www.richterzeitung.ch

Claudia Schreiber / Daniel Kettiger

Elektronische Beweismittel – neue Herausforderungen

Bereits heute werden elektronische Beweismittel verwendet und die Bedeutung der elektronischen Beweismittel wird mit der anstehenden Digitalisierung von Gerichts-Verwaltungsverfahren noch zunehmen. Dieser Beitrag versucht, sich den elektronischen Beweismitteln aus verschiedenen Blickwinkeln anzunähern, u.a. aus der Sicht deren Entstehung, aus der Sicht des Beweisrechts oder aus der Sicht der Praxis. Die Autorin und der Autor zeigen dabei die Tücken im Umgang mit elektronischen Beweismitteln auf und geben Anregungen zum sicheren Umgang mit diesen.

Beitragsart: Science

Zitiervorschlag: Claudia Schreiber / Daniel Kettiger, Elektronische Beweismittel – neue Herausforderungen, in: «Justice - Justiz - Giustizia» 2024/2

ISSN 1661-2981, richterzeitung.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

EDITIONS WEBLAW

Inhaltsübersicht

1. Einleitung

[1] Elektronische Beweismittel gewinnen an Bedeutung. Einerseits, weil Beweismittel immer häufiger (nur) in elektronischer Form vorliegen. Und andererseits, weil das geplante Obligatorium für elektronische Eingaben für die berufsmässige Vertretung im Rahmen des Vorhabens Justitia 4.0 bzw. des BEKJ[1] und die damit einhergehende Verpflichtung zur Führung elektronischer Verfahrensakten auf Behörden- bzw. Gerichtsseite dazu führen wird, dass elektronische Beweismittel künftig ausschliesslich in elektronischer Form in Verfahren eingespeist werden. Zudem werden allenfalls in Papierform bestehende Beweismittel künftig zur Einreichung in eine elektronische

[1] Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz, Ende April 2024 in Beratung in der Kommission des Ständerates, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20230022, zuletzt konsultiert am 22. April 2024.

Form überführt werden müssen. Dies führt dazu, dass sich der Umgang mit elektronischen Beweismitteln in der anwaltlichen, ebenso wie der gerichtlichen und behördlichen Praxis verändern wird. So werden das BEKJ und die Plattform Justitia.swiss und ähnliche Austauschplattformen des elektronischen Rechtsverkehrs auf kantonaler Ebene und auf Bundesebene *nolens volens* nicht nur eine «PDF-isierung» der Justiz auslösen, sondern in Einklang mit der internationalen Entwicklung und wissenschaftlichen Erkenntnissen nach und nach eine effektive Umstellung der Justiz auf elektronische Aktenführung zur Folge haben, die auch eine adäquate Analyse, Auswertung und Würdigung elektronischer Beweismittel umfasst.

[2] In diesem Aufsatz gehen wir der Frage nach, was elektronische Beweismittel sind (Ziffer 2), in welcher Form wir sie aktuell antreffen, wie Behörden und Gerichte mit ihnen umgehen und inwiefern sie im Straf-, Zivil- und Verwaltungsverfahren zulässig sind (Ziffer 3). Aus Sicht des Beweisrechts beleuchten wir die Fragen der Beweistauglichkeit und Vertrauenswürdigkeit sowie der Einreichungsform von elektronischen Beweismitteln und wir erörtern, welche Kenntnisse Richterinnen und Richter aufweisen sollten, um im Rahmen der freien Beweiswürdigung elektronische Beweismittel würdigen zu können (Ziffer 4). In Ziffer 5 schliesslich formulieren wir Empfehlungen für den praktischen Umgang mit elektronischen Beweismitteln, sowohl in der Advokatur wie bei Behörden und Gerichten. Ziffer 6 enthält zum Schluss einen Exkurs über die Beweisaufnahme in Verhandlungen mittels elektronischer Mittel zur Bild- und Tonübertragung.

2. Grundlagen

2.1. Begriffsvielfalt und (Be-)Deutungsvielfalt

[3] Befasst man sich mit elektronischen Beweismitteln, stösst man zwangsläufig auf zahlreiche Begriffe, die im Kontext mit elektronischen Beweismitteln und mit der Digitalisierung von Verwaltungs- und Gerichtsverfahren verwendet werden. An sich wäre es gerade an der Schnittstelle von Recht und Informatik wichtig, präzise und in beiden Disziplinen anerkannte Begriffe verwenden zu können. Eine kurze Analyse zeigte auf, dass es kaum möglich ist, einheitliche Begriffe zu finden und in diesem Beitrag zu verwenden. Schon nur die Begriffe «Daten» und «Information» und deren Unterscheidung bereiten Schwierigkeiten. In der Rechtswissenschaft besteht insbesondere kein einheitlicher Informationsbegriff.[2] Und obwohl heute täglich von Digitalisierung gesprochen wird, fehlt es an einem griffigen und allgemein anerkannten Begriff von «digital» bzw. «Digitalisierung».[3] Angesichts dieser Ausgangslage würde es den Rahmen der vorliegenden Abhandlung sprengen, dieser eine Liste mit Begriffsbestimmungen voranzustellen. Wo es notwendig ist, wird nachfolgend im Kontext auf Begrifflichkeiten hingewiesen.

[4] Die Begriffsvielfalt und die Bedeutungsvielfalt einiger Begriffe können beim Arbeiten mit elektronischen Beweismitteln zu Missverständnissen führen und erfordern deshalb im Umgang

2 Vgl. Daniel Kettiger, Rechtliche Aspekte der aktiven Umweltinformation, Gutachten zuhanden des Bundesamtes für Umwelt (BAFU), Umwelt-Wissen Nr. 1003, Bundesamt für Umwelt, Bern 2010, S. 16, mit Hinweisen.

3 So definiert beispielsweise das Gesetz über die digitale Verwaltung (DVG) des Kantons Bern (BSG 109.1) Digitalisierung als «die Form der Erfüllung von Aufgaben mit ICT-Mitteln» und meint dann eigentlich elektronische Form, wenn der Begriff «digitale Form» verwendet wird. Die neuste Bundesgesetzgebung verwendet gleich bedeutend den Begriff «elektronische Mittel zur Erfüllung von Behördenaufgaben» und statt von «ICT-Mitteln» wird von IKT-Mitteln gesprochen. In einem anderen kantonalen Gesetz wird «elektronisch einlesen» mit «Digitalisierung» gleichgesetzt.

– gerade in juristischen Texten – eine gewisse Sorgfalt. Leider lassen bestimmte neuere Gesetzestexte auf Bundes- und Kantonsebene diese Sorgfalt vermissen.

2.2. Was sind elektronische Beweismittel?

[5] Beginnen wir mit der Abgrenzung zwischen «digitalen» und «elektronischen» Beweismitteln. Im Alltagsgebrauch werden diese beiden Adjektive nicht selten synonym verwendet, während ihre Abgrenzung die Wissenschaftler verschiedener Disziplinen schon lange beschäftigt[4]. Wir ziehen zur Abgrenzung den vom Canadian General Standards Board herausgegebenen Standard «Electronic records as documentary evidence» (CAN/CGSB-72.34-2017)[5] bei, der elektronische Unterlagen (electronic records) und digitale Unterlagen (digital records) wie folgt unterscheidet: «Whereas the term ‹digital records› refers to a record composed of discrete binary values aggregated into one or more bit stream, the term ‹electronic record› encompasses any digital record as well as any analogue record that is carried by an electrical conductor and requires the use of electronic equipment to be made intelligible to an individual.»[6]

[6] Die ISO-Norm 27042:2015 wählt den engeren Begriff digital evidence. Gemäss dieser ISO-Norm sind digitale Beweismittel «information and data, stored oder transmitted in binary form which has been determined, through the process of analysis, to be relevant to the investigation»[7]. Diese Definition engt den Begriff zusätzlich ein, indem nur relevante Beweismittel aus der Gesamtmenge der vorhandenen «potential digital evidence» gemeint sind.[8] Carrier engt den Begriff noch weiter ein, indem er die Erfordernis der Zuverlässigkeit hinzufügt: Digitales Objekt, das zuverlässige Informationen enthält, die eine Hypothese unterstützen oder widerlegen.[9]

[7] Der Electronic Evidence Guide des Council of Europe hält folgende Definition für elektronische Beweismittel vor: «Electronic evidence is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the Internet. The information it contains does not possess an independent physical form.»[10] Diese Definition schliesst Datenträger und analoge Unterlagen ebenfalls aus, stützt sich aber umgekehrt auf die unmittelbare Quelle der Beweismittel, um sie von anderen Beweismitteln abzugrenzen.

---

4 Bspw. Johan Haugeland, Analog und Analog, Bielefeld 2015, https://www.degruyter.com/document/doi/10.1515/9783839402542-002/html?lang=de, zuletzt konsultiert am 22. April 2024, bezugnehmend auf David Lewis, Analog and Digital, in: Nous, Jg. 5 (1971), S. 321–327, https://www.andrewmbailey.com/dkl/Analog_and_Digital.pdf, zuletzt konsultiert am 24. April 2024.

5 National Standard of Canada, Electronic records as documentary evidence, CAN/CGSB-72.34-2017, März 2017, S. iv, https://publications.gc.ca/collections/collection_2017/ongc-cgsb/P29-072-034-2017-eng.pdf, zuletzt konsultiert am 22. April 2024.

6 Französische Version: «En effet, les ‹enregistrements numériques› se composent de valeurs binaires discrètes réunies en une ou plusieurs chaînes de bits, tandis que les ‹enregistrements électroniques› comprennent les enregistrements numériques ainsi que les enregistrements analogues transmis par conducteurs électriques qui nécessitent de passer par un équipement électronique pour être intelligibles à l'être humain.» Enregistrements électroniques utilisés à titre de preuves documentaires, Norme Nationale du Canada, CAN/CGSB-72.34-2017, März 2017, S. iv, https://publications.gc.ca/collections/collection_2017/ongc-cgsb/P29-072-034-2017-fra.pdf, zuletzt konsultiert am 22. April 2024.

7 Vgl. ISO/IEC 27042:2015, Ziffer 3.5.

8 Vgl. ISO/IEC 27042:2015, Figure 2, Digital evidence status transitions.

9 Brian Carrier, File System Forensic Analysis, Boston 2014, S. 4.

10 Council of Europe, Electronic Evidence Guide, Version 2.1, 2020, S. 12, https://rm.coe.int/0900001680a22757, zuletzt konsultiert am 22. April 2024.

[8] Seitens des EVIDENCE Projects schliesslich wird eine sehr breite Definition vorgeschlagen: «Electronic Evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on or transmitted by any electronic device. Digital evidence is that Electronic Evidence which is generated or converted to a numerical format.»[11]

[9] Im vorliegenden Beitrag wird auf diese breitgefasste Definition des Begriffs elektronische Beweismittel abgestützt, ohne Eingrenzungen hinsichtlich Form der Unterlagen, Eignung, Zulässigkeit in bestimmten Verfahren sowie ohne Einschränkungen hinsichtlich Quellen und Status im Verfahren (Rohdaten, Arbeitsdaten, in ein Verfahrensdossier integrierte Daten etc.) sowie Art des Verfahrensdossiers[12]. Diese breite Definition wählen wir nicht zuletzt deshalb, weil hier auch der Entstehungs-, Sicherungs- und Prüfprozess von elektronischen Beweismitteln thematisiert werden soll, weshalb auch Datenträger und Hilfsmittel in die Definition der elektronischen Beweismittel eingeschlossen sind.

[10] Der Verständlichkeit halber werden an dieser Stelle einige Praxisbeispiele elektronischer Beweismittel aufgeführt:[13]

- Elektronisches Beweismittel aus analoger Quelle: Scan-Output eines Videotapes, Scan-Output eines Papierdokuments, Scan-Output eines Mikrofilms.
- Elektronisches Beweismittel aus physischen, nicht-elektronischen Quellen: Scan-Output einer Waffe.
- Elektronisches Beweismittel aus digitalen Quellen: von einer Digitalkamera gespeicherte Datei.
- Datenträger als elektronische Beweismittel: Harddisk, Mediakarte, USB-Stick etc.
- Hilfsmittel und ergänzende Daten zu elektronischen Beweismitteln: CCTV-Kamera inkl. Zubehör (Kabel, Speichermedium etc.).

2.3. Entstehung von elektronischen Beweismitteln

[11] Elektronische Beweismittel nach der oben breit gefassten Definition können auf unzählige Arten entstehen. Für die weiteren Ausführungen unterscheiden wir vier in der Praxis relevante Entstehungsarten von elektronischen Beweismitteln. Drei der vier Kategorien (b, c, d) lehnen sich an die Verordnung über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV) vom 8. Dezember 2017 an.

- Kategorie E: Digital-born elektronische Beweismittel, die nicht über ein physisches oder analoges Ausgangsobjekt verfügen. Beispiele sind Dateien, die in einer Textverarbeitungssoftware erstellt und von einem Computer gespeichert wurden.

11 EVIDENCE Project, European Informatics Data Exchange Framework for Courts and Evidence, EVIDENCE Semantic Structure, Version 3.16, 21. September 2015, S. 16, http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d2-1-410.pdf, zuletzt konsultiert am 22. April 2024.

12 Verfahrensdossiers liegen auch bei an sich in Papierform geführten Dossiers vielfach in hybrider Form vor, indem sie beispielsweise zugezogene Vorakten, Beweismittel und weitere Unterlagen enthalten, die auf CD-ROM, DVD oder anderen Datenspeichern wie USB-Sticks in das Papierdossier eingefügt werden.

13 Vgl. dazu die Ausführungen EVIDENCE (Fn. 11), S. 23.

- Kategorie EzuE: Elektronische Beweismittel, die eine oder mehrere Konvertierungen oder Aufzeichnungen erfahren haben (bspw. Konvertierung einer E-Mail aus dem .eml-Format (MIME type message/rfc822[14]) in eine PDF-Datei, Erstellung eines Screenshots einer Webseite). Dieser Vorgang entspricht sinngemäss dem Vorgehen gemäss Art. 14 Abs. 1 EÖBV. Nachfolgend wird der Vorgang als EzuE-Vorgang bezeichnet. Den Input nennen wir in der Folge im ersten Fall der Konvertierung «Ausgangsdatei» und den Output «konvertierte Datei», im zweiten Fall der Aufzeichnung nennen wir den Output «elektronische Aufzeichnung».
- Kategorie PzuE: Elektronische Beweismittel, die durch Scannen von Papierunterlagen (und anderen physischen Objekten) entstanden sind. So beispielsweise der Scan einer Urkunde im Hinblick auf die Erstellung einer elektronischen Ausfertigung. Dieser Vorgang entspricht sinngemäss dem Vorgehen gemäss Art. 13 EÖBV. In der Folge nennen wir den Input «Papierdokument» und den Output «Scan-Output».
- Kategorie EzuPzuE: Elektronische Beweismittel, die mittels Trägerwechsel (Druckvorgang) in Papierform überführt (EzuP-Vorgang) und in einem zweiten Schritt wieder digitalisiert wurden (PzuE-Vorgang). Der erste Schritt entspricht sinngemäss dem Vorgehen gemäss Art. 17 EÖBV, der zweite Schritt wiederum Art. 13 EÖBV. Der Arbeitsvorgang EzuPzuE kann auch zusätzliche Trägerwechsel gleicher Art enthalten und kann letztlich aus einer beliebigen Kette von Trägerwechseln und Konvertierungen bestehen.

[12] Diese und ähnliche Kategorisierungen finden sich auch andernorts. Der kanadische Standard CAN/CGSB-72.34-2017 nennt ähnliche Unterscheidungen wie die EÖBV[15]: Demnach kann eine Geschäftsablage (records system) folgende Typen von Unterlagen enthalten: a) Originale Papier-Unterlagen («original paper records»), diese entsprechen dem Input des PzuE-Vorgangs. b) Elektronische Unterlagen («electronic records»), diese entsprechen den oben beschriebenen digital-born elektronischen Unterlagen der Kategorie E. c) Mikroverfilmte, gescannte oder fotografierte Unterlagen («microfilmed, digitized, or imaged records»), die gescannten und fotografierten Unterlagen entsprechen dem Vorgang PzuE. d) Beglaubigte Ausdrucke von elektronischen Unterlagen («relied upon printouts' of electronic records»), diese entsprechen dem Vorgang EzuP bzw. Art. 17 EÖBV. Auf die praktische Bedeutung der Unterscheidung der verschiedene Entstehungskategorien wird in den folgenden Kapiteln ausführlich eingegangen.

[13] Den Begriff der «Kopie» verwenden wir in der Folge nur für den PzuP-Vorgang, also die Erstellung einer physischen Papier-Kopie eines Papierdokumentes.

2.4. Eigenschaften von elektronischen Beweismitteln

2.4.1. Einleitung

[14] Elektronische Beweismittel zeichnen sich durch spezifische Eigenschaften aus, die sie von anderen Beweismitteln unterscheiden. In den Ziffern 2.4.2 bis 2.4.8 beschreiben wir einige Ei-

14 Mehr zu diesem Dateiformat vgl. bspw. Sustainability of Digital Formats: Planning for Library of Congress Collections, https://www.loc.gov/preservation/digital/formats/fdd/fdd000388.shtml, zuletzt konsultiert am 22. April 2024.

15 Vgl. Zusammenstellung in National Standard of Canada (Fn. 5), S. 9, hier ohne den Typ «records created through EDI (electronic data interchange)» aufgeführt.

genschaften von praktischer Bedeutung. Zunächst führen wir aber die «major inconveniences» auf, die das EVIDENCE-Projekt elektronischen Beweismitteln zuschreibt:[16]

- Mangel/Fehlen einer angemessenen und systematischen Regulierung (scant/lack of suitable and systematic regulation)
- Mangel an Rechtssprechung (scant jurisprudence)
- Notwendigkeit spezifischer Kenntnisse, nicht nur um die Natur elektronischer Beweise zu verstehen, sondern auch, um zu wissen, wie man Daten verarbeitet und wie man die spezifischen Gesetze zur Verarbeitung interpretiert (necessity for specific knowledge not only to understand the nature of the electronic evidence but also how to process the data and how to interpret specific processing laws)
- Schwierigkeit, einem Gericht elektronische Beweise in verständlicher Form vorzulegen (difficulty to present electronic evidence at court in an understandable manner)
- Schwierigkeit, elektronische Beweismittel in Verfahren einzubringen, falls Richter höhere Anforderungen stellen als an herkömmliche Beweismittel (difficulty electronic evidence to be accepted at court where judges ask for more guarantees than with traditional evidence)
- Mangelhafte technische Infrastruktur in den Justizbehörden (lack of technical infrastructure in judicial departments)
- hohe Kosten für die Prüfung und Auswertung der Informationen (high cost of examining and interpreting the information)
- Schwierigkeiten beim Nachweis der Authentizität, Zuverlässigkeit und Herkunft der Daten (difficulty in proving authenticity, reliability and origin of data)
- Flüchtigkeit der Daten und leichte Manipulierbarkeit (volatility of data and ease of manipulation)
- Schwierigkeiten der Zurechnung zur Täterschaft (difficulty in identifying the perpetrator of the crime)
- Schwierigkeiten bei der Aufbewahrung, Erhaltung und Speicherung elektronischer Daten (difficulty in conserving, preserving and storing electronic data)
- Schwierigkeiten bei der Festlegung des Beweiswerts der elektronischen Beweismittel (difficulty in establishing the legal value of the electronic evidence)
- fehlende rechtliche Unterstützung und Zertifizierungsmodelle (lack of legal support and certification models)

2.4.2. Papierdokumente und Dateien

[15] Elektronische Beweismittel zeichnen sich zunächst dadurch aus, dass sie in elektronischer Form vorliegen (beispielsweise als Datei). Dateien und Papierdokumente sind nicht dasselbe. Eine Datei ist nicht ein Stück Papier im Bildschirm. Ein Stück Papier besteht aus einem physischen Trägermaterial und davon unterscheidbarem Text und/oder Bilddarstellungen. Eine Datei gruppiert Daten, die von unterschiedlichen Softwares auf unterschiedliche Art und Weise interpre-

16 EVIDENCE European Informatics Data Exchange Framework for Court and Evidence, http://www.evidenceproject.eu/about-evidence/concept-and-objectives.html, zuletzt konsultiert am 22. April 2024.

tiert und dargestellt werden.[17] Ein Papierdokument kann ohne Hilfsmittel gelesen werden und präsentiert sich jedem Leser und jeder Leserin gleich, während eine Datei nur mit Hilfsmitteln betrachtet werden kann.[18]

[16] Beispielhaft zeigt die EÖBV auf, dass die versuchte Gleichstellung eines Papierdokumentes und einer Datei in die Irre führt.[19] So schlägt die EÖBV für den PzuE-Vorgang (Beglaubigung) das Verbal[20] vor, wonach «das elektronische Dokument mit dem Papierdokument» übereinstimme. Technisch betrachtet ist dies aber gerade nicht möglich. Das in der EÖBV vorgeschlagene Verbal ist deshalb untauglich, weil es unter anderem nicht darlegt, «welche Eigenschaften der [...] Datei nicht Teil der Beurkundung sind, namentlich alle durch den Scanvorgang, nachfolgende Bearbeitungen der Datei [...] notgedrungen hinzugefügten Eigenschaften»[21] oder fakultativ hinzugefügte Eigenschaften wie OCR-Layer[22]. Dasselbe gilt für den EzuP-Vorgang und den EzuE-Vorgang. Bei beiden Vorgängen werden Dateien nach meist willkürlichen, intransparenten Kriterien verändert dargestellt bzw. verändert. Beim EzuP-Vorgang gehen beim Druckvorgang[23] zahlreiche Eigenschaften einer Datei verloren, während bei der Konvertierung von Dateien in

17 Zum Unterschied electronic document im engeren Sinn und paper document ausführlich: Quynh Anh Tran, Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective of UNCITRAL, the European Union, Germany and Vietnam, Cham 2022, S. 90 f.

18 Vgl. dazu Carsten Momsen/Nils Hercher, Digitale Beweismittel im Strafprozess. Eignung, Gewinnung, Verwertung, Revisibilität, Ziffer 4, Absatz 2, http://strafverteidigervereinigungen.de/Material/Themen/Technik%20&%20Ueberwachung/37_momsen.pdf, zuletzt konsultiert am 22. April 2024, sowie Michael Knopp, Rechtliche Perspektiven zur digitalen Beweisführung, in: Informatik 2009 – Im Focus das Leben, 2009, S. 2, https://cs.emis.de/LNI/Proceedings/Proceedings154/gi-proc-154-116.pdf, zuletzt konsultiert am 22. April 2024: «Zur Würdigung digitaler Beweismittel» sind «stets Vermittlungsschritte, sei es durch Hardware und Software oder zusätzlich durch Sachverständige» erforderlich.

19 Claudia Schreiber/Fabian Mörtl, Stolpersteine bei Beglaubigungen nach EÖBV, in: 6. Schweizer Notariatskongress, Aktuelle Themen zur Notariatspraxis, 2022, S. 65.

20 Gemäss Art. 2 Bst. c EÖBV ist ein Verbal ein Vermerk, in dem die Urkundsperson die Feststellungen festhält, die sie bei der Erstellung von elektronischen öffentlichen Urkunden und elektronischen Beglaubigungen macht.

21 Schreiber/Mörtl (Fn. 19), S. 65.

22 Beim OCR-Prozess werden gedruckte oder mit Schreibmaschine geschriebene alphanumerische Zeichen gescannt, erkannt und in Code umgewandelt, vgl. Andrew Butterfield/Gerard Ekembe Ngondi/Anne Kerr (Hrsg.), A Dictionary of Computer Science, Oxford 2016, S. 379. Die erkannten Zeichen werden entweder direkt in das verarbeitete Bild integriert oder als separater oder mehrere separate Layer, also als unsichtbare Textebene(n), über der Bildebene eingeblendet. Das Problem der Optical Caracter Recognition (OCR)-Layers ist insbesondere in der notariellen Praxis im Kontext von Beglaubigungen von Bedeutung: elektronische Ausfertigungen nach Art. 11 EÖBV werden in der Praxis durch einen Scanvorgang hergestellt, der mit oder ohne OCR-Layer erstellt werden kann. In der Praxis wird bei Einfügen eines OCR-Layers kaum je geprüft, ob der im OCR-Layer hinzugefügte Text der Papier-Urschrift (Urkunde) entspricht, weshalb das Verbal eigentlich mit dem Hinweis zu ergänzen wäre, dass der OCR-Layer nicht Teil der Beglaubigung ist. Die empfangenden Behörden (Handelsregister-, Grundbuchämter) entnehmen aber trotz der ungeklärten Situation nicht selten Text aus dem OCR-Layer und fügen diesen Text händisch in die entsprechenden Registersysteme ein. Dies ist problematisch, weil sowohl bei der Erstellung des OCR-Layers wie bei der Wiedergabe des Textes vor Erstellung des OCR-Layers Fehler auftreten können. Vgl. KOST Koordinationsstelle für die dauerhafte Archivierung elektronischer Unterlagen, JBIG2-Komprimierung, https://kost-ceco.ch/cms/dl/2eca43a3b8a7cab30bcd6b003dd1e3cc/Xerox_JBIG2_Studie_v1.2.pdf, zuletzt konsultiert am 22. April 2024.

23 Beim laienhaften Ausdrucken einer PDF-Datei werden beispielsweise folgende Dateiinhalte u.U. nicht mitgeliefert: Metadaten der Datei, eingebettete Inhalte und angehängte Dateien, Skripts, ausgeblendete Ebenen, eingebettete Suchindexe, gespeicherte Formulardaten, Prüfungs- und Kommentardaten, ausgeblendete Daten aus vorherigen Speicherungen, geschwärzte Texte und Bilder, «versteckte» Texte (bspw. weisser Text in weisser Farbe oder schwarzer Text auf schwarzem Hintergrund), ausgeblendete Kommentare im Textkörper, nicht referenzierte Daten, Links, Aktionen und Javascript, Informationen zu elektronischen Signaturen sowie überlappende Objekte sowie durch Signature entstandene Versionen. Beim laienhaften Ausdrucken einer E-Mail werden u.U. die folgenden Dateiinhalte nicht mitgeliefert: Source Code der E-Mail inkl. Angaben zum Header, html-Bestandteile, Links, nachzuladende Inhalte, Informationen zu allfälligen Mailsignaturen, Absender- und Adressatenadressen (wenn nur Alias-Bezeichnungen gedruckt werden), etc.

andere Dateiformate diese Dateien verändert werden, indem – ebenfalls meist willkürlich[24] – gewisse Informationen entfernt und andere Informationen hinzugefügt werden.[25]

2.4.3. Eine Datei – zahlreiche Wahrnehmungen

[17] Je nachdem, welche Hilfsmittel (Hardware, Software und deren Konfiguration) benutzt werden, um eine Datei sichtbar zu machen, ändert sich auch deren Darstellung und damit auch die (menschliche) Wahrnehmung dieser Datei. So werden beispielsweise sowohl elektronische Signaturen[26] in PDF-Dateien wie die damit potentiell einhergehenden Versionierungen in vielen PDF-Viewern nicht erkennbar gemacht[27], die elektronische Signatur in S/MIME-signierten E-Mails kann nur von S/MIME-fähigen E-Mail-Clients ausgewertet werden[28] und Geodaten werden je nach Darstellungsmodell[29] in einem Viewer oder bei Direkterstellung einer Ansicht in einem PDF-Dokument anders dargestellt. Die oft geäusserte Ansicht, dass der Inhalt einer Datei daraus bestehe, «was ein Computer-Nutzer wahrnehmen kann», ist vor diesem Hintergrund nicht haltbar.

[18] Gerade die Dateiformat-Gruppe PDF, die eine bunte Sammlung von verschiedenen PDF-Versionen und PDF-Subtypen umfasst (PDF/A-1a, -1b, -2a, etc.), wird in der Praxis gleichzeitig unterschätzt und überschätzt. Unterschätzt, indem noch immer viele Akteure auch in der Justiz davon ausgehen, eine PDF-Datei sei in etwas dasselbe wie ein Stück Papier[30] und sei auch hinsichtlich Malware eher unproblematisch[31]. Überschätzt, indem PDF-Dateien Eigenschaften zugeschrieben werden, die sie nicht aufweisen: Namentlich die Unveränderbarkeit bzw. Veränderung nur mit Spezialsoftwares sowie die betriebssystem-, software- und konfigurationsunabhängige identische Wiedergabe von PDF-Dateien[32].

---

24 Während proprietäre Spezialsoftwares für die Konvertierung von Dateien die Parameter der Konvertierung zumeist in den groben Zügen offenlegen, enthalten proprietäre Standardsoftwares oft Konvertierungsfunktionen, die kaum parametrierbar und für den Benutzer entsprechend intransparent sind. Bei Open Source Konvertierungssoftwares gibt der publizierte Programmcode detailliert Auskunft über die Konvertierungsvorgänge.

25 Beim Konvertieren werden zentrale Inhalte der Ausgangsdatei verändert. Dateikonvertierungen produzieren je nach Ausgangsformat und Zielformat und je nach Konvertierungstool und dessen Konfiguration unterschiedliche Ergebnisse.

26 Zur Abgrenzung zwischen elektronischen Signaturen und digitalen Signaturen vgl. Reto Fanger, Digitale Dokumente als Beweis im Zivilprozess, 2005, Basel/Genf/München, S. 66f.

27 Vgl. die Musterdatei https://www.advoschreiber.ch/rz/1.pdf, die drei elektronische Signaturen je mit Änderungen und in der Folge in einer PDF-Datei drei unterschiedliche Dokument-Versionen enthält. Wird diese PDF-Datei in einem Browser geöffnet, wird der Inhalt der Datei nicht korrekt wiedergegeben. Aktuelle Versionen von Adobe Reader hingegen zeigen die durch die elektronischen Signaturen entstandene Versionierung an.

28 Jörg Schwenk, Sicherheit und Kryptographie im Internet, Wiesbaden, 2014, S. 237, mit Hinweis auf den Unterschied zwischen den Datentypen multipart/signed und application/pkcs-mime smime-type=signed-data.

29 Darstellungsmodelle sind gemäss Art. 3 Abs. 1 Bst. i GeoIG «Beschreibungen grafischer Darstellungen zur Veranschaulichung von Geodaten (z.B. in Form von Karten und Plänen)». Es handelt sich also um Übersetzungen von Daten in grafische Darstellungen.

30 PDF-Dateien können je nach Subtyp eingebettete Inhalte (bspw. andere Dateien), Skripts, Links, Aktionen und Javascript, ausgeblendete Daten aus vorherigen Speicherungen, Versionierungen und viele weitere Elemente enthalten.

31 Zu dieser Thematik vgl. auch Hack 89 in: Lorenz Kuhlee/Viktor Völzow, Computer Forensik Hacks, 2012, Heidelberg, S. 282 ff.

32 So zum Beispiel das Landessozialgericht Rheinland-Pfalz in einem Urteil vom 27. September 2023 (konsultiert auf JurPC Web-Dok. 159/2023 – DOI 10.7328/jurpcb20233811159): «Maßgeblich gewährleistet das Dateiformat PDF jedoch, dass die übersandte Datei – jedenfalls nicht fahrlässig – verändert wird.» Effektiv ist es aber so, dass PDF-Dateien alleine durch ein Abspeichern verändert werden können. Vgl. dazu die Anleitung zum Urkundspersonenregister UPREG, https://oewiki.atlassian.net/wiki/spaces/UPREG/overview, zuletzt konsultiert am

2.4.4. Kontextinformationen nötig

[19] Die Prüfung der Echtheit und Integrität von elektronischen Beweismitteln ist in vielen Fällen ohne eine erweiterte Betrachtung ihres Quell- und Entstehungskontextes nicht möglich. Die Integrität einer Datei kann beispielsweise von der Integrität des Datenträgers abgeleitet werden. Weist beispielsweise ein forensisches Duplikat vor und nach der forensischen Analyse denselben Hashwert auf wie der Hashwert des duplizierten Datenträgers, lässt sich damit belegen, dass der Forensiker die Daten und die Dateien nicht verändert hat.[33] Findet sich auf dem unveränderten forensischen Duplikat auch die Datei mit dem zu vergleichenden Hashwert, so lässt sich daraus ableiten, dass die Datei seit der Erstellung des forensischen Duplikates nicht verändert wurde, auch wenn sie beispielsweise einen anderen Dateinamen trägt.[34] Regelmässig werden deshalb bei Dateien, die aus Records-Management-Systemen stammen, die sorgfältig bzw. gesetzeskonform geführt sind[35], Vermutungen hinsichtlich Integrität formuliert.[36] In dieselbe Richtung zielen Bestimmungen, die Dateien als Beweismittel nur zulassen, wenn eine befugte Person eine eidesstattliche Erklärung über Herkunft und Eigenschaften des Beweismittels abgibt.[37]

2.4.5. Original-Kopie-Logik ist nicht anwendbar

[20] Eine Besonderheit von elektronischen Beweismitteln ist zudem auch die Nicht-Anwendbarkeit der Original-Kopie-Logik, die beispielsweise bei Beweismitteln in Papierform von Bedeutung ist. Papier-Unterlagen können als Original (bspw. ein handschriftlich unterzeichneter Vertrag) oder als Kopie (eine Papierkopie des handschriftlich unterzeichneten Vertrags) als Beweismittel in ein Verfahren eingegeben werden. Kopien und insbesondere beglaubigte Kopien stellen sicher, dass der Inhalt eines Papierdokuments mit gleicher Belegwirkung und gleicher Beweiskraft faktisch an mehreren Orten verfügbar gemacht werden kann.[38] Bei elektronischen Beweismitteln gibt es weder Original noch Kopie, vielmehr kann eine Datei vervielfacht werden[39]

13. Januar 2024: «Nach der Signatur dürfen Sie keine Änderungen am Dokument vornehmen. Es gibt Programme, die das aber tun, wenn Sie beim Schliessen des PDF die Änderungen nicht ablehnen.» Zur Frage der einheitlichen Wiedergabe zitiert das Bundesverwaltungsgericht im Entscheid E-5094/2020 vom 27. März 2023, E. 4.3, das SEM mit der Behauptung: «Das Format PDF zeichne sich gerade dadurch aus, dass beim plattformübergreifenden Lesen/Drucken von Dokumenten kein Verlust von Text/keine Änderung der Formatierung erfolge.» Dies ist in dieser absoluten Formulierung nicht korrekt.

33 Vgl. Cory Altheide/Harlan Carvey, Digital Forensic with Open Source Tools, Amsterdam/Boston/Heidelberg/London 2011, S. 56.

34 Diese Schlussfolgerung ist bei gewissen Rekonstruktionsvorgängen wie dem Carving nicht zwingend. Beim Carving-Vorgang wird in einem unstrukturierten Daten-Stream nach Datei-Headern und (möglichen) Datei-Endpunkten gesucht, wobei so gefundene Substreams in Dateien exportiert werden. Die Open Source Plattform Autopsy verwendet beispielsweise das Carving-Tool Photorec (Cory Altheide/Harlan Carvey (Fn. 33) S. 58 ff. Zu dieser Thematik sowie zum Verlust der Metadaten-Informationen aus dem Dateisystem vgl. auch Hack 34 in: Lorenz Kuhlee/Viktor Völzow (Fn. 31), S. 99 ff.

35 Bspw. Canada Evidence Act (R.S.C., 1985, c. C-5), Section 31.5, https://laws-lois.justice.gc.ca/eng/acts/c-5/page-3.html, zuletzt konsultiert am 22. April 2024; vgl. auch BGE 116 IV 343, E. 7.

36 BGE 116 IV 343 vom 14. Juni 1990, E. 7. Vgl. dazu auch Vgl. Quynh Anh Tran (Fn. 17), S. 172 ff.

37 Bspw. Affidavits gemäss section 65B(4) des Indian Evidence Act (1872).

38 Schreiber/Mörtl (Fn. 19), S. 61.

39 Dieser Vorgang wird vielfach als «Kopieren» bezeichnet. So auch im Electronic Evidence Guide des Council of Europe (Fn. 18): «It can be copied without degradation: Digital information can be copied indefinitely with each copy exactly the same as the original. This unique attribute means that multiple copies of the evidence can be examined independently and in parallel by different specialists for different reasons without affecting the original.» Der National Standard of Canada (Fn. 5) hingegen bringt etwas mehr Klarheit bei der Definition des Begriffs copy, der als «duplicate of recorded information» bezeichnet wird.

und als identische Datei (Kriterium: identischer Hashwert) an beliebig vielen Orten gleichzeitig gespeichert sein und gleichzeitig genutzt werden.[40] Tran deutet dies an, kann sich aber gleichzeitig nicht ganz von der Original-Kopie-Begrifflichkeit lösen: «Furthermore, in the paper world it is possible to distinguish between the original and copies, in particular where an original document has a written signature or seal. In contrast, it may be impossible to distinguish between the original and duplications of electronic documents.»[41] Nassehi schliesslich bringt es auf den Punkt und formuliert treffend: «Die Digitalisierung stört die Idee des Originals bzw. der Identität von Objekten. [...] Gehört die Einheit eines Objektes noch zu den klassischen Kategorien der logischen Auffassung der Welt, befreien sich digitale Objekte von der Stofflichkeit ihres Trägers. [...] Das Kopieren einer Datei erzeugt tatsächlich die Datei noch einmal, und zwar ohne jeglichen Verlust. Die Kopie ist keine Kopie, weil sie mit dem Original identisch ist, das dann auch als Original verschwindet.»[42]

[21] Daraus ergibt sich in praktischer Hinsicht, dass spätestens ab Zeitpunkt der Umstellung auf das elektronische Verfahrensdossier[43] eine Veränderung von elektronischen Beweismitteln im Hinblick auf die Einreichung bzw. Integration in die Verfahrensakten keine technisch bedingte Notwendigkeit zum Inverkehrbringen, sondern aus technischer Sicht den Ausnahmefall darstellt bzw. darstellen sollte. Beispiele solcher Veränderungen sind etwa, wenn statt eines forensischen Duplikats[44] inklusive dazugehörigem Bericht nur der Polizeibericht über das forensische Duplikat in Form einer PDF-Datei oder als Ausdruck einer Datei die Verfahrensakten fliesst[45] oder wenn eine Rechtsanwältin oder ein Rechtsanwalt eine Fotodatei statt im jpg-Format[46] als PDF-Datei einreicht. Wenn elektronische Beweismittel also verändert oder verändert wiedergegeben werden und so die Überprüfung der Chain of Custody[47] vereitelt wird, muss wiederum aus technischer Sicht, aber – wie wir sehen werden – auch aus rechtlicher Sicht, die Frage aufkommen, aus welchen Gründen die Beweismittel verändert bzw. verändert wiedergegeben wurden und ob

40 Auch das neue Bundesgesetz über die Digitalisierung im Notariat vom 16. Juni 2023 (DNG) spricht von «elektronischen Originalen» und «elektronischen Exemplaren», wobei Art. 3 Bst. c letztere wie folgt definiert: «elektronisches Exemplar: ausserhalb des elektronischen Urkundenregisters vorhandene exakte Kopie des elektronischen Originals einer öffentlichen Urkunde».

41 Vgl. Quynh Anh Tran (Fn. 17), S. 91.

42 Vgl. Armin Nassehi, Muster. Theorie der digitalen Gesellschaft, München 2019, S. 132/133.

43 D.h. die massgebliche Version des Verfahrensdossiers wird elektronisch geführt. Nicht zu verwechseln mit der Erstellung von Scans von Papier-Verfahrensdossiers, deren massgebliche Form eben diese Papierform ist.

44 Beim sogenannten Imaging wird eine Harddisk oder ein anderer Datenträger byte für byte dupliziert und als forensisches Duplikat gespeichert. Vgl. dazu Joakim Kävrestad, Guide to Digital Forensics: A Concise and Practical Introduction, Cham, 2017, S. 49 f.

45 Und so ist u.U. nicht nachvollziehbar ist, ob ein elektronisches Foto effektiv auf dem Datenträger gespeichert war, ob der Datenträger korrekt forensisch gesichert und analysiert wurde, ob die Datei im allocated space des Datenträgers vorhanden war oder ob das Foto allenfalls aus dem unallocated space des Datenträgers rekonstruiert wurde. Diese Unterscheidungen sind offensichtlich relevant, sowohl in technischer wie auch rechtlicher Hinsicht. Im Entscheid 6B_763/2020 vom 23. März 2022 äussert sich das Bundesgericht zu dieser Frage und spricht in Erwägung 3.3 einem elektronischen Beweismittel den Beweismittelcharakter ab und rechtfertigt mit Verweis auf die Inhalte des Images (pornografische Bilder und Videos) die Tatsache, dass das forensische Image nicht in die Verfahrensakten gemäss Art. 107 Abs. 1 lit. a StPO aufgenommen worden sei: «Beim forensischen Image handelt es sich weder um eine Originalakte noch um das Hauptbeweismittel, sondern lediglich um eine interne Arbeitskopie der IT-Forensik (oben E. 3.2). Der Beschwerdeführer verfügte über die massgebenden und in den Akten vorfindlichen Dateien.»

46 Vorausgesetzt, die Digitalkamera speichert das Foto auch im Format image/jpeg ab.

47 Lars E. Daniel/Larry E. Daniel, Digital Forensics for Legal Professionals, New York, 2012, S. 12: «Chain of custody logs should include every instance that a piece of evidence has been touched, including the initial collection of the device storing the evidence, the transport and storage of evidence, and any time the evidence is checked out for handling by forensic examiners or other personnel. At no time should there be a break in this chain.»

die so unterdrückten, hinzugefügten oder veränderten Informationen[48] allenfalls für das Beweisverfahren relevant sein könnten.[49]

2.4.6. Leichte Veränderbarkeit, hohe Unsicherheit

[22] Gercke[50] hält fest, dass sich elektronische Beweismitteln «leicht verändern» lassen: Es bedürfe deshalb «[...] einer stärkeren Berücksichtigung der komplexen Anforderungen an die Beweisführung mit digitalen Beweismitteln.» Momsen/Hercher führen weiter aus: «Mit dieser leichten Veränderbarkeit einher geht eine hohe Unsicherheit in Bezug auf die Richtigkeit einer Tatsache, die mit der jeweiligen Datei nachgewiesen werden soll.»[51] Gerade hinsichtlich Veränderbarkeit unterscheiden sich elektronische Beweismittel, die ausnahmslos veränderbar sind[52], von anderen Beweismitteln. Und zwar auch insofern, als zwar ein gesellschaftlicher Konsens darüber herrscht, dass im Prinzip jede Person weiss oder wissen könnte, welche Manipulation eines Papierdokuments eine Veränderung darstellt und welche nicht. Welche Manipulationen aber ein elektronisches Beweismittel verändern und wie sich (auch unbeabsichtigte) Manipulationen allenfalls verhindern bzw. feststellen lassen, gehört derzeit noch nicht zum Allgemeinwissen[53], weder bei Gerichten noch in Anwaltskanzleien. Oder wie Knopp schreibt: «Für den Umgang mit digitalen Beweismitteln und den mit diesen verbundenen Gefahren fehlen die Erfahrung und der Entwicklungsprozess von teilweise hunderten von Jahren, wie sie für analoge und verkörperte Medien bestehen.»[54]

---

48 Im Fall der als PDF-Datei eingereichten elektronischen Bilddateien werden mit einer herkömmlichen Konvertierung EXIF-Daten sowie Dateimetadaten entfernt, zudem wird durch die Konvertierung eine Prüfung der elektronischen Bilddateien hinsichtlich Manipulationen erschwert.

49 Mit dem VwVG und der VeÜ-VwV liegt eine Gesetzgebung vor, welcher das neue BEKJ nicht folgen sollte: Jede Behörde kann selbst festlegen, welche Dateiformate akzeptiert werden (Art. 4). «Kann die Behörde eine Eingabe oder Beilagen nicht lesen» (Art. 5, Abs. 2 VeÜ-VwV), kann sie die Nachreichung in konvertierter Form oder Papierform verlangen. Die Folgen eines Dateiformat-Numerus clausus sind für die Anwaltschaft fatal: Rechtsanwältinnen und Rechtsanwälte werden gezwungen, elektronische Beweismittel zu verändern (konvertieren, die Behörde definiert gemäss VeÜ-VwV das Zielformat: «noch einmal in dem von der Behörde festgelegten Format senden») oder müssen aufwändige Massnahmen (Gutachten, etc.) an die Hand nehmen.

50 Marco Gercke, Der unterbliebene Schritt vom Computer- zum Internetstrafrecht, Anwaltsblatt 2012, 709–713, https://www.anwaltsblatt-datenbank.de/bsab/document/jzs-AnwBl2012080024-000_709, S. 713, zuletzt konsultiert am 22. April 2024.

51 Momsen/Hercher (Fn. 18), Ziffer 3.

52 Ausnahmslos jedes elektronische Beweismittel kann verändert werden. Es gibt keine nicht veränderbaren Dateiformate. Dass elektronische Eingaben «unveränderbar sein» müssen, wie es die Vernehmlassungsvorlage zum Gesetz über die Verwaltungsrechtspflege (VRPG-BE) vom 19. September 2022 formuliert war, muss deshalb ein frommer Wunsch bleiben. Davon zu unterscheiden sind organisatorische und technische Vorkehrungen zur Verhinderung unbeabsichtigter Veränderungen und zur Prüfung der Nichtverändertheit einer Datei in einer bestimmten Zeitperiode, sofern ein Soll- und ein Ist-Hashwert zur Verfügung stehen.

53 Als Beispiel sei hier eine Anleitung des Amts für Informatik und Organisation des Kantons Bern (KAIO) aus der Anfangszeit des elektronischen Rechtsverkehrs genannt. Diese Anleitung wies die Gerichte an, elektronisch eingereichte, mit einer qualifizierten elektronischen Signatur nach ZertES (QES) versehene Rechtsschriften in das Verfahrensdossier abzulegen, indem das Dokument in einem PDF-Viewer geöffnet und dann mit dem Befehl «Drucken als Datei» gespeichert werden sollte. Durch diesen Vorgang wurde die qualifizierte elektronischen Signatur (QES) durch das Gericht zerstört und die betroffenen Rechtsanwälte wurden – bis zur Korrektur der entsprechenden Anleitung – zur Nachreichung der Rechtsschrift in Papierform aufgefordert.

54 Vgl. dazu auch Knopp (Fn. 18), S. 2.

2.4.7. Fehlende Erzeugungs-, Umgangs- und Prüfroutinen

[23] Eine weitere Eigenschaft von elektronischen Beweismitteln ist die Tatsache, dass in der Justiz wie in vielen Anwaltskanzleien derzeit noch keine Routinen zur Erstellung, zum Umgang und zur Prüfung sowie Validierung von elektronischen Beweismitteln vorliegen. Damit fehlt derzeit auch noch ein gemeinsames Verständnis zur Frage, welche Prüfungen überhaupt und in der Folge, welche Prüfungen durch Gerichte und Rechtsanwälte selbst[55] und welche Prüfungen durch Sachverständige durchzuführen sind[56].

2.4.8. Unsichtbar für das Laienauge, Spezialsoftwares erforderlich

[24] Der Electronic Evidence Guide des Europarates führt als weitere Eigenschaft von elektronischen Beweismitteln die Tatsache auf, dass elektronische Beweismittel an Orten gespeichert sein können, die auf den ersten (Laien-)Blick nicht sichtbar sind und für deren Erkennung spezifische Softwares nötig sind: «It is invisible to the untrained eye: Electronic evidence is often found in places where only specialists would search or in locations reachable only by means of special tools.»[57] Praktische Beispiele sind etwa Datei-Fragmente im unallocated space[58] von Datenträgern.[59] Die «Unsichtbarkeit» für das untrainierte Auge betrifft aber nicht nur die Speicherorte, sondern auch die elektronischen Beweismittel selbst: Sie können Informationen enthalten, die auf den ersten (Laien-)Blick nicht sichtbar sind, so etwa Datei-Metadaten[60], in Dateien gewrappte Dateien[61], in Dateien «versteckte» Informationen[62] etc. Bei den für das Auffinden und Analysieren von elektronischen Beweismitteln zu verwendenden Spezialsoftwares ist ebenso an umfassende forensische Tools wie etwa die Open Source Digital Forensics Platform Autopsy[63] zu denken wie an spezifische Hilfsmittel zur Analyse von elektronischen Beweismitteln.[64]

---

55 Beispielsweise unter Zuhilfenahme geeigneter Validatoren.

56 Ginge man bspw. davon aus, dass selbst die Validierung von elektronischen Signaturen grundsätzlich in die Zuständigkeit eines Sachverständigen fiele, dann hätte dies erhebliche Kostenfolgen für die Justiz.

57 Council of Europe (Fn. 10), S. 12.

58 Der Begriff unallocated space bezeichnet Datenspeicherbereiche, die vom Computer verwendet werden können. Der Bereich kann bereits zuvor gespeicherte Informationen enthalten. Quelle: SWGDE Digital & Multimedia Evidence Glossary, Scientific Working Group on Digital Evidence, https://www.swgde.org/glossary/, zuletzt besucht am 24. April 2024.

59 Zum spezifischen Problem von versteckten Dateien in sector gaps und partition gaps siehe bspw. Alexander Geschonneck, Computer-Forensik, Computerstraftaten erkennen, ermitteln, aufklären, Heidelberg, 2014, S. 135.

60 Metadaten sind Daten über Daten, vgl. dazu Cory Altheide/Harlan Carvey (Fn. 33), S. 41. Der folgende Link ermöglicht den Download einer entzippten Word-Musterdatei, die u.a. im Verzeichnis {\}docProps{\}core.xml Datei-Metadaten enthält: https://www.advoschreiber.ch/rz/2.zip.

61 Vgl. PDF-Musterdatei, die als Wrapper für je eine docx-, eine xlsx- und eine xml-Datei dient: https://www.advoschreiber.ch/rz/3.pdf.

62 Vgl. docx-Musterdatei, die eine nicht auf den ersten Blick sichtbare Fotodatei enthält: https://www.advoschreiber.ch/rz/4.docx.

63 https://autopsy.com, zuletzt konsultiert am 22. April 2024: Autopsy ist eine Plattform, die insbesondere für Anwaltskanzleien eine geeignete Alternative zu proprietären Forensic-Tools darstellt.

64 Bspw. EXIF-Tool (https://exiftool.org/), Linux-Distribution CAINE (Computer-Aided Investigative Environment), etc. Tool-Überblicke sind bspw. auf https://computer-forensik.org/tools/, https://github.com/mesquidar/ForensicsTools und weiteren Web-Ressourcen zu finden. Beide Webressourcen zuletzt konsultiert am 25. April 2024.

2.5. Stand der Wissenschaft und Standards

[25] In der Praxisanwendung bringen elektronische Beweismittel zahlreiche ungeklärte Fragen mit sich, wie wir gesehen haben. Demgegenüber stecken die Wissenschaft und die Standardisierung keineswegs in den Kinderschuhen. Die wissenschaftlichen Disziplinen der digitalen Forensik (Cell Phone Forensic, Digital Audi Forensic, Digital Camera Forensic, Game Console Forensic, GPS Forensic etc.) befassen sich mit den Arbeitsetappen (Identification, Collection, Acquisition, Preservation, Analysis, Presentation und Transmission), die im Umgang mit elektronischen Beweismittel anfallen.[65] Derweil regeln Gesetze und Soft Law[66] sowie technische Standards[67] die Regeln, welche im Umgang mit elektronischen Beweismitteln zu beachten sind.

3. Der Status quo

3.1. In welcher Form finden wir derzeit elektronische Beweismittel in Verfahrensdossiers?

[26] Elektronische Beweismittel finden sich aktuell sowohl in Verfahrensdossiers, die massgeblich in Papierform geführt werden (bspw. auf Datenträger gespeicherte Daten, beigelegte Datenträger wie CD-ROM, USB-Speichermedien selbst, ausgedruckte elektronische Beweismittel in Papierform etc.), in hybrid geführten Verfahrensdossiers wie auch in elektronischen Verfahrensdossiers. Elektronische Beweismittel können, von Datenträgern einmal abgesehen, in zahlreichen Formen vorliegen: Bilddateien von Papierunterlagen, Excel-Sheets[68], forensische Images von Datenträgern[69], E-Mails in Form von eml-Dateien[70], Audiodateien[71], proprietäre Banana-Buchhaltungs-Exportdateien, raumbezogene Daten (Geodaten, Geoinformation) in Formaten wie INTERLIS oder GML[72] ebenso wie PDF-Dateien aller Art[73], um nur einige Beispiele zu nennen.[74] Mit anderen Worten: Die Diversität elektronischer Beweismittel in Verfahrensakten entspricht,

65 http://s.evidenceproject.eu/p/e/v/evidence-categorization-portrait-a4-269.pdf, zuletzt konsultiert am 22. April 2024.

66 So u.a. Guidelines und Best Practices wie die INTERPOL Guidelines for Digital Forensics First Responders.

67 So u.a. ISO/IEC 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence), ISO/IEC 27040 (Information technology – Security techniques – Storage security), ISO/IEC 27041 (Guidance on assuring suitability and adequacy of incident investigative method), ISO/IEC 27042 (Guidelines for the analysis and interpretation of digital evidence), ISO/IEC 27043 (Incident investigation principles and processes) und ISO/IEC 30121 (Governance of digital forensic risk framework).

68 Entscheid des Verwaltungsgerichts des Kantons Zürich VB.2019.00372 vom 29. August 2019, E. 3.2.2.

69 Entscheid des Kantonsgerichts Basel-Landschaft 470 20 119 vom 4. August 2020, https://entscheidsuche.ch/view/BL_KG_001_2020-08-04-sr-5_2020-08-04.

70 Urteil des Bundesgerichts 1B_541/2021 vom 22. März 2022.

71 Urteil des Tribunal cantonal JU CC 101 / 2022 vom 16. Dezember 2022, https://entscheidsuche.ch/view/JU_TC_002_CC-2022-101_2022-12-16.

72 Es wird auf das Bundesgesetz über Geoinformation (GeoIG) vom 5. Oktober 2007 (SR 510.62) und dessen Ausführungsverordnungen verwiesen. Solche Geodaten sind beispielsweise Daten der Grundstücksgrenzen der amtlichen Vermessung; die Grundstücksgrenzen werden rechtsverbindlich durch diese Daten bestimmt und nicht etwa durch die Grenzsteine oder durch Papierpläne. Die allgemeine Beschreibungssprache für Geodatenmodelle bei staatlichen Geodaten in der Schweiz entspricht dem Standard eCH-0031 INTERLIS 2 – Referenzhandbuch (Stand 7. September 2016).

73 Dateien in einem der spezifischen PDF/A-Formate, PDF-Dateien, die als Wrapper für den Transport weiterer Dateien dienen, usw.

74 Dem Entscheid 1B_108/2022 des Bundesgerichts vom 10. Oktober 2022, E. 1.3.2, ist zu entnehmen, dass der kantonalen Staatsanwaltschaft in dieser Sache folgende elektronische Beweismittel zur Verfügung standen: Ein «voll-

nicht überraschend, der Diversität, in der heute elektronische Unterlagen erstellt, bearbeitet und übermittelt werden.

3.2. Bei Gerichten und Behörden

[27] Der Status quo in Sachen Umgang mit elektronischen Beweismitteln bei Gerichten und Behörden muss als heterogen bezeichnet werden. Während es Spruchkörper gibt, die im Umgang mit elektronischen Beweismitteln geübt sind, pflegen Spruchkörper auf der anderen Seite des Spektrums einen papierorientierten Umgang mit elektronischen Beweismitteln und weiteren elektronisch eingereichten Unterlagen, was sich regelmässig auch in Urteilsbegründungen niederschlägt, wie die nachfolgenden Beispiele zeigen:

- In einem Entscheid des Bundesverwaltungsgerichts[75] lesen wir: «Das Gesagte trifft ebenfalls auf das rund 14 Sekunden dauernde, undatierte TikTok-Video zu, welches der Beschwerde beigelegt wurde.» Der Begriff «undatiert» ist im Zusammenhang mit elektronischen Beweismitteln verwirrend. Jede Datei, also auch jede Videodatei, enthält oder erhält vom Filesystem zugewiesene Datums- bzw. Zeitangaben. Die Interpretation der verschiedenen Zeit- bzw. Datumsangaben ist eine komplexe Angelegenheit.[76]
- In StPO-Vorverfahren werden regelmässig elektronische Beweismittel verändert, indem etwa Foto-Dateien aus beschlagnahmten Geräten über im Word-Format erstellte Polizeirapporte in Verfahrensakten überführt werden, die anschliessend ausgedruckt werden, ohne dass die forensischen Rohdaten als Beilagen mitgeliefert werden bzw. zitiert werden.
- E-Mail-Nachrichten als Papierausdruck oder als PDF-Datei in Verfahren einzuführen, ist heute quasi-Standard, obwohl sowohl mit dem herkömmlichen Ausdrucken als auch mit einer herkömmlichen Konvertierung in das Format PDF zentrale Inhalte wie der Header und der übrige Source Code einer E-Mailnachricht unterdrückt werden und die E-Mail in diesem Sinne verändert wird.[77] Hier ist anzumerken, dass das Bundesgericht in einem Entscheid von 2012 festgehalten hatte, dass E-Mails Computerurkunden sind und dass das Verfälschen einer E-Mail und das anschliessende Weiterleiten den Tatbestand der Urkundenfälschung i.e.S erfüllt.[78]
- In einem Entscheid der Beschwerdekammer des Obergerichts des Kantons Solothurn[79] lesen wir: «Die Staatsanwaltschaft stellte das Verfahren gegen den Beschuldigten mit der Begründung ein, die polizeilichen Auswertungen des Büro-Laptops der A.___ AG hätten erge-

---

ständiger Dump von Fabasoft», ein «Snapshot des Amtslaufwerk des Veterinäramts», ein «Snapshot der persönlichen Laufwerke von B». sowie eine «Kopie der Mailbox von B».

Zur Vielfalt von elektronischen Beweismitteln im Verwaltungsverfahren vgl. Entscheid des Bundesverwaltungsgerichts A-2595/2020 vom 19. Dezember 2022, https://entscheidsuche.ch/view/CH_BVGE_001_A-2595-2020_2022-12-19: Das ASTRA übermittelte hier der Bundesanwaltschaft Excel-Dateien sowie eine im Entscheid nicht näher spezifizierte Datenbank.

75 Urteil des Bundesverwaltungsgerichts E-3842/2021 vom 21. August 2023, E. 10.2.2.

76 Vgl. dazu bspw. Lars E. Daniel/Larry E. Daniel (Fn. 47), S. 207 ff. (Computer Time Artifacts, MAC Times).

77 Vgl. dazu Lorenz Kuhlee/Viktor Völzow (Fn. 31): «Ohne Header geht es nicht», Hack 80, S. 255 ff.

78 BGE 138 IV 209, E. 5.4.

79 Entscheid des Obergerichts des Kantons Solothurn (Beschwerdekammer) BKBES.2023.54 vom 16. August 2023, E. 3.2, https://entscheidsuche.ch/view/SO_OG_002_BKBES-2023-54_2023-08-16.

ben, dass die ursprüngliche Datei (die fragliche Vereinbarung) am 9. August 2021 geöffnet, eventuell gedruckt oder bearbeitet worden sei. Die Originaldatei sei nicht gefunden worden und die ursprüngliche Erstellung sei nicht nachweisbar [...]. Es könne deshalb nicht gesagt werden, ob das Dokument zu einem Zeitpunkt erstellt worden sei, in welchem sich der Beschuldigte und Herr C.___ über die Abrechnung des [...] uneins gewesen seien oder nicht und entsprechend könne auch nicht gesagt werden, ob davon auszugehen sei, es handle sich um eine nachträglich erstellte Fälschung oder nicht. Zudem sei nicht klar, durch wen das Dokument am 9. August 2021 geöffnet, evtl. gedruckt und bearbeitet worden sei. Aus dem auf dem Laptop noch vorhandenen Fragment lasse sich somit kein Beweis ableiten, der nur ansatzweise die Anschuldigungen der Anzeigeerstatter zu stützen vermöchten. Ebenso wenig sei eine Überprüfung der Echtheit der Handschrift auf der Vereinbarung möglich.» Während dieser Absatz die Schwierigkeit der Zurechnung von elektronischen Beweismitteln zu bestimmten Personen unterstreicht und festhält, dass der Scan-Output einer Handunterschrift keine Echtheits-Prüfung einer Handunterschrift erlaubt, sorgt er auch für Verwirrung. Was wäre in diesem Kontext eine «ursprüngliche Datei» oder eine «Originaldatei» und wie würde sie sich forensisch als solche erkennen lassen?

- Im Vorhaben Justitia 4.0 war in der Anfangsphase vorgesehen, dass jede via die Plattform Justitia.swiss eingereichte Datei von der Plattform direkt mit einem elektronischen Siegel versehen werden sollte[80]. Dies hätte, je nach Umsetzungsvariante, zur Folge gehabt, dass eingereichte elektronische Beweismittel bei der Übermittlung an die Plattform systematisch verändert worden wären. Inzwischen ist vorgesehen, dass die Quittung, welche die Hashwerte der übermittelten Dateien enthält, elektronisch gesiegelt wird.[81]
- In einem Entscheid des Bundesverwaltungsgerichts[82] wird die Vorinstanz, die eine Verfügung mit offensichtlichen Leerräumen erstellt hat, mit folgender Erklärung zur Entstehung der Datei zitiert: «Der Einladung eine fehlerfreie Fassung einzusenden und zu den Leerräumen in der angefochtenen Verfügung Stellung zu nehmen kam die Vorinstanz am 24. Februar 2021 nach und erläuterte, der Entscheid vom 1. Dezember 2020 sei auch mit den Leerräumen vollständig gewesen. Das Dokument sei von einer Word- zu einer PDF-Datei konvertiert worden, wodurch sich einzelne Absätze verschoben und sich die Lücken auf Seite 5 und 6 ergeben hätten.»
- In einem Vorverfahren nach Art. 299 StPO, in das die Co-Autorin als Strafverteidigerin involviert ist, wird das Gesuch um Einsicht in die erhobenen elektronischen Beweismittel (forensische Duplikate) mit folgender Begründung abgelehnt: «Die Sichtung der Rohdaten erfolgt gemäss Angaben der Forensiker über eine Software, welche durch Privatpersonen grundsätzlich nicht erhältlich gemacht werden kann.» Offenbar ist nicht allgemein bekannt, dass es neben «law enforcement only»-Softwares auch Open Source Digitalforensik-

80 So auch E-BEKJ, Art. 22 Abs. 3, Fahne 2023 III Nationalrat: «Bei den Dokumenten der übrigen Benutzerinnen und Benutzer bringen die Plattformen selbst ein Siegel und einen Zeitstempel an.»

81 Vgl. dazu die Stellungnahme des Bernischen Anwaltsverbandes BAV zur Vernehmlassung des BEKJ, https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/e-kommunikation/stellungnahmen.pdf, zuletzt besucht am 22. April 2024.

82 Urteil des Bundesverwaltungsgerichts B-65/2021 vom 4. Januar 2022, E. 2.2.1.

Plattformen wie Autopsy gibt, die gängige Formate forensischer Duplikate[83] analysieren können.

- In einem BVGER-Entscheid vom März 2022[84] wird der Beweiswert von Beweismitteln, die der Beschwerdeführer aus dem türkischen UYAP[85] einreicht, mit folgender Begründung angezweifelt: «Im Übrigen erscheinen die Verfahrensakten nicht einheitlich (z.B.: nicht auf allen Akten befindet sich ein QR-Code [vgl. z.B. Beweismittel Nrn. 1a und 1d], die elektronische Signatur ist teils völlig unterschiedlich und es werden verschiedene Adressen des Gesuchstellers genannt [vgl. Beweismittel Nrn. 1c und 3a; 1a, 1e und 3]).» Nach diesen Ausführungen ist unklar, um welche Art von elektronischen Signaturen es sich handelte und wie das Gericht diese validierte.
- In einem Entscheid vom 18. März 2022 beschreibt das BVGER Zustellungsprobleme im elektronischen Austausch mit bulgarischen Behörden: «Wer im vorliegenden Fall die technischen Schwierigkeiten zu verantworten hat, wo im elektronischen Kommunikationskanal des DubliNet die Probleme der Lesbarkeit der PDF-Dokumente lagen, kann anhand der Aktenlage nicht abschliessend geklärt werden.»
- Die Chambre pénale d'appel et de révision der Genfer Cour pénale beschreibt in einem Entscheid vom April 2022[86], wie ein ursprünglich elektronisches Beweismittel ausgedruckt wurde, in der zweiten Instanz dann aber das elektronische File wieder hinzugezogen wurde, wobei der Begriff «optimisation de l'image» die Frage aufwirft, ob die Bilddatei vom Gericht verändert wurde: «La version papier de la photographie radar du véhicule au moment de l'excès de vitesse figurant à la procédure, floue et sombre, ne permet pas de discerner la personne au volant, si ce n'est qu'il s'agit d'un homme et qu'il semble avoir un visage fin et les cheveux foncés avec une implantation garnie sur le dessus du crâne. La version numérique versée à la procédure par la Chambre pénale d'appel et de révision (CPAR), de meilleure qualité avec les différentes options d'optimisation de l'image, corrobore ce qui précède et permet de constater, avec les policiers ayant établi le rapport, ‹qu'il s'agit d'un homme beaucoup plus jeune› que B_____, né en 1956.» Eine Nachfrage bei zuständigen Gericht ergab, dass hier offenbar keine eigentliche Bildbearbeitung vorgenommen wurde, obwohl der Begriff der Bildoptimierung dies nahelegen könnte[87].
- In einem Entscheid des Bundesstrafgerichts vom Mai 2022[88] wird die Bundesanwaltschaft wie folgt zitiert: «Die Bundesanwaltschaft teilte mit Antwortschreiben vom 8. Dezember

83 Autopsy (Version 4.21.0) kann beispielsweise folgende disk image-Formate verarbeiten: Raw Single (*.img, *.dd, *.raw, *.bin), Raw Split (*.001, *.aa), EnCase (*.e01), Virtual Machine Disk (*.vmdk), Virtual Hard Disk (*.vhd).

84 Urteil des Bundesverwaltungsgerichts E-737/2022 vom 14. März 2022, E. 4.2.

85 Ulusal Yargi A Biliim Sistemi, vgl. dazu Herkunftsländerbericht der Schweizerischen Flüchtlingshilfe, Türkei: Zugang zu verfahrensrelevanten Akten, Auskunft vom 1. Februar 2019, https://www.fluechtlingshilfe.ch/fileadmin/user_upload/Publikationen/Herkunftslaenderberichte/Europa/Tuerkei/190201-tur-verfahrensrelevante-akten-de.pdf , zuletzt konsultiert am 22. April 2024.

86 Entscheid der Cour de justice GE, Chambre pénale d'appel et de révision, P/14894/2020 vom 27. April 2022, https://entscheidsuche.ch/view/GE_CJ_009_P-14894-2020_2022-04-27.

87 Auszug aus der E-Mailnachricht der zuständigen Gerichtspräsidentin vom 16. April 2024 an die Autorin: «J'ai pris bonne note de votre demande et vérifié l'affaire en question. Nous avions sollicité le fichier source de la police qui a été remis à la Cour sous forme électronique et transmis aux parties sur clé USB. Aucun traitement de données n'a été nécessaire – la simple visualisation de l'image à l'écran permettait déjà d'obtenir une bien meilleure qualité que la photo imprimée au dossier (qui était une impression ‹ordinaire› noir-blanc, vraisemblablement imprimée sur imprimante de bureau et non sur papier photo).»

88 Urteil des Bundesstrafgerichts BB.2021.147 vom 25. Mai 2022.

2017 dem Verteidiger zu dessen Antrag Ziff. 1 mit, dass er mit der Ausnahme von gewissen Beweismitteln, die nur in elektronischer Form erhoben worden und daher aufzubereiten sind, bevor sie ihm bald zugestellt werden können, vollumfänglich mit den vorhandenen Akten bedient worden sei.» Unklar ist hier, was mit «Aufbereiten» gemeint ist und die Tatsache, dass Beweismittel, die nur in elektronischer Form erhoben wurden, in einer bestimmte Form aufzubereiten wären, ist aus technischer Sicht nicht zwingend.

[28] Während einerseits wie oben beispielhaft erläutert vielfach papierorientierte Methoden und Begrifflichkeiten im Umgang mit elektronischen Beweismitteln zur Anwendung kommen, beschäftigt sich beispielsweise das Staatssekretariat für Migration SEM intensiv mit der Frage von elektronischen Beweismitteln und deren Beweiswert. Zahlreiche Entscheide des Bundesverwaltungsgerichts lassen Rückschlüsse darauf zu, wie Behörden, die elektronische Beweismittel primär aus technischer Sicht im Sinne der Erkennung von Fälschungen betrachten, den Beweiswert von elektronischen Beweismitteln einschätzen:

- In einem Entscheid des Bundesverwaltungsgerichts vom März 2022[89] legt ein Gesuchsteller ein Foto eines elektronischen Flugtickets vor. Das BVGER schreibt dazu in Ziffer 4.3 des Entscheids: «Es ist vorab festzustellen, dass das Beweismittel an sich nur eine sehr geringe Beweiskraft aufweist, zumal nur ein Foto eines elektronischen Flugtickets vorliegt, leicht zu fälschen ist und auch keine entsprechende Korrespondenz hinsichtlich des Erhältlichmachens beigebracht wird.»
- In einem BVGER-Entscheid vom 20. September 2022 (E-2330/2020) wird einem Screenshot lediglich ein schwacher Beweiswert attestiert, weil es sich dabei um eine Kopie handle: «Enfin, le document présenté comme une capture d'écran du fichier des personnes recherchées à l'aéroport de Colombo n'a qu'une faible valeur probante, s'agissant d'une copie, [...].» Hier ist festzuhalten, dass ein Screenshot keine Kopie darstellt.
- In einem BVGER-Entscheid vom Oktober 2022[90] wird die Einschätzung des SEM zum Beweiswert eines Scan-Outputs wiedergegeben: «Des Weiteren handle es sich beim eingereichten Beweismittel um einen Scan und nicht um das Original. Eine eingehende Untersuchung des Dokuments werde dem SEM schon allein dadurch verunmöglicht, weil kein originales Dokument vorliege. Zudem könne nicht ausgeschlossen werden, dass dieses Dokument, welches nachweislich digitalisiert worden sei, allenfalls einer elektronischen Nachbehandlung unterzogen worden sei.»

[29] Die oben aufgeführten Beispiele zeigen, dass die in Ziffer 2.4.7 beschriebenen fehlenden Routinen teilweise auch in der Praxis der Gerichte zu beobachten sind und dass sich derzeit in Bezug auf elektronische Beweismittel noch keine «unité de doctrine» herausgebildet hat.

89 Entscheid des Bundesverwaltungsgerichts E-5584/2021 vom 9. März 2022.

90 Entscheid des Bundesverwaltungsgerichts D-5276/2020 vom 14. Oktober 2022.

3.3. Zulässigkeit elektronischer Beweismittel im aktuellen Prozessrecht

3.3.1. Zivilprozess

[30] Der Beweismittelkatalog der ZPO (Art. 168 ZPO) ist abschliessend und stellt einen *numerus clausus* dar[91]. Im summarischen Verfahren stellen Urkunden mit gewissen Ausnahmen sogar das einzig zulässige Beweismittel dar (Art. 254 Abs. 1 ZPO).[92]

[31] Der Begriff der Urkunde wird in Art. 177 ZPO künftig wie folgt definiert sein: «Als Urkunden gelten Dokumente, die geeignet sind, rechtserhebliche Tatsachen zu beweisen, wie Schriftstücke, Zeichnungen, Pläne, Fotos, Filme, Tonaufzeichnungen, elektronische Dateien und dergleichen sowie private Gutachten der Parteien.»[93] Der weit gefasste Urkundenbegriff umfasst damit ausdrücklich auch elektronische Daten.

[32] Der zivilprozessrechtliche Urkundenbegriff ist weiter gefasst als der strafrechtliche (Art. 110 Abs. 4 StGB), da anders als im Strafrecht nicht gefordert wird, dass das Dokument bei seiner Erstellung zum Beweis bestimmt war, und da die Authentifizierbarkeit der Ausstellerin bzw. des Ausstellers nicht von Belang ist.[94] Mithin sind alle Urkunden im Sinne von Art. 110 Abs. 4 StGB auch solche im Sinne von Art. 177 ZPO. Die Aufzeichnung auf Bild- und Datenträgern – und damit elektronische Unterlagen – stehen der Schriftform gleich, sofern sie demselben Zweck dient.[95]

3.3.2. Strafprozess

[33] Das Strafprozessrecht geht bei den sog. sachlichen Urkunden (Art. 192–195 StPO) erkennbar dem Grundsatz nach noch von Papierdokumenten aus, obwohl die StPO erst kürzlich revidiert wurde.

[34] Urkunden im Sinne von Art. 192 Abs. 2 StPO können grundsätzlich nur Schriftstücke sein.[96] Elektronische Datenaufzeichnungen gehören zu den «weiteren Aufzeichnungen» im Sinne von Art. 192 Abs. 2 StPO.[97] Sie werden aber den Urkunden gleichgestellt.[98] Deshalb werden in der Lehre und Rechtsprechung die weiteren Aufzeichnungen vereinfachend als Urkunden bezeichnet;[99] auch das Bundesgericht subsumiert offenbar die weiteren Aufzeichnungen unter die Urkunden[100]. Gemäss der Lehre und Rechtsprechung sind mithin elektronische Aufzeichnungen gleichermassen zugelassen wie Papierdokumente.

---

91 Vgl. Sven Rüetschi, Berner Kommentar Band 11 Schweizerische Zivilprozessordnung, Bern 2012, Art. 168, Rz. 2.

92 Vgl. Stefan Fink/Stephan Kesselbach, II. Beweismittel, in: Ulrich Haas/Reto Marghitola (Hrsg.), Fachhandbuch Zivilprozessrecht, Zürich 2020, S. 566 ff., Rz. 20.135; Andreas Güngerich, Berner Kommentar Band 11 Schweizerische Zivilprozessordnung, Bern 2012, Art. 254, Rz. 2.

93 Fassung gemäss Ziff. I des BG vom 17. März 2023 (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung), in Kraft ab 1. Januar 2025 (AS 2023 491; BBl 2020 2697).

94 Vgl. Rüetschi (Fn. 91), Art. 177, Rz. 6.

95 Dazu ausführlich Wolfgang Wohlers, in: Wolfgang Wohlers/Gunhild Godenzi/Stephan Schlegel (Hrsg.), Handkommentar StGB, 4. Aufl., Bern 2020, Art. 110, Rz. 12 ff.

96 Vgl. Martin Bürgisser, BSK StPO, 2. Aufl., Basel 2014, Rz. 5.

97 Vgl. Bürgisser (Fn. 96), Rz. 8.

98 Vgl. Bürgisser (Fn. 96), Rz. 8, mit weiteren Hinweisen.

99 Vgl. Bürgisser (Fn. 96), Rz. 8, mit weiteren Hinweisen.

100 Vgl. Bürgisser (Fn. 96), Rz. 8, mit Hinweis auf Urteil 6B_383/2012 des Bundesgerichts vom 29. November 2012, E. 7.1.

3.3.3. Verwaltungsverfahren

[35] Elektronische Dateien sind Urkunden im Sinne von Art. 12 VwVG[101] und sind im Bundesverwaltungsverfahren mithin zugelassen.

[36] Die Verwaltungsverfahrensgesetze der Kantone verweisen in der Regel beim Beweisrecht integral oder subsidiär auf die ZPO, so dass auch in kantonalen Verwaltungsverfahren der Urkundenbegriff von Art. 177 ZPO zur Anwendung gelangt und mithin elektronische Dokumente prozessrechtlich als Urkunde gelten.[102]

3.3.4. Fazit zur Zulässigkeit elektronischer Beweismittel

[37] Im gesamten schweizerischen Prozessrecht stellen Dateien als häufigste Erscheinungsform elektronischer Beweismittel Urkunden dar und können als solche als Beweismittel eingesetzt werden.

4. Aus der Sicht des Beweisrechts

4.1. Freie Beweiswürdigung: Überzeugung als Maxime

[38] Das schweizerische Zivilprozessrecht kennt explizit den *Grundsatz der freien Beweiswürdigung* (Art. 157 ZPO[103]).[104] Das schweizerische Strafprozessrecht wird ebenfalls vom Grundsatz der freien und umfassenden Beweiswürdigung beherrscht (Art. 10 Abs. 2 StPO).[105] Auch im Bundesverwaltungsprozess gilt der Grundsatz der freien Beweiswürdigung (Art. 19 VwVG[106] i.V.m. Art. 40 BZP[107]).[108] Die Verwaltungsverfahrensgesetze der Kantone verweisen in der Regel beim Beweisrecht integral oder subsidiär auf die ZPO, so dass auch in kantonalen Verwaltungsverfahren der Grundsatz der freien Beweiswürdigung gilt. Zudem hat das Bundesgericht folgendes festgehalten: «Im Verwaltungsprozessrecht gilt ganz allgemein der Grundsatz der freien Beweiswürdigung.»[109] Vorbehältlich ausdrücklicher gesetzlicher Abweichungen (meistens in der Spezi-

---

101 Christoph Auer/Anja Martina Binder, in: Christoph Auer/Markus Müller/Benjamin Schindler (Hrsg.), Kommentar VwVG, 2. Aufl., Zürich/St. Gallen 2019, Art. 12, Rz. 28; Urteil A-6640/2010 des Bundesverwaltungsgerichts vom 19. Mai 2011, E. 5.5.2.

102 Siehe oben Ziff. 3.3.1.

103 Schweizerische Zivilprozessordnung (Zivilprozessordnung, ZPO) vom 19. Dezember 2008, SR 272.

104 Vgl. dazu ausführlich Jürgen Brönnimann, Berner Kommentar Band 11 Schweizerische Zivilprozessordnung, Bern 2012, Art. 157.

105 Vgl. Brönnimann (Fn. 104), Art. 157, Rz. 2; Urteil 6B_804/2017 des Bundesgerichts vom 23. Mai 2018, E. 2.2.3.1; ausführlich Thomas Hofer, BSK StPO, 2. Aufl., Art. 10, Rz. 41 ff.; auch dem früheren Bundesstrafprozess war der Grundsatz der freien Beweiswürdigung inhärent (vgl. BGE 133 I 33, E. 2.1).

106 Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG) vom 20. Dezember 1968, SR 172.021.

107 Bundesgesetz über den Bundeszivilprozess vom 4. Dezember 1947, SR 273.

108 Vgl. Brönnimann (Fn. 104), Art. 157, Rz. 2; Auer/ Binder (Fn. 101), Art. 12, Rz. 18; BGE 130 II 482, E. 3.2; Urteil 2C_169/2018 vom 17. August 2018, E. 3.3.6; Urteil 1C_398/2010 des Bundesgerichts vom 5. April 2011, E. 2.2.3.1.

109 Urteil 2C_169/2018 des Bundesgerichts vom 17. August 2018, E. 3.3.6; es handelte sich um eine Beschwerde gegen ein Urteil des Verwaltungsgerichts des Kantons Zürich und es ging um die Frage der Beweiswürdigung durch die kantonalen Instanzen.

algesetzgebung, selten im Prozessgesetz) ist somit das schweizerische Prozessrecht generell vom Grundsatz der freien Beweiswürdigung geprägt.

[39] Die Quintessenz der freien Beweiswürdigung wird in Gesetzgebung, Rechtsprechung und Lehre wie folgt charakterisiert:

- «Das Gericht bildet sich seine Überzeugung nach freier Würdigung der Beweise.» (Art. 157 ZPO);
- «Das Gericht würdigt die Beweise frei nach seiner aus dem gesamten Verfahren gewonnenen Überzeugung.» (Art. 10 Abs. 2 StPO);
- «Der Grundsatz bezieht sich zunächst auf die Würdigung der erhobenen Beweise, deren Überzeugungskraft der Richter von Fall zu Fall anhand der konkreten Umstände zu prüfen und bewerten hat, ohne dabei an gesetzliche Regeln gebunden zu sein oder sich von schematischen Betrachtungsweisen leiten zu lassen.»[110]
- «Die Organe der Strafrechtspflege sollen frei von Beweisregeln und nur nach ihrer persönlichen Überzeugung aufgrund gewissenhafter Prüfung der vorliegenden Beweise darüber entscheiden, ob sie eine Tatsache für bewiesen halten (BGE 127 IV 172, E. 3a S. 174). Dabei sind sie freilich nicht nur der eigenen Intuition verpflichtet, sondern auch an (objektivierende) Denk-, Natur- und Erfahrungssätze sowie wissenschaftliche Erkenntnisse gebunden.»[111]
- «Die Beweiswürdigung endet mit dem richterlichen Entscheid darüber, ob eine rechtserhebliche Tatsache als erwiesen zu gelten hat oder nicht. Der Beweis ist geleistet, wenn das Gericht gestützt auf die freie Beweiswürdigung zur Überzeugung gelangt ist, dass sich der rechtserhebliche Sachumstand verwirklicht hat.»[112]
- «Gradmesser soll dabei die eigene Überzeugung sein – sowohl in Bezug auf die Aussagekraft jedes einzelnen Beweismittels als auch auf das Beweisergebnis als Ganzes.»[113]
- «Bei der Würdigung der Beweise ist die Behörde keinen Beweisregeln unterworfen. Es gilt der Grundsatz der freien Beweiswürdigung, das heisst, die Behörde entscheidet nach ihrer freien Überzeugung darüber, ob ein Beweis erbracht wurde oder nicht.»[114]
- «Im Zusammenhang mit Gerichtsgutachten heisst freie Beweiswürdigung somit, dass der Richter an die Tatsachenfeststellungen und Schlussfolgerungen des Gutachters nicht gebunden ist, sondern nach seiner freien Überzeugung entscheidet, ob und in welchem Masse er das Ergebnis des Gutachtens als richtig und beweiskräftig erachtet.»[115]
- «Diesem Prozess der freien Beweiswürdigung ist nach Auffassung des Autors immanent, dass der Richter in seinem Meinungsbildungsprozess einen Punkt erreicht, an dem er davon überzeugt ist, dass seine Meinung über das Vor- oder Nichtvorliegen einer Tatsachenbe-

110 BGE 133 I 33, E. 2.1.

111 Urteil 6B_804/2017 des Bundesgerichts vom 23. Mai 2018, E. 2.2.3.1.

112 Urteil A-1620/2018 des Bundesverwaltungsgerichts vom 10. Januar 2019, E. 1.4.2.

113 Hofer (Fn. 105), Art. 10, Rz. 41.

114 Auer/Binder (Fn. 101), Art. 12, Rz. 18.

115 Alfred Bühler, Die Beweiswürdigung von Gerichtsgutachten im Zivilprozess, Jusletter vom 14. Mai 2007, Rz. 2.

> hauptung feststeht und durch die Abnahme des (weiteren) offerierten Gegenbeweismittels nicht mehr beeinflusst werden kann.»[116]

[40] Kernelement der freien Beweiswürdigung ist mithin nach der Gesetzgebung sowie nach der herrschenden Lehre und Rechtsprechung die *Überzeugung* der Richterin bzw. des Richters bezüglich der mit einem Beweis bzw. Beweismittel zu beweisende Tatsache.[117] Behörden und Gerichte sollen einzig nach ihrer persönlichen Überzeugung auf Grund gewissenhafter Prüfung darüber entscheiden, ob sie eine Tatsache für bewiesen halten oder nicht.[118] In der Lehre findet sich denn die freie Beweiswürdigung auch unter dem Titel «Beweiswürdigung nach Überzeugung»[119]. «Zu seiner Überzeugung gelangt das Gericht durch Anwendung von Denk- Natur- und Erfahrungssätzen, durch Zuhilfenahme wissenschaftlicher Erkenntnisse, aber auch über Intuition und Gefühl.»[120] Die Überzeugung muss durch Fakten und durch logische Folgerungen begründet, das Beweisergebnis mithin objektiv nachvollziehbar sein.[121]

[41] Dies bedeutet, dass bei der freien Beweiswürdigung wohl auch Analogieschlüsse zur Anwendung gelangen (müssen), dies insbesondere dann, wenn noch keine gefestigte Praxis besteht.

[42] Bei elektronischen Beweismitteln setzt die Beweiswürdigung durch freie Überzeugung die Verfügbarkeit von geeigneten Softwares zur Analyse von e-Beweismitteln und ein gewisses Mass an Kenntnissen voraus[122], insbesondere:

- Basiskenntnisse im Bereich IT-Grundschutz
- Basiskenntnisse im Bereich der digitalen Forensik, insbesondere Datei-Analysen[123]
- Berechnung und Abgleich von Hashwerten, um bspw. Dateien rechtssicher identifizieren zu können.
- Sichtbarmachen von Metadaten von Dateien
- Sichtbarmachen von EXIF-Daten[124] von Dateien
- Sichtbarmachen des Source Codes von Dateien (bspw. von E-Mails)
- Basiskenntnisse über die gängigsten Entstehungsarten von elektronischen Beweismitteln und die Auswirkungen auf deren Eigenschaften.

---

116 Philipp Haberbeck, Abgrenzung der zulässigen antizipierten Beweiswürdigung von der Verletzung des Rechts auf Beweis im Zivilprozess, Jusletter 3. Februar 2014, Rz. 39.

117 Vgl. Daniel Kettiger, NetzBeweis als Beweismittel im schweizerischen Prozessrecht, in: Jusletter IT 16. Dezember 2021, Rz. 11.

118 Vgl. Hofer (Fn. 105), Art. 10, Rz. 48, mit Hinweis auf BGE 133 I 33, E. 21. und BGE 127 IV 172, E. 3a.

119 Hofer (Fn. 105), Art. 10, Rz. 58.

120 Hofer (Fn. 105), Art. 10, Rz. 60, mit Hinweisen u.a. auf Isaak Meier, das Beweismass – ein aktuelles Problem des schweizerischen Zivilprozessrechts, BJM 1989, S. 61; Walter Wüthrich, Die Hochrechnung gewonnener Erkenntnisse als Mittel der Beweisführung im Wirtschaftsstrafprozess, ZStrR 2005, S. 284; sowie Esther Topinke, Das Grundrecht der Unschuldsvermutung, Diss. Bern 2000, S. 339.

121 Vgl. Hofer (Fn. 105), Art. 10, Rz. 61.

122 Nicht nur seitens der Richterschaft, sondern auch auf Anwaltsseite, vgl. Vgl. Emma Jones/Francine Ryan/Ann Thanaraj/Terry Wong, Digital Lawyering, Technology and Legal Practice in the 21st Century, London, New York, 2022, S. 260.

123 Zu Datei-Analysen (Inhalts-Identifikation und Metadaten-Extraktion) vgl. Cory Altheide/Harlan Carvey (Fn. 33), S. 169 ff.

124 EXIF-Daten (Exchangeable Image File Format) speichern Angaben über das Gerät, welches ein Bild aufgezeichnet hat, bspw. eine Kamera, in der erstellten Bilddatei. Weitere Typen von Bild-Metadaten sind IPTC und XMP, vgl. Cory Altheide/Harlan Carvey (Fn. 33) S. 177.

- Basiskenntnisse über die Entstehung, den Aufbau und die Eigenschaften gängiger Dateiformate wie:
  - E-Mail-Dateiformate (.eml, .msg)
  - Bild- und Video-Dateiformate (.jpg, .png, .tiff, .mp4, .wav, .mp4, .mov etc.)
  - PDF sowie PDF/A-Dateiformate
  - «Archiv»-Formate wie .zip, .rar etc.
  - weitere gängige Dateiformate (.odt, .docx, .txt, .xlsx etc.)
- Basiskenntnisse über Validierungs-Softwares, mit denen gewisse elektronische Eigenschaften von Dateien geprüft werden können.[125] Fähigkeit, einfache Validierungen selbst vorzunehmen und Validierungsberichte interpretieren zu können.
- Basiskenntnisse über elektronische Signaturen, Signatur-Zertifikate, elektronische Zeitstempel und deren Eigenschaften.
- Basiskenntnisse über Webinhalte und deren Entstehung.

[43] Wenn Überzeugung die prägende Maxime der Beweiswürdigung im schweizerischen Prozessrecht ist, so ist der *Beweiswert* eines Beweises bzw. Beweismittels gleichzusetzen mit dessen *Überzeugungskraft*.[126] Der angebotene Beweis hat dann einen hohen Beweiswert, wenn er in hohem Mass geeignet ist, die Behörde oder das Gericht von einer bestimmten Tatsache zu überzeugen. Zur Überzeugungskraft bezüglich des Beweises einer Tatsache tragen zwei Komponenten bei:[127]

- *Beweistauglichkeit:* Der Beweis bzw. das Beweismittel muss sachlich geeignet sein, die betreffende Tatsache zu beweisen (vgl. nachfolgend Ziff. 4.2);
- *Vertrauenswürdigkeit:* Der Beweis bzw. das Beweismittel muss vertrauenswürdig sein, d.h. an der Echtheit und Unverfälschtheit sowie an der Quelle des Beweismittels dürfen keine Zweifel bestehen (vgl. nachfolgend Ziff. 4.3).

4.2. Beweistauglichkeit

[44] Ein Beweismittel muss grundsätzlich geeignet sein, eine bestimmte Tatsache zu beweisen; nur so ist es zum Beweis überhaupt tauglich. Explizit spricht dies in der Prozessgesetzgebung in genereller Weise nur Art. 139 Abs. 1 StPO an, welcher den Einsatz von nach dem Stand von Wissenschaft und Erfahrung geeigneten Beweismitteln fordert. Das Zivilprozessrecht fordert die Geeignetheit explizit für Urkunden (Art. 177 ZPO).[128] Das Beweismittel muss es somit ermöglichen, zuverlässige Rückschlüsse auf das Vorliegen einer Tatsache in der Vergangenheit zu ziehen.[129]

125 Vgl. dazu Prototyp einer Validatorenliste, die im Rahmen der Fachgruppe Validatoren der Digitalen Gesellschaft erarbeitet wurde: https://validatoren.ch/prototyp/, zuletzt konsultiert am 22. April 2024.

126 Vgl. Kettiger (Fn. 117), Rz. 12.

127 Vgl. Kettiger (Fn. 117), Rz. 12.

128 Vgl. auch Andreas Binder/Roman S. Gutzwiller, das Privatgutachten – eine Urkunde nach Art. 177 ZPO, Z.Z.Z. 2013, S. 172.

129 Vgl. Sabine Gless, BSK StPO, 2. Aufl., Art. 139, Rz. 28; Kettiger (Fn. 117), Rz. 13.

[45] Doch welche elektronischen Beweismittel sind geeignet, zuverlässige Rückschlüsse auf das Vorliegen von Tatsachen in der Vergangenheit zu erlauben und welche nicht? Dies hängt sowohl von der zu beweisenden Tatsache wie auch der Art des elektronischen Beweismittels ab, wie die folgenden Beispiele zeigen:

- Mit einem einem laienhaft erstellten Screenshot (bspw. PDF-Datei mit qualifiziertem Zeitstempel) einer Webseite lässt sich u.U. darlegen, dass eine bestimmte Webseite zum geltend gemachten Zeitpunkt einen bestimmten Text für gewisse Browser sichtbar machte.[130]
- Mit einem via die kostenlose Version für Privatanwender von netzbeweis.com erstellten Screenshot einer Webseite lässt sich nicht darlegen, dass eine bestimmte Webseite zum geltend gemachten Zeitpunkt einen bestimmten Hyperlink auf eine andere Webseite enthielt. Denn diese Version von netzbeweis.com bildet nur die Wiedergabe von Code durch einen Browser ab, nicht aber den Code selbst, in dem der Hyperlink gespeichert ist. Das kostenpflichtige Browser-Plugin von netzbeweis.com hingegen dokumentiert zusätzlich den Source Code der Webseite sowie gewisse vom Webserver bereitgestellte Files (bspw. Fotodateien).
- Mit einem sorgfältig erstellten Screenshot lassen sich gewisse Inhalte einer Webseite unter Umständen darlegen, aber nicht, dass diese Inhalte vom Bewirtschafter der URL erstellt wurden. Es gibt beispielsweise Webseiten, die on the fly aus verschiedenen Datenquellen zusammengestellt werden.
- Mit einer laienhaft in ein PDF-Format konvertierten E-Mailnachricht lässt sich u.U. darlegen, dass die Nachricht einen bestimmten Text enthalten hat.
- Mit einer laienhaft in ein PDF-Format konvertierten E-Mailnachricht lässt sich nicht darlegen, dass die Nachricht einen bestimmten Text nicht enthalten hat.[131]
- Mit einer laienhaft in ein PDF-Format konvertierten E-Mailnachricht lässt sich nicht darlegen, dass die Nachricht bei der Übermittlung einen bestimmten Server durchlaufen hat.[132]
- Mit einer E-Mailnachricht im .eml-Format lässt sich u.U. darlegen, dass die Nachricht Malware im Source-Code enthielt, dass der Body der Nachricht signiert war oder dass die Nachricht bestimmte Attachements enthielt.

4.3. Vertrauenswürdigkeit

[46] Bestimmte Beweismittel erscheinen auch in einem System der freien Beweiswürdigung nach der allgemeinen Lebenserfahrung als zuverlässiger als andere; so gelten Sachbeweise (Urkunden, Augenscheine) grundsätzlich als zuverlässiger als Personalbeweise (Zeugen, Parteien).[133] Im Zivilprozess wird dem Urkundenbeweis im Verhältnis zu anderen Beweismitteln regelmässig eine

130 Auch die Wiedergabe von Code durch Browser hängt u.a. vom eingesetzten Browser und dessen Einstellungen sowie von den Einstellungen allfällig eingesetzter Personal Firewalls ab.

131 Insbesondere HTML-E-Mails können Texte im Source-Code enthalten, die bei einer Konvertierung in ein PDF-Format mit gängigen Tools entfernt werden.

132 Je nach Konvertierungs-Tool und dessen Konfiguration wird auch die Sender- und Empfänger-E-Mailadresse nicht abgebildet, sondern nur der Alias-Name von Sender und Empfänger.

133 Vgl. Brönnimann (Fn. 104), Art. 157, Rz. 17.

höhere Beweiskraft zu attestieren sein.[134] Der qualitative Vorteil der Urkunde als Beweismittel liegt darin, dass sie einen Sachverhalt zeitlich authentisch und nicht im Nachhinein veränderbar wiedergibt[135], jedenfalls in der herkömmlichen Papierform. Dabei dürfte genuinen Schriftstücken ein höherer Beweiswert zukommen als elektronischen Daten oder Ausdrucken von solchen.[136] Im Strafverfahren geniessen allerdings Urkunden – zumindest formell – keinen qualifizierten Beweiswert.[137]

[47] Eine Urkunde ist allerdings nicht per se vertrauenswürdig. Sowohl die Echtheit wie auch die inhaltliche Richtigkeit kann bestritten werden. Weiter kann im Zivilverfahren die Echtheit sowohl eines Originals der Urkunde wie auch die Echtheit der Kopie einer Urkunde bestritten werden. Den ersten Fall regelt im Zivilprozess Art. 178 ZPO, den zweiten Fall Art. 180 Abs. 1 ZPO.

[48] Sowohl Art. 178 ZPO wie auch Art. 180 Abs. 1 ZPO stellen auf die Original-Kopie-Logik ab. Diese besagt, dass es im Prinzip im Erstellungszeitpunkt nur ein Original[138] geben kann und dass von einem Original nachträglich potentiell unzählige Kopien erstellt werden können, die anstelle des Originals in Verkehr gebracht werden.

[49] Art. 177 ZPO postuliert, dass auch «elektronische Dateien und dergleichen» als Urkunden gelten. In der Literatur wird diese Original-Kopie-Logik in der Folge auch auf elektronische Beweismittel ausgeweitet. So wird beispielsweise postuliert, dass «in Bezug auf Kopien herkömmliche und elektronische Datenträger gleichgestellt» seien[139], wobei andernorts präzisiert wird, «c'est le document qui constitue le titre et non pas le support qui le contient». An anderer Stelle wird festgehalten, dass es unerheblich sei, ob es sich um eine klassische Fotokopie, [...] oder den Ausdruck einer elektronischen Datei handle und dass «elektronische Kopien sogar Originalqualität» aufweisen könnten, namentlich wenn ihre Archivierung dem handelsrechtlichen Standard entspreche.[140] Weiter findet sich in der einschlägigen Literatur der Hinweis, dass elektronische Urkunden den Beweiswert eines Originals hätten, sofern sie gewisse Voraussetzungen erfüllten.[141] Ebenfalls zu finden ist die Feststellung, dass «Kopien leichter zu fälschen sind als Originale»[142] oder die Feststellung, dass es bei der Zulassung von digitalisierten Dokumenten und Kopien keine Rolle spiele, ob es sich um «genuin digitale Dateien oder bspw. um eingescannte Papierdokumente handelt».[143]

[50] Die Anwendung der Original-Kopie-Logik auf Urkunden in Dateiform ist technisch und rechtlich aber nicht haltbar. Dies bedeutet, dass sich insbesondere die Regelung von Art. 180 Abs. 1 ZPO, wonach anstelle von Urkunden auch Kopien eingereicht werden, nur auf analoge Urkunden und deren Kopien sowie – mit Vorbehalten hinsichtlich der beim Scannen hinzuge-

134 Vgl. Fink/Kesselbach (Fn. 92), Rz. 20.136.

135 Vgl. Fink/Kesselbach (Fn. 92), Rz. 20.136.

136 Vgl. Rüetschi (Fn. 91), Art. 178, Rz. 16.

137 Vgl. Bürgisser (Fn. 96), Art. 192, Rz. 7.

138 Bzw. mehrere unterschiedliche Originale, falls Verträge in Papierform im Doppel erstellt werden.

139 Thomas Sutter-Somm/Benedikt Seiler, Handkommentar zur Schweizerischen Zivilprozessordnung, Zürich, 2021, Art. 180, Rz. 2.

140 Annette Dolge, Basler Kommentar Schweizerische Zivilprozessordnung, Basel 2017, Art. 180, Rz. 9.

141 Hans Schmid/Samuel Baumgartner, Kurzkommentar ZPO, Basel, 2021, Art. 177, Rz. 6.

142 Hans Schmid/Samuel Baumgartner, Kurzkommentar ZPO (Fn. 141), Art. 180, Rz. 2.

143 Annette Dolge, Basler Kommentar Schweizerische Zivilprozessordnung, (Fn 140), Art. 177. Rz. 7; Bemerkung dazu: elektronische Beweismittel der Kategorie E sind nicht «digitalisiert».

fügten Informationen[144] – auf Scan-Output von Papierurkunden (Entstehungskategorie PzuE) beziehen kann. Sie ist hingegen nicht auf elektronische Beweismittel der Entstehungskategorien E, EzuE, EzuP und EzuPzuE anwendbar. Und zwar aus den folgenden Gründen: Bei der Entstehungskategorie E wird die Datei zur Inverkehrbringung vervielfacht, d.h. die Ausgangs-Datei und die bei der Vervielfältigung erzeugte Datei sind identisch, sie weisen denselben Hashwert auf. Bei den EzuE- und EzuPzuE-Vorgängen wird die Datei verändert[145]. Bei den EzuP-Vorgängen wird schliesslich ein erheblicher Teil der in einer Datei enthaltenen Informationen bei einem herkömmlichen Druckvorgang nicht wiedergegeben.

[51] Als Fazit lässt sich festhalten, dass Art. 180 Abs. 1 ZPO zwar Kopien (und *a fortiori* auch Vervielfältigungen von Dateien, sofern diese denselben Hashwert aufweisen) vom Grundsatz her zulässt, nicht aber die Einreichung von veränderten elektronischen Beweismitteln (zur Einreichungsform siehe nachfolgend Ziffer 4.4).[146]

4.4. Einreichungsform von elektronischen Beweismitteln

[52] A contrario ergibt sich aus Art. 180 Abs. 1 ZPO, dass Urkunden nicht in veränderter Form eingereicht werden dürfen bzw. sollten. Dies ist eine Selbstverständlichkeit im analogen Kontext und muss für elektronische Urkunden (und generell elektronische Beweismittel) gleichermassen gelten. Daraus lässt sich zunächst ableiten, dass Dateien nicht durch die Parteien und die Gerichte bzw. Behörden verändert werden dürfen. Doch wie sind elektronische Beweismittel der Entstehungskategorien E, EzuE, EzuPzuE denn nun einzureichen? Was ist das Äquivalent eines Papier-Originals in der Welt der elektronischen Beweismittel? Einzureichen ist eine Vervielfältigung einer Datei der Entstehungskategorie E respektive die Ausgangsdatei beim EzuE- sowie beim EzuPzuE-Vorgang.

[53] Wenn in der Praxis dennoch veränderte Beweismittel eingereicht werden müssen[147], empfiehlt es sich, sowohl die Ausgangsdateien wie auch die in veränderter Form eingereichten Dateien in Rechtsschriften bzw. in Beweismittelverzeichnissen eineindeutig sowohl mit dem Hashwert (bspw. dem verbreiteten SHA-256[148]), dem Dateinamen der Ausgangsdatei und der Dateiformat-Angabe als MIME type zu versehen und den Grund für die Veränderung anzugeben. Ein solcher Nachweis könnte wie folgt aussehen:

[54] Beweismittel 1: E-Mailnachricht vom 11.11.2011

Eingereichte, konvertierte Datei	Ausgangsdatei
Begründung Veränderung: Dateiformat numerus clausus der Übermittlungsplattform	
Dateiname: [11.11.2011.pdf]	Dateiname: [RE: 11.11.2011_Müller.msg]

144 Metadaten, OCR-Layer.

145 Vgl. Fn. 25.

146 Ob die Veränderungen beweisrelevant sind, ist eine Frage, die sich regelmässig dann beantworten lässt, wenn die Veränderungen überhaupt erst ersichtlich sind.

147 Beispielsweise weil eine Übermittlungsplattform einen Dateiformat numerus clausus vorsieht und keine alternative elektronische Übermittlung (bspw. per vertraulichem E-Mail oder Datenträger-Versand) möglich ist.

148 Der Hashwert SHA-256 wird bspw. auch bei den vom Bund zur Verfügung gestellten diskreten und nicht-diskreten Validatorentools ausgewiesen.

MIME type: [application/pdf]	MIME type: [application/vnd.ms-outlook]
SHA-256: [79b1684dc17f8e41dc9ffce8cb04e0eccb 2e4684bd18a0813dfff2efb45ea047]	SHA-256: [207010de06aec701dc4c9462e f4aedec 542e4736803411c6419bae031e81ad6c].

[55] Doch auch bei unabsichtlich veränderten elektronischen Beweismitteln stellt die Frage nach der Echtheit und Integrität eine Herausforderung dar. Dies insbesondere, weil auch die Ursachen für versehentliche[149] Veränderungen von Dateien mannigfaltig sind[150]. Zudem ist der Nachweis der Nichtveränderung bzw. Veränderung allein aufgrund der vorgelegten Datei oft nicht möglich[151], wie die folgenden zwei Beispiele zeigen:

- Mit verschriftlichten Hashwerten von Dateien, die zu Dokumentationszwecken mit qualifizierten Zeitstempeln versehen wurden, lässt sich die Tatsache festhalten, dass eine bestimmte Datei (identifiziert anhand ihres Hashwerts) zu einem bestimmten Zeitpunkt existierte.
- Mit qualifizierten elektronischen Zeitstempeln und qualifizierten elektronischen Signaturen, die bspw. in PDF-Dateien angebracht werden, lässt sich die Tatsache festhalten, dass ein bestimmter Teil einer Datei (identifiziert anhand des Hashwerts dieses Dateiteils) zu einem bestimmten Zeitpunkt existierte.
- Hashwerte, die mit qualifiziertem elektronischen Zeitstempel dokumentiert wurden, lassen hingegen keinen Rückschluss auf die Tatsache zu, dass eine bestimmte Datei (identifiziert anhand ihres Hashwerts) zu einem bestimmten Zeitpunkt effektiv auf einem bestimmten Datenträger gespeichert war.

5. Fazit, Vorkehrungen in der Praxis

[56] Das Fazit aus den vorstehenden Ausführungen ist, dass sowohl in Anwaltskanzleien wie auch bei Behörden und Gerichten Vorkehrungen für einen sorgfältigen Umgang mit elektronischen Beweismitteln nötig sind. Nachfolgend führen wir mögliche minimale Vorkehrungen auf:

1. Elektronische Beweismittel müssen so gespeichert werden, dass sie nicht (unbeabsichtigt) verändert werden (können).[152,153]
2. Elektronische Beweismittel müssen so gespeichert werden, dass das Speichern bei einschlägigen Inhalten nicht den Tatbestand des strafbaren Inverkehrbringens erfüllt.

149 Elektronische Beweismittel sind so zu speichern, dass sie nicht versehentlich verändert werden (können). Sowohl Gerichte/Behörden wie auch Rechtsanwältinnen und Rechtsanwälten müssen in der Lage sein, die Integrität der gespeicherten Dateien anhand von Soll- und Ist-Werten zu überprüfen.

150 Dateien werden bspw. von bestimmten GEVER-Softwares verändert (Hinzufügen von Datei-Metadaten) oder etwa beim Versand über gewisse E-Mail-Apps (Veränderung u.a. der EXIF-Daten von Bilddateien).

151 Vgl. dazu auch Ziffer 2.4.4.

152 Insbesondere Geschäftsverwaltungssoftwares und Fachanwendungen sind dazu u.U. nicht geeignet, vgl. Fn 150. Für elektronische Beweismittel sind u.U. separate geeignete Speicherinfrastrukturen nötig.

153 Vergleichbare Anforderungen an Systeme formuliert Art. 9 ff. der Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung; GeBüV) vom 24. April 2002 (SR 221.431). Dass Analysen von elektronischen Beweismitteln mit vervielfältigten Daten durchgeführt werden, versteht sich von selbst.

3. Insbesondere einschlägige elektronische Beweismittel müssen so gespeichert werden, dass Dritte (auch Dienstleister) zu keinem Zeitpunkt Kenntnis der Hashwerte der Dateien erlangen können.[154]
4. Elektronische Beweismittel müssen so gespeichert werden, dass sie bei Bedarf vernichtet werden können.[155] Gleichzeitig dürfen elektronische Beweismittel nicht ohne Bedacht gelöscht werden. Es sind – wie bei Papierdokumenten – die gesetzlichen Vorschriften über minimale und maximale Aufbewahrungsdauern zu beachten. Die erschöpfende (z.B. erfolgreiche) Verwendung eines Beweismittels in einem Verfahren befreit nicht von den noch andauernden Aufbewahrungsfristen.
5. Elektronische Beweismittel müssen beim Empfang und vor dem Versand eindeutig identifiziert werden (Hashwert), so dass Veränderungen bei der aufbewahrenden Stelle nachvollziehbar sind.
6. Elektronische Beweismittel sind hinsichtlich Entstehungsart und Entstehungskontext zu kategorisieren. Sind die Beweismittel durch EzuE- sowie EzuPzuE-Vorgänge entstanden, ist zu klären, ob die Ausgangsdatei (inkl. Kontextinformationen) erhältlich gemacht werden kann und weshalb die Veränderungen vorgenommen wurden. PzuE-Vorgänge (Scans) sind standardisiert und nach einschlägigen Standards (bspw. gemäss der Technischen Richtlinie TR Resiscan) durchzuführen.
7. Elektronische Beweismittel müssen so übermittelt werden, dass sie bei der Übermittlung nicht verändert werden.
8. Elektronische Beweismittel sind einzeln und ohne vorgängige Veränderung durch die Parteien, Behörden und Gerichte in Verfahren einzubringen.[156]
9. Elektronische Beweismittel werden mittels Hashwert(en) identifiziert (und nicht etwa anhand ihres Dateinamens). Softwares zur Berechnung und Überprüfung von Hashwerten[157] gehören deshalb zur Grundausstattung.
10. Elektronische Beweismittel sind nach vorgängiger Risikoanalyse vor der Einführung in ein Verfahren mit geeigneten Softwares zu analysieren.

[57] Hinsichtlich Sicherung (acquisition) von elektronischen Beweismitteln sowie hinsichtlich IT-Grundschutz wird auf die einschlägige Fachliteratur verwiesen.

154 Um vom Inhalt von elektronischen Beweismitteln Kenntnis zu erhalten, müssen die entsprechenden Dateien nicht zwingend «geöffnet» werden. Auch Hashwerttreffer (Abgleich von Hashwerten mit Sets von Hashwerten) lassen Rückschlüsse auf Inhalte zu. Beispiele von Hashwert-Sets: Reference Data Set (RDS) der National Software Reference Library (NSRL), https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download; Child Abuse Image Database (CAID) sets, https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download/non-rds-hash, beide Webseiten zuletzt besucht am 24. April 2024.

155 Dies bedeutet u.U. dass die elektronischen Beweismittel separat auf physisch vernichtbaren Datenträgern gespeichert werden müssen.

156 Es gibt Softwares, die Beweismittelverzeichnisse in Papierform zu simulieren versuchen und elektronische Beweismittel ungeachtet ihres Formats zu PDF-Bundles gruppieren und mit «Stempeln» und dergleichen verzieren und die Beweismittel dadurch verändern.

157 Bspw. Powershell (Windows), Total Commander (Windows).

6. Exkurs: Beweisaufnahme in Verhandlungen mittels elektronischen Mitteln zur Bild- und Tonübertragung

6.1. Grundsätzliches

[58] Der vorliegende Artikel befasste sich bisher vor allem mit jener Art von Beweismitteln, welche im schweizerischen Strafprozessrecht als «sachliche Beweismittel» (Art. 192–195 StPO) bezeichnet werden, also mit Unterlagen (in elektronischer Form meistens Dateien), die von Verfahrensparteien eingereicht oder von den instruierenden Behörden beschafft werden. Klassischerweise kennen aber das Zivil- und Strafprozessrecht – eher weniger das Verwaltungsverfahrensrecht[158] – auch Beweismittel, welche in Instruktions- oder Hauptverhandlungen durch mündliche Aussagen von Verfahrensbeteiligten, Dritten oder Sachverständigen entstehen, insbesondere durch Befragungen von Zeuginnen und Zeugen, von Sachverständigen oder der Verfahrensparteien.

[59] Wenn diese Instruktions- oder Hauptverhandlungen nicht vollständig unter physischer Anwesenheit aller Beteiligten in einem Gerichtssaal stattfinden, sondern unter Zuhilfenahme von elektronischen Mitteln zur Bild- oder Tonübertragung (d.h. Videokonferenz-Tools, Telefonkonferenz-Tools o.ä.) durchgeführt werden, dann erfolgt die Beweisaufnahme elektronisch und mit den Aufzeichnungen solcher Verhandlungen liegen ebenfalls elektronische Beweismittel vor. Auf diese soll nachfolgend in diesem Exkurs eingegangen werden. Bewusst ausgeklammert werden hier Fragen des Datenschutzes und der Prozessöffentlichkeit.

6.2. Regelungen im schweizerischen Zivil- und Strafprozessrecht

[60] Gerichtsverhandlungen mit elektronischen Mitteln zur Bild- und Tonübertragung (insb. Videokonferenz-Tools) sind in zahlreichen europäischen Staaten seit Längerem geregelt und eingesetzt.[159] In Deutschland beispielsweise gehört die Möglichkeit der «Verhandlung im Wege der Bild und Tonübertragung» mit § 128a ZPO-DE als Variante des Vorgehens zum ordentlichen Zivilprozessrecht. Die Regelung wurde durch das ZPO-Reformgesetz[160] per 1. Januar 2002 eingeführt.

[61] Das schweizerische *Zivilprozessrecht* kennt heute keine Gerichtsverhandlungen mit elektronischen Mitteln zur Bild- und Tonübertragung. Das Bundesgericht hat festgehalten, dass die ZPO die Durchführung von Gerichtsverhandlungen per Videokonferenz nicht zulasse[161] Während der Covid-19-Pandemie war das vorübergehend anders: Am 16. April 2020 erliess der Bundesrat die COVID-19-Verordnung Justiz und Verfahrensrecht[162], mit welcher er Video- und Telefon-

158 Etwa in bau-, planungs- und umweltrechtlichen Verfahren in der Form von Augenscheinen, die dann zu einem Protokoll und allenfalls zu fotografischen oder anderen technischen Aufnahmen bzw. Messungen führen.

159 Siehe die Übersicht bei Anne Sanders, Video Hearings in Europe Before, During and After the COVID-19 Pandemic, International Journal for Court Administration, 2021, Volume 12, Issue 2, DOI: 10.36745/ijca.379, zuletzt konsultiert am 22. April 2024.

160 BGBl. I S. 1887; Art. 2 Nr. 18a.

161 Urteil 4A_180/2020 des Bundesgerichts vom 6. Juli 2020, E. 3.7.

162 Verordnung über Massnahmen in der Justiz und im Verfahrensrecht im Zusammenhang mit dem Coronavirus (COVID-19-Verordnung Justiz und Verfahrensrecht) vom 16. April 2020, AS 2020 1229, SR 272.81; in Kraft vom 20. April 2020 bis 31. Dezember 2022.

konferenz-Anwendungen in zivilrechtlichen Verfahren zuliess und regelte.[163] Die Verordnung sah die Möglichkeit von Verhandlungen per Videokonferenz (in bestimmten Fällen per Telefon) für Verhandlungen, Anhörungen und Einvernahmen von Gerichten, Schlichtungsbehörden sowie Kindes- und Erwachsenenschutzbehörden vor. Evaluiert wurden diese Anwendungen während der Pandemie nicht, so dass kaum gesicherte Erfahrungen bestehen. Die beschlossene Änderung der ZPO, die auf den 1. Januar 2025 in Kraft treten wird, sieht nun in Art. 141a und 141b ZPO[164] vor, dass ein Gericht mündliche Prozesshandlungen auf Antrag oder von Amtes wegen mittels elektronischer Mittel zur Ton- und Bildübertragung, insbesondere mittels Videokonferenz, durchführen oder den am Verfahren beteiligten Personen die Teilnahme mittels solcher Mittel gestatten kann.[165] Der Entwurf der zugehörigen Verordnung über den Einsatz elektronischer Mittel zur Ton- und Bildübertragung in Zivilverfahren (VE-VEMZ) befindet sich bis zum 22. Mai 2024 in der Vernehmlassung. Die Verordnung regelt die technischen Voraussetzungen sowie die Anforderungen an den Datenschutz und die Datensicherheit. Ein Gericht kann künftig auch die Einvernahme einer Zeugin oder eines Zeugen mittels Videokonferenz oder anderen elektronischen Mitteln zur Ton- und Bildübertragung durchführen oder eine Zeugin oder einen Zeugen mittels solcher Mittel befragen, während die übrigen Teilnehmerinnen und Teilnehmer in den Räumlichkeiten des Gerichts anwesend sind, sofern keine überwiegenden öffentlichen oder privaten Interessen, namentlich die Sicherheit der Zeugin oder des Zeugen, entgegenstehen (Art. 170a ZPO[166]). Bei der Anhörung eines Kindes soll allerdings der Einsatz elektronischer Mittel zur Ton- und Bildübertragung weiterhin unzulässig sein. Bei Zeugeneinvernahmen, Parteibefragungen, Beweisaussagen und persönlichen Anhörungen erfolgt eine Aufzeichnung; bei den übrigen Verhandlungen kann ausnahmsweise auf Antrag oder von Amtes wegen eine Aufzeichnung erfolgen, soweit eine Verhandlung nicht ausschliesslich der freien Erörterung des Streitgegenstandes oder dem Versuch der Einigung dient (Art. 141b Abs. 1 Bst. b ZPO[167]). Die Aufzeichnungen werden zu den Akten genommen (Art. 176a Bst. c ZPO[168]), ersetzen aber nicht die ordentliche Protokollierung. Die Aussagen von Einvernahmen (namentlich von Zeugeneinvernahmen) können auch sonst zusätzlich auf Tonband, auf Video oder mit anderen geeigneten technischen Hilfsmitteln aufgezeichnet werden (Art. 176 Abs. 2 ZPO).

[62] Das *Strafprozessrecht* sieht den Einsatz solcher elektronischen Mittel schon seit 2011 vor: Staatsanwaltschaft und Gerichte können eine Einvernahme mittels Videokonferenz durchführen, wenn das persönliche Erscheinen der einzuvernehmenden Person nicht oder nur mit grossem Aufwand möglich ist (Art. 144 Abs. 1 StPO). Die Einvernahme wird in Ton und Bild festgehalten (Art. 144 Abs. 2 StPO). Zudem kann die Verfahrensleitung anordnen, dass Verfahrenshandlungen

163 Ausführlich dazu Daniel Kettiger, Gerichtsverhandlungen, Anhörungen und Einvernahmen mittels Videokonferenz, in: Jusletter 4. Mai 2020.

164 Fassung gemäss Ziff. I des BG vom 17. März 2023 (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung), in Kraft ab 1. Januar 2025; BBl 2020 2697).

165 Ausführlich dazu Sandra Mariot, Le recours à des moyens électroniques de transmission du son et de l'image (audience par vidéoconférence) selon le CPC révisé.

166 Fassung gemäss Ziff. I des BG vom 17. März 2023 (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung), in Kraft ab 1. Januar 2025 (AS 2023 491; BBl 2020 2697).

167 Fassung gemäss Ziff. I des BG vom 17. März 2023 (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung), in Kraft ab 1. Januar 2025 (AS 2023 491; BBl 2020 2697).

168 Fassung gemäss Ziff. I des BG vom 17. März 2023 (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung), in Kraft ab 1. Januar 2025 (AS 2023 491; BBl 2020 2697).

zusätzlich zur schriftlichen Protokollierung ganz oder teilweise in Ton oder Bild festgehalten werden (Art. 76 Abs. 4 StPO).

6.3. Beweisrechtliche Herausforderungen

6.3.1. Identitätsprüfung der Teilnehmenden

[63] Insbesondere dann, wenn Zeuginnen und Zeugen oder Sachverständige einvernommen werden, muss Sicherheit über ihre Identität bestehen. Technisch ist es nämlich möglich, dass sich durch «Identitätsdiebstahl» Dritte Zugang zu den Zugangsdaten und damit zur Einvernahme per Videokonferenz verschaffen könnten, dies mit der Absicht, das Gerichtsverfahren zu manipulieren. Eine Einvernahme hat nur dann einen Beweiswert, wenn Sicherheit über die Identität der befragten Person besteht. Erstaunlicherweise ist man offenbar der Ansicht, das Gericht habe – zumindest im Zivilprozess – nicht die Pflicht, die Identität der teilnehmenden Personen zu überprüfen; diese Pflicht soll nur bestehen, wenn Zweifel an der Identität bestehen (vgl. Art. 7 Abs. 2 VE-VEMZ).[169] Wie eine Identitätsprüfung sicher vorgenommen werden soll, ist auch relativ unklar: Offenbar wird davon ausgegangen, dass sich eine teilnehmende Person vor der Videokamera mit einem Lichtbildausweis ausweisen soll.[170)] Eine einigermassen sichere Identitätsprüfung kann aber wohl nur mit Mitteln einer elektronischen Identität (eID) stattfinden. Eine andere Möglichkeit könnte darin bestehen, einer teilnehmenden Person bei sicherer Kenntnis von deren Mobiltelefonnummer je Teile der Zugangsdaten via E-Mail und SMS zukommen zu lassen bzw. für den Zugang eine Zweiphasen-Authentifizierung vorzusehen.

6.3.2. Aufbewahrung der Aufzeichnungen

[64] Ton- und Bildaufzeichnungen können heute relativ einfach manipuliert werden – neu auch mit Hilfe von Künstlicher Intelligenz (KI)[171]. Eine Herausforderung ist somit, die Aufzeichnungen von Verhandlungen zu erhalten und vor Veränderungen geschützt aufzubewahren. Das dürfte insbesondere dann nicht ganz trivial sein, wenn die Aufzeichnung durch Dritte, d.h. von den Betreibern von Systemen von elektronischen Mitteln zur Bild- und Tonübertragung erfolgt (siehe auch Art. 8 VE-VEMZ). Das Problem entsteht allenfalls dadurch, dass solche Aufzeichnungen zu den Akten genommen werden müssen. Nun ist aber bei bestimmten Videokonferenz-Tools die Aufzeichnung nur beim Anbieter bzw. auf den von diesem betriebenen Servern vorhanden und zum Transfer auf Datenträger der Justizbehörde sowie zur Verwendung auf herkömmlichen Geräten ist u.U. eine Konvertierung notwendig (i.d.R. ins MP4-Format). Mit einer solchen Konvertierung wird aber die Aufzeichnung verändert. Eine mögliche Lösung besteht darin, dass der Hashwert sowohl der Rohdateien (Ausgangsdatei) der Aufzeichungen wie auch die konvertierte Form der Aufzeichnung vom Dienstleister in geeigneter Form beglaubigt wird und dass die Rohdaten bei Bedarf ebenfalls übermittelt werden.

169 Vgl. dazu auch die Erläuterungen zum VE-VEMZ, S. 21.

170 Vgl. dazu auch die Erläuterungen zum VE-VEMZ, S. 21.

171 Man spricht auch von Deepfakes: Deepfakes sind täuschend echt wirkende, jedoch künstlich erstellte oder veränderte Foto-, Video- oder Sprachaufzeichnungen. Dabei kann es sich um einzelne Bilder von realen oder gänzlich neu erschaffenen Personen handeln. Stimmen können imitiert oder neu erschaffen werden.

[65] Die Verwendung von elektronischen Mitteln zur Bild- und Tonübertragung bei Verhandlungen erfordert, dass die neu zu schaffende elektronische Akte auch Formate von Bild- und Tonaufzeichnungen enthalten darf.

Claudia Schreiber, lic. en droit, Rechtsanwältin und dipl. Ing. ETH, ist Inhaberin einer Anwaltskanzlei in Bern und Projektleiterin im Bereich Records Management und Archivierung.

Daniel Kettiger, Mag. rer. publ., Rechtsanwalt, ist Inhaber einer Anwaltskanzlei in Bolligen und Justizforscher.

Die Autoren danken Dr. Jörn Erbguth und Dr. Andreas Flückiger für die kritische Durchsicht des Manuskripts und die wertvollen Hinweise.