„Elektronische Beweisführung“ - rechtliche Grundlagen -

Deutscher EDV-Gerichtstag e.V.

Dennis Hillemann
Rechtsanwalt
Fachanwalt für Verwaltungsrecht,

20.09.2019

Agenda Rechtliche Grundlagen (I)

1. Grundsätze der Beweisführung im Zivilrecht
2. Beweiskraft elektronischer Beweismittel in der ZPO
3. eIDAS-VO
4. eIDAS-Durchführungsgesetz und Vertrauensdienstegesetz
5. Auslegungsfragen

Agenda Rechtliche Grundlagen (II)

6	Elektronische Beweismittel im Strafverfahren
7	Elektronische Beweissicherung in der unternehmerischen Praxis
8	Aktuelle Entwicklungen

Grundsätze der Beweisführung im Zivilrecht

Grundsätze der Beweisführung im Zivilrecht

- Beweis = Überzeugung des Gerichts von der Wahrheit einer Behauptung
- Beweislast (Risiko des misslungenen Beweises) trägt die Partei, für die Behauptung einer Tatsache günstig ist
- Grundsatz ist Dispositionsmaxime aufgrund von Privatautonomie
  (im Gegensatz zum Amtsermittlungsgrundsatz)

- Systematik:
  - **Eignung** als Beweismittel
  - **Zulässigkeit** als Beweismittel (nächste Folie)
  - **Beweiskraft**
    - Grundsatz: freie Beweiswürdigung des Gerichts (§ 286 Abs. 1 ZPO)
    - Ausnahme: Gesetzliche Beweisregeln (286 Abs. 2 ZPO)
      1. Anscheinsbeweis (keine Legaldefinition, Bezug darauf in einzelnen Normen)
         → Erschütterung nur durch ernsthafte Zweifel
      2. Gesetzliche Vermutung (§ 292 ZPO)
         → Widerlegung nur durch Erbringung Gegenbeweis

Beweismittel in der Zivilprozessordnung

Sachverständige

Zeugen

Parteivernehmung

Urkunden

- Urkunde = verkörpert dauerhaft eine Gedankenerklärung und lässt ihren Aussteller erkennen
- Besondere Regelungen, insb. zur Beweiskraft in den §§ 415 bis 444 ZPO [Einschr. freie Beweiswürdigung]

Augenschein

- Gericht vermittelt sich optisch, akustisch, sensorisch persönl. Eindruck
- Entscheidung über die Beweiskraft nach den Grundsätzen der „freien Beweiswürdigung“
  → Gericht kann Integrität und Authentizität anzweifeln und Objekt für ungeeignet als Beweis erklären

Beweiskraft elektronischer Beweismittel in der ZPO

Elektronische Dokumente als Beweismittel

- **Elektronische Beweismittel** mangels dauerhafter Verkörperung **≠ Urkunde**
  - nichtsdestotrotz zulässig als Beweismittel
  - grds. finden **Vorschriften über den Augenscheinsbeweis** (§§ 371 bis 372a ZPO) Anwendung
  - z.B. Entscheidung über Beweiskraft durch „freie Beweiswürdigung“ durch das Gericht (§ 286 Abs. 1 ZPO)

! **Problem:** ungesicherte elektronische Dokumente haben aufgrund Veränderbarkeit und Manipulationsmöglichkeiten bei freier Beweiswürdigung nur geringe Beweiskraft

→ Mithilfe von **Sicherungsverfahren**, insb. gesetzlich anerkannten, kann die **Beweiskraft elektronischer Dokumente erhöht** werden

! **Probleme:** einmal eingesetzte Verfahren verlieren i.d.R. mit der Zeit an Sicherheit, Dokument muss ununterbrochen mit sicherem/gültigen Verfahren versehen sein
→ ggf. Neusignierung notwendig (permanente Überprüfung des Verfahrens / Entwicklung neuer Verfahren)

Besondere Beweiswirkungen für elektr. Dokumente

- **Sicherungsverfahren, insb. gesetzlich anerkannte, werten Beweiswert elektronischer Dokumente auf:**
  - **Qualifizierte elektronische Signaturen (§ 371a ZPO)**
    - Anwendung der Regeln über Beweiskraft privater Urkunden (§371a Abs. 1 S. 1 ZPO)
    - **Beweiskraft: Anscheinsbeweis** (Erschütterung nur durch ernstliche Zweifel)
    - **Rechtliche und technische Anforderungen** seit 29.07.2017 **eIDAS-VO** i.V.m. eIDAS-Durchführungsgesetz vom 18.07.2017 geregelt (nicht mehr im SigG; dazu später)
  - **De-Mail mit Absenderbestätigung (§ 371a ZPO)**
    - Beweisrechtlich weitgehend qualifiziert elektronischer Signatur gleichgestellt (§ 371 Abs. 2 ZPO)
    - Nachricht muss mit qualifiziert elektronischer Signatur des De-Mail-Providers versehen sein
  - **Gescannte öffentliche Urkunden (§ 371b ZPO)**
    - Beweiskraft öffentlicher Urkunden: Vermutung der Echtheit, Erschütterung nur durch Gegenbeweis
    - Voraussetzung: Scan nach Stand der Technik (BSI), wird von Behörde oder mit öffentlichem Glauben versehene Person erstellt und enthält Bestätigung der Übereinstimmung mit Original
  - **Ausgedruckte öffentliche elektronische Dokumente (§ 416 a ZPO)**
    - Beweiskraft öffentlicher Urkunden
    - Voraussetzung: Dokument nach § 371a Abs. 3 ZPO erstellt und Ausdruck mit Beglaubigungsvermerk versehen

Differenzierung nach privaten / öffentlichen Erstellern

eIDAS-VO

(VO (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt)

EU-eIDAS-VO

- Verordnung über „elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO)“
- seit dem 01.07.2016 Teil der deutschen Rechtsordnung mit Anwendungsvorrang vor deutschem Recht

- Erweiterung des Katalogs der Vertrauensdienste:
  1. **Elektronische Signaturen**
  2. **Elektronische Siegel (neu)**
  3. **Elektronische Zeitstempel (neu)**
  4. **Dienste für die Zustellung elektronischer Einschreiben (neu)**
  5. Website-Authentifizierung (neu)
  6. Validierungs- und Bewahrungsdienste (neu)
  7. **(Elektronische Dokumente)**
- Bestimmung eigener beweisrechtlicher Folgen für Nr. 1, 2, 3, 4, 7

- Aufhebung der Signaturrichtlinie 1999/93/EG

Beweisregelungen in der eIDAS-VO

Allgemeine Beweisregelung (Art. 46 eIDAS-VO):

Einem elektronischen Dokument darf Rechtswirkung und Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil der Vertrauensdienst in elektronischer Form vorliegt oder nicht die Anforderungen für qualifizierte Vertrauensdienste erfüllt.

→ Beweis des Augenscheins nach bestehendem deutschen Beweisrecht (keine beweisrechtliche Veränderung)

Elektronische Signaturen:

- Verschiedene Signaturqualitäten: Einfache elektr. Signatur, Fortgeschrittene elektr. Signatur, Qualifiziert elektr. Signatur (Voraussetzungen Art. 3 Nr. 10-12 eIDAS-VO)
- Keine besondere Beweisregelung für qualifizierte elektronische Signatur (ergibt sich aus deutschem Zivilprozessrecht)

Spezifische Beweisregelung für neue Vertrauensdienste:

Elektronische Siegel:
- juristischer Person zugeordnet
- Voraussetzungen Sicherheits-stufen wie bei Signatur
- **Beweisregelung** qualifiziert elektronisches Siegel: Vermutung hinsichtlich der Integrität und Authentifizierung der gesiegelten Daten (Art. 35 Abs. 2 eIDAS-VO)

Elektronischer Zeitstempel:
- Voraussetzung Qualifizierung in Art. 42 eIDAS-VO
- **Beweisregelungen:**
  - Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind
  - Vermutung der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten

Elektronisches Einschreiben (Art. 3 Nr. 36 eIDAS-VO):
- Voraussetzung Qualifizierung in Art. 44 Abs. 1 eIDAS-VO)
- **Beweisregelungen:** Vermutung Unversehrtheit der Daten, Korrektheit Datum und Uhrzeit (Absendung, Empfang) und Identität Absender und Empfänger

eIDAS-Durchführungsgesetz und Vertrauensdienste-gesetz

eIDAS-Durchführungsgesetz

- Seit 29.07.2017 in Kraft
- eIDAS-VO zu unvollständig, um ohne mitgliedstaatliche Ergänzungen vollzogen werden zu können; in dem Rahmen wurde eIDAS-Durchführungsgesetz erlassen
- ersetzt das Signaturgesetz (SigG) und die Signaturverordnung (SigV)

Inhaltliches:

- *Art. 1 und 2*: „Herzstück“ ist das Vertrauensdienstegesetz (VDG)
- *Art. 3 bis 11 enthalten Regelungen zur Anwendung qualifizierter Vertrauensdienste im deutschen Recht*
  - Anscheinsbeweis hinsichtlich Echtheit qualifizierter elektr. Signaturen unverändert (keine Annährung an Wortlaut der eIDAS-VO, welche „Vermutungswirkung“ bei anderen qualifzierten Vertrauensdiensten vorsieht)
  - keine Anpassung/Einführung weiterer Beweisregelungen
- *Art. 10 Nr. 3:* Regelungen zur Beweiswirkung von Vertrauensdiensten (nächste Folie)

VDG

- Regelt nicht nur elektronische Signaturen, sondern auch weitere Vertrauensdienste, die das nationale Recht zuvor nicht kannte
- wesentliche Regelungen zu Vertrauensdiensten in eIDAS-VO, wg. Anwendungsvorrang der VO kann VDG nur „präzisierende, konkretisierende und ergänzende Regelungen“ enthalten
- zusätzlich wurde Vertrauensdiensteverordnung (VDV) erlassen

Teil 1: §§ 1-8	Teil 2: §§ 9-16	Teil 3 und 4	Teil 5
Ergänzungen zu den allgemeinen Bestimmungen für alle Vertrauensdiensteanbieter (Artt. 13-15 eIDAS-VO)	**Ergänzungen zu den allgemeinen Bestimmungen für qualifizierte Vertrauensdienste (Artt. 20-24 eIDAS-VO), u.a.:** • **Langfristige Beweiserhaltung** (§ 15 VDG) • **Auf Dauer prüfbare Vertrauens-dienste** (§ 16 Abs. 4 und 5 VDG)	**Spezifische Regelungen zu den einzelnen Vertrauensdiensten (Artt. 25-40 eIDAS-VO)**	**Schluss-bestimmungen**

VDG: Langfristige Beweiserhaltung

- **Regelung zur langfristigen Beweiserhaltung wie bisher in § 17 SigV fehlt in eIDAS-VO**
- **Daher durfte VDG die VO ergänzen:**

§ 15 VDG Langfristige Beweiserhaltung

„[1]Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. [2]Die neue Sicherung muss nach dem Stand der Technik erfolgen."

vermutet, wenn entsprechende, aktuellste Schutzprofile und Technische Richtlinien des BSI eingehalten (Bekanntmachung im Bundesanzeiger)

VDG: Auf Dauer prüfbare Vertrauensdienste (1)

- **Langfristige Prüfbarkeit von Zertifikaten in eIDAS-VO ungeregelt**

- **§ 16 Abs. 4 VDG:**

  „Qualifizierte Vertrauensdiensteanbieter haben für die gesamte Zeit ihres Betriebs

  *1.die in Absatz 1 Satz 1 genannten Zertifikate auch **über den Zeitraum ihrer Gültigkeit hinaus** zusammen mit den dazugehörigen Widerrufsinformationen in einer **Zertifikatsdatenbank** nach Artikel 24 Absatz 2 Buchstabe k und Absatz 4 der Verordnung (EU) Nr. 910/2014 zu führen*

  und

  2.die dazugehörigen Aufzeichnungen nach Artikel 24 Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 aufzubewahren.“

➢ **Ziel: Sicherstellung der langfristigen Überprüfbarkeit der Authentizität signierter oder gesiegelter Daten**

VDG: Auf Dauer prüfbare Vertrauensdienste (2)

- **§ 16 Abs. 5 VDG:**

  „[1]Die Bundesnetzagentur hat eine Vertrauensinfrastruktur zur dauerhaften Prüfbarkeit qualifizierter elektronischer Zertifikate und qualifizierter elektronischer Zeitstempel einzurichten, zu unterhalten und laufend zu aktualisieren. [2]Näheres regelt die Rechtsverordnung [Anm. gemeint ist VDV] nach § 20 Absatz 2 Nummer 5.“

➢ **Regelung für den Fall der Übernahme von qualifizierten elektronischen Zertifikaten durch die BNetzA**

➢ **qualifiziertes Zertifikat wird ungültig durch Zeitablauf/Widerruf/Sperrung; bereits erzeugte qualifizierte elektronische Signaturen und Siegel werden dadurch nicht unwirksam, aber langfristige Beweiswerterhaltung (§ 15 VDG) in jedem Fall zu beachten**

Auslegungsfragen

Auslegungsfragen

- **Es bestehen zwei wesentliche Auslegungsfragen hinsichtlich des Zusammenspiels der ZPO und der eIDAS-VO:**

Begriff des „elektronischen Dokuments“

- **ZPO:** keine Legaldefinition, sowohl weites als auch enges Begriffsverständnis denkbar (beachte Wortlaut: 371a Abs. 1 S. 1 ZPO: *„Erklärung“* – demnach könnten nur qualifiziert elektr. Signierte Erklärungen Anscheinsbeweis darstellen; andere qualif. Elektr. Sig. Dokumente unterlägen freier Beweiswürdigung)
- **eIDAS-VO:** *„alle in elektronischer Form, insb. Text-, Ton-, Bild-, oder audiovisuelle Aufzeichnungen gespeicherte Inhalte“* bei neuen Vertrauensdiensten gleichgestellt

Beweiskraft qualifizierter Vertrauensdienste

- **eIDAS-VO:** keine Regelung zur Stärke der *„Vermutung“ (Wortlaut zur Beweisregelung)* oder Widerlegbarkeit

→ Vermutung i.S.d. gesetzlichen Vermutung des § 292 ZPO (dann wäre Beweiskraft der qualifizierten neuen Vertrauensdienste ggü. der Beweiskraft von qualif. elektr. Signaturen erhöht) oder i.S.d. Anscheinsbeweises (gleiche Beweiskraft für alle qualif. Vertrauensdienste)?

Beide Fragen nicht in Durchführungs-VO (und VDG geklärt!)

Elektronische Beweismittel im Strafverfahren

Gewinnung elektronischer Beweismittel im strafrechtlichen Ermittlungsverfahren

- **Stellungnahme BRAK 2018: elektronische Beweismittelgewinnung wichtigste Erkenntnisquelle des Strafverfahrensrechts**

- **Sicherung elektronischer Daten von Inlandsservern über verfügbare Speichermedien zulässig, § 110 Abs. 3 S. 2 StPO**

- **§ 94 StPO (Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken) anwendbar sowohl auf Datenträger als auch auf Daten**

- **Einsatz von IT-Forensik zur Duplikation der Datensätze: Schutz vor Verlust von Daten und Unabhängigkeit vom (beschlagnahmten) Datenträger**

- **§ 94 StPO kann auch (analog) Überwindung einer Verschlüsselung der Daten rechtfertigen (str., ob auch bei Live-Forensik – Live-Zugriff auf Daten, die auf Servern gespeichert sind)**

- **Konflikt zwischen Datenschutz und Ermittlungsinteresse: Anspruch auf Löschung irrelevanter Daten nach §§ 58, 75 BDSG**

Einführung elektronischer Dokumente in die Hauptverhandlung

- **Elektronische Dokumente – soweit verlesbar – als Urkunden, § 249 Abs. 1 S. 2 StPO n.F.**

- **Erkennbarkeit des Ausstellers für Verlesung nicht erforderlich, qualifizierte elektronische Signatur daher für Verlesung nicht benötigt**

- **Kein Urkundenbeweis durch reine Audio- und Videodateien sowie sonstige nicht zur Wiedergabe in verkörperter Form geeignete Informationen**

- **Einführung nicht verlesbarer Dateien als Augenscheinsobjekte oder über Zeugen- und Sachverständigenbeweis (Eindrücke Dritter von der Datei)**

Elektronische Beweissicherung in der unternehmerischen Praxis

Banken zwischen besonderen und allgemeinen Anforderungen

- **Beispiele besonderer Regulierung von Finanzdienstleistern: Ausgabe elektronischer Kontoauszüge mit elektronischem Siegel bzw. qualifizierter elektronischer Signatur zur Sicherung der Unveränderbarkeit nach den PSD2-Vorschriften; Verpflichtung zu Aufzeichnungen von internen und externen Kommunikationen im Verlauf von Vertragsgesprächen mit Kunden und Interessenten nach MiFiD II-Richtlinie: danach fünfjährige verschlüsselte Speicherung der Dokumentation**

- **Banken wesentlich vor den gleichen Herausforderungen wie andere Unternehmen, die Daten archivieren**

Beweissicherung in Unternehmen durch elektronische Archive

- **KPMG-Studie zur Wirtschaftskriminalität (2016): 24 % der befragten Unternehmen attestieren sich selbst Versäumnisse bei der Beweissicherung**

- **Herausforderung der Medienbruchfreiheit: Umstellung von Papier auf elektronische Datenträger häufig erst teilweise verwirklicht**

- **Interne Maßnahmen: Einhaltung der gesetzlichen Aufbewahrungspflichten (insb. nach HGB und AO), Einhaltung der einschlägigen Technischen Richtlinien des BSI, Einhaltung der GoBD**

- **Aufträge an externe Dienstleister: insbesondere elektronische Validierungs- und Bewahrungsdienste zur stetigen Aktualisierung der verwendeten Algorithmen (vgl. Art. 34 eIDAS-VO, Zertifizierung erfolgt durch BNetzA)**

Aktuelle Entwicklungen

Datenspeicher als Beweismittel im Verkehrsprozess

- **dem Ministerrat zur Entscheidung vorgelegter EU-Verordnungsvorschlag will Autohersteller ab 2024 zum Einbau von „black boxes“ (nur ereignisbezogene Datenerfassung) in Neuwagen verpflichten – Daten sollen nur anonymisiert erhoben und für Verkehrsforschung verwendet werden**

- **Konflikt zwischen Aufklärungsinteresse und Datenschutz, falls aufgezeichneter Unfall Verletzungs- oder Todesopfer fordert (Herausgabeersuchen der Staatsanwaltschaft möglich)**

- **§ 63a Abs. 2 StVG verlangt Übermittlung von Lokalisationsdaten aus hoch- oder vollautomatisierten Fahrzeugen an Strafverfolgungs- und Ordnungswidrigkeitsbehörden bei Anfangsverdacht: kein Richtervorbehalt wie bei Durchsuchung im Strafverfahren – verhältnismäßiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung?**

EU-Reformbestrebungen zur Harmonisierung der grenzüberschreitenden Beweissicherung

- **Elektronische Beweismittel relevant für 85 % aller Strafverfahren; in zwei Dritteln dieser Verfahren befinden sich Beweismittel jedoch im Ausland (Bsp.: Daten eines GoogleMail-, WhatsApp- oder Facebook-Kontos)**

- **Rechtshilfe zwischen Behörden der Mitgliedstaaten verzögert und erschwert Beweissicherung (Einschaltung einer Bewilligungsbehörde)**

- **Freiwillige Zusammenarbeit zwischen Behörden der EU-Mitgliedstaaten und Dienste-Anbietern in den USA ist zu wenig transparent und gewährleistet keinen ausreichenden Rechtsschutz**

- **Entwurf einer Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen: Dienstanbieter als Adressaten können Daten in Drittstaaten speichern – nur Dienstleistung muss im EU-Gebiet angeboten werden (Art. 1 Abs. 1 VO-E)**

- **Rechtsschutzdefizite (z.B. kein durchgehender Richtervorbehalt, keine Mitteilung der Gründe für die Anordnung gegenüber dem Diensteanbieter)**

CV

Dennis Hillemann

Senior Manager

KPMG Law, Hamburg
T +49 40 360994-5045
F +49 1802 11991-1670
M +49 151 50638412
dhillemann@kpmg-law.com

BEI KPMG Law SEIT 2016

GESCHÄFTSBEREICH	— KPMG Law, Public Sector Nord/Transparenzrecht/Wissenschaft
QUALIFIKATION	— Rechtsanwalt (Zulassung 2006) — Fachanwalt für Verwaltungsrecht (2010)
FACH- UND BRANCHENERFAHRUNG	— 13 Jahre einschlägige Berufserfahrung im Public Sector (Verwaltungsrecht, Beihilferecht, Fördermittelrecht, Haushaltsrecht) — Head der KPMG-Solution „Beratung in komplexen Verwaltungsverfahren“ und damit Ansprechpartner für Ministerien, Behörden und öffentliche Unternehmen insb. bei Gestaltungsfragen neuer Formen der Zusammenarbeit und deren Finanzierung. — Engagement im Bereich Blockchain und Recht; Mitarbeit an der DIN-SPEC 4997: „privacy by blockchain design“ — Speaker bei verschiedenen Events (z.B. OECD Global Blockchain Policy Forum).
AUSGEWÄHLTE MANDATE	— **Bundesministerium:** Laufende gerichtliche Vertretung in Verfahren hinsichtlich der Abwehr von Informationsansprüchen nach UIG und IFG. — **Forschungseinrichtungen und Hochschulen**: Laufende Rechtsberatung in allen wissenschaftsrechtlichen Fragen (insbesondere zur Governance, IT, Hochschulrecht, gemeinsame Berufungen, Technologietransfer, Kooperationsvereinbarungen), Beratung zu hochschulrechtlichen sowie zu beihilfe- und fördermittelrechtlichen Themen
SPRACHEN	— Deutsch (Muttersprache) — Englisch (Verhandlungssicher) — Französisch (sicher in Wort und Schrift)