Rechtliche Anforderungen an den Einsatz moderner Kommunikationsmittel durch den Anwalt sowie Anforderungen an die elektronische Prozessführung

Stand: 05.11.2004

Rechtsanwalt
Helmut Becker
Rheinsteig 9
78462 Konstanz
Tel.: 07531-90900
Fax.: 07531-909090
Internet: http://www.becker-helmut.de
e-mail: helmut.becker@becker-helmut.de

Inhaltsübersicht

Vorbemerkung

1

Wir sind derzeit zwar nicht mehr in einer Phase des Experimentierens, aber wir sind noch dabei zu erproben und **Erfahrungen zu sammeln**.

Das **Gesetz** ist selbst noch nicht so gefestigt, dass es zur Richtschnur geworden wäre. **Weitere Entwicklungen** sind notwendig; **Gestaltungsspielräume** sind – noch - vorhanden. Es ist noch nicht sicher, ob die gesetzlichen Lösungen, die bereits gefunden sind, sich bewähren werden. Und es ist auch noch nicht sicher, ob die Schwerpunkte in der Realität so liegen werden, wie das Gesetz sie jetzt sieht.

Ansatz unserer Überlegungen kann und muss daher nur sein, **die praktischen Bedürfnisse und die Bedürfnisse, die der Rechtsstaatlichkeit und ihren Grundsätzen folgen**. Zu diesen Grundsätzen gehören auch **wesentliche Teile des anwaltlichen Berufsrechts**.
Mit diesen Grundsätzen müssen einerseits die Lücken, die das Gesetz noch bietet, geschlossen werden. Andererseits aber müssen die bereits vorhandenen gesetzlichen Vorschriften im Lichte dieser Grundsätze angewandt und ausgelegt werden.

Einstieg in die Problematik

2

Die Betrachtung hat daher an folgenden Gesichtspunkten anzusetzen:

- Sicherheitsaspekte (--> 3)
- Elektronische Akten-, Kanzlei- und Prozessführung (--> 12)
- Überwindung von System- und Medienbrüchen zwischen den Beteiligten (--> 14)
- Überwindung von Kompatibilitätsproblemen, die dabei auftreten (--> 15)
- Der Anwalt im Rahmen der Justizkommunikation (--> 16)

Sicherheitsaspekte

3

Unter Sicherheitsgesichtspunkten sind folgende Teilaspekte zu berücksichtigen:

- Sicherheit des Computersystems (--> 4)
- Sicherheit der Daten (--> 8)
- Sicherheit der Kommunikation zwischen verschiedenen Systemen (--> 9)
- Sicherheit der Organisation, die auf dem System basiert. (--> 11)

Sicherheit des Computersystems

4

Das ist die Basis für die Sicherheit der gesamten IT-gestützten anwaltlichen Tätigkeit. Die wesentlichen praktischen Aspekte dabei sind folgende:

- Zugang zum System, seinen Komponenten und den gespeicherten Daten.
- Verfügbarkeit des Systems insbesondere bei unerwarteten Zwischenfällen. Dabei ist besonders wichtig:
    - die Schnittstelle zur notfallmäßigen Weiterarbeit des Anwalts bzw. seiner Kanzlei ohne das System.
    - die Wiederanlaufeigenschaften des Systems.

5

Die hier geschilderten Problemfelder treten in der Praxis vor allem bei folgenden Anlässen auf:

- Befall mit Viren, trojanischen Pferden, Spyware u.ä.

- Stromausfälle
- „Normale“ Systemabstürze
- Installations- und Wartungsarbeiten am System durch Dritte

6

Gesetzliche Orientierungshilfe dabei bieten die Gebote des Datenschutzrechts gemäß Anhang zu § 9 Satz 1 BDSG. Diese Gebote können aus praktischer Sicht auch dort angewandt werden, wo die rechtlichen Bedingungen für die Anwendbarkeit des BDSG nicht gegeben sind. Der Begriff „Datenschutz“ wird deshalb im Folgenden etwas weitergehend im Sinne von „Geheimnisschutz“ benutzt.

- „Äußerer“ Datenschutz (Gebote 1 – 3):
  - Zutrittskontrolle: Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, zu verwehren. Das ist z.B. baulich, örtlich und organisatorisch zu gewährleisten.
  - Zugangskontrolle: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können
  - Zugriffskontrolle: Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können
- „Innerer“ Datenschutz (Gebote 5 und 7):
  - Eingabekontrolle: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten eingegeben, verändert oder entfernt worden sind.
  - Verfügbarkeitskontrolle: Es ist zu gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

7

Unabhängig von der Anwendbarkeit des Datenschutzrechts im Einzelnen ist aber bei den Daten, die in einer Anwaltskanzlei anfallen, von einer sehr hohen Sensibilität auszugehen. Dies äußert sich in einer ganzen Reihe von Berufsspezifischen Pflichten, wie z.B. insbesondere

- Schweigepflicht
- Interessenwahrungspflicht
- Aktenführungspflicht

Sicherheit der Daten

8

Hier geht es neben den vorerwähnten Datenschutzaspekten um Datensicherheitsaspekte wie z.B.:

- Datensicherung
  - Organisation und Systematik
  - Regelmäßige Durchführung
  - Aufbewahrung und Lagerung der Sicherungsdaten
- Verschlüsselung, insbesondere als
  - Zugriffsschutz (Geheimhaltung)
  - Änderungsschutz
  - Identifizierung
  - Authentifizierung

Sicherheit der Kommunikation

Ein wesentliches Problem hierbei stellt die Vielfalt und gegenseitige Vernetztheit der in der Praxis verwendeten Kommunikationsmöglichkeiten dar. Dies ermöglicht und fördert zahlreiche – oft auch nur sehr schwer durchschaubare – Manipulationsmöglichkeiten. So insbesondere in folgenden Ausprägungen:

- Interne Kommunikation
    - Kommunikation in einem Kanzleinetzwerk
        - Benutzerverwaltung und Zugriffskontrolle
    - Kommunikation über DFÜ- und WLAN-Netzwerke
        - hier ist zu berücksichtigen, dass lediglich die organisatorische Einheit als intern betrachtet werden kann; faktisch erfolgt die Kommunikation extern, mit allen damit verbundenen Konsequenzen und Risiken.

- Externe Kommunikation
    - Computerfax mit folgenden Manipulationsmöglichkeiten:
        - alle faxspezifischen Metadaten wie z.B.
            - Datum und Uhrzeit der Versendung
            - Absenderangaben
        - eingescannte Unterschriften
    - Kommunikation über das Internet, bei der es – zumindest für den Normalanwender – völlig undurchschaubar ist, welche Dritte
        - standardmäßig an der Kommunikation beteiligt sind, z.B.
            - Provider
            - Netzbetreiber
        - sich im Einzelfall in die Kommunikation einschalten können, z.B.
            - um sie abzuhören
            - um sie zu verändern

10

Abhilfe verspricht hier die elektronische Signatur nach Signaturgesetz und Signaturverordnung. Fraglich ist aber, ob damit nicht eine Einschränkung der nützlichen Möglichkeiten zudem auf Kosten des Komforts und der Schnelligkeit einhergeht.

Sicherheit der Organisation

11

Hier ist die Frage der Systemverantwortung aufzuwerfen.

Elektronische Akten- und Kanzleiführung

12

Sind die unter dem Sicherheitsaspekt aufgeworfenen Probleme gelöst, dann kann man daran gehen und seine Akten, seine Kanzlei und schließlich einzelne oder alle Prozesse elektronisch führen.

Hier geht es um solche Dinge wie die Verwaltung von Fristen und Terminen, teilweise damit zusammenhängend aber auch Möglichkeiten und Probleme des elektronischen Zahlungsverkehrs.

Im Hinblick auf Fristen ist zu differenzieren zwischen den damit verbundenen Rechtspflichten und den Möglichkeiten der Arbeitsplanung bzw. Arbeitsvorbereitung durch den Anwalt.

Elektronische Prozessführung

13

Zentrale Vorschrift der ZPO sind

- § 130a und die
- neu vorgeschlagene Regelung des § 130b.

Elektronisches Dokument (§ 130a):

> (1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung **als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist**. Die verantwortende Person **soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen**.

(2) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.

(3) Ein elektronisches Dokument **ist eingereicht, sobald die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat**.

Dem Absatz 1 dieser Bestimmung soll folgender Satz hinzugefügt werden:
Ist ein übermitteltes elektronisches Dokument für das Gericht zur Bearbeitung nicht geeignet, ist dies dem Absender unter Angabe der geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen.

Gerichtliches elektronisches Dokument (§ 130b E):

Soweit dieses Gesetz dem Richter, dem Rechtspfleger, dem Urkundsbeamten der Geschäftsstelle oder dem Gerichtsvollzieher die handschriftliche Unterzeichnung vorschreibt, genügt 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 versehen

Weitere Detailregelungen:

Zum Umgang mit diesen Gegenständen finden sich – je nach Zielrichtung – folgende Vorschriften:

Aktenführung; Akteneinsicht:

- Aktenausdruck: § 298
- Elektronische Akte: § 298a
- Akteneinsicht: § 299 Abs. 3 E
  - durch Aktenausdruck
  - Wiedergabe auf einem Bildschirm
  - Übermittlung der Gesamtheit der Dokumente der elektronischen Akte mit einer qualifizierten elektronischen Signatur

  Alle diese Arten der Akteneinsicht haben erhebliche praktische Konsequenzen im Hinblick auf **Verfahrensbeschleunigung** bzw. Taktiken zur **Verfahrensverzögerung**.

Beweisantritt und Beweisführung

- **Beweisantritt** bei elektronischen Dokumenten: § 371 Abs. 1 S. 2
  Der Beweis durch Augenschein wird durch Bezeichnung des Gegenstandes des Augenscheins und durch die Angabe der zu beweisenden Tatsachen angetreten. Ist ein **elektronisches Dokument** Gegenstand des Beweises, wird der Beweis durch **Vorlegung oder Übermittlung der Datei** angetreten.

Anscheinsbeweis bei qualifizierter elektronischer Signatur: § 292a:

> Der Anschein der Echtheit einer in elektronischer Form (§ 126a des Bürgerlichen Gesetzbuchs) 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.

- **Beweiskraft** elektronischer Dokumente: § 371a E
  - Verweisung auf die Vorschriften des **Urkundenbeweises**
  - Beweiskraft des Ausdrucks eines öffentlichen elektronischen Dokuments: § 416a E

Formalien:

- Kostenfestsetzung in der Form des § 130b E (gerichtliches elektronisches Dokument)
- Generell:
  - „Dokument“ statt „Schriftstück“
  - „Formular“ statt „Vordruck“
  - „Übermitteln“ statt „übergeben“ bzw. „zusenden“
  - Öffentliche Bekanntmachungen des Gerichts durch elektronische Informations- und Kommunikationssysteme (z.B. § 948 Abs. 1 E; in diesem Fall auch im elektronischen Bundesanzeiger)
- Einheitliche Zustellungsformulare: § 190 E

Sonderregelungen in den Verfahrensordnungen anderer Gerichtsbarkeiten, z.B.:

- § 55a VwGO E
- § 52a FGO E

Elektronik in der mündlichen Verhandlung

Hier ist insbesondere § 128a ZPO zu nennen:

(1) Im **Einverständnis** mit den Parteien **kann** das Gericht den Parteien sowie ihren Bevollmächtigten und Beiständen auf Antrag gestatten, sich während einer Verhandlung an einem anderen Ort aufzuhalten und dort Verfahrenshandlungen vorzunehmen. Die Verhandlung wird **zeitgleich in Bild und Ton** an den Ort, an dem sich die Parteien, Bevollmächtigten und Beistände aufhalten, und in das Sitzungszimmer übertragen.

(2) Im **Einverständnis** mit den Parteien **kann** das Gericht gestatten, dass sich ein Zeuge, ein Sachverständiger oder eine Partei während der Vernehmung an einem anderen Ort aufhält. Die Vernehmung wird **zeitgleich in Bild und Ton** in das Sitzungszimmer übertragen. Ist Parteien, Bevollmächtigten und Beiständen nach Absatz 1 gestattet worden, sich an einem anderen Ort aufzuhalten, so wird die Vernehmung zeitgleich in Bild und Ton auch an diesen Ort übertragen.

(3) Die Übertragung wird nicht aufgezeichnet. Entscheidungen nach den Absätzen 1 und 2 sind nicht anfechtbar.

Wesentlich dabei ist, dass

- das Gericht auch bei Einverständnis der Parteien nicht gezwungen ist.
- Das Gericht in keinen Fall ohne Zustimmung beider Parteien eine Anordnung treffen kann
- Die getroffenen Anordnungen nicht anfechtbar sind.

Was bleibt zu tun?

14

- Überwindung von System- und Medienbrüchen

15

- Überwindung von Kompatibilitätsproblemen

Der Anwalt im Rahmen der Justizkommunikation

16

Gegenstand der Betrachtung ist der Regierungsentwurf vom 28.07.2004; wesentlich sind dabei insbesondere folgende Gesichtspunkte:

- Der Anwalt als Organ der Rechtspflege
- Elektronische Akteneinsicht
- Das Berufsattribut bei der elektronischen Signatur.

Fazit

17

Ziel der Bemühungen:

- Kein primär effizienz- und kostenorientiertes Rechts- und Justizsystem, das wäre gewissermaßen „lausig“.
- Sondern ein auf persönlicher Verantwortung der Träger des Rechtssystems fußende Verpflichtung zu Gerechtigkeit – auch wenn das manchmal weh tut (und teuer ist).