspflichtigen Tatsache geschützt (Handelsregister, negative Publizität). Beide Male wird die Frage nach der Sicherheit und Echtheit der elektronischen Dokumentation zu einem zentralen Problem. Dabei ist die Sicherheitsfrage nicht nur eine Frage des Schutzes vor Verfälschungen, sondern auch eine Frage der Nachhaltigkeit und Beständigkeit der elektronischen Register, die in Jahrzehnten oder gar Jahrhunderten noch ihre Dokumentationsfunktion erfüllen müssen.

B. Thesen zur Sicherheit und Echtheit

Elektronische Akten und elektronische Register müssen (mindestens) dieselben Sicherheitsstandards gegen Verfälschungen bieten wie Papierakten und Papierregister. Die Echtheit der Dokumente in der Papierwelt wird durch Unterschriftserfordernisse gewährleistet. Unterschriftserfordernisse gelten für die Schriftsätze der Parteien ebenso wie für die gerichtlichen Entscheidungen (Verfügungen, Beschlüsse, Urteile). Auch Dritte stehen mit ihrer Unterschrift für die Echtheit von Dokumenten (Zustellungsurkunden, Dokumentation von Zahlungseingängen) ein. Die Integrität und Korrektheit der Gerichtsakten wird durch Paginierungserfordernisse, Aufbewahrungsvorschriften und Zugangsregelungen geschützt. Änderungen durch nicht Zugangsbefugte oder ungetreue Zugangsbefugte werden in der Praxis nicht als ernsthaftes Risiko angesehen. Sollten Sie dennoch einmal vorkommen, so vertraut man auf die kriminaltechnischen Entdek-

kungsmöglichkeiten der Änderungen, die bei einer Papierdokumentation Spuren hinterlassen.

B.I. Sicherheit und Authentizität einer elektronischen Dokumentation

Von elektronischen Dokumentationen behauptet man, dass sie geändert werden könnten, ohne Spuren zu hinterlassen.[1] Wenn dem so ist, bedarf es in der elektronischen Welt besonderer Vorkehrungen, um Änderungen und Verfälschungen elektronischer Dokumentationen in elektronischen Akten und elektronischen Registern auszuschließen oder doch derart zu erschweren, dass ein dem Sicherheitsniveau der Papierwelt vergleichbares Sicherheitsniveau erreicht wird. Das bedeutet im Einzelnen:

- Der Server, der die elektronische Dokumentation vorhält, muss in einem Rechenzentrum stehen, das höchsten Sicherungsanforderungen genügt.
- Der Zugang zu den Informationen muss durch ein ausdifferenziertes Rechtesystem der Lese- und Schreibrechte geregelt sein, das nur Berechtigten Zugangs- und gegebenenfalls Ergänzungs- und Änderungsrechte gewährt (und das lediglich im Rahmen der jeweiligen Berechtigung).
- Alle Zugriffe müssen protokolliert werden.
- Einträge sind mit einem Zeitstempel zu versehen.
- Wo in der Papierwelt Unterschriften gefordert sind, bedarf es in der elektronischen Welt einer qualifizierten elektronischen Signatur.
- Wo in der Papierwelt Paraphen (Handzeichen) ausreichen, bedarf es in der elektronischen Welt einer fortgeschrittenen elektronischen Signatur.
- Für auch nach Abschluss eines Verfahrens aufzubewahrende Dokumente und für Register bedarf es einer dem Stand der Technik entsprechenden sicheren Archivierung.

---

[1] Siehe 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, Band 8 der Veröffentlichungen der Wissenschaftlichen Vereinigung für Internationales Verfahrensrecht, 1997, S. 137 (151 f.).

B.II. Die elektronische oder digitale Signatur

In den Anforderungen ist von fortgeschrittenen und qualifizierten elektronischen Signaturen die Rede. Das sind Signaturen, die auf eine asymmetrische Verschlüsselung setzen. Das Verfahren der asymmetrischen Verschlüsselung 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".

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

B.II.1. Sicherung der Vertraulichkeit

Wenn nun ein Rechtsanwalt dem Gericht eine Mitteilung zukommen lassen will, sucht er auf dem Server den öffentlichen Schlüssel des Gerichts. Mit diesem verschlüsselt er seine geheime Nachricht (die Klage) und sendet sie ab. Aufgrund der mathematischen Beschaffenheit der Schlüssel kann diese Information jetzt nur noch mit dem privaten Schlüssel des Gerichts gelesen werden. Selbst die nochmalige Anwendung des öffentlichen Schlüssels bringt die vertrauliche Nachricht nicht wieder zum Vorschein. Sofern man nun davon ausgeht, dass das Gericht sehr gut auf seinen Schlüssel aufgepasst hat, wird man weiter davon ausgehen können, dass nur noch das Gericht in der Lage ist, die Nachricht zu entziffern. Wenn das Gericht dem Rechtsanwalt antworten möchte, sucht es dessen Schlüssel auf dem öffentlichen Server und sendet seine Nachricht ebenso wie der Rechtsanwalt dies eben mit dem Gerichtsschlüssel getan hat.

B.II.2. Sicherung der Authentizität (Echtheit)

Woher aber weiß nun das Gericht, dass die Nachricht wirklich von dem Rechtsanwalt kam? Der öffentliche Schlüssel des Gerichts ist ja jedem

zugänglich und daher kann auch jedermann diese Nachricht geschickt haben. Die Lösung liegt im privaten Schlüssel des Rechtsanwalts: Er signiert die Nachricht. Wie geht das vonstatten? Ganz einfach: Er schreibt seine geheime Nachricht. Dann verschlüsselt er sie mit dem öffentlichen Schlüssel des Gerichts. 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.

Der Rechtsanwalt signiert also die verschlüsselte Botschaft mit seinem privaten Schlüssel. Das Gericht bekommt die so signierte und verschlüsselte Botschaft und überprüft, ob die Nachricht von dem Rechtsanwalt stammt. Dazu wendet sie seinen öffentlichen Schlüssel auf die Botschaft an. Da der private Schlüssel des Rechtsanwalts sich nur von seinem öffentlichen Schlüssel wieder entschlüsseln lassen kann, weiß das Gericht sicher, dass die Nachricht von dem Rechtsanwalt ist, sofern ihm die Entschlüsselung mit dessen öffentlichen Schlüssel gelingt. Nun hat das Gericht lediglich noch den Klartext der Botschaft mit dem eigenen privaten Schlüssel herzustellen.

B.II.3. Digitale Signatur

Geht es dem Rechtsanwalt 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 so genanntes 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). Der Rechtsanwalt 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 das Gericht von dem Rechtsanwalt eine mit einer digitalen Signatur versehene Nachricht, so wendet es hierauf den öffentlichen Schlüssel des Rechtsanwalts an. Dabei geschieht dann zweierlei: Zum einen wird die digitale Signatur (= die verschlüsselte Prüfsumme) entschlüsselt und das Gericht erhält die von dem Rechtsanwalt erzeugte Prüfsumme im Klartext. Zum anderen wird aus dem unverschlüsselten Text der Nachricht erneut ein Hash-Komprimat gebildet. Stimmen das durch das Gericht neu gebildete Komprimat und die in der digitalen Signatur befindliche Prüfsumme überein, so kann das Gericht sicher sein, dass der Inhalt der von dem Rechtsanwalt 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.

B.II.4. Zuordnung der Schlüssel zu Personen

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. 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.

Also muss sichergestellt werden, dass die ausgelegten Schlüssel tatsächlich den richtigen Personen gehören. Wie macht man das? Es gibt mehrere (unterschiedlich wirksame) Möglichkeiten.

B.II.4.1. Web of Trust

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 Alice sich mal treffen und per Zufall ihre Schlüssel „dabei" haben, kann Alice mit ihrem Privatschlüssel den öffentlichen Schlüssel von Bob signieren. Dies drückt für Peter, der später mit Bob Geschäfte machen will, aus, dass Alice 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 Alice signiert, dann wird Peter (hoffentlich) diesen wählen. Dies wird er um so lieber tun, wenn er Alice persönlich kennt und ihr vertraut. Natürlich kann Alice 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 Alice verlassen, wie dies im obigen Beispiel Peter tat.

B.II.4.2. Trustcenter

Im heutigen Rechtsverkehr wird es unwahrscheinlich sein, dass sich Unternehmen oder Behörden darauf verlassen, dass eine ihnen Unbekannte namens Alice den Schlüssel von Bob signiert hat, wenn sie Bob eine wichtige Nachricht zustellen will und sichergehen will, dass diese Nachricht auch den Richtigen erreicht. Den Beteiligten 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.

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 so genannten „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 „Trustcenter". Damit ein „Trustcenter" „Trustcenter" sein kann, muss es bestimmte Anforderungen erfüllen; diese sind in Deutschland im Signaturgesetz geregelt.

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.

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.

Diese qualifizierten Signaturen, die auf einem qualifiziertem Zertifikat beruhen, bieten die höchste Sicherheit. Qualifizierte Zertifikate können

nur so genannte 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 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 Zertifizierungdienstes 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.

C. Die elektronische Akte im gerichtlichen Verfahren

In Deutschland hat die Bund-Länder-Kommission (BLK) für die Datenverarbeitung und Rationalisierung in der Justiz eine Unterarbeitsgruppe E-Akte gebildet, die im Jahre 2008 den Auftrag bekommen hat, eine Bestandsaufnahme der vorhandenen Lösungen vorzunehmen, Verbesserungsansätze zu sammeln und die Anforderungen an eine justizspezifische Lösung zur Substituierung der Papierakte aus richterlicher Sicht zu definieren. Der endgültige Bericht der Arbeitsgruppe liegt heute (23. März 2011) noch nicht vor. Er wird wahrscheinlich noch im Jahre 2011 im In-

ternet veröffentlicht werden.[2] Auf dem Deutschen EDV-Gerichtstag wurde im September 2009 ein Zwischenbericht vorgestellt.[3] Er enthielt zur Situation in Deutschland folgende Aussagen zur Rechtslage verbunden mit Anforderungen für die elektronische Gerichtsakte.[4]

C.I. Rechtliche Rahmenbedingungen

C.I.1. Keine umfassenden Regelungen

Umfassende Regelungen für eine elektronische Gerichtsakte für das gerichtliche Verfahren gibt es nicht. Schon für die Papierakte selbst gilt, dass sie in den Prozessordnungen mehr vorausgesetzt denn geregelt wird. Der Informationsträger Papier ist für die Prozessordnung derart selbstverständlich, dass es keine ausdrücklichen Regelungen gibt, dass eine Gerichtsakte zu führen ist, welches Medium für die Führung der Akte vorzusehen ist und wie im einzelnen Aufbau und Gestalt der Gerichtsakte sind. Dass es Gerichtsakten gibt, ist im Prozessrecht in zahlreichen Einzelregelungen mehr oder minder eindeutig vorausgesetzt. Am deutlichsten ergibt sich dies aus den Regelungen zu Akteneinsicht (z.B. § 299 ZPO; § 46 Abs. 2 ArbGG i.V.m. § 299 ZPO; § 147 StPO; § 474 f. OWiG; § 100 VwGO; § 78 FGG; § 120 SGG), nach denen die Beteiligten die Gerichtsakte und die dem Gericht vorgelegten Akten einsehen können. Zum Rechtsproblem jenseits des Datenschutzrechts wird eine elektronische Gerichtsakte erst dann, wenn sie die Papierakte nicht nur ergänzen, sondern ersetzen soll („führende“ elektronische Gerichtsakte).

C.I.2. Prozessordnungen

Ermächtigung zur Führung: Die Möglichkeit einer elektronischen Gerichtsakte ist – mit Ausnahme der Strafprozessordnung, die eine entsprechende Ermächtigung noch nicht enthält - in den Prozessordnungen mit Unterschieden im Detail im Kern übereinstimmend vorgesehen (s.

---

2 http://www.justiz.de/BLK/schlussberichte/index.php

3 https://www.edvgt.de/pages/startseite/18.-deutscher-edv-gerichtstag/arbeitskreise--mit-praesentationen-und-protokollen/blk-ii-elektronische-akte.php

4 Der Autor dieses Teils der Studie ist der Richter am Bundesverwaltungsgericht Professor Dr. Dietmar Berlitz.

etwa § 298a ZPO; § 110b OWiG; § 46e ArbGG; § 55b Abs. 1 Satz 1 VwGO; § 52b FGO; § 65b SGG). Danach können die Prozessakten (dieser Begriff wird ersichtlich synonym mit dem der Gerichtsakte verwendet) elektronisch geführt werden. Voraussetzung hierfür ist der Erlass einer entsprechenden Rechtsverordnung, die nicht nur den Zeitpunkt festgelegt, von dem an die Prozessakten elektronisch geführt werden, sondern in der auch die organisatorisch-technischen Rahmenbedingungen für die Bildung, Führung und Verwahrung der elektronischen Akten festzulegen sind. Für die obersten Bundesgerichte ist eine solche Rechtsverordnung bislang nicht ergangen. Auch aus dem Bereich der Ländergerichte ist eine entsprechende Rechtsverordnung nicht bekannt. Eine Zulassungsrechtsverordnung, die eine Nutzung elektronischer Akten im gerichtlichen Verfahren erlaubt, ist für das Verfahren vor dem Bundespatentgericht in Vorbereitung; Einzelheiten hierzu sind nicht bekannt. Für den Erlass der Rechtsverordnung ist davon auszugehen, dass zwischen den technischen und/oder organisatorischen Möglichkeiten, mit einem DMS/VBS-System[5] als Ergänzung der Fachanwendung GO§A eine elektronische Gerichtsakte abzubilden, und den in einer Rechtsverordnung aufzunehmenden Regelungen, welche die Einzelheiten über Bildung, Führung und Verwahrung der elektronischen Akte festlegen, eine enge Beziehung besteht und die Ausgestaltung der Rechtsverordnung wesentlich auch von den technischen Möglichkeiten geprägt wird: Es macht keinen Sinn, durch Rechtsverordnung eine elektronische Gerichtsakte einzuführen, die technisch nicht umgesetzt werden kann. Die Rechtsverordnung hat so im Kern die Funktion, Rechtssicherheit und Rechtsklarheit zu schaffen und eine grundlegende Festlegung in solchen Bereichen zu schaffen, in denen alternative Gestaltungen möglich sind.

Aktenfunktionen: Aus dem Prozessrecht selbst ergeben sich keine klaren, bindenden Vorgaben für die Ausgestaltung der elektronischen Gerichtsakte. Das Prinzip der Aktenmäßigkeit des gerichtlichen Verfahrens ist aber diesem Verfahren immanent. Es folgt aus der Funktion von Rechtsprechung, in einem geordneten Verfahren zu einer Streitentscheidung zu gelangen, und hat so auch eine Verankerung in Art. 19 Abs. 4 GG. Das Gebot der Aktenmäßigkeit des Handelns von Trägern öffentlicher Gewalt

[5] DMS Dokumenten-Management-System; VBS Vorgangs-Bearbeitungs-System.

wird weiterhin aus dem allgemeinen Rechtsstaatsgebot abgeleitet. Die genaue dogmatische Herleitung des Prinzips der Aktenmäßigkeit ist indes nachrangig, weil die hieraus folgenden Vorgaben für die Ausgestaltung einer elektronischen Akte vage und konkretisierungbedürftig sind. Festzuhalten sind (mindestens) drei wechselseitig aufeinander bezogene Grundfunktionen, die eine elektronische Gerichtsakte erfüllen muss.

C.I.2.1. Dokumentationsfunktion

Die elektronische Gerichtsakte muss nach Inhalt und Aufbau eine sichere, vollständige und integre Dokumentation ermöglichen, dass

- die nach dem anzuwendenden Prozessrecht zu beachtenden Vorgaben tatsächlich auch eingehalten worden sind,
- einzelne, für das gerichtliche Verfahren und seine Förderung wesentliche Teilschritte (z.B. Schriftsatzübersendungen, Ladungen, Zustellungen) verfahrensrechtskonform durchlaufen worden sind (bzw. Fehler festhalten) und
- auch sonstige Verfahrensgrundsätze einschließlich der Beachtung des Grundsatzes der Gewährung rechtlichen Gehörs gewahrt worden sind.

Das DMS/VBS muss sicherstellen können, dass der Stand des Verfahrens und sein Fortgang anhand der elektronischen Gerichtsakte nachvollzogen werden können, dass die elektronische Gerichtsakte als zentrale „Aufbewahrungseinheit“ alle auf das jeweilige Verfahren bezogenen Dokumente enthält, bündelt und so zugänglich macht, dass das gerichtliche Verfahren nachvollziehbar dokumentiert wird. Die elektronische Gerichtsakte muss hierfür vollständig, authentisch, wahrheitsgetreu und - innerhalb vernünftiger Grenzen – auch manipulationssicher („integer“) sein, und zwar - bis zum rechtskräftigen Abschluss des gerichtlichen Verfahrens - auch im Zeitverlauf. Eine elektronische Gerichtsakte darf insoweit nicht hinter der Papierakte zurückbleiben und muss die spezifischen Risiken, die sich aus einer elektronischen Bearbeitung ergeben können (z.B. elektronische Manipulationen des Akteninhalts), bewältigen; sie muss aber keine „absolute“ Sicherheit gewähren, die auch die Papierakte nicht gewährleistet.

C.I.2.2. Informationsfunktion

Die Gerichtsakte muss den mit der „Sachbearbeitung“ (spruchrichterliche Tätigkeit; „Nebenverfahren“ wie z.B. der Kostenfestsetzung) betrauten Personen eine vollständige, zuverlässige und beweissichere Grundlage für die jeweils zu treffende Entscheidung zur Verfügung stellen. Für diese Informationsfunktion ist es regelmäßig unerheblich, ob eine Sachinformation im Original oder als Kopie bereitgestellt wird, soweit es nicht gerade auf die Authentizität/die Beweiskraft eines bestimmten Dokumentes ankommt. Im Rahmen der Informationsfunktion, die auf der Dokumentationsfunktion aufbaut, kommt es regelmäßig nicht darauf an, den umfassenden Zugriff auf alle Teile der Gerichtsakte nehmen zu können. Für die jeweilige Sachbearbeitung in den jeweiligen Teilschritt ist in aller Regel nur ein kleiner Ausschnitt aus der Gesamtakte erforderlich. Die Informationsfunktion ist aus der richterlichen Sicht die zentrale Funktion. Durch das VBS/DMS muss sichergestellt sein, dass die elektronische Gerichtsakte alle für die Sachbearbeitung notwendigen Informationen zuverlässig bereitstellt und ermöglicht, sich punktuell von der prozessrechtskonformen Durchführung einzelner Bearbeitungsschritte zu überzeugen (z.B. Gewährung rechtlichen Gehörs durch Übersendung von Schriftsätzen, ordnungsgemäße Ladung zur mündlichen Verhandlung, Fristwahrung bei Rechtsmitteln durch Nachweis der Zustellung). Vollständigkeit, Authentizität und Integrität der elektronischen Gerichtsakte sind auch hier von zentraler Bedeutung. Sie bilden aber lediglich die Verlässlichkeitsgrundlage für die eigentliche Bearbeitung. Im Vordergrund stehen der schnelle, leichte, direkte, strukturierte und strukturierbare Zugang zu den jeweils für die Sachbearbeitung erforderlichen Informationen.

- Die Arbeit mit der elektronischen Akte muss durch Such-, Filter-, Sortier- und Strukturierungsmöglichkeiten ergonomisch unterstützt werden.
- Es muss Übersichtsfunktionen geben, die ein elektronisches „Blättern“ in der Akte ermöglichen.
- Unter ergonomischen Gesichtspunkten sind hier auch relevant Zugriffszeiten auf einzelne Dokumente und/oder die Akte insgesamt, die Möglichkeit, individuelle Bearbeitungsnotizen/-

vermerke anzubringen, die nur für den jeweiligen Bearbeiter sichtbar sind oder jedenfalls nicht dauerhaft mit der elektronischen Akte verbunden werden (elektronische „Gelbzettel“).

C.I.2.3. Kontrollfunktion

Die elektronische Akte ist Grundlage für eine externe „Kontrolle“ des gerichtlichen Verfahrens. Diese kann erfolgen im Instanzenzug, durch das Bundesverfassungsgericht im Rahmen der Verfassungsbeschwerde oder durch den EGMR (im Rahmen z.B. einer Rüge überlanger Verfahrensdauer), durch Beteiligte (im Rahmen der Akteneinsicht) und -mit hier nicht weiter zu vertiefenden Einschränkungen - im Rahmen der parlamentarischen Kontrolle. Die Kontrollfunktion baut auf der Dokumentationsfunktion auf. Für sie muss gewährleistet sein, dass die elektronische Gerichtsakte nicht nur vollständig, integer, authentisch und wahrheitsgetreu ist. Es müssen alle für eine Kontrolle erforderlichen Zusatzinformationen über den Gang der Bearbeitung nachprüfbar, zugänglich, zuverlässig, vollständig und manipulationssicher vorgehalten werden.

C.I.3. Speicherort der elektronischen Gerichtsakte

Für die elektronische Gerichtsakte ist die Unabhängigkeit der Justiz als gesonderter Staatsgewalt zu berücksichtigen. Dies gilt in besonderem Maße für die allgemeine und besondere Verwaltungsgerichtsbarkeit, deren Aufgabe die Kontrolle der (allgemeinen) öffentlichen Gewalt ist.

Bestand, Sicherheit und Integrität sind durch die Justiz selbst zu gewährleisten. Die elektronische Gerichtsakte muss so gespeichert werden, dass bereits die Möglichkeit der Manipulation des Aktenbestandes durch justizfremde Personen technisch-physikalisch im Rahmen praktischer Vernunft ausgeschlossen ist. Schutz ist hier nicht allein gegen unbefugte Zugriffe nichtstaatlicher Dritter, sondern auch gegen „interne Angriffe“ durch solche Personen/Institutionen zu gewährleisten, die der Dienst- oder Fachaufsicht nichtjustizieller Personen/Institutionen unterstehen. Die Dokumentationsfunktion der elektronischen Gerichtsakte erfordert ein hinreichend ausdifferenziertes, zuverlässig funktionierendes Datensicherungskonzept.

C.I.4. Verfügbarkeit und Beständigkeit der elektronischen Gerichtsakte

Die elektronische Gerichtsakte als zentrale Voraussetzung der Transparenz und Nachvollziehbarkeit des gerichtlichen Verfahrens und als Grundlage der prozessrechtskonformen Rechtsschutzgewähr muss bei ausschließlich elektronischer Bearbeitung gewährleisten, dass die Verfahren kontinuierlich und ohne erhebliche technische Hindernisse/ Ausfälle bearbeitet werden können. Dies erfordert für das Vorhalten der Akten ein hohes, näher zu definierendes Maß an Verfügbarkeit (Schutz gegen Systemausfälle); dabei ist die mit der richterlichen Unabhängigkeit verbundene Bestimmungsmacht über den Zeitpunkt der Aktenbearbeitung zu beachten. Jedenfalls aus Akzeptanzgründen erforderlich ist, dass technisch und organisatorisch eine sichere, datenschutzkonforme Bearbeitung der elektronischen Gerichtsakte auch an einem häuslichen richterlichen Arbeitsplatz ermöglicht wird und die Gerichtsakte auch in dem Sinne „mobil" ist, dass sie z.B. bei Ortsterminen und/oder auswärtigen Sitzungen mitgeführt werden kann. Verfügbarkeit in der Zeit bedeutet auch Beständigkeit. Es muss sichergestellt sein, dass zumindest für die „Lebensdauer" einer Akte (Zeitraum bis zur Langzeitarchivierung) der Nutzungszugriff (Lesen, Bearbeiten, Zugang zu Protokollierungsdaten etc.) auch langfristig gewährleistet ist (Sicherung der langfristigen Verfügbarkeit, Vollständigkeit, Integrität, Vertraulichkeit, Unverfälschbarkeit und Verkehrsfähigkeit der elektronischen Dokumente im DMS/VBS). Jedenfalls muss die Anwendung sicherstellen, dass die in einer elektronischen Gerichtsakte bearbeiteten Dokumente (einschließlich der zu den Dokumenten gespeicherten Metainformationen) und die für die Transparenz und Nachvollziehbarkeit des gerichtlichen Verfahrens erforderlichen Zusatzinformationen über den Bearbeitungsgang ohne Informations- und/oder Beweisverlust in Nachfolgesystemen bereitgestellt werden können.

C.I.5. Elektronische Gerichtsakte und Signaturen

Die Prozessordnungen enthalten kein umfassendes, selbständiges Regelungskonzept für den Einsatz elektronischer Signaturen. Für den „gerichtinternen Verkehr" bzw. für elektronische gerichtliche Dokumente

genügt in den Fällen, in denen eine handschriftliche Unterzeichnung durch den Richter oder den Urkundsbeamten der Geschäftsstelle vorgeschrieben ist, dieser Form die Aufzeichnung als elektronisches Dokument, wenn die verantwortenden Personen am Ende des Dokuments ihren Namen hinzufügen und das Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 des Signaturgesetzes versehen wird (s. z.B. nach § 130b ZPO; § 110c OWiG; § 46d ArbGG; § 55a Abs. 3 VwGO; § 52a FG=; § 65a Abs. 3 SGG).

C.I.5.1. Qualifizierte Signatur

Eine gesonderte, abschließende Auflistung der Dokumente, die in diesem Sinne der handschriftlichen Unterschrift bedürfen, enthalten die Prozessordnungen nicht. Eine handschriftliche Unterschrift ist im Gesetz ausdrücklich vorgesehen z.B. bei

- Urteilen
- Gerichtsbescheiden sowie
- Protokollen.

Auch ohne ausdrückliche gesetzliche Regelung ist eine Unterschrift (und damit eine qualifizierte Signatur) erforderlich z.B. bei Urteilsformeln, Beschlüssen, Rechtshilfeersuchen und – nach der Rechtsprechung – bei prozessleitenden Verfügungen mit besonderer Tragweite (z.B. eine Fristsetzung nach § 87b VwGO [BVerwG NJW 1994, 746], einer Anhörung zur Entscheidung nach § 130a VwGO [Buchholz 310 § 130a VwGO Nr 11]). Qualifizierte Signaturen sind auch bei gesonderten Vermerken erforderlich, die mit einem anderen Dokument zu verbinden sind (z.B. bei der Urteilsberichtigung, der Tatbestandsberichtigung oder dem Verkündungsvermerk); eine elektronische „Paraphe“ reicht hier nicht aus. Für ein VBS/DMS ergibt sich als Konsequenz:

- Soweit die elektronische Signatur nicht über die Fachanwendung abgedeckt wird, muss das VBS/DMS-System es ermöglichen, jedes beliebige Dokument auch qualifiziert zu signieren.
- Erforderlich ist auch die Möglichkeit einer dokumentbezogenen Signatur; Containersignaturen dürfen nicht ausgeschlossen sein.

- Insbesondere für Urteile und Beschlüsse muss die Möglichkeit der Mehrfachsignatur bestehen.
- Das System sollte über die Möglichkeit verfügen, dass im Rahmen der Anwenderadministration (also ohne Einschaltung des Anbieters) die Dokumente/Dokumenttypen, die handschriftlich unterschrieben/qualifiziert signiert werden müssen, bezeichnet werden und mit einer entsprechenden System“kontroll“anfrage bzw. einen „Erinnerungshinweis“ verbunden werden.

C.I.5.2. Textform; sonstige Authentifizierung

Im gerichtsinternen Verkehr ist bei nicht ausdrücklich der Unterschrift bedürftigen Verfügungen, Kenntnisnahmen etc. eine qualifizierte elektronische Signatur nicht erforderlich, wenn und soweit die für eine bestimmte Verfügung, Maßnahme oder Handlung „verantwortliche Person“ anderweitig im System hinreichend sicher identifiziert und der Bearbeitungsvorgang entsprechend protokolliert wird. Dies erfasst all die Fälle, in denen bei papiergebundener Bearbeitung heute eine Paraphe erfolgt. In diesem Fällen ist es eine Frage der Praktikabilität (und künftiger gerichtsinterner Festlegungen), ob eine qualifizierte elektronische Signatur eingesetzt werden oder eine geringere Form der Identifizierung ausreichen soll.

In solchen Fällen bedarf es regelmäßig dann auch keiner gesonderten (fortgeschrittenen) Signatur, wenn und soweit die eindeutige personale Zuordnung einer elektronischen Aktion hinreichend durch den Systemanmeldevorgang gewährleistet ist. Erforderlich, aber auch ausreichend ist dann, dass das System diese Information leicht reproduzierbar protokolliert. Konzeptionelle Leitlinie ist, eine gesonderte (qualifizierte oder fortgeschrittene) Signatur nur dort einzusetzen, wo dies aus Rechtsgründen geboten ist, und Paraphierungen durch Protokollierungen zu ersetzen.

C.I.5.3. Eingehende elektronische Dokumente

Für verfahrensbezogene Dokumente, die einem Gericht nach Maßgabe der jeweils erforderlichen Zulassungsrechtsverordnung übermittelt wer-

den dürfen, ist für Dokumente, die einem schriftlich zu unterzeichnenden Schriftstück gleichstehen, regelmäßig eine qualifizierte Signatur vorzuschreiben (§ 130a ZPO; § 46c ArbGG; § 41a StPO; § 110a OWiG; § 55a VwGO; § 65a SGG; § 52a FGO). Für gerichtliche Verfahren ist bislang noch nicht von der prozessrechtlich teils eröffneten Alternativmöglichkeit Gebrauch gemacht worden, neben der qualifizierten elektronischen Signatur auch ein anderes sicheres Verfahren zuzulassen, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Als Anforderungen an ein DMS/VBS folgt hieraus:

- Für elektronische eingehende Dokumente muss die Möglichkeit bestehen, eine Signaturprüfung durchzuführen oder doch das Ergebnis einer außerhalb des Systems durchgeführten Signaturprüfung automatisch mit dem eingehenden Dokument überprüfbar verbunden zu speichern.
- Es muss die durch den Anwenderadministrator leicht zu konfigurierende Möglichkeit bestehen, dies über die Verknüpfung zweier Dokumente (eingehendes Dokument und Dokument zur Signaturprüfung) zu organisieren oder das Ergebnis der Dokumentprüfung als Metadatum zu speichern.
- Weiterhin sollte die Möglichkeit bestehen, eine durch den Anwenderadministrator leicht zu konfigurierende Liste solcher Dokumente/Dokumenttypen im System zu hinterlegen, bei denen aus Rechtsgründen eine Signaturprüfung erforderlich ist. Für die Zwecke des Fachkonzeptes ist eine abschließende Auflistung aller elektronischer Dokumente, die einem schriftlich zu unterzeichneten Schriftstück gleichstehen, nicht erforderlich.

C.I.6. Medientransfer

Bei Einführung einer elektronischen Akte ist für einen längeren Übergangszeitraum damit zu rechnen, dass in erheblichem Umfange Dokumente mit Verfahrensbezug an das Gericht übermittelt werden, die nicht der Form entsprechen, in der die Akte geführt wird. § 55b Abs. 2 VwGO sieht für diesen Fall vor, dass - vorbehaltlich einer anderweitigen Bestimmung in der Zulassungsrechtsverordnung - Dokumente, die nicht der Form entsprechen, in der die Akte geführt wird, in die entsprechende

Form zu übertragen und in dieser Form zur Akte zunehmen sind (Medientransfer).

Einzelheiten zu diesem Medientransfer bestimmen § 298a Abs. 2, 3 ZPO, § 46e Abs. 2, 3 ArbGG; § 110b Abs. 2 OWiG, § 55b Abs. 4 VwGO, § 52a FGO und § 65b Abs. 2, 3 SGG im sachlichen Kern ähnlich, wenn auch im mit im Detail beachtlichen Abweichungen dahin, dass, wenn ein in Papierform eingereichtes Dokument in ein elektronisches Dokument übertragen worden ist, dieses den Vermerk enthalten muss, wann und durch wen die Übertragung vorgenommen worden ist. Soweit auch der umgekehrte Fall (Überführung eines elektronischen Dokuments in die Papierform) geregelt ist, ist für den Ausdruck ein Vermerk vorgesehen, welches Ergebnis die Integritätsprüfung des Dokuments ausweist, wen die Signaturprüfung als Inhaber der Signatur ausweist und welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist. Zur Frage der Gestaltung des Transfervermerks bei der Überführung eines in Papierform eingereichten Dokuments in ein elektronisches Dokument ist umstritten, ob es eines gesonderten, auf dem Dokument anzubringenden oder mit diesem zu verbindenden Dokuments bedarf oder es hinreicht, dass der Transfervermerk (bzw. die von Gesetzes wegen in diesen aufzunehmenden Informationen) in die Metadaten des transferierten Dokuments aufgenommen werden oder sonst in einer Art und Weise protokolliert werden, dass eine hinreichende, dauerhafte und integre Verbindung zwischen Transfervermerk und Dokument gewährleistet ist. Vorzugswürdig ist die Ansicht, dass eine Aufnahme in den Transfervermerk ausreicht. Eine Klarstellung in den Rechtsverordnungen zur Zulassung der elektronischen Gerichtsakte ist anzustreben. Denkbar ist auch, bereits bei dem Scannvorgang auf dem Dokument selbst – nach Art eines Eingangsstempels – (automatisch oder händisch) sichtbar einen „Scan-Transfervermerk“ anzubringen. Das Gesetz fordert für den Transfervermerk keine Unterschrift/kein Handzeichen und gibt – jenseits der Wahrnehmbarkeits- und Lesbarkeitsschwelle – auch nicht eine bestimmte Mindestgröße vor.

C.II. Datenschutzrecht

C.II.1. Allgemeines

Eine weitere Randbedingung der elektronischen Gerichtsakte bildet das (materielle) Datenschutzrecht. Zwar ist der Rechtsprechungsbereich in den Ländern vom Anwendungsbereich des Bundesdatenschutzgesetzes ausgenommen (§ 1 Abs. 2 Nr. 2 lit. b BDSG). Die Bundesgerichte sind als Organe der Rechtspflege indes öffentliche Stellen des Bundes (§ 2 Abs. 1 BDSG) und dem Datenschutzrecht unterworfen. Nach der allgemeinen Subsidiaritätsklausel (§ 1 Abs. 3 Satz 1 BDSG) gehen aber den Vorschriften des Bundesdatenschutzgesetzes andere Rechtsvorschriften des Bundes vor, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind. Zu solchen vorrangigen Regelungen gehören auch prozessrechtliche Vorschriften, welche die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Rahmen eines gerichtlichen Verfahrens (implizit) voraussetzen oder (ausdrücklich) regeln. Sie bestimmen auch die „Aktenwürdigkeit" eines Dokuments (und damit der aktengebundenen Verarbeitung der in einem Dokument enthaltenen personenbezogenen Daten). Bei der Führung einer elektronischen Gerichtsakte ist sicherzustellen, dass den Anforderungen des Datenschutzrechts entsprochen wird. Es sind die spezifischen Risiken, die sich durch die erweiterte Verfügbarkeit und die erleichterten Zugriffsrechte auf eine elektronische Akte ergeben (können), zu bewältigen.

C.II.2. Technische und organisatorische Schutzvorkehrungen

Für die elektronische Gerichtsakte gelten in vollem Umfange die Anforderungen über technische und organisatorische Maßnahmen, die erforderlich sind, um die Ausführung des Bundesdatenschutzgesetzes und insbesondere die in der Anlage zu § 9 BDSG genannten Anforderungen zu gewährleisten (§ 9 BDSG). Dies erfordert Zutrittskontrollen, Zugangskontrollen, Zugriffskontrollen, Weitergabekontrollen, Eingabekontrollen, Aufgabekontrollen und Verfügbarkeitskontrollen. Diese Anforderungen gehen angesichts des in der Justiz bereits erreichten Standes der elektronischen Verarbeitung (auch) personbezogener Daten

über den status quo bereits getroffener Maßnahmen wohl nicht qualitativ hinaus. Denn schon heute sind die Stammdaten elektronisch erfasst und können von einer Vielzahl im Gericht tätigen Personen abgerufen werden. Ob/welche neuen Datenschutz- und/oder Datensicherungsvorkehrungen zu treffen sind, hängt u.a. davon ab, welche gerichtlichen Verfahren künftig mit einer „führenden" elektronischen Gerichtsakte bearbeitet werden sollen. Für die elektronische Gerichtsakte ist davon auszugehen, dass die Bearbeitung von Verfahren mit (sehr) hohem Schutzbedarf, in denen z.B. klassifizierte Dokumente verarbeitet werden (müssen), bis auf weiteres wegen des hiermit verbundenen Sicherungs- und Sicherheitsaufwandes zurückgestellt wird.

C.II.3. Löschung/Aufbewahrung

Datenschutzrechtlich ist neben der Erfassung und Verarbeitung personenbezogener Daten im Rahmen eines gerichtlichen Verfahrens auch die datenschutzkonforme Löschung solcher Daten in den Blick zu nehmen.

C.II.3.1. Bundesgerichte

Für die Bundesgerichte gilt das „Gesetz zur Aufbewahrung von Schriftgut der Gerichte des Bundes und des Generalbundesanwalts nach Beendigung des Verfahrens" –Schriftgutaufbewahrungsgesetz - (v. 22.3.2005, BGBl. I, 837). Hiernach darf Schriftgut der Gerichte des Bundes, das für das Verfahren nicht erforderlich ist, nach Beendigung des Verfahrens nur so lange aufbewahrt werden, wie schutzwürdige Interessen der Verfahrensbeteiligten oder sonstiger Personen oder öffentliche Interessen dies erfordern; Schriftgut im Sinne dieses Gesetzes sind dabei Akten Register, Namensverzeichnisse, Karteien, Urkunden, Akten und Blattsammlungen sowie einzelne Schriftstücke, Bücher, Drucksachen, Karten, Pläne, Zeichnungen, Lichtbilder, Filme, Schallplatten, Tonträger und sonstige Gegenstände, die Bestandteile oder Anlagen der Akten geworden sind; im Falle elektronisch geführter Akten sind die entsprechenden Dateien erfasst. Die Rechtsverordnung, die zur näheren Ausformung der allgemeinen Aufbewahrungsfristen zu erlassen ist (§ 2 Schriftgutaufbewahrungsgesetz), ist noch nicht ergangen. Fest steht

jedenfalls, dass die Aufbewahrungsfristen mit Ablauf des Jahres, in dem nach Beendigung des Verfahrens die Weglegung der Akten angeordnet wurde, beginnen.

Für die obersten Bundesgerichte ist zu berücksichtigen, dass in Rechtsmittelverfahren die anfallenden, zur Gerichtsakte zu nehmenden Dokumente nach Abschluss des Rechtsmittelverfahrens mit den Vorinstanzakten verbunden werden und mit der Gerichtsakte als der instanzübergreifenden Einheit an die Vorinstanz zurückgegeben werden. Aufbewahrungs- und Aussonderungs- und damit Löschungsprobleme ergeben sich mithin vor allem für die Verfahrensregister (Löschung von Datensätzen in den jeweiligen Fachanwendungen), die teils geführten Senatshefte, die nicht Teil der „offiziellen" Gerichtsakte sind, für die Verfahrensakten etwaiger erstinstanzlich zugewiesener Verfahren, vorbereitende Dokumente, die nicht Bestandteil oder Anlagen der Akten geworden sind (Materialsammlungen, Entwürfe etc.), einschließlich der bei der Entscheidungsfindung gefertigten „Handakten" (Arbeitskopien/ Doppel von Akten Bestandteile für die Sachbearbeitung) sowie der Anlagen zu den Gutachten, die durch die Richterschaft „verwaltet" werden.

C.II.3.2. Ländergerichte

Für die Ländergerichte gibt es – vorbehaltlich näherer Prüfung – keine dem Schriftgutaufbewahrungsgesetz vergleichbare Regelungen. Detaillierte, in einem VBS/DMS umzusetzende Vorgaben erhalten regelmäßig Akten- bzw. Aussonderungsordnungen.

C.III. Archivrecht

Die Bundesgerichte unterliegen dem „Gesetz über die Sicherung und Nutzung von Archivgut des Bundes" – Bundesarchivgesetz (BArchG). Nach § 2 Abs. 1 BArchG haben auch die obersten Bundesgerichte alle Unterlagen, die sie zur Erfüllung ihrer öffentlichen Aufgaben einschließlich der Wahrung der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder nicht mehr benötigen, dem Bundesarchiv oder dem zuständigen Landesarchiv zur Übernahme anzubieten und, wenn es sich um Unterlagen von bleibendem Wert im Sinne des § 3 handelt, als

Archivgut des Bundes zu übergeben. Für die Ländergerichte gelten der Sache nach vergleichbare Landesregelungen. Es muss daher sichergestellt sein, dass ein künftiges VBS/DMS elektronische Dokumente dem jeweils zuständigen Archiv in der gebotenen Form anbieten und/oder übergeben kann.

C.IV. Aktenordnung

Für die obersten Bundesgericht gibt es keine durch Dritte vorgegebene Anweisung für die Verwaltung des Schriftgutes, wie sie in den Ländern regelmäßig durch entsprechende Anweisungen in der Justizressorts vorzufinden ist (sog. Aktenordnung, z.B. „Anweisung für die Verwaltung des Schriftgutes bei den Geschäftsstellen der Gerichte, der Staatsanwaltschaften und der Amtsanwaltschaften“ – Aktenordnung – bzw. „Allgemeine Verfügung über die Geschäftsordnung für die Gerichte, Staatsanwaltschaften und der Amtsanwaltschaft“ Geschäftsordnungsvorschriften – GOV [AV des Justizsenators Berlin v. 28.8.1974]). Bei den Bundesgerichten sind die typischerweise in den Aktenordnungen der zuständigen Ressorts zusammengefassten Bestimmungen in Geschäftsstellenordnungen geregelt. Diese Geschäftsstellenordnungen regeln u.a. den Aufbau der Geschäftsstelle, die Arbeitsteilung zwischen den Beschäftigten(gruppen) in der Geschäftsstelle (soweit keine „echten“ Serviceeinheiten bestehen), die Register und Registerzeichen, die Aktenzeichen und die Registerführung, die Aufbewahrung der Akten und den Nachweis ihres Verbleibs, die Behandlung und Vorlage von Eingängen, die Durchsicht von Entscheidungen sowie das Weglegen von Akten. Im Rahmen der Vorgaben durch Gesetz und Recht sind die Bundesgerichte in der Gestaltung der Geschäftsstellenordnungen autark; in den Ländern können die Aktenordnungen mit überschaubarem Aufwand angepasst werden. Akten- bzw. Geschäftsstellenordnungen sind insoweit kein fest vorgegebener Rahmen für die Einführung einer elektronischen Akte, sondern im Rahmen der gesetzlichen Vorgaben Mittel ihrer Ausgestaltung und der Ort, in dem ergänzende organisatorische Regelungen zu treffen sind.

Soweit die Bund-Länder-Kommission zu den rechtlichen Rahmenbedingungen einer elektronischen Gerichtsakte als führender Akte in Deutsch-

land.[6] Sie bestätigt die eingangs formulierten Anforderungen an Sicherheit und Authentizität einer elektronischen Gerichtsakte.

D. Die Beweisführung mit elektronischen Dokumenten

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?

[6] Der Bericht enthält im Weiteren eine Bestandsaufnahme von im praktischen Einsatz befindlichen Systemen, eine Liste der technischen Anforderungen, die Beschreibung von Anwendungsszenarien für das Zivilverfahren, das Strafverfahren, das sozialgerichtliche Verfahren, das verwaltungsgerichtliche Verfahren und das arbeitsgerichtliche Verfahren.

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

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[7].

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.[8] Urkunden i.S.d. Beweismittelrechts der ZPO sind durch Niederschrift verkörperte Gedankenerklärungen, die geeignet sind, Beweis für streitiges Parteivorbringen zu erbringen.[9] Bei elektronischen Willenserklärungen fehlt es an der notwendigen Verkörperung.[10] 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.[11] Der Beweis mit elektronischen Dokumenten unterfällt damit nicht den Regeln über den Urkundenbeweis, sondern den Vorschriften über den Beweis durch Augenschein.[12] Um einen Sachverständigenbeweis handelt es sich hingegen, wenn die Visualisierung oder auch die Prüfung der

---

7 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.).

8 Ahrens, Elektronische Dokumente und technische Aufzeichnungen als Beweismittel. Zum Urkunden- und Augenscheinsbeweis, in: *Festschrift für Geimer*, 2002, S. 3.

9 Zöller/Geimer, ZPO, 28. Aufl. 2010, Vor § 414, Rdnr. 2.

10 Köhler/Arndt, Recht des Internet, 6. Aufl. 2008, Rdnr. 289; Scherer/Butt, Rechtsprobleme bei Vertragsschluss via Internet, DB 2000 S. 1009 (1016).

11 Zöller/Geimer, a.a.O., Vor § 414, Rdnr. 2 m.N.

12 Zöller/Geimer, a.a.O., Vor § 414, Rdnr. 2.

zur Sicherung der Authentizität und Integrität eingesetzten Verfahren besondere Kenntnisse und Fertigkeiten voraussetzen.[13]

D.II. Beweiswert elektronischer Dokumente

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[14]

> *§ 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, unterlagen elektronische Erklärungen nach dem bis 2005 geltenden Recht der freien Beweiswürdigung nach § 286 BGB:

> *§ 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.*

Der Richter hatte 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

---

[13] Rüssmann, a.a.O., S. 157.

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

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.

D.II.1. Die elektronische Lüge

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.

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.[15] Die uns aus dem PC-Bereich vertrauten Betriebssysteme und Programme bieten solche Funktionen jedoch nicht standardmäßig an.

D.II.2. Unberechtigte Eingriffe Dritter

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

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

[15] Vgl. zu Protokolldateien allgemein Runge, Protokolldateien zwischen Sicherheit und Rechtsmäßigkeit, CR 1994, 710.

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 schon oben näher erläuterte elektronische Signatur.

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

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[16] und TAN[17] 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.

D.II.3. Zwischenergebnis zum Beweiswert elektronischer Dokumente

Nach all dem ist im elektronischen Rechtsverkehr eine erhebliche Beweisunsicherheit der Geschäftspartner gegeben. Nach der Auffassung des Bundesgerichtshofs[18] 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.

---

16 Personal Identification Number.
17 Transaction Number.
18 BGH NJW 1995,665.

Teilweise wurde versucht, diese Beweisprobleme mit Hilfe einer Beweisvereinbarung zu lösen[19]. 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.

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.

D.III. Digitale Signatur, Urkundsbeweis und Anscheinsbeweis

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.

Die Funktionsweise digitaler Signaturen ist unter B II) vorgestellt worden. Jetzt geht es um den Beweiswert, die Beweiskraft, so signierter elektronischer Dokumente.

D.III.1. Beweiswert digital signierter Dokumente

Fraglich ist, 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

[19] Dazu Köhler/Arndt, a.a.O., Rdnr. 292.

nicht verfälscht wurde, steht fest. Damit ist dem Gericht im Rahmen des § 286 ZPO aber noch kein Beweisergebnis vorgeschrieben.[20] Daran ändert auch die Gleichstellung des mit qualifizierter elektronischer Unterschrift versehenen elektronischen Dokuments mit einer Urkunde nichts (§ 371a Abs. 1 Satz 1 ZPO). Denn die damit in Bezug genommene 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.

Die Gleichstellung hat der deutsche Gesetzgeber im Jahre 2005 im Rahmen der Regelung des Augenscheinsbeweises angeordnet. Sie lautet:

> *§ 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*

[20] Scherer/Butt, a.a.O., S. 1016.

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.

Die Musik und das heißt hier die Bindung des Richters in der Beweiswürdigung für Privaturkunden steckt in § 371a Abs. 1 Satz 2 ZPO. Der Nachweis der Echtheit der in elektronischer Form abgegebenen Willenserklärung wird nach dieser Norm 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.

Die Regelung des § 371a 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 sich zweitens als ein Fremdkörper im System des Zivilprozessrechts erweist, weil sie eine gesetzliche Beweiswürdigungsregel für einen Einzelfall enthält.

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.[21] Sie würde auch die Fälle der elektronischen

[21] Dazu Rüssmann, Haftungsfragen und Risikoverteilung bei ec-Kartenmißbrauch, DuD 1998, 395 bis 400.

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 PIN-geschützte Zugang zur Chipkarte ist eine ernsthafte Schwachstelle in der Verknüpfung der elektronischen Signatur zu einer Person.

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.[22] Diese Gefahr ist aber nie völlig auszuschließen. Letzte Sicherheit kann hier wohl nur ein Zugangsverfahren auf Grundlage biometrischer Merkmale bieten.

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.

Angesichts der genannten Schwachstellen war die gesetzliche Normierung des Anscheinsbeweises heftiger Kritik ausgesetzt.[23]

---

[22] 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.

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

Es wurde geltend gemacht, dass die Voraussetzungen für einen Beweis des ersten Anscheins nicht gegeben seien.[24] 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.

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.[25] 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. Diese anderen Verfahren sind Zugangskontrollen durch nicht manipulierbare biometrische Merkmale. Die jetzt getroffene Regelung behindert die Fortentwicklung sicherer

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

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

Verfahren, statt sie zu fördern.[26] 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.

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

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.[27] 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.

D.IV.1. Eigene elektronische Dokumente

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

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

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

gewünschte Aktivitäts- und Mitwirkungsniveau. Wir haben es mit einem Fall der Mitwirkungslast zu tun.

D.IV.2. Elektronische Dokumente in der Verfügungsgewalt des Prozessgegners

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[28]. Andere versuchten dagegen dem deutschen Zivilprozess den Weg in die „prozessuale Moderne“[29] zu weisen und eine allgemeine prozessuale Aufklärungs- und Mitwirkungspflicht der nicht beweisbelasteten Partei zu begründen.[30]

Die traditionelle deutsche Prozessrechtswissenschaft[31] und die Rechtsprechung des Bundesgerichtshofs[32] hielten an dem Grundsatz:

---

[28] Lüke, Gerhard, Der Informationsanspruch im Zivilrecht, *JuS* 1986, 2 (3); Greger in: Zöller, 28. Aufl. 2010, § 138 Rdnr. 8a.

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

[30] 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, AK-ZPO/ Eike Schmidt, § 138 Rdnr. 17 ff.

[31] Arens, Zur Aufklärungspflicht der nicht beweisbelasteten Partei im Zivilprozeß, *ZZP* 96 (1983), 1; Lüke, *JuS* 1986, 2.

[32] 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 substan-

„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[33], prozessuale Sonderregeln ausfindig machen,[34] Überlegungen zum Umfang der Substantiierungslast für Behauptungen und Gegenbehauptungen anstellen[35] und eventuell zum Instrument der Beweisvereitelung mit seinen prozessualen Sanktionen greifen.[36] Diesen Bemühungen hat erst der Gesetzgeber ein Ende bereitet und Theorie und Praxis den Weg in die prozessuale Moderne gewiesen (dazu unten).

D.IV.3. Elektronische Dokumente in der Verfügungsgewalt Dritter

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.

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,

---

tiierten 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.

33 Etwa für die Offenlegung ärztlicher Dokumentationen.

34 Wie § 258 Abs. 1 HGB für Handelsbücher.

35 Das ist die Lösung des Bundesgerichtshofs in Fußnote 32.

36 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.

worüber man unter Zwang (§ 390 ZPO[37]) 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[38] auch verpflichtete, eine Sache vorzulegen oder bereitzuhalten[39]. 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.*

---

[37] § 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.

[38] 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.

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

(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.

Damit hat die Bundesrepublik Deutschland Anschluss an die internationale Entwicklung gefunden, auch wenn die Reichweite der neu geschaffenen Normen bis heute umstritten ist und große Teile der Literatur in der alten Welt verharren.[40] Das Recht auf Information und Beweis war in anderen Rechtsordnungen wesentlich stärker ausgeprägt als im Recht der Bundesrepublik Deutschland. Auch in diesen Rechtsordnungen hatte einmal der Grundsatz gegolten: „Nemo contra se edere tenetur!“ Sie hatten

[40] Siehe dazu den Überblick von Prütting in: Prütting/Gehrlein, ZPO, 1. Auflage 2010, § 142 Rdnr. 2. Gegen eine weite Aufklärungspflicht sprechen sich Rosenberg/Schwab/Gottwald, Zivilprozessrecht, 17. Auflage 2010, § 109 Rdnr. 8; Leipold in: Stein/Jonas, ZPO, 22. Auflage 2005, § 138 Rdnr. 28, § 142 Rdnr. 17 ff. und BGH NJW 2007, 155, 156 aus; a.A. Stadler in: Musielak, ZPO, 7. Auflage 2009, § 138 Rdnr. 11; einschränkend Greger in: Zöller, 28. Auflage 2010, § 142, Rdnr. 2; Wagner in: Mü-Ko, ZPO, 3. Auflage 2008, § 138 Rdnr. 22, §§ 142 – 144 Rdnr. 1; Prütting in Prütting/Gehrlein: ZPO, 1. Auflage 2010, § 142 Rdnr. 2.

den Grundsatz aber schon vor Deutschland in zum Teil dramatischen Kehrtwendungen verabschiedet.[41]

D.V. Zusammenfassung

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.

Der Anscheinsbeweis des § 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.

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.

---

41 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.).