eJustice im Gerichtssaal – Teil 2: das digitale Beweisrecht[1]

Prof. Dr. Henning Müller, Darmstadt

Zum „eJustice"-Veränderungsprozess der Justiz gehört auch, dass zunehmend elektronische Dokumente, Bilder und Dateien als Beweismittel zur Verfügung stehen. Das wichtigste Beweismittel im sozialgerichtlichen Verfahren ist die (elektronische) Behördenakte, die gemäß § 104 SGG bereits zu Beginn des Verfahrens beigezogen wird. Die Digitalisierung des Beweisrechts zwingt dazu, Begriffe neu zu denken, den Beweiswert verschiedener Medien und Dateitypen zu hinterfragen und auch Beweislastverteilungen neu zu bewerten. Der folgende Beitrag soll eine Übersicht über die Herausforderungen eines digitalisierten Beweisrechts bieten.

1. Der Beweis mit elektronischen Dokumenten

Digitale Fotos, eingescannte Dokumente und natürlich Schriftsätze, die im Wege des elektronischen Rechtsverkehrs vorgelegt werden, vor allem aber die elektronischen Behördenakten: Die Beweisführung mit elektronischen Dokumenten hat eine zunehmende Bedeutung in Gerichtsverfahren. Trotz des modernen Beweisgegenstands kommt das Prozessrecht mit den klassischen Beweismitteln aus. Unterschiede in der Beweisführung bestehen dennoch. Es handelt sich insoweit nicht nur um Details, sondern um ein wichtiges Grundlagenwissen, das auch prozesstaktisch ein Umdenken erfordert. Hinzu kommt aber, dass gerade die Beweisführung mit elektronischen Behördenakten nur dann sicher gelingt, wenn das Beweisrecht bereits bei der Organisation und der Technik der eAkte selbst, sowie von Scanprozessen mitgedacht wird.

1.1 Rechtliche Grundlagen des digitalen Beweisrechts

Der Urkundsbeweis gemäß § 415 ff. ZPO (Zivilprozessordnung) bindet die Gerichte in ihrer freien Beweiswürdigung gemäß § 286 Abs. 1 Satz 1 ZPO und stärkt damit die Beweissicherheit, letztlich also die Vorhersehbarkeit des Ausgangs des Gerichtsverfahrens. In der „Papierwelt" wird der Urkundsbeweis durch Vorlage des Originals der privaten oder öffentlichen Urkunde angetreten und erbringt für private Urkunden den Vollbeweis für die in der Urkunde enthaltene Erklärung, für die öffentliche Urkunde den Vollbeweis für den beurkundeten Vorgang, die Anordnung, Verfügung oder Entscheidung.

1.1.1 Abgrenzung zum Urkundsbeweis

Elektronische Dateien können keine Urkunden im Rechtssinne darstellen, selbst dann, wenn das Ziel der Beweiserhebung ausschließlich der in der Datei verkörperte Gedankeninhalt ist. Es fehlt einer elektronischen Datei jedenfalls an der Verkehrsfähigkeit.[2] Der in einer elektronischen Datei verkörperte Gedankeninhalt ist nämlich nur durch den Einsatz technischer Hilfsmittel verfügbar zu machen.[3] Der Ausdruck einer elektronischen Datei auf Papier ist dagegen kein elektronisches Dokument und grundsätzlich

1 Der Autor ist Direktor des Sozialgerichts Darmstadt und Honorarprofessor der Hochschule für Wirtschaft und Gesellschaft Ludwigshafen. Er betreibt einen Blog zum elektronischen Rechtsverkehr und zur eAkte unter https://ervjustiz.de.

2 Festmachend an der Verkörperung: *Wagner*, JuS 2016, 29, 30.

3 Anderer Auffassung *Rüßmann*, JurPC 1995, 3212; *Zimmermann*, in: MünchKomm-ZPO, § 371 ZPO Rn. 4; vgl. ferner BGH vom 28.11.1975 – V ZR 127/74.

auch keine Urkunde[4], sondern ein Augenscheinsobjekt im Sinne des § 371 Abs. 1 Satz 1 ZPO, das in Form eines Augenscheinsurrogats als Beweismittel dienen kann.[5] Die Urkundeneigenschaft ist deshalb nicht gegeben, weil der Ausdruck regelmäßig nicht selbst dazu dient, die in dem elektronischen Dokument verkörperte Gedankenerklärung in den Rechtsverkehr zu bringen, sondern nur eine Information über die elektronische Gedankenerklärung zu erlangen.[6] Der Ausdruck einer E-Mail kann – wenn überhaupt – als Augenscheinsobjekt allein Beweis dafür erbringen, dass die E-Mail mit den dort aufgeführten Anhängen versandt worden ist, nicht aber für den Inhalt ihrer Anhänge.[7]

Elektronische Dateien sind deshalb grundsätzlich Augenscheinsbeweismittel. Nachteil des Augenscheinsbeweises ist, dass das Gesetz im Gegensatz zum Urkundsbeweis grundsätzlich keine gesetzlichen Beweisregeln vorsieht, sondern das Augenscheinsobjekt – die elektronische Datei – (nur) der freien richterlichen Beweiswürdigung und damit der Subjektivität der Wahrnehmung der Richterin oder des Richters unterliegt. Entsprechend wenig vorhersehbar kann im Einzelfall der Ausgang der Beweiserhebung sein.

§ 371 Abs. 1 Satz 2 ZPO beinhaltet eine Sonderregel für den Beweisantritt mit elektronischen Dokumenten. Die Norm dürfte aber auch über Dokumente hinaus auf elektronische Dateien im Allgemeinen anwendbar sein, sofern sie nicht nur einem Sachverständigenbeweis zugänglich sind. Aus der Sondervorschrift ergibt sich letztlich, dass der Beweis durch elektronische Dateien grundsätzlich durch Inaugenscheinnahme erbracht wird.

1.1.2 Beweisregeln für elektronische Dokumente

Die §§ 371a, 371b ZPO enthalten Sonderregeln zur Beweiskraft bestimmter Typen elektronischer Dokumente, aufgrund deren diese ganz oder teilweise nach den Beweisregeln für Urkunden zu behandeln sind. Wesentlicher Vorteil der Einhaltung der Voraussetzungen der §§ 371a, 371b ZPO ist deshalb die Berechenbarkeit der Beweisführung. Durch die dortigen Beweisregeln wird die Subjektivität des Augenscheinsbeweises gemäß § 371 ZPO teilweise umgangen.

Historisch bedingt knüpfen die Beweisregeln der §§ 371a, 371b ZPO vor allem an der Anbringung qualifizierter elektronischer Signaturen an. Andererseits ist zu beachten, dass die Nichterfüllung der Voraussetzungen der §§ 371a, 371b ZPO nicht dazu führen, dass ein Beweiswert gar nicht vorhanden ist[8], sondern das Verfehlen ihrer Voraussetzungen führt lediglich zurück zum Augenscheinsbeweis des § 371 ZPO.

Gemäß § 371a Abs. 1 Satz 1 ZPO können private elektronische Dokumente den Beweiswert privater Urkunden erreichen. Hierzu müssen sie vom Aussteller des Dokuments mit seiner qualifizierten elektronischen Signatur versehen werden. Dies ist beim Scan eines eingehenden Papier-Schriftstücks (beispielsweise eines Bürgers) in der Behörde nicht der Fall, denn dort könnte ja maximal eine qualifizierte elektronische Signatur der Behörde aufgebracht werden. Die Signatur wäre daher ungeeignet, den Beweiswert des § 371a Abs. 1 Satz 1 ZPO zu erbringen, sie könnte lediglich den Nachweis bieten, dass das Dokument nach dem Scanvorgang nicht mehr verändert wurde – sie ist also nur ein Sicherungsmittel. Es bleibt dabei, dass das gescannte Dokument nur als Augenscheins-

4 So auch *Feskorn*, in: Zöller, ZPO, Vorbemerkungen zu §§ 415–444 ZPO Rn. 5; anderer Auffassung *Sander*, CR 2014, 292, 294; vgl. ferner *Ortner*, in: Hoeren/Sieber und Holznagel, MMR-HdB, Teil 13.2 Beweisqualität elektronischer Dokumente Rn. 45 unter Bezugnahme von AG Bonn vom 25.10.2001 – 3 C 193/01; LG Bonn vom 07.08.2001 – 2 O 450/00; LG Konstanz vom 19.04.2002 – 2 O 141/01 A; AG Erfurt vom 14.09.2001 – 28 C 2354/01; OLG Köln vom 06.09.2002 – 19 U 16/02.

5 OLG Thüringen vom 28.11.2018 – 2 U 524/17.

6 *Schreiber*, in: MünchKomm-ZPO, § 415 ZPO Rn. 9; so auch *Walter* (NJW 2021, 2367) unter Bezug auf das Urteil des BGH vom 27.04.2021 – VI ZR 84/19 zu einem Ausdruck einer elektronisch geführten Patientenakte gemäß § 630f BGB als Beweismittel.

7 Sächsisches LSG vom 12.10.2023 – L 3 AS 1050/19.

8 So wohl aber *Schild*, in: BeckOK DatenschutzR, Syst. E. Datenschutz bei Gerichten und Staatsanwaltschaften Rn. 87.

objekt im Rahmen der freien Beweiswürdigung in Betracht kommt.
§ 371a ZPO bezieht elektronische Dokumente unabhängig vom Dateiformat in den Anwendungsbereich ein. Erfasst sind damit insbesondere sämtliche Kommunikationsformate (E-Mails, Messengerdienste, Nachrichten in sozialen Medien et cetera) und Speicherformate für Dokumente (Office-Software Dateitypen, reine Textdateien et cetera). § 371a ZPO ist ferner auf Dokumente mit Erklärungen jeglichen Inhalts anwendbar, das heißt sowohl Willens- als auch Wissenserklärungen.[9]
§ 371a Abs. 2 ZPO enthält eine Beweiserleichterung gegenüber § 371a Abs. 1 ZPO bei Verwendung eines De-Mail-Dienstes, sofern der Absender der De-Mail sicher angemeldet war und die De-Mail absenderbestätigt versandt wurde. Die Nutzung des De-Mail-Dienstes entspricht daher dem Anscheinsbeweis, der in § 371a Abs. 1 ZPO durch die qualifizierte elektronische Signatur erzeugt wird und ersetzt damit das am Dokument selbst angebrachte Sicherungsmittel der qualifizierten elektronischen Signatur durch einen speziell gesicherten Übermittlungsweg. Allerdings ist die De-Mail nicht mehr praxisrelevant, nachdem die großen Telekommunikationsanbieter ihr De-Mail-Angebot für Bürgerinnen und Bürger aufgegeben haben.
§ 371a Abs. 3 ZPO bestimmt, dass auf öffentliche elektronische Dokumente die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung finden. Wesentlicher Unterschied zwischen § 371a Abs. 1 und Abs. 3 ZPO ist, dass die entsprechende Anwendung der Beweisregeln von Urkunden keine qualifizierte elektronische Signatur voraussetzt; lediglich die Vermutung der Echtheit gemäß § 437 ZPO tritt nur bei qualifiziert elektronisch signierten Dokumenten ein. Entsprechend anwendbare Vorschriften sind insbesondere die §§ 415 Abs. 1, 417, 418 Abs. 1 ZPO und für gerichtliche Dokumente § 165 ZPO und § 314 ZPO. Öffentliche elektronische Dokumente sind nach der Definition des § 371a Abs. 3 Satz 1 ZPO alle elektronischen Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind.[10] Dies entspricht der Definition des § 415 Abs. 1 ZPO. Öffentliche elektronische Dokumente sind insbesondere gemäß §§ 3a, 33, 37 VwVfG beziehungsweise § 36a SGB I, §§ 29, 33 SGB X errichtete elektronische Verwaltungsakten oder elektronische Beglaubigungen. Ferner sind öffentliche elektronische Dokumente gerichtliche Dokumente, wie Urteile, Beschlüsse und Protokolle.[11]
Während grundsätzlich die Beweiswirkung öffentlicher Urkunden für öffentliche elektronische Dokumente auch ohne qualifizierte elektronische Signatur besteht, setzt jedoch der Eintritt der Echtheitsvermutung des § 437 ZPO eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel als zusätzliches Sicherungsmittel gegen die nachträgliche Veränderung (Integritätsschutz) und zur Feststellung der Identität des Urhebers (Authentizität) voraus.

1.1.3 Die elektronische Datei

Eine elektronische Datei ist eine strukturierte Ansammlung von Daten und damit ein Objekt, das sowohl als Ganzes angesprochen, be- oder verarbeitet werden kann, als auch in seinen Teilen, also in seinem Inneren. Eine Datei befindet sich aus technischer Sicht zunächst im Arbeitsspeicher eines Computers, auf einem Datenträger oder in einem physikalischen (meist elektromagnetischen) Signal im Rahmen einer Datenübertragung.[12]
Als elektronische Dateien kommen daher neben elektronischen Dokumenten und Akten insbesondere in Betracht: Bilddateien,

9 *Musielak/Voit* und *Huber*, 16. Auflage 2019, ZPO § 371a Rn. 2.
10 Beck-TMG und *Roßnagel*, 1. Auflage 2013, ZPO § 371a Rn. 18.
11 BT-Drs. 15/4067, 34.
12 MüKoZPO und *Zimmermann*, 5. Auflage 2016, ZPO § 371 Rn. 9.

Videos, auch sogenannte Dashcam-Aufzeichnungen, Audiodateien, Protokolldateien, GPS-Daten[13], Fahrzeugdaten, die nur vom Kfz-Hersteller auslesbar sind[14], Internetinhalte[15], E-Mails[16], ferner SMS, Messenger-Nachrichten, Chatverläufe in sozialen Medien, Sprachnachrichten und Videos, E-Mails, Digitalfotos, Internetquellen[17] et cetera[18].

Zur elektronischen Datei gehören möglicherweise auch umgebende Daten oder Metadaten sowie eventuell erforderliche Passwörter oder andere Schlüssel zur Zugänglichmachung ihres Inhalts.[19] Die Nichtmitteilung von Zugangsschlüsseln kann als Beweisvereitelung nach § 371 Abs. 3 ZPO behandelt werden. Voraussetzung hierfür ist, dass die Partei den Schlüssel auch kennt beziehungsweise sich ohne Weiteres Kenntnis verschaffen kann, beispielsweise durch den Einblick in entsprechende Aufzeichnungen.[20]

1.2 Veränderte Begrifflichkeiten

Etablierte Begrifflichkeiten müssen im Rahmen der Digitalisierung neu durchgedacht werden. War in der Papierwelt noch eindeutig, was Original, Kopie und Abschrift bedeutet und unterscheidet, erhalten diese auf Papier gemünzten Zuweisungen neue Funktionen, wenn ein Dokument elektronisch vorliegt.

Ein „Original“ ist bei elektronischer Aktenführung stets das elektronische Dokument in seinem ursprünglichen und unveränderten Dateiformat. Der Begriff des „Originals“ ist dabei freilich anachronistisch, weil eine elektronische Datei in ihrem originalen Zustand grundsätzlich beliebig vervielfältigbar ist und deshalb die Grenzen der Begriffe „Original“ und „Kopie“ verschwimmen.[21] Die bitgleiche Kopie einer Datei ist eben gar keine Kopie, sondern letztlich ein zweites Original.

Jede Wandlung des Dateiformats oder Veränderung ihres Codes führen allerdings dazu, dass aus einer dem Augenschein zugänglichen elektronischen Datei im „Original“ ein Augenscheinsurrogat wird. Ein „Original“ sind bei elektronischer Aktenführung stets elektronische Dokumente in ihrem ursprünglichen und unveränderten Dateiformat (Grundsatz der Formattreue). Es kommt letztlich auf die „Bitgleichheit“ an. Augenscheinsurrogate sind selbstredend ebenfalls als Beweismittel denkbar. Liegt das Augenscheinsurrogat elektronisch vor, ist deshalb auch § 371 Abs. 1 Satz 2 ZPO einschlägig. Manifestiert sich die Datei beispielsweise in einem Ausdruck, handelt es sich um ein Augenscheinsobjekt im Sinne des § 371 Abs. 1 Satz 1 ZPO.

Der Beweiswert des Augenscheinsurrogats ist allerdings gemäß § 286 ZPO unter Berücksichtigung der vorgenommenen Veränderungen zu würdigen. Die freie richterliche Beweiswürdigung bedeutet, die umfassende Würdigung der vorgetragenen Tatsachen, der vorgelegten und erhobenen Beweise und des gesamten Prozessstoffes.[22] Dies beinhaltet insbesondere Hinweise auf mögliche Manipulationen an der elektronischen Datei. Die Echtheit und Unverfälschtheit der Datei sind Hilfstatsachen. Die Beweislast hierfür trägt der Beweisführer. Die Feststellung wird regelmäßig nur durch Sachverständigenbeweis oder durch Indizien möglich sein. Möglicherweise kann sich hier auch das Beweisthema verändern und sich eher auf den (ursprünglichen) Datenträger selbst beziehen, dessen Vorlage eventuell den Nachweis einer späteren Manipulation ermöglicht.[23]

13 OLG Celle vom 24.09.2018 – 8 U 73/18 – juris Rn. 42.
14 *Balzer* und *Nugel*, NJW 2016, 193, 198 f.; *Greger*, in: Zöller, ZPO, § 371 ZPO Rn. 4b.
15 OLG Koblenz vom 02.10.2014 – 6 U 1127/13; OLG Thüringen vom 28.11.2018 – 2 U 524/17.
16 Ausführlich *Ernst*, MDR 2003, 1091; *Sander*, CR 2014, 292, 294.
17 *Brand* und *Skowronek*, RDi 2021, 178, 181 f.
18 Mit weiteren (teilweise freilich veralteten) Beispielen: *Bergmann* und *Streitz*, CR 1994, 77.
19 *Musielak/Voit* und *Huber*, 16. Auflage 2019, ZPO § 371 Rn. 13.
20 *Berger*, NJW 2005, 1016, 1020.
21 *Müller*, KrV 2019, 99, 105 f.; *Sander*, CR 2014, 292, 293.
22 OLG Thüringen vom 28.11.2018 – 2 U 524/17.
23 *Berger*, NJW 2005, 1016, 1020.

1.3 Die besondere Bedeutung elektronischer Zertifikate

Zentral für den Beweiswert elektronischer Dateien sind elektronische Zertifikate.[24] Sie ermöglichen in verkehrsfähiger Weise den Nachweis, dass eine Datei unverändert geblieben ist (sogenannter Integritätsschutz) und erlauben Rückschlüsse auf den Urheber, das heißt die verantwortende Person (bei Signaturen) beziehungsweise die verantwortende Institution (bei Siegeln).

Technisch basieren elektronische Zertifikate auf einem asymmetrischen kryptografischen Verfahren. Ein öffentlicher Schlüssel dient der Prüfung eines privaten Schlüssels. Hierzu wird aus dem signierten Dokument nach einem festgelegten Algorithmus ein sogenannter Hashwert erzeugt. Dieser Hashwert wird mit dem privaten Schlüssel des „Unterzeichnenden" kombiniert und hierdurch verschlüsselt. Der unverschlüsselte Text wird dem Empfänger zusammen mit dem verschlüsselten Hashwert übermittelt. Letzterer lässt sich mit dem öffentlichen Schlüssel öffnen. Den öffentlichen Schlüssel erhält der Empfänger von einer Zertifizierungsstelle (Vertrauensdiensteanbieter). Sodann kann der Empfänger aus dem unverschlüsselten Dokument den Hashwert berechnen und diesen Wert mit dem ihm übermittelten decodierten Hashwert vergleichen.[25] Stimmen diese Werte überein, wurde der Text nicht nachträglich verändert. Die Signaturprüfung ist mithin nur demjenigen möglich, der über die unveränderte, auch nicht formatgewandelte, signierte Datei (nicht nur ihren Inhalt) und die Signatur selbst (letztlich den Hashwert) verfügt. Praktisch übernimmt diese Signaturprüfung eine Software, die das Ergebnis in Form eines Prüfprotokolls oder auch einer Kurzdarstellung ausgibt. Es handelt sich aber bei der Prüfung der qualifizierten elektronischen Signatur um einen mathematischen Rechenvorgang, der einer Beweiserhebung zugänglich ist.[26]

Praktisch erfolgt die Anbringung der Signatur dadurch, dass ein sogenannter Hardware-Token (regelmäßig eine Signaturkarte[27]) in eine Signaturerstellungseinheit[28] (regelmäßig ein Kartenlesegerät) eingeführt wird und auf diesem eine PIN oder ein Passwort eingegeben wird; der Vorgang dauert nur wenige Sekunden. Die konkrete Ausgestaltung des Signaturprozesses muss die Verwendung der Signatur durch andere Personen als den Signaturinhaber verlässlich ausschließen, Anhang II zur eIDAS-Verordnung (Englisch: electronic IDentification, Authentication and trust Services). Diese erfolgt typischerweise dadurch, dass die Anbringung der Signatur den Besitz der Karte und die Kenntnis der PIN (= sogenannte Zwei-Faktor-Authentifizierung) erfordert, was einen Missbrauch bei sorgfältiger Behandlung durch den Inhaber fast unmöglich macht. Aufgrund ihres hochkomplexen mathematischen Aufbaus ist die Signatur ohne Besitz der Karte und Kenntnis der PIN praktisch unfälschbar – zumeist ganz im Gegensatz zur händischen Unterschrift, die sie ersetzt.

Die eIDAS-Verordnung lässt daneben auch sogenannte Fernsignaturverfahren für qualifizierte elektronische Signaturen zu.[29] Die Anbieter erstellten hierbei die qualifizierte Signatur nach vorheriger Identifizierung des Unterzeichnenden. Damit werde sich die Verbreitung der qualifizierten elektronischen Signatur aller Voraussicht nach künftig erhöhen, weil die Vertragsparteien für das Verfahren keine eigene Hardware mehr anschaffen müssten. Damit entsprechende Signaturprodukte von der Aufsichtsstelle zugelassen werden, müssten die Anbieter jedoch spezielle technische Sicherheitsverfahren anwenden und nachweisen.

24 BT-Drs. 15/4067, S. 34; *Roßnagel*, in: Beck-TMG, § 371a ZPO Rn. 25.

25 *Müller*, eJustice-Praxishandbuch, 6. Auflage 2021, S. 139 ff.

26 Siehe im Detail *Fischer-Dieskau/Gitter/Paul* und *Steidle*, MMR 2002, 709, 711 f.

27 Regelmäßig eine Chipkarte, auf der ein Zertifikat eines sogenannte Vertrauensdiensteanbieters (Art. 3 Nr. 15 eIDAS-VO) aufgespielt ist, das wiederum die Identität des Zertifikatsinhabers, zum Beispiel des Rechtsanwalts, geprüft hat (beispielsweise durch ein Post-Ident-Verfahren) und das nur eine bestimmte zeitliche Gültigkeit hat.

28 Art. 3 Nr. 23, 22 eIDAS-VO.

29 *Voigt/Herrmann* und *Danz*, NJW 2020, 2991, 2992.

Die qualifizierte elektronische Signatur ersetzt bei elektronischen Dokumenten einerseits die Unterschrift des Urhebers des Dokuments.[30] Andererseits dient sie im Beweisrecht als Sicherungsmittel. Das qualifizierte elektronische Siegel ist vor allem im Beweisrecht anwendbar, findet sich aber mittlerweile auch in den Normen zum elektronischen Verwaltungsverfahren (§ 3a Abs. 3 Nr. 3a VwVfG beziehungsweise § 36a Abs. 2a Nr. 3 SGB I).
Die gesetzliche Grundlage findet die früher in § 2 Nr. 3 SigG geregelte qualifizierte elektronische Signatur mittlerweile in der eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste.[31]

1.3.1 Authentizitätssicherung

In § 371a Abs. 1 ZPO dient die qualifizierte elektronische Signatur zwei Zwecken. Sie dokumentiert einerseits die Identität des Ausstellers des Dokuments (Authentizität) und ersetzt damit seine handschriftliche Unterschrift. Um die Authentizität des Dokuments zu sichern, muss die qualifizierte elektronische Signatur die des Ausstellers des Dokuments sein. Aussteller des Dokuments ist, wer die Verantwortung für die im Dokument enthaltene Erklärung übernimmt („verantwortende Person“). Die Anbringung einer qualifizierten elektronischen Signatur für eine andere Person in Vertretung ist vom Gesetz nicht vorgesehen, weil dann die qualifizierte elektronische Signatur zwar ihre Funktion als Sicherungsmittel gegen Manipulationen erbringen kann, nicht aber die Authentifizierungsfunktion. Das „in Vertretung“ signierte Dokument unterfällt daher nicht § 371a Abs. 1 ZPO, sondern dem Augenscheinsbeweis des § 371 Abs. 1 Satz 2 ZPO ohne feste Beweisregeln und deshalb der freien richterlichen Beweiswürdigung. Hierbei ist jedoch die qualifizierte elektronische Signatur als weiterer Umstand zu berücksichtigen, weil durch sie nachgewiesen ist, dass jedenfalls eine nachträgliche Veränderung des elektronischen Dokuments ausgeschlossen werden kann.

1.3.2 Integritätsschutz

Zum anderen sichert die qualifizierte elektronische Signatur für das Beweisrecht die Integrität des Dokuments. Das elektronische Dokument ist zwar trotz der elektronischen Signatur inhaltlich veränderbar, also durch die Signatur nicht „schreibgeschützt“. Durch eine nachträgliche Veränderung jeder Art (also auch durch eine Veränderung, die den Erklärungswert des Dokuments nicht betrifft) wird aber der Hashwert des signierten Dokuments verändert, sodass eine nachträgliche Signaturprüfung auf die Manipulation hinweist. Im Rahmen der nachträglichen Überprüfung lässt sich nicht feststellen, was verändert worden ist, sondern nur, ob das Dokument verändert wurde.

1.3.3 Bedeutung in der forensischen Praxis

Die praktische Bedeutung des § 371a Abs. 1 ZPO ist noch gering, weil qualifizierte elektronische Signaturen vor allem im privaten Bereich kaum eine Verbreitung haben.[32] Etwas anderes gilt aber für § 371a Abs. 3 ZPO, weil die Formvorschriften des elektronischen Rechtsverkehrs, insbesondere des elektronischen Verwaltungsverfahrens (§ 3a VwVfG und § 36a SGB I) jedenfalls für schriftformbedürftige Dokumente im Postausgang der Behörde (beispielsweise für den Widerspruchsbescheid) eine qualifizierte elektronische Signatur oder ein solches Siegel vorsehen.
In der forensischen Praxis wird der Anwendungsbereich der Beweisregeln in §§ 371a, 371b ZPO oft übersehen und – wenn überhaupt – lediglich der Augenschein im Sinne des § 371 ZPO gewürdigt. Andererseits führt das Nichtvorliegen der Voraussetzungen der §§ 371a, 371b ZPO auch nicht zu Beweis-

30 *Müller*, NJW 2015, 822.
31 VO (EU) 910/2014; beachte aber *Kranz/Hildebrandt* und *Müller*, NVwZ 2019, 1495.
32 *Horn*, AnwBl 2021, 292.

losigkeit.[33] Zu beachten ist letztlich das Regelungsgefüge, in dem der Augenscheinsbeweis gemäß § 371 ZPO gegenüber den §§ 371a, 371b ZPO eigenständig ist. Richtig ist zwar, dass durch die Anbringung gerade einer qualifizierten elektronischen Signatur ein besonders hoher Beweiswert (gegebenenfalls sogar das Greifen der Beweisregel der §§ 371a f. ZPO) erzeugt werden kann. Auch andere Sicherungsmittel (beispielsweise Dokumentenmanagementsysteme, elektronische Siegel, elektronische Zeitstempel, fortgeschrittene Signaturen) haben aber ebenfalls einen Beweiswert, der im Einzelfall auch für einen Vollbeweis im Rahmen des Augenscheins ausreichen kann. § 371a ZPO ist ohne eine qualifizierte elektronische Signatur aber selbstredend nicht anwendbar.

1.4 Das digitale Beweisrecht und die elektronische Aktenführung

Die behördliche Aktenführung ist in den Verwaltungsverfahrensgesetzen nicht gesetzlich vorgeschrieben oder gar inhaltlich präziser gefasst. Erst recht nicht ist eine Behörde auf die Führung von Akten in Papierform oder einer anderen Form festgelegt. Nach allgemeiner Meinung ergibt sich aber die Pflicht zur Aktenführung aus dem Recht auf Akteneinsicht.[34] Für öffentlich-rechtliche Einrichtungen (zum Beispiel Gerichte, Behörden) ist die Pflicht zur Aktenführung Folge des Rechtsstaatsprinzips, das die Behörde zur objektiven Dokumentation des bisherigen wesentlichen, sachbezogenen Geschehensablaufs anhält[35], um sowohl nachträglich eine Überprüfung der behördlichen Entscheidung zu ermöglichen, als auch eine mögliche Erkenntnisquelle für zukünftiges Handeln zu schaffen.[36]

Dass das Akteneinsichtsrecht der Ausgangspunkt des Aktenbegriffs ist, hat zur Folge, dass die Auffindbarkeit der hiervon umfassten Inhalte von der Behörde sicherzustellen ist. Die Behörde muss sich daher eine Aktenordnung geben – regelmäßig eine verwaltungsinterne Verfahrensanweisung. Diese muss vorsehen, dass die Vorgänge zu einer registrierten, das heißt auffindbaren, Akte zusammenzuführen[37] sind. Zudem ist eine geheime Aktenführung ausgeschlossen. Es gilt das Prinzip der „beschränkten Aktenöffentlichkeit".[38]

Dem Aktenbegriff unterfallen also zunächst die gesammelten, in der Regel gehefteten oder sonst papiergebundenen schriftlichen „herkömmlichen" Vorgänge (einschließlich Zeichnungen, Pläne, Skizzen und Ähnliches) in einer Verwaltungsangelegenheit, aus denen sich der wesentliche Inhalt und Ablauf des Verwaltungsverfahrens ergeben.

1.4.1 Authentizität der eAkte

Spezifische Probleme bereitet die Authentizität der eAkte als Gesamtheit und ihrer einzelnen Dokumente kaum. Ebenso wie in einer Papierakte ist stets fraglich, wer tatsächlicher Urheber eines Dokuments ist. Die Urheberschaft wird regelmäßig durch eine Signatur (Papierwelt: Unterschrift, Paraphe et cetera; eAkte: einfache, fortgeschrittene oder qualifizierte elektronische Signatur oder Ähnliches oder die Dokumentation des Ergebnisses einer Zugriffs- beziehungsweise Schreibbefugnis im Rahmen eines Rechte- und Rollenkonzepts) nachgewiesen. Dieser „Nachweis" ist aber nicht mehr als eine formelle Verantwortungsübernahme für den Inhalt, der ja mitnichten selbst erstellt sein muss.

Zu beachten ist beim Medienwechsel dagegen der Verlust an Authentizität im weiteren Sinne – besser der Verlust an Originalität – durch den Scanvorgang. Je nach Scan-

33 Vgl. beispielhaft *Schild*, in: BeckOK DatenschutzR, Syst. E. Datenschutz bei Gerichten und Staatsanwaltschaften Rn. 87.
34 *Kallerhoff*, in: Stelkens/Bonk und Sachs, VwVfG, 8. Auflage, 2014 § 29 Rn. 30; *Kopp* und *Ramsauer*, VwVfG, § 29 Rn. 1a; zum Akteneinsichtsrecht: *Bohl*, NVwZ 2005, 133.
35 Vgl. nur BVerwG, Beschluss vom 16.12.2008 – 1 WB 19/08.
36 *Müller*, ZFSH-SGB 2019, 73, 76 ff.; *Kallerhoff*, in: Stelkens/Bonk und Sachs, VwVfG, 8. Auflage, 2014 § 29 Rn. 30.
37 Zur „untrennbaren Verbindung" bei elektronischen Akten: *Schmieder* und *Ulrich*, NJW 2015, 3482.
38 *Bohl*, NVwZ 2005, 133, 134.

qualität und Scanvorgaben (beispielsweise aufgrund des Verlusts von Farbinformationen), kann es zu Beweisschwierigkeiten hinsichtlich des Urhebers kommen. Als Beispiel sei hier der Prozess um fehlerhafte Angaben hinsichtlich vorhandenen Einkommens im Sozialhilferecht genannt, wenn sich der Kläger darauf beruft, der Behördenmitarbeiter habe ihm ein vorausgefülltes Formular lediglich noch zur Unterschrift vorgelegt; die falschen Angaben seien daher gar nicht von ihm zu vertreten. Während sich bei Vorlage des Originalformulars möglicherweise verwendete Stifte, die Handschrift und so weiter noch unterscheiden lassen, können die hierfür nötigen Details bei schlechter Scanqualität verloren gehen.[39]

1.4.2 Integrität und Stabilität der eAkte

Auch die Papierakte muss davor geschützt werden, dass Aktenbestandteile nachträglich entfernt werden oder einer anderweitigen Manipulation unterfallen (Integrität). Darüber hinaus muss die Akte als Erkenntnisquelle langfristig gesichert werden (Stabilität).[40]

Während die Integrität durch die Nutzung von revisionssicheren Dokumentenmanagementsystemen bei einer elektronischen Akte sogar leichter sicherzustellen ist als bei der für eine nachträgliche und unbemerkte Manipulation sowie Schimmel et cetera oder Verlust im Geschäftsgang beziehungsweise auf dem Postweg höchst anfälligen Papierakte, ist die vor allem langfristige Stabilität der elektronischen Akte technisch durchaus anspruchsvoll. Zum einen muss die Ablage in einer Infrastruktur erfolgen, die auch langfristig vor externer Zerstörung (beispielsweise Brände, Überschwemmung, Hacker) oder vor Zerfall durch Alter (beispielsweise „Materialermüdung“ des Datenträgers) geschützt ist. Zum anderen muss das Ablageformat so gewählt sein, dass langfristig Anzeigeprogramme zur Verfügung stehen, die die Lesbarkeit und Überprüfbarkeit der Dokumente, Daten und Metadaten, die zur vollständigen Akte gehören, ermöglichen. Die Ablage der Dokumente in einem Dateiformat, das das (noch) funktionsfähige Vorgangsbearbeitungsprogramm erfordert, ist angesichts der Geschwindigkeit der Weiterentwicklung von Hard- und Software sehr risikobehaftet, nicht zukunftssicher und daher kaum denkbar. Archive müssten andernfalls auch „historische“ Hardware mit nicht mehr unterstützten Betriebssystemen vorhalten (einschließlich der darauf geschulten Techniker). Richtigerweise muss deshalb ein archivierbares Exportformat gewählt werden, das möglichst unabhängig von einem sehr speziellen „IT-Ökosystem“ ist. Besondere technische und organisatorische Herausforderungen ergeben sich auch bei qualifizierten elektronischen Signaturen beziehungsweise funktionsäquivalenten Produkten.[41] Letzteres ist deshalb beachtlich, weil die Anbringung der qualifizierten elektronischen Signatur naturgemäß den größtmöglichen Schutz gegen eine nachträgliche Veränderung sicherstellt.[42]

1.4.3 Vollständigkeit der eAkte

Dass eine behördliche Akte vollständig zu sein hat, liegt auf der Hand. Dieses Erfordernis ergibt sich schon daraus, dass ein Akteneinsichtsrecht nur in eine vollständige Akte sinnhaft ist. Umso überraschender ist, dass selbst „der notwendige Akteninhalt“ gesetzlich oder gewohnheitsrechtlich nicht definiert ist. Nicht einmal in der Rechtsprechung und Literatur hat sich in der Vergangenheit anhand der Papierakte eine auch nur ansatzweise unstreitige Meinung herausgebildet. Dennoch entspinnt sich erst jetzt bei der Einführung elektronisch geführter Akten in der

39 Mit ähnlichen Beispielen aus dem Strafverfahren: *von Stetten*, ZRP 2015, 138.

40 *Kallerhoff*, in: Stelkens/Bonk und Sachs, VwVfG, 8. Auflage, 2014 § 29 Rn. 31.

41 Hierzu *Jandt*, NJW 2015, 1205; *Roßnagel* und *Nebel*, NJW 2014, 886; vgl. auch *Roßnagel*, MMR 2002, 215, 218 f.; siehe ferner *Müller*, NJW 2015, 822 zum Prüfungsrecht der Verfahrensbeteiligten.

42 *Wagner*, JuS 2016, 29.

Praxis schnell ein ebenso leidenschaftlicher, wie (oft) uninformierter Streit über den Begriff der Vollständigkeit der Akte, der schnell den eigentlichen Streitgegenstand aus dem Fokus geraten lässt.

Die elektronische Vorgangsbearbeitung führt bereits heute zu Besonderheiten hinsichtlich des Akteninhalts. Dies gilt völlig unabhängig vom gewählten Medium für die rechtsverbindliche Akte. Das eingesetzte Vorgangsbearbeitungsprogramm wird, insbesondere bei Einsatz einer Papierakte oder einer hybriden Akte, parallel zur eigentlichen Aktenpflege mit zahlreichen Daten bestückt, die oft, aber nicht zwingend, unterstützende Bedeutung haben (insbesondere sogenannte Metadaten zu Dokumenten, die zum Vorgang gereicht oder genommen werden) oder aber über den individuellen Vorgang hinaus benötigt werden (Geschäftsverteilungspläne, Adressdaten, Statistikdaten et cetera). Hinzu kommt die oft sehr informelle Kommunikation inner- oder intrabehördlich per E-Mail, die sich nicht selten in einer Grauzone zwischen vorbereitender Tätigkeit und aktenrelevanter Vorgangsbearbeitung bewegt.

Jedenfalls ist eine Verwaltungsakte mit elektronischen Bestandteilen mehr als eine chronologische Ablage eingegangener oder selbsterstellter Dokumente. Dies hat auch der Gesetzgeber erkannt und sich zwar nicht zu einer gesetzlichen Definition durchgerungen, aber jedenfalls in der Gesetzesbegründung zum EGovG (E-Government-Gesetz) Stellung bezogen, in dem die elektronische Akte als „eine logische Zusammenfassung sachlich zusammengehöriger oder verfahrensgleicher Vorgänge und/oder Dokumente, die alle bearbeitungs- und aktenrelevanten E-Mails, sonstigen elektronisch erstellten Unterlagen sowie gescannten Papierdokumente umfasst und so eine vollständige Information über die Geschäftsvorfälle eines Sachverhalts ermöglicht“ beschrieben wird.[43]

Da sich sachverhaltsrelevante Informationen nicht zwingend nur aus den eingegangenen oder selbsterstellten Dokumenten ergeben müssen, besteht die elektronische Verwaltungsakte also aus Dokumenten und „weiteren Daten“.[44]

Diese Erkenntnis führt jedoch nicht zu einer eindeutigen Definition des Maßstabs für die Vollständigkeit einer elektronischen oder hybriden Verwaltungsakte. Seit jeher besteht Einigkeit, dass beispielsweise Entwürfe, Notizen, Handakten oder sogenannte Non-Papers nicht Aktenbestandteile werden.[45] Es besteht die praktische Notwendigkeit, dass die Behörde auch die Möglichkeit hat, gewisse Vorbereitungshandlungen undokumentiert zu erarbeiten, um überhaupt eine Entscheidung reifen zu lassen. Andererseits müssen nicht nur außerhalb von Dokumenten gefertigte Aktenvermerke von Sachbearbeitern, sondern auch Informationen, die sich in der Papierakte oft in handschriftlichen Einträgen oder gar auf Klebezetteln wiederfanden, Aktenbestandteil sein: Beispielsweise Wiedervorlagedaten, Eingangs- und Ausgangsdaten, Ab-Vermerke, Angaben zu genutzten Kommunikationswegen, Erstellerinformationen – eventuell einschließlich möglicher elektronischer Signaturen – und gegebenenfalls weiterer Informationen beispielsweise aus einem genutzten Dokumentenmanagementsystem, die Rückschlüsse auf die Integrität und Authentizität zulassen. Mitnichten werden reine Interna grundsätzlich keine Aktenbestandteile. Diese Metadaten und Dokumentenattribute müssen bei Vorlage der Akte an einen akteneinsichtsberechtigten Dritten auslesbar, das heißt darstellbar, sein. Würde man sämtliche das Dokument „umgebende“ Daten und Metadaten nicht für eine vollständige Akte verlangen, würde diese gewissermaßen leblose Akte ihrer Sachzusammenhänge beraubt und damit ihre nachträgliche Überprüfbarkeit jedenfalls erschwert, möglicherweise sogar unmöglich gemacht.

Bei der Organisation und Ablage einer elektronischen Behördenakte ist daher kritisch

43 BT-Drs. 17/11473, S. 37.
44 *Müller*, NZS 2014, 929, 930.
45 *Kallerhoff*, in: Stelkens/Bonk und Sachs, VwVfG, 8. Auflage, 2014 § 29 Rn. 32; vgl. aber auch *Bohl*, NVwZ 2005, 133, 135.

zu überprüfen, ob sämtliche Daten und Metadaten, die einen inhaltlichen Informationswert haben, der infolge des Akteneinsichtsrechts vorzulegen wäre, bei der Vorlage/Übermittlung der Akte dargestellt werden können. Zwei Beispiele, in denen dies nicht gelungen ist, lassen sich einem Beschluss des BPatG (Bundespatentgerichts) vom 10. Juni 2013 – 20 W (pat) 24/12 – entnehmen:

> „[…] gleichwohl ist der elektronischen Verfahrensakte aber kein entsprechender Absendevermerk für den (Prüfungs-)bescheid vom 11.07.2011 zu entnehmen, was verfahrensrechtlich schon deshalb bedenklich erscheint, weil damit der Fristablauf nicht eindeutig bestimmt werden kann. […] Insgesamt gibt die Verfahrensakte des DPMA den chronologischen und aus sich heraus verständlichen Verlauf der Fristgesuche und -verlängerungen nicht lückenlos und nachvollziehbar wieder, den das Gebot der Aktenwahrheit und -klarheit stets gebietet.
>
> […]
>
> Darüber hinaus befindet sich anscheinend in der übermittelten elektronischen Verfahrensakte des DPMA [Deutsches Patent- und Markenamt] kein elektronisches Dokument, das als ordnungsgemäße, vom zuständigen Prüfer unterzeichnete, d. h. elektronisch signierte Urschrift […] angesehen werden könnte. […] da eine eindeutige Zuordnung einer Signatur zum Beschluss gerade nicht gewährleistet ist.“

1.5 Scannen von Papier als besondere Herausforderung

Führt die Behörde ihre Akten ganz oder teilweise elektronisch, legt sie selbst erstellte oder elektronisch eingesandte Dokumente (rechtssicher) elektronisch ab. Eingehende Papierdokumente müssen dann eingescannt werden. Im Rahmen rechtlicher Streitigkeiten dienen diese Dokumente dann dem Beweis der tatsächlichen Vorgänge.

Der Scanvorgang ist bei (noch) vorherrschender Papierkorrespondenz allerdings ein organisatorisches Nadelöhr und hat auch im Hinblick auf den Beweiswert des Scanergebnisses technisch-organisatorisch hohen Anforderungen zu genügen.[46]

Im Scanvorgang sind das kopierende Scannen und das ersetzende Scannen zu unterscheiden.

Kopierendes Scannen meint:

- Das digitalisierte Papier steht weiter zur Verfügung.
- Das elektronische Dokument dient nur als rechtlich nicht verbindliche Arbeitshilfe.
- Für eine mögliche Beweiserbringung kommt es auf das Papierdokument an.
- Die TR RESISCAN (Technische Richtlinie „Ersetzendes Scannen“ des Bundesamtes für Sicherheit in der Informationstechnik, BSI) ist auf das kopierende Scannen nicht unmittelbar anwendbar; lediglich ihre Grundsätze können entsprechend/orientierend herangezogen werden.

Unter ersetzendem Scannen ist zu verstehen:

- Das digitalisierte Papier steht nach dem Scanvorgang nicht mehr/nur noch zeitlich übergangsweise zur Verfügung (das heißt es wird vernichtet oder aus der Hand gegeben).
- Das elektronische Dokument ersetzt damit das Papierdokument; es ist das neue „Original“.
- Für eine mögliche Beweiserbringung kommt es auf das elektronische Dokument an.
- Für das ersetzende Scannen gilt die TR RESISCAN als Handlungsempfehlung und (unverbindliche) Definition des „Standes der Technik“.

46 Vgl. *Müller*, ZFSH-SGB 2019, 73, 80.

Die rechtlichen Anforderungen an das ersetzende Scannen sind selbstredend deutlich höher als die an das kopierende Scannen.
Ziel des ersetzenden Scannens muss es sein, für den Fall eines gerichtlichen Verfahrens den Beweiswert des digitalisierten Papiers möglichst weitgehend zu erhalten.
Ziel des kopierenden Scannens ist es dagegen lediglich, dem Entscheider eine verlässliche Arbeitsgrundlage zu liefern. Völlig anspruchslos ist allerdings auch dies nicht; beispielsweise muss der Entscheider gegebenenfalls vor der Entscheidung Kenntnis vom Vorhandensein eines Schriftstücks erlangen, damit die auf dem „Arbeitshilfsmittel elektronisches Dokument" basierende Entscheidung nicht fehlerhaft ist. Für spätere Gerichtsprozesse kann allerdings auf das ja noch vorhandene Papier zurückgegriffen werden, weshalb der Beweiswert des Papiers nicht (vollständig) erhalten werden muss.

1.5.1 Rechtliche Grundlagen

Gemäß § 7 Abs. 1 Satz 2 EGovG ist bei der Übertragung in elektronische Dokumente (Scanvorgang) nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. Den Stand der Technik gibt nach allgemeiner Auffassung insbesondere die Technische Richtlinie „Ersetzendes Scannen" (TR RESISCAN) des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) wieder. Gesetzeskraft kommt dieser Richtlinie andererseits nicht zu, obschon sie nicht selten mantraartig zitiert wird; durchaus denkbar ist auch die Orientierung an anderen – allerdings vergleichbaren – Scanverfahren. Nach dem Willen des Gesetzesgebers ebenso wie nach dem Sinn und Zweck der Vorschrift und vor allem im Hinblick auf die Bedürfnisse der behördlichen und forensischen Praxis ist ausschließlich entscheidend, dass die Qualität des Scanguts vollständig inhaltserhaltend ist. Die TR RESISCAN hat keinen Rechtsnormcharakter, sondern dient nur der Ausfüllung des unbestimmten Rechtsbegriffs des Stands der Technik. Unmittelbar anwendbar ist die TR RESISCAN nur für das ersetzende Scannen, also die Digitalisierung mit dem Ziel, dass das Scangut vernichtet oder jedenfalls nach der Digitalisierung wieder aus der Hand gegeben wird.
Inhaltlich gilt, dass weder die technische Perfektion der Digitalisierung entscheidend ist[47], noch das Vorliegen einer (externen) Zertifizierung nach einer bestimmten Richtlinie oder einem bestimmten Verfahren andererseits.[48] Maßgeblich ist mithin, dass durch das Einscannen keine Informationen verloren gehen oder verändert werden, die einen inhaltlichen Informationsgehalt haben. Der Stand der Technik muss sich dementsprechend neben der Nutzung hinreichender Hard- und Software insbesondere in der Formulierung der Arbeitsanweisungen für Scanstellen oder bei der Wahl von Voreinstellungen des Scanners niederschlagen.[49]
Dies ist freilich nur für das ersetzende Scannen erforderlich, das heißt, wenn das Papieroriginal nach dem Scanvorgang vernichtet oder jedenfalls aus der Hand gegeben wird. Wird das Papieroriginal nach dem Scanvorgang beweissicher aufbewahrt und steht weiterhin bei Bedarf zur Verfügung, handelt es sich lediglich um kopierendes Scannen. Hierfür sind die hohen Anforderungen der TR RESISCAN nicht einzuhalten. Die TR RESISCAN orientiert sich bezüglich der zu beachtenden Maßnahmen im Rahmen des Scannings an den Schutzbedarfsanforderungen entsprechend der Kategorien des BSI IT-Grundschutzes – Verfügbarkeit, Integrität und Vertraulichkeit, die jeweils den Stufen „normal" (Schadensauswirkung sind begrenzt und überschaubar), „hoch" (Schadensauswirkungen können beträchtlich sein)

47 BT-Drs. 17/12634 S. 30.
48 OVG Münster vom 17.12.2018 – 1 A 203/17 mit Anmerkungen *Müller*, NVwZ 2019, 576, 579.
49 *Müller*, ZFSH-SGB 2019, 73, 80; ders., KrV 2019, 99, 104.

oder „sehr hoch“ (Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen) zugeordnet werden können.[50] Ziel einer Schutzbedarfsfeststellung ist es, den Schutzbedarf zu klären und damit die Festlegung der Sicherheitsanforderungen und die Auswahl angemessener Sicherheitsmaßnahmen für die einzelnen Zielobjekte des betrachteten Informationsverbundes zu steuern. Die Definitionen lassen keine allgemeingültigen Zuordnungen zu den einzelnen Schutzbedarfen zu; letztlich handelt es sich um einen risikobasierten Ansatz, der eine Kosten-Nutzen-Abwägung erforderlich macht.[51]

Der Schutzbedarf wird für die Kategorien betroffener Dokumente einzeln bestimmt. Für alle Dokumente, die dem gleichen Scanverfahren zugeordnet werden, gilt das sogenannte Maximalprinzip. Das heißt, der Schutzbedarf des schutzwürdigsten Dokuments, das einem bestimmten Scanverfahren zugeführt wird, bestimmt, nach welchem Schutzbedarf dieses konkrete Scanverfahren betrachtet werden muss („Vererbung“, „Infizierung“).

Entsprechend ist es möglich, Dokumente mit einem bestimmten (beispielsweise besonders hohen) Schutzbedarf nicht einem Scanverfahren zuzuordnen, sondern sie entweder gar nicht, nicht ersetzend oder nach einem anderen Verfahren zu scannen (Verteileffekt). So lässt sich der Schutzbedarf für ein zentrales Scanverfahren niedrig halten, obwohl in Einzelfällen auch Dokumente mit einem besonders hohen Schutzbedarf eingehen können.

Die TR RESISCAN bietet ein Basismodul mit den minimalen Anforderungen an den Scanprozess. Aufgeteilt auf die Schutzbedarfskategorien kommen jeweils Aufbaumodule mit zusätzlichen Anforderungen zur Anwendung, wenn der Schutzbedarf „hoch“ oder „sehr hoch“ anzusiedeln ist.[52] Grundsätzlich zu beachten sind ein weitgehend arbeitsteiliges Vieraugenprinzip innerhalb der Scanstelle im Rahmen des Scan- und Kontrollvorgangs sowie eine jedenfalls stichprobenartige Qualitäts- und Vollständigkeitskontrolle.

1.5.2 Verfahrensdokumentation

Das Scankonzept ist in einer Verfahrensdokumentation festzuhalten. Diese Verfahrensdokumentation ist letztlich eine behördeninterne Konzeption oder Dienstanweisung.

Die Verfahrensdokumentation erlangt in einem Prozess, bei dem es auf den Beweiswert des erstellten elektronischen Dokuments ankommt, allerdings Außenwirkung. Ihre prozessuale Bedeutung ist erheblich. Durch Vorlage dieser Verfahrensdokumentation kommt die Behörde ihrer Darlegungslast hinsichtlich der Güte des Scanverfahrens nach. Im Rahmen eines „prozessualen Ping-Pong-Spiels“[53] liegt es nach der Vorlage der Verfahrensdokumentation am Verfahrensgegner vorzutragen, wo er meint, Fehler oder Lücken im Scanprozess der Behörde zu erkennen. Gelingt dies, wird dadurch der Beweiswert des elektronischen Dokuments geschwächt, mit der Folge, dass gegebenenfalls ein Beweis nicht mehr mittels der Behördenakte erbringbar ist.

Fehlerquellen haben ihren Ursprung oft lange vor dem konkreten Streitfall in der Planungsphase des Digitalisierungsprozesses der Behörde. Aus Zeitnot oder wegen des gefürchteten Aufwands ist oft bereits die Schutzbedarfsanalyse unzureichend. Dreh- und Angelpunkt einer Auseinandersetzung im Scanprozess ist zumeist aber die auf den eigentlichen Scanvorgang folgende sogenannte „Integritätsprüfung“ und die hierdurch sichergestellte Ausfüllung des (unbe-

50 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_01/Lektion_4_01_node.html.

51 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_02/Lektion_4_02_node.html.

52 *Roßnagel* und *Nebel*, NJW 2014, 886, 887.

53 Vgl. VG Karlsruhe vom 21.2.2023 – A 19 K 304/23 mit Anmerkungen *Müller*, NVwZ 2023, 651.

stimmten Rechts-)Begriffs der „bildlichen und inhaltlichen Übereinstimmung“. Im Detail liegt hier bereits eine erhebliche Herausforderung bei der Formulierung von Arbeitsanweisungen für Scanstellen oder bei der Wahl von Voreinstellungen beim Scanner.
Wichtig ist deshalb, sich bei der Formulierung einer Verfahrensdokumentation vor Augen zu führen, dass die Dokumentation nicht (nur) für die eigene Behörde, beispielsweise als Dienstanweisung für die Scanmitarbeitenden, erfolgt, sondern dass die Verfahrensdokumentation Gegenstand einer gerichtlichen Auseinandersetzung sein kann. Ein möglicher Adressat ist deshalb jeder potenzielle Verfahrensgegner.
Gemäß Ziffer 4.2.1.1 A.G.1 der TR RESISCAN (Verfahrensdokumentation) muss eine Verfahrensdokumentation existieren, um einen geordneten Ablauf beim ersetzenden Scannen zu ermöglichen.
Die TR RESISCAN sieht für die Verfahrensdokumentation insbesondere die folgenden Inhalte vor: Die Verfahrensdokumentation umfasst insbesondere eine von der TR RESISCAN als Verfahrensanweisung bezeichnete Ablaufbeschreibung oder Dienstanweisung, die sich an die in den Scanprozess eingebundenen Personen richtet. Daneben wird die Verfahrensdokumentation regelmäßig weitere Unterlagen, wie beispielsweise ein Sicherheitskonzept, umfassen. Die Verfahrensanweisung kann auf mitgeltende Unterlagen, wie zum Beispiel Konzepte, Spezifikationen, Handbücher, Arbeitsanweisungen und Stellenbeschreibungen, verweisen. Diese sollten dann ebenfalls als Anlagen hinzugefügt werden.

1.5.3 Strukturanalyse

Gemäß Ziffer 3.1 der TR RESISCAN muss ein Anwender (= „Nutzerbehörde“) eine Strukturanalyse für sein Scansystem durchführen und hierbei die für seinen Scanprozess relevanten IT-Systeme, Netze, Anwendungen und Datenobjekte identifizieren und einen bereinigten Netzplan erstellen.
Erforderlich ist es hierzu, dass im Zuge der Identifikation der relevanten IT-Systeme und Anwendungen des Scansystems zunächst ein Netzplan erstellt wird, der auch Ausgangspunkt für die Betrachtung des Scanprozesses ist. Das zu betrachtende Scansystem umfasst dabei die zum Scannen notwendigen Komponenten inklusive der Schnittstellen zu den angrenzenden Systemen (insbesondere der Kommunikationskomponenten (beispielsweise der Schnittstelle zum beBPO (besonderes Behördenpostfach) oder zu Outlook) und der eAkte/des Dokumentenmanagementsystems). Die hierbei identifizierten Systeme und Anwendungen bilden die Grundlage für die Bestimmung der notwendigen Sicherheitsmaßnahmen bei der Umsetzung der relevanten Maßnahmen aus dem Grundschutz-Kompendium des BSI (BSI-GSK).
Zusätzlich zur Identifikation der IT-Systeme und Anwendungen müssen im Rahmen der Strukturanalyse auch die Netze und Kommunikationsbeziehungen identifiziert werden, damit später adäquate Sicherheitsmaßnahmen ausgewählt und umgesetzt werden können. Wie in der TR RESISCAN gefordert, müssen im Rahmen der Strukturanalyse ferner die relevanten Dokumente und Datenobjekte identifiziert werden; auch hierzu ist letztlich eine Posteingangsanalyse durchzuführen, die aber ohnehin im Rahmen der Schutzbedarfsanalyse erforderlich ist.
Das BSI hat einen Leitfaden für die Erstellung einer Strukturanalyse in Bundesbehörden erstellt, der aber auch durch Landes- und Kommunalbehörden ohne Weiteres nutzbar ist.[54]

1.5.4 Schutzbedarfsanalyse

Die Schutzbedarfsanalyse gemäß Ziffer 4.2.1.2 A.G.2 der TR RESISCAN dient der Feststellung des Sicherheitsniveaus für die

54 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/Praxis_E-Scannen/leitfaden_praxisbeispiel_escannen_anlage_str.pdf?__blob=publicationFile&v=2.

zu verarbeitenden Dokumente. Sie richtet sich nach den Grundwerten der IT-Sicherheit („Integrität“, „Vertraulichkeit“ und „Verfügbarkeit“) und muss durchgeführt werden, um diesbezüglich die Schutzbedarfsklasse („normal“, „hoch“ oder „sehr hoch“) zu bestimmen.
Problematisch ist an dieser Stelle der Zielkonflikt bei der Festlegung des Schutzbedarfs, der – nicht selten unzutreffend – nur mit „hoch“ oder gar „normal“ angesetzt wird, weil der Aufwand für die Implementation der Aufbaumodule für den Schutzbedarf „sehr hoch“ gescheut wird. Schließlich wird die Schadensauswirkung oft nur aus Sicht der Behörde und rein finanziell betrachtet und deshalb zu gering taxiert, während aus Sicht des Bürgers bereits ein beträchtlicher Schaden droht. Schutzbedarf „sehr hoch“ liegt auch dann vor, wenn aus Sicht des Bürgers ein existenzbedrohendes Szenario denkbar ist. Mit „Existenz“ ist in diesem Zusammenhang zunächst die physische Existenz gemeint; die aber gerade in Asylsachen, im Gefahrenabwehrrecht, aber auch im Sozialrecht (Grundsicherungsrecht, Gesetzliche Krankenversicherung) durchaus tangiert sein kann. Umfasst ist aber darüber hinaus auch die rein wirtschaftliche Existenz; also das Insolvenzrisiko betroffener Bürgerinnen und Bürger.
Hingegen nimmt beispielsweise die KGSt (Kommunale Gemeinschaftsstelle für Verwaltungsmanagement) in der Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESISCAN[55] für Kommunen grundsätzlich den Schutzbedarf „normal“ an. Schutzbedarf „hoch“ gebe es nur ausnahmsweise. Schutzbedarf „sehr hoch“ falle im kommunalen Bereich nicht an. Gerade dort, wo es um Gefahrenabwehrrecht, um Asylrecht und um Existenzsicherungsrecht geht, muss dieses Ergebnis aber sehr kritisch hinterfragt werden. Insbesondere hilft es nicht immer, dass Papier ganz oder für einen gewissen Zeitraum aufbewahrt wird, wenn sich ein vollständig elektronisch arbeitender Sachbearbeiter auf die Vollständigkeit der elektronischen Akte verlässt und deshalb gegebenenfalls nichts von der Existenz eines aufbewahrten Papiers weiß.
Wird als Ergebnis der Schutzbedarfsanalyse festgestellt, dass Dokumente mit unterschiedlichen Schutzbedarfen zu scannen sind, so gibt es drei strategische Vorgehensweisen.

1.5.4.1 „Vererbung“/„Infizierung“

Sämtliche Dokumente werden so eingescannt, wie es nach dem Schutzbedarf des Dokuments mit dem höchsten Schutzbedarf erforderlich ist. Der Vorteil ist, dass die Behörde ein einheitliches Scankonzept nutzen kann. Der Nachteil besteht darin, dass dann für sämtliche Dokumente entsprechend aufwendige Sicherheitsmaßnahmen erforderlich sind.

1.5.4.2 „Verteileffekt“

Dokumente mit „hohem“ oder „sehr hohem“ Schutzbedarf werden in einem gesonderten Verfahren unter Beachtung ihres Schutzbedarfs gescannt; alle Dokumente mit niedrigerem Schutzbedarf werden mit den entsprechend geringeren Sicherheitsmaßnahmen gesondert gescannt. Die Behörde muss entsprechend mehrere verschiedene Scanverfahren etablieren. Der Vorteil liegt darin, dass nur für die (wenigen) Dokumente mit hohem/sehr hohem Schutzbedarf der zusätzliche Aufwand erforderlich ist, während die Masse der Dokumente mit geringerem Schutzbedarf unter wenigen Sicherheitsanforderungen gescannt werden kann. Es besteht lediglich ein zusätzlicher Aufwand in der Vorsortierung.

55 https://www.kgst.de/dokumentdetails?path=/documents/20181/1379003/08-B-2017_Ersetzendes-Scannen.pdf/1876dad3-fed1-6633-8651-7ba06ee3cf7a.

1.5.4.3 „Papierdoppelakte“

Schließlich können Dokumente mit hohem oder sehr hohem Schutzbedarf in einer Papierdoppelakte aufbewahrt werden. Diese Dokumente werden dann nicht ersetzend, sondern nur kopierend gescannt. Entsprechend geringer sind die erforderlichen Sicherheitsanforderungen. Nur Dokumente mit Schutzbedarf normal – oder sogar gar keine Papierdokumente – werden ersetzend gescannt. Der Vorteil liegt darin, dass der Aufwand für das Scanning sehr gering gehalten werden kann. Der Nachteil besteht darin, dass weiterhin Papier aufbewahrt werden muss. Um diesen Aufbewahrungsaufwand gering zu halten, lohnt sich ein solches Vorgehen nur dort, wo bereits weit überwiegend im elektronischen Rechtsverkehr kommuniziert wird.

1.5.5 Posteingangserhebung

Hinsichtlich der Art der betroffenen Dokumente ist eine Erhebung des Scanguts erforderlich. Dies kann für den Bereich des Posteingangsscannings insbesondere durch eine Posteingangserhebung über einen längeren Zeitraum erfolgen. Hierbei sind die eingehenden Dokumente im Hinblick auf ihren weiteren Workflow und im Hinblick auf ihren Schutzbedarf zu kategorisieren. Das Ergebnis kann wie folgt aussehen:

1.5.6 Darstellung des Scanprozesses

Zentral in der Verfahrensdokumentation ist die Darstellung des Scanprozesses. Hierbei ist vor allem darauf zu achten, dass bei der rechtlichen Prüfung der Darstellung ersichtlich wird, dass es keine beweiswertrelevanten Lücken gibt. Insoweit sind die neuralgischen Punkte sämtliche Situationen im Scanprozess, in denen eine Veränderung des Scanguts selbst oder des Scanprodukts möglich sind.

1.5.7 Qualitätskontrolle im Scanverfahren

Qualitätskontrolle und Integritätssicherung schließen sich an die eigentliche Digitalisierung an. Je nach Scanvolumen und Schutzbedarf erfolgt die Qualitätskontrolle stichprobenartig.
Die Stichprobe kann im Rahmen der Einführung des Scanprozesses abhängig von der pilothaft festgestellten Fehlerhäufigkeit, des weiteren Fehlercontrollings im Linienbetrieb und dem Schutzbedarf festgelegt werden. Sie ist Gegenstand ständiger Überprüfung. Bei seltenen Fehlern kann sie je nach Vertretbarkeit hinsichtlich des Schutzbedarfs herabgesetzt werden. Werden häufige Fehler festgestellt, kann auch ein Heraufsetzen der Qualitätskontrolle erforderlich werden.
Es ist empfehlenswert, jedenfalls auch eine (geringere) Stichprobe außerhalb der eigentlichen Scanstelle vorzusehen, um das Ergebnis weiter zu objektivieren.

1.5.8 Bildliche und inhaltliche Übereinstimmung

Auslegungsbedürftig ist ferner der (unbestimmte Rechts-)Begriff der „bildlichen und inhaltlichen Übereinstimmung“. Auch insoweit ist der Maßstab ausschließlich die inhaltserhaltende Qualität des Scanguts, nicht die technische Perfektion der Digitalisierung. Dies klingt einfach, ist aber im Detail eine Herausforderung bei der Formulierung von Arbeitsanweisungen für Scanstellen oder bei der Wahl von Voreinstellungen beim Scanner. Als Beispiel sei genannt, dass die Erkennung – und automatische Aussortierung – von Leerseiten durch die Definition eines Schwellwertes in Kilobyte kaum möglich ist, wenn Scangut gemischt aus reinweißem Papier und „Umweltpapier“ besteht und wenn Papier teilweise gelocht und teilweise ungelocht ist.
Aus praktischen Erfordernissen heraus muss klar sein, dass kein Farbscan erforderlich ist, nur weil das Behördenlogo einen Farbanteil hat. Unnötige Farbscans sind unbedingt zu

vermeiden; Farbscans haben nämlich eine erheblich größere Dateigröße und kosten daher Rechenleistung und damit Ergonomie beim Aktenhandling. Ebenso klar muss aber sein, dass ein Farbscan erforderlich ist, um rechtserhebliche Farbinformationen zu erhalten oder solche, die einen tatsächlichen Beweiswert haben könnten (beispielsweise die unterschiedlichen Farben eines Kugelschreibers auf einem handschriftlich ausgefüllten Formular, weil diese ein Indiz dafür sein könnten, dass verschiedene Personen die Eintragungen vorgenommen haben). Trivial ist die Erstellung einer Organisationsanweisung daher nicht.

1.5.9 Der Transfervermerk im Scanverfahren

Die Bestätigung der bildlichen und inhaltlichen Übereinstimmung erfolgt in einem sogenannten Transfervermerk.
Im Falle eines Rechtsstreits soll der Transfervermerk ermöglichen, den Ablauf des Medienbruchs sowie der weiteren Prozessschritte entlang des Scanprozesses bis zur beweiswertsichernden Aufbewahrung nachzuvollziehen, um hieraus eine Schlussfolgerung zum Beweiswert des elektronischen Abbilds eines Papierdokuments zu ziehen.
Der Transfervermerk kann in Form eines (elektronischen) Dokuments dem Scanprodukt hinzugefügt oder beigelegt werden; er muss dann mit diesem untrennbar verbunden werden (beispielsweise mittels einer elektronischen Signatur). Der Transfervermerk kann aber auch selbst als elektronische Signatur oder maschinenlesbar als XML-Datei ausgestaltet werden.
Die inhaltliche und technische Ausgestaltung ist vom Gesetz nicht weiter vorgeschrieben. Einen Anhalt für den Mindestinhalt gibt die TR RESISCAN. Gemäß Ziff. 4.2.7.4 der TR RESISCAN soll der Transfervermerk für jedes Scanprodukt erstellt werden und insbesondere folgende Aspekte dokumentieren:

- Ersteller des Scanproduktes,
- technisches und organisatorisches Umfeld des Erfassungsvorganges,
- etwaige Auffälligkeiten während des Scanprozesses,
- Zeitpunkt der Erfassung,
- Ergebnis der Qualitätssicherung und
- die Tatsache, dass es sich um ein Scanprodukt handelt, das bildlich und inhaltlich mit dem Papierdokument übereinstimmt.

Der Transfervermerk muss mit dem Scanprodukt logisch verknüpft oder in das Scanprodukt integriert werden. Die Integrität des Transfervermerks muss entsprechend dem Schutzbedarf der verarbeiteten Dokumente geschützt werden. Regelmäßig bietet sich daher die Nutzung qualifizierter elektronischer Signaturen – gegebenenfalls qualifizierter elektronischer Containersignaturen – an. Für die Dokumentation des technischen und organisatorischen Umfelds kann der Transfervermerk auf die zu diesem Zeitpunkt gültige Verfahrensdokumentation verweisen.

1.6 Der Beweis mit rechtswidrig erlangten Daten

Zivilprozessual besteht bei rechtswidrig erlangten Beweismitteln (Beweiserhebungsverbot) kein grundsätzliches Beweisverwertungsverbot. Zwischen rechtswidriger Beweismittelgewinnung und späterer Beweismittelverwertung besteht kein Rechtswidrigkeitszusammenhang.[56] Erst recht gilt dies im Regime des Amtsermittlungsprinzips.
Die ZPO enthält keine Vorschriften zur Beweisverwertung rechtswidrig erlangter Erkenntnisse und Beweise. Daraus folgt, dass auch rechtswidrig erlangte Beweismittel grundsätzlich der freien richterlichen Beweiswürdigung unterliegen. Hierfür spricht insbesondere der Anspruch der Parteien auf recht-

56 *Ahrens*, NJW 2018, 2837, 2837.

liches Gehör gemäß Art. 103 Abs. 1 GG.[57] Dieses Prozessgrundrecht ist andererseits in schonenden Ausgleich mit durch die Beweiserhebung oder -erlangung verletzten Grundrechten zu bringen. Hierzu zählen insbesondere das Recht auf informationelle Selbstbestimmung oder der grundrechtliche Schutz der Wohnung oder der Geschäftsräume. Der schonende Ausgleich erfolgt in Form einer Abwägung der wechselseitigen Rechtspositionen der Betroffenen, wobei der unantastbare Kernbereich der Persönlichkeit, also der persönliche Lebensbereich, nicht verletzt werden darf.[58]

Die fundamentalen rechtsstaatlichen Grundsätze des rechtlichen Gehörs sowie des effektiven Rechtsschutzes gehen datenschutzrechtlichen Belangen vor.[59] Auch der BGH (Bundesgerichtshof) geht hinsichtlich der Verwertung von Dashcam-Aufnahmen beispielsweise davon aus, die permanente anlasslose Videoaufzeichnung durch eine Dashcam während der Fahrt sei als datenschutzrechtlich unzulässig einzustufen. Gleichzeitig hat der BGH aber auf entsprechende Rüge beanstandet, dass die als Beweismittel vorgelegte Videoaufnahme nicht gemäß § 371 ZPO in Augenschein genommen worden sei. Aus der Rechtswidrigkeit eines Beweismittels – so der BGH – folge nicht automatisch ein prozessuales Verwertungsverbot. Die Verwertung unzulässig erlangter Beweismittel sei in der ZPO nicht ausdrücklich geregelt.[60]

Im Ergebnis gilt deshalb: Datenschutzrechtliche Erwägungen sind ein wichtiger, aber nicht alleiniger Faktor bei der Ausgestaltung und Auslegung von prozessualen Normen. Es verbleibt daher eine „Mehrdimensionalität von Prozessordnungen“, die auch eine Stütze in der DSGVO (Datenschutz-Grundverordnung) selbst findet.[61] Gemäß EG 4 Satz 2 ist das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht; es muss gegen andere Grundrechte abgewogen werden. Dazu zählt unter anderem auch das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren (EG 4 Satz 3). Die Abwägung unterschiedlicher Grundrechtspositionen und die damit angestrebte Herstellung praktischer Konkordanz obliegt jedoch dem nationalen Gesetzgeber.[62]

Eine Güterabwägung zwischen dem allgemeinen Persönlichkeitsrecht und Prozessgrundrechten ist insbesondere in datenschutzrechtlich sensiblen Bereichen erforderlich, weil das Datenschutzrecht seine grundrechtliche Basis im Recht auf informationelle Selbstbestimmung hat.[63]

Insbesondere Gegenstand arbeitsrechtlicher Verfahren waren Fälle von offener oder verdeckter Videoüberwachung am Arbeitsplatz.[64] Eine offene Videoüberwachung samt Speicherung der Bildsequenzen, die vorsätzliche Handlungen eines Arbeitnehmers (beispielsweise Unterschlagungen) zulasten des Arbeitgebers zeigen sollen, hat das BAG (Bundesarbeitsgericht) für zulässig gehalten, um der dem Arbeitgeber obliegenden Darlegungs- und Beweislast in einem potenziellen Rechtsstreit genügen zu können.[65] Auch eine heimliche Videoüberwachung eines Arbeitnehmers hält das BAG dagegen nur für zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zulasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung ausgeschöpft sind und die Videoüberwachung insgesamt nicht unverhältnismäßig ist.[66]

57 Zu Recht *Huber*, in: Musielak und Voit, § 371 ZPO Rn. 15 mit weiteren Nachweisen.
58 BVerfG vom 09.10.2002 – 1 BvR 1611/96; *Ahrens*, NJW 2018, 2837, 2838.
59 BSG vom 18.12.2018 – B 1 KR 40/17 R; *Schütz*, NZS 2019, 719.
60 BGH vom 15.05.2018 – VI ZR 233/17.
61 *Krüger/Resch* und *Vogelgesang*, jM 2022, 8, 12.
62 *Krüger/Resch* und *Vogelgesang*, jM 2022, 8, 12.
63 Hierzu *Brand* und *Skowronek*, RDi 2021, 178, 180; siehe zu Privatsphäre im Hinblick auf Internetinhalte *Bieresborn*, NZS 2016, 531.
64 Umfassend hierzu *Bauer* und *Schansker*, NJW 2012, 3527.
65 BAG vom 23.08.2018 – 2 AZR 133/18 mit Anmerkungen *Fuhlrott*, NZA-RR 2018, 597, 597.
66 BAG vom 21.06.2012 – 2 AZR 153/11 (Diebstahl aus Warenbestand des Arbeitgebers); BAG vom 27.03.2003 – 2 AZR 51/02 (überdurchschnittliche hohe Inventurdifferenzen); *Huber*, in: Musielak und Voit, § 371 ZPO Rn. 16a.

Mit einem entsprechenden Vorgehen behandelt der BGH[67] Aufzeichnungen sogenannter Dashcams zur Aufklärung des Unfallhergangs bei Straßenverkehrsunfällen. Der BGH sieht Dashcam-Aufzeichnungen als zulässiges Beweismittel im Unfallhaftpflichtprozess an, selbst wenn die jeweilige Aufzeichnung nicht den datenschutzrechtlichen Anforderungen entsprach. Im Rahmen einer Güterabwägung sei dem Interesse des Geschädigten an einer Sachverhaltsaufklärung angesichts ansonsten bestehender Beweislosigkeit der Vorrang gegenüber dem Datenschutzrecht einzuräumen.[68] Das Gericht kann im Rahmen seines Ermessens von Amts wegen die Vorlage der Dashcam-Aufnahme gemäß § 144 ZPO anordnen.

Grundsätzlich in Betracht kommen auch digitale Videoaufnahmen einer stationären Videokamera. Insoweit ist allerdings zu beachten, dass permanent laufende, stationäre Kameras – insbesondere solche, die heimlich das öffentliche Leben aufnehmen – regelmäßig einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht der heimlich aufgenommenen Personen darstellen.[69] Zu beachten ist in jedem Fall, dass die Prüfungen auf der Ebene der Beweiserhebung und der Beweisverwertung durchaus zu unterschiedlichen Ergebnissen führen können.[70]

Neben dem Recht auf informationelle Selbstbestimmung kann auch Art. 10 GG als abwägungsrelevantes Grundrecht in Betracht kommen.

2. Fazit

Problematisch ist, wenn die beweisrechtlichen Folgen des Verlusts der Urkundseigenschaft im Rahmen von Digitalisierungsprojekten übersehen werden. Wenn eine nur noch digital vorgehaltene Information (hier: Posteingangsdatum) eine bisher verwendete (öffentliche) Urkunde ersetzt (hier: behördlicher Posteingangsstempel), ist für den dann erforderlichen Augenscheinsbeweis die Anforderung aufzustellen, dass das stattdessen eingesetzte elektronische System eine vergleichbare Richtigkeitsgewähr und einen identischen Informationsgehalt aufweisen muss, wie die bisherige papiergebundene Sachbearbeitung um einen entsprechenden Beweiswert zu erhalten.[71] Es geht insoweit nicht darum, papiergebundene Vorgänge digital nachzubilden (und hierdurch Rationalisierungspotenzial beziehungsweise Optimierungsmöglichkeiten zu vergeben), sondern die bisherigen Funktionalitäten (hier: rechtssichere Bestimmung des Eingangszeitpunkts) müssen digital abgebildet werden. Es ist deshalb erforderlich zu betrachten, ob der gegebenenfalls notwendige Beweis im Wege des Augenscheinsbeweises erbracht werden kann. Hierzu sind gegebenenfalls Indizien (wie beispielsweise ein lückenloses Posteingangsbearbeitungskonzept oder eine Scandokumentation) beziehungsweise anderweitige Beweismittel (beispielsweise Zeugen) vorzuhalten.

Anschrift des Verfassers:

Prof. Dr. Henning Müller
Sozialgericht Darmstadt
Steubenplatz 14
64293 Darmstadt

67 BGH vom 15.05.2018 – VI ZR 233/17.

68 *Huber*, in: Musielak und Voit, § 371 ZPO Rn. 16b; siehe hierzu ferner: *Ahrens*, NJW 2018, 2837; *Prütting*, RAW 2018, 15; *Kuntz*, jM 2018, 354; *Froitzheim*, NZV 2018, 109; *Radke*, jM 2018, 148; *Kunkel* und *Kunkel*, jurisPR-Compl 2/2018 Anm. 2; *Kunkel* und *Kunkel*, jurisPR-StrafR 12/2018 Anm. 3; *Kaiser*, NJW 2016, 2790; *Ernst*, CR 2015, 620; *Pötters* und *Wybitul*, NJW 2014, 2074; *Balzer* und *Nugel*, NJW 2014, 1622; *Günther*, ZfSch 2018, 552.

69 Vgl. BGH vom 21.10.2011 – V ZR 265/10; LG Memmingen vom 14.01.2016 – 22 O 1983/13; LG Mühlhausen vom 12.05.2020 – 6 O 486/18; AG Geilenkirchen vom 05.01.2023 – 10 C 114/21.

70 *Nugel*, jurisPR-VerkR 12/2023 Anm. 4.

71 So beispielsweise das LSG Berlin-Brandenburg vom 05.11.2020 – L 9 KR 204/19 für den Posteingangszeitpunkt. Siehe hierzu auch *Müller*, NZS 2021, 445 und *Engin*, RDi 2021, 264.