DIGITALE BEWEISE IM STRAF- UND ZIVILPROZESS

Frederik Möllers / Simone Salemi / Natascha Schliwinski

Stellv. Geschäftsführer, Saarbrücker Zentrum für Recht und Digitalisierung, Universität des Saarlandes
Campus C3 1, 66123 Saarbrücken, DE
frederik.moellers@zrd-saar.de; https://www.zrd-saar.de

Wissenschaftliche Mitarbeiterin, Saarbrücker Zentrum für Recht und Digitalisierung, Universität des Saarlandes
Campus C3 1, 66123 Saarbrücken, DE
simone.salemi@zrd-saar.de; https://www.zrd-saar.de

Studentische Mitarbeiterin, Lehrstuhl für Rechtsinformatik, Universität des Saarlandes
Campus C3 1, 66123 Saarbrücken, DE
natascha.schliwinski@uni-saarland.de; https://www.legalinf.de

Schlagworte: ***Digitale Beweise, Beweismittel, Beweiswert, Zivilprozess, Strafprozess, Signaturen, Siegel, Authentizität***

Abstract: *Das Einbringen von Screenshots, ausgedruckten E-Mails oder Videoaufzeichnungen als Beweise in ein Gerichtsverfahren gewinnt verstärkt an Bedeutung. Dies ist darauf zurückzuführen, dass Kommunikation in weiten Teilen online stattfindet und kriminelle Handlungen über das Internet geplant oder sogar durchgeführt werden. Problematisch erscheint die Würdigung solcher digitalen Spuren vor Gericht, als an diese aufgrund vergleichsweise leichter Fälschbarkeit besondere Anforderungen hinsichtlich ihrer Authentizität zu stellen sind. Bei der Verwendung elektronischer Signaturen, Zeitstempel oder Siegel kann diese zwar validiert werden. Diese Möglichkeiten finden in der Praxis jedoch nur vereinzelt Anwendung. Gleichzeitig werden die Chancen, die digitale Spuren bieten, oft nicht wahrgenommen. Es zeigen sich Unstimmigkeiten hinsichtlich der Einschätzung des Beweiswertes elektronischer Spuren aus technischer und juristischer Sicht. Dieser Beitrag zeigt auf, welche Schwierigkeiten sich bei der Verwendung digitaler Spuren vor Gericht ergeben und in welchen Bereichen noch Potential für Reformen oder Handlungsbedarf besteht.*

1. Einleitung

Technologischer Fortschritt bringt im Alltag unbestreitbar Vorteile und Arbeitserleichterungen mit sich. Anders sieht es teilweise bei der Tätigkeit von Ermittlungsbehörden und Gerichten aus. Die zunehmende Digitalisierung der Gesellschaft ist zugleich Einfallstor für kriminelle Handlungen. So entstehen nicht nur neue Sphären der Kriminalität (insbesondere im Bereich der Wirtschaftskriminalität)[1], sondern auch neue Herausforderungen für Ermittlungsbehörden. Digitale Spuren gewinnen zunehmend an Bedeutung. So findet eine wachsende Anzahl an Beleidigungsdelikten auf Sozialen Netzwerken statt[2], die Betäubungsmittelkriminalität wird in das „Darknet" verlegt[3] und Amazons „Alexa" kann eine potenzielle „Zeugin" darstellen[4]. Die Probleme, die sich hieraus ergeben, liegen auf der Hand: Für die zuverlässige Sicherung der digitalen Spuren ist eine besondere Expertise erforderlich, da diese nicht physikalisch greifbar sind. Auch die Verwertung digitaler Beweise im Gerichtsverfahren stellt sich als komplex dar. Einerseits wird der Beweiswert von besonders manipulationssicheren digitalen Beweisen häufig unterschätzt, andererseits wird teilweise (technisch gesehen)

1 Müller, NZWiSt 2020, 96 (96).
2 Brodowski/Jahn in: Hoven/Kudlich, Digitalisierung und Strafverfahren, S. 70.
3 Brodowski/Jahn in: Hoven/Kudlich, Digitalisierung und Strafverfahren, S. 70.
4 Blechschmitt, MMR 2018, 361 (363).

unzuverlässigen Beweisen fälschlicherweise Authentizität zugesprochen. Hier zeigt sich eine Diskrepanz zwischen technischem Sachverstand und juristischer Expertise bei der Beweisverwertung. Die vorliegende Abhandlung widmet sich dieser Herausforderung und soll einen Beitrag zur Lösungsfindung bei einem Problem leisten, welches voraussichtlich auch in Zukunft immer relevanter wird.

2. Beweise im Zivilprozess

Das Verfahren vor einem deutschen Zivilgericht zeichnet sich insbesondere dadurch aus, dass es vom Willen der beteiligten Parteien (Kläger und Beklagter) bestimmt wird. Als Ausfluss der das Zivilrecht bestimmenden Privatautonomie besagt die Dispositionsmaxime, dass die Gestaltung des Prozesses hinsichtlich Beginn, Gegenstand und Ende des Verfahrens allein den Parteien obliegt.[5] Das Verfahren beginnt erst mit dem Klagevorbringen des Klägers (§ 253 Zivilprozessordnung, ZPO) und kann von den Parteien selbstbestimmt zu einem vorzeitigen Ende ohne Urteil des Richters in der Sache gebracht werden.[6] Bspw. ergeht im Falle einer Klagerücknahme (§ 269 ZPO) oder einer beiderseitigen Erledigungserklärung (§ 91a ZPO) nur noch eine Kostenentscheidung.[7] Auch hinsichtlich der dem Urteil zugrundeliegenden Tatsachen ist das Vorgehen der Parteien entscheidend.[8] Das Gericht darf nämlich nur diejenigen Tatsachen in das Urteil miteinfließen lassen, die von den Parteien vorgebracht wurden.[9] Dies geht auf den sogenannten Beibringungsgrundsatz zurück.[10] Aus diesem folgt auch, dass die Beweisermittlung und Nachforschung durch den entscheidenden Richter grundsätzlich unzulässig ist.[11] Die Parteien sind vielmehr dazu verpflichtet, die für sie günstigen Tatsachen, die für den Prozess von Bedeutung sind, vorzutragen.[12] Zwar existieren auch Ausnahmen vom Beibringungsgrundsatz, wie sich bspw. aus § 139 Abs. 3 ZPO ergibt. Dies stellt jedoch nicht die grundsätzliche Geltung des Beibringungsgrundsatzes in Frage.[13] Der zuständige Richter prüft mittels der sogenannten „Relationstechnik" zunächst die Schlüssigkeit der Klage und sodann die Erheblichkeit des Beklagtenvortrags.[14] Im Rahmen der Schlüssigkeitsprüfung wird überprüft, ob der Tatsachenvortrag des Klägers in Verbindung mit einem Rechtssatz dazu geeignet ist, den geltend gemachten Anspruch zu begründen[15], während bei der Erheblichkeitsprüfung Einreden und Einwendungen des Beklagten geprüft werden müssen.[16]

2.1. Beweisarten

In das Verfahren eingebrachte Beweise lassen sich in verschiedene Kategorien unterteilen. Man kann nach Ziel, Zweck, Art der Beweisführung sowie nach dem Beweisverfahren unterscheiden.[17] Hinsichtlich des Ziels wird zwischen Vollbeweis und Glaubhaftmachung differenziert. Beide unterscheiden sich im Beweismaß[18], welches den Maßstab richterlicher Überzeugung betrifft.[19] Für die Glaubhaftmachung genügt es, wenn die zugrundeliegende Tatsache überwiegend wahrscheinlich ist,[20] während beim Vollbeweis die vollständige

5 Jacoby, Zivilprozessrecht, Rn. 84.
6 Saenger in: Saenger, Zivilprozessordnung, Einführung Rn. 63, 64.
7 Saenger in: Saenger, Zivilprozessordnung, Einführung Rn. 63.
8 BVerfG, NJW 1995, 40 (40).
9 BVerfG, NJW 1995, 40 (40).
10 BGH, NJW 1994, 3295 (3296); BGH, NJW 1998, 156 (159).
11 BGH, NJW 1994, 3295 (3296).
12 Möller, JA 2010, 47 (49).
13 Rosenberg, Zivilprozessrecht, § 77 Rn. 5.
14 Jacoby, Zivilprozessrecht, Rn. 528 ff.
15 BGH, NJW 1984, 2888 (2889).
16 Jacoby, Zivilprozessrecht, Rn. 532.
17 Prütting in: MüKo ZPO, § 284 Rn. 19.
18 Prütting in: MüKo ZPO, § 284 Rn. 23.
19 Prütting in: MüKo ZPO, § 286 Rn. 28.
20 BGH, NJW 1998, 1870 (1870).

richterliche Überzeugung vorliegen muss.[21] Nach dem Zweck des Beweises unterscheiden sich Haupt- und Gegenbeweis. Der Hauptbeweis wird von der beweisbelasteten Partei erbracht und dient dazu, das Gericht von der Wahrheit einer Tatsachenbehauptung zu überzeugen.[22] Der Gegenbeweis wird von der Gegenpartei erbracht und zielt darauf ab, beim Richter Zweifel an der Richtigkeit der Tatsachenbehauptungen der beweisbelasteten Partei zu säen und seine Überzeugungen zu erschüttern.[23] Voneinander zu trennen sind ebenfalls der unmittelbare und der Indizienbeweis. Der Indizienbeweis wird auch als mittelbarer Beweis bezeichnet und bezieht sich auf Hilfstatsachen oder Vorfragen zu einer Tatsache[24], die den Schluss auf das Vorliegen eines Tatbestandsmerkmals zulassen.[25] Mit dem unmittelbaren Beweis wird hingegen unmittelbar das Vorliegen eines Tatbestandsmerkmals bewiesen.[26] Nach dem Beweisverfahren lassen sich Streng- und Freibeweis voneinander unterscheiden. Der Strengbeweis ergeht mittels der förmlichen, gesetzlich geregelten Beweismittel aus den §§ 371 ff ZPO in einem dafür gesetzlich vorgesehenen Verfahren.[27] Davon abzugrenzen ist der Freibeweis, welcher nicht an die gesetzlich geregelten Beweismittel gebunden ist.[28]

2.1.1. Strengbeweis

Das förmliche Strengbeweisverfahren ist gesetzlich in den §§ 355 ff. ZPO geregelt.[29] Die Beweismittel, die den Parteien dann ausschließlich zustehen, sind in den §§ 371 ff. ZPO normiert. Es existieren Augenscheinsbeweis, Zeugenbeweis, Sachverständigenbeweis, Urkundsbeweis und Parteivernehmung. Beim Beweis durch Augenschein (§§ 371 ff. ZPO) wird der Gegenstand des Augenscheins sowie die zu beweisende Tatsache angegeben, § 371 Abs. 1 S. 1 ZPO. Diese wird durch eine Sinneswahrnehmung des Gerichts bewiesen[30] (hierzu gehören neben dem Sehen bspw. auch das Hören und Riechen)[31]. Die gesetzliche Normierung des Zeugenbeweises findet sich in den §§ 373 ff. ZPO. Sowohl der Zeuge als auch die zu beweisende Tatsache müssen benannt werden; hierbei muss das Thema des Zeugenbeweises substantiiert vorgetragen werden.[32] Der Sachverständige (§§ 402 ff. ZPO) zieht, im Gegensatz zu einem Zeugen, aus dem Sachverhalt Schlussfolgerungen, die auf seinen besonderen Erfahrungssätzen und Fachkenntnissen beruhen[33] und ist dabei Gehilfe des Gerichts.[34] Die Urkunde ist eine verkörperte Gedankenerklärung, wobei es nicht erforderlich ist, dass sie eine rechtlich relevante Erklärung enthält.[35] Handelt es sich um eine schriftliche Urkunde, gilt diese als Beweismittel unabhängig davon, ob sie von Anfang an dazu bestimmt war und unabhängig von ihrem Beweiswert.[36] Der Urkundsbeweis ist in den §§ 415 ff. ZPO geregelt. Bei der Parteivernehmung werden die primär am Verfahren beteiligten Personen – die Parteien – vernommen (§§ 445 ff. ZPO). Es handelt sich jedoch um ein subsidiäres Beweismittel, welches erst zum Einsatz kommt, wenn die Partei den ihr obliegenden Beweis mit anderen Beweismitteln nicht vollständig geführt oder andere Beweismittel nicht vorgebracht hat.[37]

---

21 Prütting in: MüKo ZPO, § 286 Rn. 41.
22 Jacoby, Zivilprozessrecht, Rn. 523.
23 Prütting in: MüKo ZPO, § 284 Rn. 21.
24 Foerste in: Musielak/Voit, ZPO, § 284 Rn. 7.
25 Pohlmann, Zivilprozessrecht, § 8 Rn. 365.
26 Pohlmann, Zivilprozessrecht, § 8 Rn. 365.
27 Foerste in: Musielak/Voit ZPO, § 284 Rn. 5.
28 Foerste in: Musielak/Voit ZPO, § 284 Rn. 5.
29 Pohlmann, Zivilprozessrecht, § 8 Rn. 367.
30 Bach in: BeckOK ZPO, § 371 Rn. 1.
31 Zimmermann in: MüKo ZPO, § 371 Rn. 2.
32 Scheuch in: BeckOK ZPO, § 373 Vorbemerkung.
33 BGH, NJW 2007, 2122 (2124 Rn. 21).
34 BGH, DS 2006, 354 (355 Rn. 11).
35 BGH, NJW 1998, 58 (59); BGH, NJW 1976, 294 (294); Krafka in: BeckOK ZPO, § 415 Rn. 1; Huber in: Musielak/Voit ZPO, § 415 Rn. 4.
36 Rosenberg, Zivilprozessrecht, § 120 Rn. 2.
37 Bechteler in: BeckOK ZPO, § 445 Rn. 1.

3. Beweise im Strafprozess

Der Strafprozess vor einem deutschen Gericht unterscheidet sich grundlegend vom Zivilprozess. Die dort geltenden Verfahrensgrundsätze sind nicht zu übertragen. Aus §§ 152, 170 Strafprozessordnung (StPO) ergeben sich die Offizialmaxime sowie das Legalitätsprinzip.[38] Die Offizialmaxime stellt das Gegenteil der im Zivilprozessrecht geltenden Dispositionsmaxime dar. Nach § 152 Abs. 1 StPO ist nämlich die Staatsanwaltschaft dazu berufen, öffentlich Anklage zu erheben und damit ein Verfahren einzuleiten. Das Legalitätsprinzip ist in §§ 152 Abs. 2, 170 Abs. 1 StPO normiert. Demnach ist die Staatsanwaltschaft dazu verpflichtet, einem Anfangsverdacht nachzugehen und ein Ermittlungsverfahren einzuleiten.[39] Dementsprechend unterscheiden sich auch die Grundsätze der Beweiserhebung.

3.1. Beweisgrundsätze

Der Strafprozess dient der Erforschung des wahren Sachverhalts.[40] Das zuständige Gericht ist daher gemäß § 244 Abs. 2 StPO dazu verpflichtet, von Amts wegen den Sachverhalt, der dem Urteil zugrunde gelegt werden soll, zu untersuchen[41] und dabei alle relevanten Tatsachen zu ermitteln[42]. Dabei dürfen nur solche Tatsachen in das Urteil miteinfließen, die in der Hauptverhandlung vor dem entscheidenden Gericht dargelegt und erörtert wurden (Mündlichkeits- und Unmittelbarkeitsgrundsatz).[43]

3.2. Beweisarten

Auch im Strafprozess ist zwischen verschiedenen Beweisarten zu unterscheiden. So existieren auch hier der unmittelbare Beweis und der Indizienbeweis.[44] Daneben kann noch der Beweis für Haupt- und Nebentatsachen vom Beweis für Hilfstatsachen abgegrenzt werden. Hilfstatsachen belegen den Beweiswert eines originären Beweises einer Tatsache, die nicht zum gesetzlichen Tatbestand der vorgeworfenen Straftat gehört.[45] Zudem existieren auch im Strafverfahren Frei- und Strengbeweisverfahren, wobei ausschließlich letzteres zur Sachverhaltsklärung im Hauptverfahren eines Strafprozesses zulässig ist.[46]

3.2.1. Strengbeweis

Im Strengbeweisverfahren dürfen nur die gesetzlich geregelten Beweismittel verwendet werden. Die im Strengbeweisverfahren zugelassenen Beweismittel werden in der StPO abschließend geregelt[47]; keine eigene Kategorie stellt dabei die Beschuldigtenvernehmung dar.[48]

3.2.1.1. Beweismittel

In der StPO sind die folgenden Beweismittel normiert: Zunächst existiert der Augenscheinsbeweis (§ 86 StPO). Dieser beruht auf der sinnlichen Wahrnehmung des Gerichts, welche sich auf Sachen oder Personen beziehen kann.[49] Ferner gibt es den Zeugenbeweis (§§ 48 ff. StPO). Der Zeuge berichtet vor Gericht von sei-

[38] Hussels, Strafprozessrecht – Schnell erfasst, S. 20 f.
[39] Walter, Strafprozessrecht – Ein Lehrbuch für Studenten und angehende Praktiker, Rn. 114.
[40] Eisenberg in: Eisenberg, Beweisrecht der StPO, Rn. 1 f.
[41] Krehl in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 244 Rn. 27.
[42] Eisenberg in: Eisenberg, Beweisrecht der StPO, Rn. 1.
[43] Eisenberg in: Eisenberg, Beweisrecht der StPO, Rn. 64, 65.
[44] Kudlich in: MüKo StPO, Einleitung Rn. 408.
[45] Bspw. die Glaubwürdigkeit eines Zeugen, vgl. dazu Kudlich in: MüKo StPO, Einleitung Rn. 410.
[46] Kudlich in: MüKo StPO, Einleitung Rn. 411, 413.
[47] Trüg/Habetha in: MüKo StPO, § 244 Rn. 35; BGH, NJW 1961, 1486 (1487).
[48] Eisenberg in: Eisenberg, Beweisrecht der StPO, Rn. 927.
[49] Goers in: BeckOK, StPO, § 86 Rn. 1.

nen Wahrnehmungen über Tatsachen, die im Zusammenhang mit der Tat stehen.[50] Daneben gibt es den Sachverständigen (§§ 78 ff. StPO). Dieser wird eingesetzt, wenn es Gericht und Staatsanwaltschaft an der nötigen Sachkunde fehlt und es zur Ermittlung der relevanten Tatsachen des Fachwissens eines Experten bedarf.[51] Auch im Strafprozess gibt es den Urkundsbeweis. Urkunden (§§ 249 ff. StPO) sind schriftlich verkörperte Gedankenerklärungen, die allgemein verständlich oder deren Inhalt zumindest durch Auslegung ermittelbar ist und die zu Beweiszwecken verlesen werden können.[52]

4. Freie richterliche Beweiswürdigung

Die freie richterliche Beweiswürdigung ist sowohl für den Strafprozess (§ 261 StPO) als auch für den Zivilprozess (§ 286 ZPO) von Bedeutung. Im Strafrecht bedarf es der subjektiven richterlichen Überzeugung von der Schuld des Angeklagten, die jedoch ausreichend durch die Erkenntnisse, die im Hauptverfahren gewonnen wurden, gestützt werden muss. Es braucht eine tragfähige Beweisgrundlage, die die objektiv hohe Wahrscheinlichkeit der Richtigkeit der Beweise beinhaltet.[53] Die Beweiswürdigung ist zwar an sich „frei", aber sie unterliegt trotzdem gewissen Regeln, die aus der forensischen, kriminalistischen und wissenschaftlichen Erfahrung gewonnen wurden.[54] Es bedarf der bestmöglichen Erforschung der materiellen Wahrheit mit den im Strengbeweisverfahren zur Verfügung stehenden Mitteln.[55] Auch im Zivilprozess gilt die freie richterliche Beweiswürdigung. Der Richter unterliegt im Zivilprozess grundsätzlich keinen gesetzlichen Beweisregeln (es sei denn das Gesetz sieht bindende Beweisregeln vor, § 286 Abs. 2 ZPO) und entscheidet selbst, wie er die vorgetragenen Beweise bewerten und in seine rechtliche Würdigung miteinbeziehen will.[56] Trotzdem müssen aus dem Urteil die für die richterliche Entscheidung leitenden Gründe hervorgehen (§ 286 Abs. 1 S. 2 ZPO).

5. Praxis digitaler Beweise

Die bisherigen Ausführungen beziehen sich auf abstrakte Kategorisierungen, welche die Behandlung im Prozess bestimmen und dafür unabhängig von der Ausprägung und Beschaffenheit eines konkreten Beweisstücks sind. Auch lässt sich ein Beweisstück nicht eindeutig und ausschließlich einer Kategorie zuordnen. Bspw. kann der Screenshot eines Kommentars in einem sozialen Netzwerk als Augenscheinsbeweis eingebracht werden. Alternativ kann das Gericht aber auch Zeugen zum Inhalt des Kommentars befragen oder die Metadaten durch Sachverständige analysieren lassen.[57] Damit wird derselbe Sachverhalt auf unterschiedliche Weise aufgeklärt.

Betrachtet man die Verbreitung und den Einsatz digitaler Beweismittel in der Praxis, so ist festzustellen, dass digitale Beweismittel bereits 2018 in rund 85% der Fälle für Ermittlungen in Europa Relevanz besaßen.[58] Im Zuge der Corona-Pandemie hat darüber hinaus Cyberkriminalität in Deutschland weiter an Bedeutung gewonnen, was unweigerlich die Signifikanz von digitalen Beweisen in den Fokus der Justiz rückt.[59] Im folgenden Abschnitt werden daher verschiedene technische Datenformate hinsichtlich ihrer Eignung und Aussagekraft als Beweisstücke in Gerichtsverfahren untersucht. Ziel ist es, einen Bezug zwischen technischen Gegebenheiten und ihrer juristischen Würdigung herzustellen.

---

50 BGH, NJW 1969, 1219 (1220); Eisenberg in: Eisenberg, Beweisrecht der StPO, Rn. 1000.
51 Eisenberg in: Eisenberg, Beweisrecht der StPO, Rn. 1500.
52 Eisenberg in: Eisenberg, Beweisrecht der StPO, Rn. 2000.
53 BVerfG, NJW 2003, 2444 (2445); BGH, NStZ-RR 1996, 202 (202); BGH, NStZ-RR 1997, 42 (43).
54 BVerfG, NJW 2003, 2444 (2445).
55 BVerfGE 133, 168 (226 Rn. 104), Brodowski/Jahn in: Hoven/Kudlich, Digitalisierung und Strafrecht, S. 88.
56 Prütting in: MüKo ZPO, § 286 Rn. 13.
57 Vgl. dazu auch Krüger/Möllers, MMR 2016, S. 728.
58 Dies betrifft strafrechtliche Ermittlungen vor Prozessbeginn, vgl. Folgenabschätzung der Europäischen Kommission SWD (2018) 118 final, S. 14.
59 Vgl. Bundeskriminalamt, Cybercrime, Bundeslagebild 2020, S. 9 f.

Entgegen der gesetzgeberischen Bestrebung, rechtlich akzeptierte technische Maßnahmen zum Erreichen und Einhalten der angestrebten Schutzziele der IT-Sicherheit (z.B. Authentizität) für digitale Beweismittel zu schaffen, mangelt es in der Praxis teils an deren Verbreitung. Deutlich zeigt sich dies am Beispiel der Signaturfunktionen des neuen Personalausweises.

Für die qualifizierte elektronische Signatur ist bspw. nur der Besitz eines neuen Personalausweises sowie die Aufbringung eines Signaturzertifikates notwendig.[60] Für diese Signaturzertifikate gibt es aktuell jedoch keine Anbieter, sodass die qualifizierte elektronische Signatur auf diese Weise nicht ausgestellt werden kann.[61]

Eine Alternative ist die Fernsignatur. Bei dieser wird keine Signaturkarte benötigt, sondern auf einen qualifizierten Drittanbieter vertraut, der die qualifizierte elektronische Signatur nach eindeutiger Identitätsfeststellung für die Person ausstellt.[62] Für die Identitätsfeststellung könnte dabei erneut der Personalausweis verwendet werden. Die dazu erforderliche Online-Ausweisfunktion wird jedoch ebenfalls kaum genutzt.[63]

Die geringe Verbreitung von gesetzlich gewürdigten technischen Maßnahmen schlägt sich auch in der Rechtsprechung nieder. Es werden selten ohne Zeugen oder einen Sachverständigen die technischen Manipulationsmöglichkeiten von digitalen Beweisen thematisiert.[64] Allgemein bleibt das Potential digitaler Beweise ungenutzt, obwohl diese im Verlauf der Jahre immer weiter an Bedeutung gewonnen haben und – mit Blick auf die momentane gesellschaftliche und technologische Entwicklung – auch weiter gewinnen werden.

Besonders die Optionen der qualifizierten elektronischen Signatur und der qualifizierten elektronischen Siegel könnten stärker genutzt werden, da sich diese mit Hilfe eines Validierungsdienstes ohne nennenswerten Mehraufwand prüfen lassen.[65] Ein Anreiz für eine Nutzungssteigerung könnte dabei die Bereitstellung lokaler Validierungsdienste sein. Das *EU Trust Services Dashboard* der EU-Kommission listet für die EU nur 18 Dienste. Acht davon entfallen auf Ungarn, Tschechien und die Slowakei; in Deutschland ist kein Anbieter ansässig.[66]

Verschafft man sich einen Überblick über die in Prozessen vorherrschenden digitalen Beweismittel, so finden sich zwei wesentliche Vorgehensweisen. E-Mails, Websites, Chatprotokolle und andere verlesbare elektronische Dokumente werden einerseits häufig über Screenshots eingereicht.[67] Andererseits werden Audio- und Videodateien oft über eine Plattform (bspw. YouTube) oder nach dem Download in Augenschein genommen.[68]

Betrachtet man die Beweiskraft von Screenshots anhand technischer Kriterien, so bieten diese viele triviale Manipulationsmöglichkeiten. Bereits ein Smartphone mit Bildbearbeitungsfunktion kann zur Manipulation eingesetzt werden. Mit entsprechendem Know-How und geeigneter Technik sind auch täuschend echte Manipulationen komplexer Fotos möglich.[69] Je nach Qualität der Manipulation kann diese dann erst mit Hilfe einer forensischen Analyse eines Sachverständigen aufgedeckt werden.

Im Bereich der Chatlogs existiert ein besonders breites Spektrum an verfügbaren Tools, mit denen Chatverläufe von Grund auf erstellt oder verändert werden können. Die Besonderheit ist dabei, dass kein Vorwissen

---

60 https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/funktionen/funktionen-node.html.

61 Siehe Fn. 59.

62 https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/eIDAS-konforme-fernsignatur/eidas-konforme-fernsignatur-node.html.

63 Initiative D21 und Technische Universität München, eGovernment MONITOR 2020: Staatliche Digitalangebote – Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz, S. 20.

64 Sieber/Brodowski in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 19.3 Rn. 164.

65 Bundesamt für Sicherheit in der Informationstechnik, Grundlagen der elektronischen Signatur, Stand 2021, S. 64 f.

66 https://esignature.ec.europa.eu/efda/tl-browser/ (Suche nach „trust service by type“: „Qualified validation service for qualified electronic signature“ und „Qualified validation service for qualified electronic seal“, alle Länder).

67 BGH, NJW 2015, 2119 (2122 Rn. 28); BGH, NJW 2016, 942 (945 Rn. 34 ff.); BGH, GRUR-RS 2020, 10653, Rn. 4; OLG Hamburg, BeckRS 2010, 8444OLG München GRUR-RR 2016, 495 (497 Rn. 34); OLG Stuttgart, GRUR-RS 2019 16939 Rn. 26; OLG Jena, GRUR-RR 2019, 238 (238 Rn. 14 ff.); OLG Köln, BeckRS 2019, 32281 Rn. 7; OLG München GRUR 2020, 770 (771); LG Dresden, ZUM-RD 2019, 108 (111).

68 BGH, NJW 2019, 2552 (2556 Rn. 42); OLG Stuttgart, NJW 2016, 2280 (2282 Rn. 24); OLG Köln, NJW 2005, 2997 (2997 ff.).

69 Vgl. https://www.vcl.fer.hr/comofod/examples.html.

oder technische Expertise erforderlich ist, um Fälschungen zu erstellen, die visuell nicht von Originalen zu unterscheiden sind.[70] Auch Posts bekannter sozialer Netzwerke lassen sich auf diese Weise fälschen.[71]

In vielen Fällen könnte die Authentizität dieser Chatverläufe in Zusammenarbeit mit der Herkunftsplattform überprüft werden. Problematisch ist dies bei Nutzung einer Ende-zu-Ende-Verschlüsselung; hier könnten jedoch zumindest die Metadaten wie Zeitpunkt und Größe der Nachrichten abgeglichen werden. In jedem Fall bedarf es einer Schärfung des Bewusstseins für die vorhandenen technischen Möglichkeiten.

E-Mails lassen sich auf der Empfängerseite ähnlich einfach manipulieren oder von Grund auf fälschen. Der Inhalt sowie die Metadaten (unter anderem Absender und Empfangsdatum) liegen auf dem Mailserver i.d.R. in Textform vor. Technisch ist es daher ohne weiteres möglich, die Meta- und Inhaltsdaten einer E-Mail beliebig zu gestalten oder zu modifizieren und diese dann auf einem Server zu speichern. Die Fälschung von E-Mails auf Absenderseite gestaltet sich nicht in jedem Fall ebenso einfach. Während der angezeigte Name des Absenders in der Regel frei gewählt werden kann, lassen sich Absender-Domains aufgrund weit verbreiteter Techniken wie DKIM und SPF nicht ohne weiteres fälschen.[72] Die genaue Überprüfung der Adresse – also, ob eine E-Mail tatsächlich von alice@beispiel.de und nicht etwa von bob@beispiel.de versendet wurde – kann nur vom versendenden E-Mail-Server mit nicht standardisierten Verfahren oder bei Nutzung wenig verbreiteter Techniken wie PGP oder S/MIME durchgeführt werden.

Ähnliches gilt für Websites: Der Quellcode lässt sich lokal speichern und verändern; von der so modifizierten Webseite können dann Screenshots angefertigt werden, ohne dass der Ursprung erkenntlich ist.

Textdokumente wie etwa gängige Office-Formate sind bereits konzeptionell für die Bearbeitung ausgelegt. Je nach Programm werden Details über die Autoren in Form von Metadaten erfasst. Faktisch handelt es sich sowohl bei den Textinhalten als auch bei den Metadaten in der Regel um unverschlüsselte und nicht signierte Klartextdaten, die je nach konkretem Format maschinenlesbar in einer Datei gespeichert werden.[73]

Zwar existieren bspw. mit dem *Portable Document Format* (PDF) Formate, die vorrangig für das Lesen bestimmt sind. Diese können mit entsprechender Software jedoch inhaltlich wie visuell verändert werden. Die einzigen Hürden sind dabei die Bedienbarkeit der Programme sowie die technischen Kenntnisse der Nutzer.

In all diesen Fällen sollte den eingebrachten Beweisen – also Screenshots und elektronischen (nicht signierten) Dokumenten – aus technischer Sicht nicht ohne Weiteres ein großes Maß an Vertrauen geschenkt werden. Die Beweise selbst bzw. die zugrundeliegenden elektronischen Dokumente sind in der Regel leicht manipulierbar.

Im Strafprozessrecht gelten elektronische Dokumente hingegen gemäß § 249 Abs.1 S. 2 StPO als Urkunden, wenn sie verlesbar sind. Maßnahmen wie eine qualifizierte elektronische Signatur werden nicht gefordert. Dies hat zur Folge, dass auch leicht fälschbaren Dokumenten ohne fortgeschrittene elektronische Signatur eine hohe Beweiskraft zugesprochen wird, obwohl keine Aussage zur Authentizität oder Integrität gemacht werden kann.

Die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung) regelt die Anforderungen an sowie die Rechtswirkung von fortgeschrittenen und qualifizierten elektronischen Signaturen, fortgeschrittenen und qualifizierten elektronischen Siegeln sowie qualifizierten elektronischen Zeitstempeln.

Elektronische Siegel sind dabei technisch eng verwandt mit elektronischen Signaturen, erlauben jedoch keine Zuordnung zu einer natürlichen Person und können somit bspw. von einer ganzen Behörde genutzt werden.

---

70 Vgl. bspw. https://www.fakewhats.com.

71 Vgl. bspw. https://instalized.com und https://fakedetail.com/fake-tiktok-post-generator.

72 Vgl.etwa zur Verbreitung von SPF, DKIM und DMARC: Deccio/Yadav/Bennett/Hilton/Howe/Norton/Rohde/Tan/Taylor, CoNEXT 2021.

73 Castiglione/De Santis/Soriente, JSS 2007, 750.

Mit Zeitstempeln lässt sich die Existenz von Daten beweisen, indem ein Hashwert der Daten zusammen mit einem aktuellen Zeitstempel (fortgeschritten) signiert bzw. besiegelt wird.

Die Anforderungen sollen dabei die technischen Voraussetzungen bspw. im Hinblick auf die Authentizität schaffen, um den so signierten Dokumenten die gewünschte Rechtswirkung zusprechen zu können. So gilt im Falle von qualifizierten elektronischen Siegeln etwa gemäß Art. 35 Abs. 2 eIDAS-VO die Vermutung für die Unversehrtheit und die Richtigkeit der Herkunftsangabe der mit dem Siegel verbundenen Daten.

In der ZPO ist grundsätzlich der Augenscheinsbeweis nach § 371 Abs.1 ZPO möglich, jedoch müssen elektronische Dokumente für eine höhere Beweiskraft gesetzlich anerkannte Sicherungsverfahren vorweisen. Ist ein Dokument bspw. mit einer qualifizierten elektronischen Signatur versehen, so finden nach § 371a Abs. 1 S. 1 ZPO die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Zudem wird gemäß § 371a Abs. 1 S. 2 ZPO eine gesetzliche Vermutung aufgestellt, dass eine in elektronischer Form vorliegende Erklärung, die mit einer qualifizierten elektronischen Signatur versehen wurde, einen Anscheinsbeweis darstellt.[74] Daraus folgt, dass die Echtheit des Dokuments vermutet und nur durch Tatsachenbehauptungen in Frage gestellt wird, die ernsthafte Zweifel begründen.[75] Eine äquivalente Vorschrift in der StPO fehlt.

In Anbetracht des stetigen technologischen Fortschritts und der damit einhergehenden Manipulationsmöglichkeiten an elektronischen Dokumenten stellt sich daher die Frage, weshalb die Anforderungen an die Beweiskraft eines elektronischen Dokuments gemäß § 371a Abs. 1 S. 2 ZPO nicht in die StPO übernommen wurden.

Die Manipulation von Videoaufzeichnungen erfordert im Gegensatz zur Veränderung von Bildern oder Texten sowohl komplexere Software als auch spezifisches Wissen. Da sich ein Video – vereinfacht dargestellt – aus vielen aufeinanderfolgenden Bildern und ggf. einem synchron laufenden Ton zusammensetzt, müssen diese Elemente gemeinsam und konsistent verändert werden, um weiterhin als stimmiges Gesamtkonstrukt wahrgenommen zu werden. Mutmaßlich aus diesem Grund wurde insbesondere in der Vergangenheit Videoaufzeichnungen ein höherer Beweiswert zugesprochen als bspw. der Aussage von Zeugen bei einem Verkehrsunfall.[76]

Bedingt durch den Fortschritt insbesondere im Bereich des Deep Learning existieren jedoch Dienste und Programme, mit deren Hilfe Nutzer auch ohne Fachkenntnisse Gesichter in Videos verändern können.[77] Diese sog. *Deep Fakes* sind mitunter mit dem bloßen Auge nicht von unveränderten Videos zu unterscheiden.

Auch Sprachaufnahmen sind von dieser Entwicklung betroffen. So wurden bereits 2019 mindestens drei Fälle bekannt, in denen manipulierte Sprachaufnahmen für Betrugstaten verwendet wurden.[78] Dies wirft aus technischer Perspektive die Frage auf, ob Video- und Audioaufzeichnungen in kritischen Bereichen wie Gerichtsverfahren überhaupt noch ein signifikanter Beweiswert zugesprochen werden kann.

Eine weitere Problematik liegt darin, dass in der Praxis häufig bereits auf die Einführung digitaler Beweismittel in das Beweisverfahren verzichtet wird. Gerne wird auf andere Beweismittel, wie bspw. die Aussage eines Zeugen oder den Bericht eines Ermittlungsbeamten zurückgegriffen.[79] Bestätigt beispielweise der Angeklagte oder ein Zeuge, einen bestimmten Beitrag in einem sozialen Netzwerk verfasst zu haben, kann darauf verzichtet werden, nach digitalen Spuren auf seinem Rechner zu suchen.[80] Dies führt dazu, dass auch besonders manipulationssichere digitale Beweise trotz ihres hohen Beweiswerts nicht verwertet werden. Bei Zeugen hingegen ist die Gefahr von (auch unbeabsichtigt) fehlerhaften Aussagen wegen Erinnerungslücken ungleich höher.

---

74 Zimmermann in: MüKo ZPO, § 371a Rn. 4.

75 Ernsthafte Zweifel können entstehen durch technische Mängel wie die fehlerhafte Zuordnung von Zertifikaten, vgl. Zimmermann in: MüKo ZPO, § 371a Rn. 4.

76 BGH, NJW 2018, 2883 (2888 Rn. 37).

77 Vgl. dazu Westerlund, Technology Innovation Management Review 2019 (Volume 9 Issue 11), S. 39.

78 BBC, Fake voices 'help cyber-crooks steal cash'.

79 Brodowski/Jahn in: Hoven/Kudlich, Digitalisierung und Strafrecht, S. 86 f.

80 Vgl. bezüglich einer ausgedruckten E-Mail Brodowski/Jahn in: Hoven/Kudlich, Digitalisierung und Strafrecht, S. 89.

5.1. Verwendung von Metadaten

Wie bereits am Beispiel der Textdokumente erläutert, fallen bei der Verwendung von Computersystemen zahlreiche Metadaten an.[81] Diese können – unabhängig vom Format der Primärdaten – selbst wiederum als Beweis in Betracht kommen und bspw. im Rahmen eines Sachverständigengutachtens verwertet werden. Metadaten lassen sich jedoch nicht pauschal hinsichtlich ihres Beweiswertes beurteilen, da sie in verschiedensten Ausprägungen und in unterschiedlichen Anwendungsbereichen vorkommen. Zugriffsprotokolle einer Webseite lassen sich bspw. nur mit großem Aufwand – i.d.R. nach einem erfolgreichen Angriff auf den Server – von Besuchenden manipulieren. Demgegenüber lassen sich die zuvor erwähnten Autoreninformationen in Textdokumenten sowie Daten zu Aufnahmeort und -datum eines Digitalfotos beinahe trivial und beliebig verfälschen.

6. Fazit

Zusammenfassend lässt sich festhalten, dass die Würdigung digitaler Beweise im Straf- und Zivilprozess große Unterschiede aufweist. In der ZPO existiert mit dem 2005 eingeführten § 371a eine Regelung, wonach eine qualifizierte elektronische Signatur ein elektronisches Dokument hinsichtlich des Beweiswerts einer Privaturkunde gleichstellt. Gemäß § 371a Abs. 1 S. 2 ZPO besteht der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, soweit eine qualifizierte elektronische Signatur vorliegt. Im Strafprozess gelten nach § 249 Abs. 1 StPO elektronische Dokumente bereits dann als Urkunde, wenn sie verlesbar sind. Zurecht gilt bei diesen dann jedoch keine entsprechende Echtheitsvermutung. Dabei spielen digitale Beweise und insbesondere deren Sicherung mit Hilfe beweiswerterhaltender und beweiswertsteigernder Techniken im Strafprozess eine zentrale Rolle. Hier bleiben Möglichkeiten ungenutzt, technische Werkzeuge wie bspw. qualifizierte elektronische Signaturen im Rahmen der ihnen innewohnenden Aussagekraft zu würdigen.

Die geringe Verbreitung beweiswertsteigernder Maßnahmen stellt eine Herausforderung in allen Rechtsgebieten dar. So könnten etwa fortgeschrittene und qualifizierte elektronische Signaturen auch in der privaten Kommunikation Auseinandersetzungen vorbeugen. Nicht zuletzt dienen sie gleichzeitig dazu, die Sicherheit der eigenen privaten wie beruflichen IT zu erhöhen. Für die Verbesserung der Situation auf diesem Gebiet bedarf es insbesondere eines gesteigerten Bewusstseins für die vorhandenen Möglichkeiten sowie niedrigschwelliger technischer Angebote für die Allgemeinheit. Dies erfordert eine interdisziplinäre Zusammenarbeit aus den Bereichen der Rechtswissenschaften, der Informatik, aber auch der Gesellschaftswissenschaften.

Eine intensivere Zusammenarbeit sowie eine größere Verbreitung beweiswertsteigernder Maßnahmen in der gesamten Gesellschaft könnten dazu beitragen, dass auch in der Justiz die Sensibilität im Umgang mit digitalen Beweisen erhöht wird. Im Idealfall können so die Gerichte bereits einschätzen, wie wertvoll ein konkreter digitaler Beweis ist. Ist hingegen besondere Expertise notwendig, könnte etwa der Rückgriff auf einen Sachverständigen Abhilfe schaffen, ähnlich wie bei einem Glaubwürdigkeitsgutachter für einen Zeugen. Werden diese Standards eingehalten, so kann das Potential digitaler Beweismittel in Zukunft voll ausgeschöpft werden.

7. Literatur

Blechschmitt, Lisa, Strafverfolgung im digitalen Zeitalter, MMR 2018, S. 361–366.

BBC, Fake voices ‘help cyber-crooks steal cash’, https://www.bbc.com/news/technology-48908736, aufgerufen 07.11.2021.

Bundesamt für Sicherheit in der Informationstechnik, Grundlagen der elektronischen Signatur, 2006 (Stand 2021), S. 64 f.

Bundeskriminalamt, Cybercrime, Bundeslagebild 2020, 2020.

Bundesministerium des Innern, für Bau und Heimat, Die elektronischen Funktionen des Personalausweises, https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/funktionen/funktionen-node.html, aufgerufen 07.11.2021.

Bundesministerium des Innern, für Bau und Heimat, Fernsignaturen mit der Online-Ausweisfunktion, https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/eIDAS-konforme-fernsignatur/eidas-konforme-fernsignatur-node.html, aufgerufen 07.11.2021.

[81] Dazu näher Castiglione/De Santis/Soriente, Fn. 73 sowie Krüger/Möllers, Fn. 57.

Castiglione, Aniello/De Santis, Alfredo/Soriente, Claudio, Taking advantages of a disadvantage: Digital forensics and steganography using document metadata, Journal of Systems and Software 80(5), 2007, S. 750–764.

Deccio, Casey/Yadav, Tarun/Bennett, Nathaniel/Hilton, Alden/Howe, Michael/Norton, Tanner/Rohde, Jacob/Tan, Eunice/Taylor, Bradley, Measuring Email Sender Validation in the Wild, Conference on emerging Networking EXperiments and Technologies (CoNEXT), 2021 (zur Veröffentlichung angenommen).

Eisenberg, Ulrich, Beweisrecht der StPO, 10. Auflage, Verlag C.H. Beck, München 2017.

Europäische Kommission, EU Trust Services Dashboard, https://esignature.ec.europa.eu/efda/tl-browser/, aufgerufen 07.11.2021.

Europäische Kommission, Impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Folgenabschätzung SWD (2018) 118 final, 2018. (Zitiert: Folgenabschätzung der Europäischen Kommission SWD (2018) 118 final, S.).

Fake Details Online Generator, Fake TikTok Post Gererator, https://fakedetail.com/fake-tiktok-post-generator, abgerufen 07.11.2021.

Graf, Jürgen (Hrsg.), Beck'scher Onlinekommentar StPO mit RiStBV und MiStra, 41. Edition, Verlag C.H. Beck, München 2021 (Zitiert: Autor in: BeckOK StPO, § Rn.).

Hannich, Rolf, Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage, Verlag C.H. Beck, München 2019.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, 56. EL, Verlag C.H. Beck, München 2021.

Hoven, Elisa/Kudlich, Hans (Hrsg.), Digitalisierung und Strafverfahren, 1. Auflage, Nomos Verlagsgesellschaft, Baden-Baden 2020.

Hussels, Martin, Strafprozessrecht – Schnell erfasst, 4. Auflage, Springer, Berlin/Heidelberg 2020.

Initiative D21 und Technische Universität München, eGovernment MONITOR 2021: Staatliche Digitalangebote – Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz, 2020.

Instalized, Instalized, https://instalized.com, aufgerufen 07.11.2021.

Jacoby, Florian, Zivilprozessrecht, 17. Auflage, Verlag Franz Vahlen, München 2020.

Knauer, Christoph/ Kudlich, Hans/Schneider, Hartmut (Hrsg.), Münchener Kommentar zur StPO, Band I §§ 1–150, 1. Auflage, Verlag C.H. Beck, München 2014 (Zitiert: Autor in: MüKo StPO, § Rn.).

Knauer, Christoph/ Kudlich, Hans/Schneider, Hartmut (Hrsg.), Münchener Kommentar zur StPO, Band II §§ 151–332, 1. Auflage, Verlag C.H. Beck, München 2016 (Zitiert: Autor in: MüKo StPO, § Rn.).

Krüger, Jochen/Möllers, Frederik, Metadaten in Justiz und Verwaltung, MMR 2016, S. 728–731.

Krüger, Wolfgang/Rauscher, Thomas (Hrsg.), Münchener Kommentar zur Zivilprozessordnung, Band 1, §§ 1–354, 6. Auflage, Verlag C.H. Beck, München 2020 (Zitiert: Autor in: MüKo ZPO, § Rn.).

Möller, Christian, Die Verfahrensgrundsätze des Zivilverfahrens, JA 2010, S. 47–52.

Müller, Sebastian T., Internetermittlungen und der Umgang mit digitalen Beweismitteln im (Wirtschafts)Strafverfahren, NZWiSt 2020, S. 96–101.

Musielak, Hans-Joachim/Voit, Wolfgang, Zivilprozessordnung, 18. Auflage, Verlag Franz Vahlen, München 2021.

Pohlmann, Petra, Zivilprozessrecht, 4. Auflage, Verlag C.H. Beck, München 2018.

Rosenberg, Leo (Begr.)/Schwab, Karl Heinz/Gottwald, Peter (Bearbeiter), Zivilprozessrecht, 18. Auflage, Verlag C.H. Beck, München 2019.

Saenger, Ingo (Hrsg.), Zivilprozessordnung, 9. Auflage, Nomos Verlagsgesellschaft, Baden-Baden 2021.

University of Zagreb, CoMoFoD – Image Database for Copy-Move Forgery Detection, Video Communications Laboratory, https://www.vcl.fer.hr/comofod/examples.html, aufgerufen 07.11.2021.

Vorwerk, Volkert/Wolf, Christian (Hrsg.), Beck'scher Onlinekommentar ZPO, 42. Edition, Verlag C.H. Beck, München 01.09.2021 (Zitiert: Autor in: BeckOK ZPO, § Rn.).

Walter, Tonio, Strafprozessrecht – Ein Lehrbuch für Studenten und angehende Praktiker, 1. Auflage, Mohr Siebeck, Tübingen 2020.

Westerlung, Mika, The Emergence of Deepfake Technology: A Review, Technology Innovation Management Review 2019 (Volume 9 Issue 11), S. 39–52.