Deutsche Stiftung für Recht und Informatik

Elektronische Beweismittel vor Gericht

Dr. Florian Deusch
ANWALTSKANLEI DR. GRETTER

Prof. Dr. Tobias Eggendorfer
Technische Hochschule Ingolstadt

Herbstakademie 2025

Überblick

- Elektronische Daten als Beweismittel
- Verfassungsrechtliche Anforderungen
- Technischer Anforderungen
- Vorgaben im Zivilprozess
- Vorgaben im Strafprozess
- Vorgaben im Verwaltungsrechtsstreit
- Zusammenfassung und Fazit

Elektronische Daten als Beweismittel

Wer digitale Angebote nutzt, hinterlässt Spuren…
(Locard'sches Austauschprinzip)

Elektronische Daten als Beweismittel

Juristisch formuliert:

Es entstehen

„elektronische Dokumente“

iSd Art. 3 Nr. 35 eIDAS VO (VO (EU) 910/2014).

Verfassungsrechtliche Anforderungen

- Faires Verfahren (Art. 6 Abs. (1) EMRK)
- Rechtsstaatsprinzip (Art. 20 Abs. (3) GG) iVm den Grundrechten

à Tatsachenfeststellung nachvollziehbar und nicht willkürlich

à Einhaltung der Prozessordnungen

à Recht auf Beweis

à Art. 46 eIDAS-VO: Gerichte müssen elektronische Dokumente annehmen und würdigen

Allerdings:

Herausforderungen bei der Beweiswürdigung aufgrund technischer Sachverhalte

Technische Anforderungen

- Beweismittel identifizieren
- Beweismittel sichern
- Beweismittel aufbewahren:
  - unveränderbar "Chain of Custody“
  - lesbar

Nadel im Heuhaufen

Datenmenge und Bandbreite

WordPerfect 1.0…

Lesbar aufbewahren

Ein anderer Vortrag

Beweismittel identifizieren

- Physisch identifizieren
- Als Beweismittel erkennen

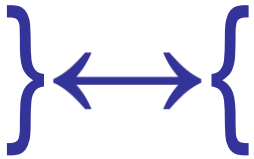
- Zugang erlangen

Beweismittel identifizieren

- Datenmenge
  - Mit Cloud / Datenträgern:
    counter forensics durch schiere Menge
- Verschlüsselung
  - Unterscheiden verschlüsselter von Zufallsdaten
- Steganographie
  - Detektion Steganograpie Regelmäßig Immenser Aufwand
  - Sonderformen
    - Covert Channels
    - Polyglotte Dateien
    - Tunnel

Beweismittel auswerten

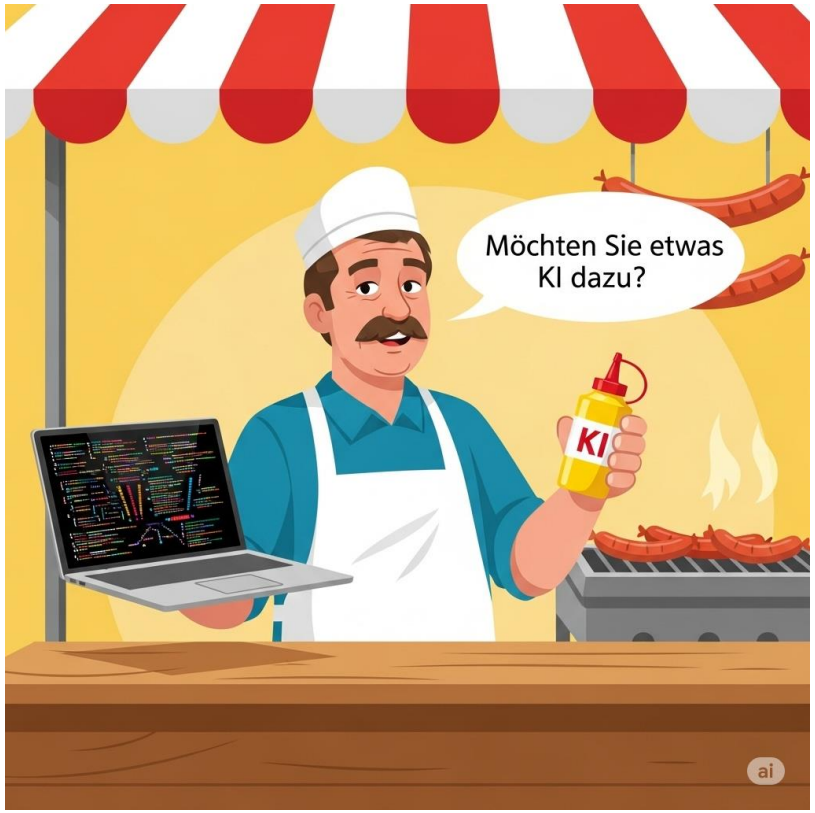
- Datenmenge
- Verschlüsselung
- Steganographie
- Obfuskation
- Datenformate
- Dateiformate
- Datenträgerformate
- Gerätespezifika
- Maschinensprachen
- Verkapslung
- …



- Fachkunde
- Erfahrung
- Stand der Wissenschaft
- Prüfbarkeit
- Dokumentation
- …

Wann ist ein Forensiker ein Forensiker?

- Keine verbindliche Qualifikation
  - Vom X-Ways-Klicker bis zum Reverse-Engineer
  - Gerne mit etwas KI
- Risiko:
  - Unverstandene Tools
  - Faktisch automatisierte Entscheidung (obwohl „vom Mensch“)
- Mehr dazu:
  - Andresen/Eggendorfer, Vom Fach, INF 4/24



Chain of Custody - Unverändert von Quelle bis heute

- „Lokal“
  - kryptographisch sicherer Hash
  - Sorgfältig dokumentiert
- Übertragung:
  - kryptographisch sicherer Hash
  - geschützt durch Private Key

} Digitale Signatur

Grenzen von Signaturen

- Aktive Inhalte (wie JavaScript) können
  - die Darstellung / Inhalte ändern
  - sind Teil des Signierten
- Darstellungsänderungen können Signaturen daher nicht erfassen

- Randnotiz:
  Digitalisieren heißt nicht, analoge Prozesse 1:1 abzubilden.

Vorgaben im Zivilprozess

Sachverständiger **A**ugenschein **P**arteivernahme **U**rkunde **Z**euge

Elektronische Dokumente:
§ 371 Abs. (1) S. 1 ZPO

Beweisantritt | Beweiserhebung | Beweiskraft

Beweisantritt: § 371 Abs. 1 S. 1 ZPO

- Benennung des Beweisthemas
- Vorlage oder Übermittlung der Datei an das Gericht
  Nicht: Übermittlung des PDF-Ausdrucks von E-Mails

- Probleme bei der Vorlage/Übermittlung an das Gericht:
  - Formate und Datenmengen per beA begrenzt
  - IT-Sicherheitsrisiken bei schadhaften Dateien
  - Authentizität bei Angabe von URL oder Vorlage von Screenshots

Beweiserhebung

- Augenschein: Sinneswahrnehmung des Gerichts

- Interessant:
  - Hinzuziehung von Sachverständigen (§ 372 Abs. (1) ZPO) zur erschöpfenden Auswertung des Beweismittels
  - Anwesenheit der Parteien und ihrer Privatgutachter zulässig, § 357 Abs. (1) ZPO

Beweiskraft

Erst bei der Beweiskraft unterscheidet die ZPO:

- §§ 371a, 371b ZPO: Dateien mit qualifizierter elektronischer Signatur
  - à Beweiswürdigung wie Urkunde, wobei der Signierende als Verfasser gilt

- Dateien ohne qualifizierte elektronische Signatur:
  Freie Beweiswürdigung, § 286 ZPO
  - à Relevanz einer fortgeschrittenen elektronischen Signatur?
  - à „Festschreibung“ der Beweiskraft durch Beweissicherung, § 485 ZPO?

Vorgaben im Strafprozess (1)

- Im Ermittlungsverfahren:
  - Vorgaben der StPO bei Datenerhebung und –Auswertung
  - Herausfordernd: Auswertung großer Datenmengen
  - Aktuelles Sonderproblem: Unterstützung durch US-Anbieter Palantir, obwohl der Palantir-Quellcode mangels Offenlegung nicht unabhängig prüfbar ist
  - Keine gesetzlichen Regelungen zur Authentizität der polizeilich bearbeiteten Ermittlungsdaten

Vorgaben im Strafprozess (2)

- In der Hauptverhandlung:
  - Soweit elektronische Daten verlesbar sind: Urkundbeweis (§ 249 Abs. (1) S. 2 StPO)
  - Im Übrigen: Augenschein (z.B. Fotos, Videos oder Audio-Dateien) oder: Ermittlungsbeamte als Zeuge über die Auswertung der Dateien
  - Beweiswürdigung nach freier Überzeugung, § 261 StPO

  Spätestens hier stellen sich indes Fragen der Authentizität und Integrität der elektronischen Beweismittel

Vorgaben im Verwaltungsrechtsstreit (1)

- Im vorausgehenden Verwaltungsverfahren:
  - Amtsermittlung, Abs. (1) § 24 VwVfG
  - Keine Bindung an die Einteilung der Beweismittel aus ZPO und StPO, § 26 VwVfG
  - „elektronische Äußerungen“, § 26 Abs. (1) Nr. 2 VwVfG
  - i.Ü. ist Sachverhaltsermittlung aktenkundig zu machen, § 24 VwVfG
  - Besonders relevant für technische Fehler bei der Ermittlung und Auswertung: § 44a S. 1 VwGO

    Nur relevant, wenn sie die Nichtigkeit oder materielle Rechtswidrigkeit der Verwaltungsentscheidung begründen

    i.Ü.: Verfahrensfehler unbeachtlich, wenn sie die Sachentscheidung nicht beeinflusst haben, § 46 VwVfG

Vorgaben im Verwaltungsrechtsstreit (2)

- Im Gerichtsprozess:
  - Vollumfängliche und eigenständige Prüfung durch das Gericht, § 86 VwGO
    - à Authentizität und Integrität elektronischer Beweismittel sind
      - ➢ Gegenstand des Verwaltungsrechtsstreits (im Rahmen des § 44a VwGO)
      - ➢ von den Prozessbevollmächtigten kritisch zu hinterfragen (insbesondere bei der Einsicht in die Akten der Behörde)
  - Im Übrigen: Verweis auf Vorgaben der ZPO (§ 98 VwGO).

Zusammenfassung und Fazit

- Vorlage und Auswertung elektronischer Beweismittel in allen Gerichtszweigen ein Gebot des fairen Verfahrens und des Rechtsstaats
- Immanente Risiken: Fehlende Authentizität und Integrität
- Expertise der Informatik für erschöpfende Auswertung elektronischer Beweismittel erforderlich
- Im Zivilprozess: Vorlage von Dateien zum Augenschein
- Im Strafprozess: Integrität und Authentizität der Daten aus dem Ermittlungsverfahren prüfen
- Im Verwaltungsrechtsstreit: Fehler bei Datenerhebung nur bei Auswirkung auf die Sachentscheidung.
- Wünschenswert: verbindliche Standards und technisches Know-How im Umgang mit elektronischen Beweismitteln

Kontakt

Dr. Florian Deusch
Rechtsanwalt und
Fachanwalt für IT-Recht

Anwaltskanzlei Dr. Gretter
Eisenbahnstraße 41
88212 Ravensburg

mailrae@bjkgretter-rae.de
http://www.bjkgretter.de

Professor Dr. Tobias Eggendorfer
Professor für Sicherheit in vernetzten Anwendungen

TH Ingolstadt
Fakultät für Informatik
Esplanade 10
85049 Ingolstadt

https://www.eggendorfer.info