Rechtliche Perspektiven zur digitalen Beweisführung

Michael Knopp

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Universität Kassel
Wilhelmshöher Allee 64-66
34109 Kassel
michaelknopp@uni-kassel.de

Abstract: Digitale Inhalte werden künftig mehr noch als heute auch als Beweismittel genutzt werden. Gesetzliche Regelungen und rechtliche Untersuchungen hierzu haben sich bislang hauptsächlich auf elektronische Textdokumente bezogen. Bezüglich digitaler Fotos, Filme, Audioaufnahmen oder der Beweisführung zu Sachverhalten im virtuellen, digitalen Raum herrscht jedoch noch große Unsicherheit. Angesichts der berechtigten Manipulationsbefürchtungen sind sowohl technisch als auch rechtlich Wege für den Umgang mit digitalen Beweismitteln jeglicher Art zu finden, die eine verlässliche Beweisführung ermöglichen.

1 Digitale Beweisführung

Mit der Bedeutungszunahme digitaler Medien ist auch deren rechtliche Relevanz gestiegen. Das Recht ist mit einer Reihe von Gesetzen und Einzelnormen, durchaus auch vorgreifend, angepasst worden.[1] Digitaltechnik spielt jedoch nicht nur eine große Rolle als Quelle oder Rahmen neuer Konflikte. Ein wesentlicher Bestandteil bei der Entscheidung rechtlicher Konflikte ist die Feststellung des Sachverhaltes, der der gerichtlichen Entscheidung zugrunde gelegt wird. Genau wie der rechtliche Teil der Entscheidung ist auch der Sachverhalt zu begründen. Häufig ist die Feststellung des Sachverhalts umstrittener als die darauf folgende rechtliche Wertung. Entscheidend für den Prozess der Sachverhaltsermittlung sind Beweise. Es mehren sich Sachverhalte, die vollständig in digitalen, virtuellen Räumen angesiedelt sind, etwa wettbewerbswidrige Angebotsseiten, strafrechtlich relevante Inhalte im Internet oder E-Commerce

[1] Wichtige Etappen in Bezug auf den hier besprochenen Kontext waren das Signaturgesetz von 1997 und 2001, das Formanpassungsgesetz (Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr vom 13. Juli 2001, BGBl. I 1542 vom 18.6.2001), das JKomG (Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz – Justizkommunikationsgesetz vom 22.3.2005, BGBl. I 837) und das 3. Verwaltungsverfahrensänderungsgesetz (Drittes Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 21.8.2002, BGBl. I 3322), die Regelungen mit Bezug zu Beweisfragen im Umgang mit elektronischen Dokumenten enthalten.

Streitigkeiten. Bisher analog präsentierte Textdokumente, Photos, Filme, Audio- und technische Aufzeichnungen werden nun in digitaler Form vorgelegt oder beruhen auf digitalen Ursprüngen. Selbst vermeintlich herkömmliche, analoge Beweismittel werden von den Manipulationsmöglichkeiten des digitalen Raums beeinflusst. Ein Beispiel hierfür sind Photos, die als Negative oder Abzüge nicht auf einen digitalen Hintergrund schließen lassen, aber tatsächlich ohne weiteres Ergebnisse vorheriger digitaler Bearbeitung sein können. Digitale Beweisführung ist daher kein genau abgrenzbares rechtliches Forschungsfeld und kein feststehender Begriff. Im Folgenden ist damit die Beweisführung mittels Beweisen in digitaler Form gemeint.

Für den Umgang mit digitalen Beweismitteln und den mit diesen verbundenen Gefahren fehlen die Erfahrung und der Entwicklungsprozess von teilweise hunderten von Jahren, wie sie für analoge und verkörperte Medien bestehen. Digital gespeicherte Daten stehen – überwiegend durchaus berechtigt – in dem Ruf spurlos verändert werden zu können. E-mails oder elektronische Textdokumente sind hierfür gute Beispiele. Die Bindung an körperlich vorhandene Träger, die einmal beschrieben nicht mehr so leicht unbemerkt zu ändern sind, fehlt bei digitalen Beweismitteln oftmals. Selbst nicht wieder beschreibbare Datenträger sind in dieser Hinsicht nicht mit Papier oder Filmnegativen vergleichbar, da ihre Inhalte verändert und auf einen anderen Datenträger gebrannt werden können. Hinzu kommt, dass Digitaltechnik bei Photos, Filmen und Tonaufnahmen zunehmend das Erstellen täuschend echt wirkender, aber künstlicher Aufnahmen ermöglicht.[2] Es ist lediglich die entsprechende Software zusätzlich zu der heute beinahe omnipräsenten Hardware erforderlich. Nachdem dem Anschein nach sogar Großkonzerne vor der Fälschung von beweiserheblichen Metadaten oder der Herstellung gefälschter digitaler Beweise nicht zurückschrecken, dürfte das Vertrauen in digitale Beweismittel weiter sinken.[3] Die bisherige Grundannahme der Vertrauenswürdigkeit von bestimmten Institutionen oder Personen dürfte durch derartige Vorfälle genauso erschüttert werden wie eine Tendenz, Manipulationen zunächst für unwahrscheinlich zu halten. Je nach Rechtsmaterie und Prozessordnung stellen sich hierdurch unterschiedliche Herausforderungen.[4] Ein weiteres Grundproblem neben der erleichterten Manipulierbarkeit ist jedoch, dass zur Würdigung digitaler Beweismittel stets Vermittlungsschritte, sei es durch Hardware und Software oder zusätzlich durch Sachverständige, erforderlich sind.

In Bezug auf Dokumente mit Erklärungsinhalten wird dieser Entwicklung bereits eine große Aufmerksamkeit geschenkt.[5] Erklärungen und ihre Niederlegung in Schriftzeichen

---

[2] Zu Digitalfotos als Beweismittel [Kn08]; zur Bildmanipulation [Tr08a]; [De07]; [Ja05].

[3] S. zu einer anscheinend bi der Deutschen Bahn vorgenommenen Manipulation http://www.zeit.de/2009/18/Bahn?page=6.

[4] Für den Zivilprozess ergeben sich etwa Beweisschwierigkeiten und Probleme einer fairen Beweislastverteilung, im Strafprozess stellt sich beispielsweise die Frage, wie weit die Prüfung digitaler Beweismittel zu gehen hat und wie hoch ein grundsätzlicher Zweifel anzusetzen ist, s. grundsätzlich zu den Anforderungen an die Überzeugungsbildung BGH, Urteil v. 8.1.1988, NJW 1988, 3273; zur Vollständigkeit und Inhalt der Beweiswürdigung BVerfG, Beschluss v. 30.4.2003, NJW 2003, 2444.

[5] Jeweils mit weiteren Nachweisen und weiteren Problemfeldern wie der dauerhaften Aufbewahrung, dem Scannen und Transformieren [Fi06]; [Ro09]; rechtsvergleichend [Br96]; [En99]; [Be06]; [Ro98]; [Ro01]; [Fi02]; [Dä01]; [Fi03]; [RF06]; [RP03]; [Vi05]; zu gescannten Dokumenten [RW06].

sind Grundsäulen jeglichen Rechtsverkehrs, daher galt es hier als erstes für digitale Formen Lösungen und Sicherheiten zu schaffen.[6] Die Vielfalt weiterer digitaler Beweismittel und die digitale Beweisführung jenseits des Beweises von Erklärungen werden jedoch seltener diskutiert. Von der technischen Seite her werden auch die Beweisführung zu strafrechtlich relevanten Sachverhalten und der richtige Umgang mit Datenträgern oder dem beweissicheren Nachvollzug von Handlungen im virtuellen Raum in wachsendem Maße untersucht.[7] Diesen Bemühungen fehlt bislang eine intensive rechtliche Begleitung. Aus rechtlicher Sicht müssen Kriterien für die Sicherheit und Verlässlichkeit digitaler Beweismittel bereitgestellt werden und Regelungsmechanismen erdacht werden, die für den Umgang mit Beweisbedürfnissen im digitalen Raum und digitalen Beweismitteln Rechtssicherheit schaffen. Diesen Kriterien und Regelungsmechanismen entsprechend müssen technische Hilfsmittel entwickelt werden, die auch dem technischen Laien den Umgang mit und die rechtssichere Erzeugung von digitalen Beweismitteln erlauben.

Da die Bandbreite digitaler Beweismittel zwar vielleicht nicht ganz so weit ist wie die der herkömmlichen, aber dennoch gerade auch durch die ständige Fortentwicklung schwer überschaubar, soll im Folgenden vor allem von Digitalphotos ausgegangen werden. Soweit möglich erfolgt die Übertragung auf weitere Typen digitaler Beweismittel.

2 Rechtliche Perspektiven zu digitalen Beweismitteln

Digitale Beweismittel als Betrachtungsgegenstand erlauben zwei Perspektiven: Die eine Perspektive ist eine ex post Perspektive, wie sie etwa die Gerichte einnehmen. Hier stellen sich die Fragen, wie mit einem vorhandenen Beweismittel umzugehen ist, was sich ableiten lässt und wie der Beweiswert einzuschätzen ist. Diese Perspektive beschäftigt jedoch nicht nur die Gerichte bei der Beweiswürdigung. Auch die Prozessparteien versuchen im Vorfeld ihre Erfolgsaussichten einzuschätzen, einen bestimmten Sachverhalt beweisen oder widerlegen zu können. Genauso betrifft diese Perspektive jede andere Institution, der gegenüber Nachweise zu erbringen sind.[8] Eine andere Perspektive ergibt sich, wenn ein Sachverhalt von vornherein so gestaltet und geschaffen oder festgehalten werden soll, dass er im Streitfall mit hoher Sicherheit gegenüber Dritten bewiesen werden kann. Das wichtigste Beispiel ist regelmäßig der Vertrag, der fixiert wird um später aus ihm abgeleitete Rechte durchsetzen zu können. Aber das photographische Festhalten störender Eingriffe, sei es die zugeparkte Einfahrt vor dem Abschleppen oder die grenzverletzende Bepflanzung des Nachbarn, das Festhalten einer Rechtsverletzung durch Inhalte im Internet, die Sachverhaltsdokumentation vor einem behördlichen Eingriff sowie die Dokumentation einer Tätigkeit zum Nachweis ordnungsgemäßen Handelns, etwa einer forensische

---

[6] BT-Drs. 14/4987, 10; BT-Drs. 15/4067, 24.
[7] Jeweils mit weiteren Nachweisen [Kn08, Fn. 14-18]; [Ba99]; [Tr08]. Eine interdisziplinäre Herangehensweise findet sich in dem Forschungsprojekt Cased, s. unter http://www.cased.de.
[8] Beispiele sind etwa Versicherungen, die öffentliche Verwaltung oder Arbeitgeber.

Untersuchung, führt zu ganz ähnlichen Bedürfnissen. Hier sollen ex ante Beweismittel mit einem hohen Beweiswert geschaffen werden.

In Bezug auf die Frage nach dem richtigen Umgang mit vorhandenen Beweismitteln ist die bestehende Rechtslage darzustellen. Zur Bewertung der Beweismittel stellt sich die Frage nach Anhaltspunkten für das Vertrauen in gesicherte und ungesicherte digitale Beweismittel sowie nach dem bisherigen tatsächlichen Vorgehen der Rechtsprechung. Hinsichtlich der Erzeugung sicherer Beweismitteln sind die zur Verfügung stehenden Sicherungsmittel zu untersuchen. Aus rechtlicher Sicht gilt es herauszuarbeiten, woran die Bildung von Anscheinsbeweisen oder ein regelmäßig hoher Beweiswert anknüpfen können.

3 Bestehende Rechtsregeln

Für die bestehende Rechtslage zu digitalen Beweismitteln ist zum einen die Beweisregel des § 371a Abs. 1 ZPO, die Rolle der Signaturgesetzgebung und die Einführung des Begriffs des elektronischen Dokuments relevant, zum anderen die Einordnung digitaler Beweismittel in die prozessrechtlichen Kategorien von Beweismitteln.

3.1 Elektronische Dokumente und § 371a ZPO

Der Begriff des elektronischen Dokuments ist mit dem Formanpassungsgesetz in die Zivilprozessordnung und zahlreiche weitere Gesetze eingeführt worden. Er wird durch das Gesetz nicht weiter definiert. Es hat sich jedoch ein weites Verständnis durchgesetzt, so dass nicht nur Textdokumente sondern sämtliche Medieninhalte in einem elektronischen Dokument enthalten sein können.[9] Aus dem Zusammenhang von §§ 130a, 130b, 298, 298a, 371a ZPO und auch den weiteren durch das Formanpassungsgesetz geänderten Gesetzen, vor allem den §§ 126, 126a, 126b BGB, wird zwar klar, dass sich der Gesetzgeber beim Prägen des Begriffs elektronisches Dokument vordringlich mit Textdokumenten beschäftigt hat. § 298a Abs. 2 Satz 1 ZPO, der die Führung elektronischer Prozessakten und die Übertragung von Papierdokumenten regelt, spricht mit der Erwähnung von „in Papierform eingereichten Schriftstücken und sonstige[n] Unterlagen“ aber dafür, dass der Gesetzgeber das breitere Inhaltsspektrum durchaus gesehen hat und von dem Begriff nicht ausschließen wollte.

Mit § 371a Abs. 1 ZPO wird die Beweiskraft elektronischer Dokumente durch einen Anscheinsbeweis geregelt, wenn diese mit einer gültigen qualifizierten elektronischen Signatur versehen sind. Ein Anscheinsbeweis beruht auf der Annahme eines Erfahrungssatzes, der besagt, dass beim Vorliegen eines bestimmten Sachverhaltes mit hoher Wahrscheinlichkeit eine bestimmte Wirkung eintritt. Das Vorliegen dieses

[9] [MK08, Zimmermann, § 371 Rn. 8]; [Be05, 1017]; [Fi06, 55]; mit weiteren Nachweisen [Be06, 76 ff.]; entgegen verschiedener Darstellungen lässt sich der Begründung des Regierungsentwurfs des Formanpassungsgesetzes, das § 371 Abs. 1 Satz 2 ZPO eingefügt hat, keine Stellungnahme hierzu entnehmen, BT-Drs. 14/4987.

Sachverhaltes genügt dem Gericht zur Überzeugungsbildung über den erfahrungsgemäß typischen Geschehensablauf, so dass dieser von der an sich beweisbelasteten Partei nicht weiter unter Beweis gestellt werden muss. Ursprung eines Erfahrungssatzes kann die allgemeine Lebenserfahrung, wissenschaftliche Forschung oder, wie hier, eine gesetzliche Anordnung sein.[10] Im Fall des § 371a Abs. 1 Satz 2 ZPO regelt das Gesetz selbst, dass zur Erschütterung des Anscheins das Vorbringen von Tatsachen erforderlich ist, die ernstliche Zweifel an der Authentizität der Erklärung begründen. Der Anscheinsbeweis des § 371a Abs. ZPO bezieht sich auf die Integrität und Authentizität elektronischer Erklärungen.[11] Über § 371a ZPO werden die Regeln über die Beweiskraft von Urkunden entsprechend angewandt. Auf andere Inhalte elektronischer Dokumente findet der Anscheinsbeweis keine Anwendung. Aus diesem Grund ergibt sich aus rechtlicher Sicht zunächst eine Zweiteilung digitaler Beweismittel: zum einen qualifiziert signierte elektronische Dokumente mit Erklärungsinhalt, die der Beweisregel des § 371a ZPO unterfallen, zum anderen elektronische Dokumente ohne Erklärungsinhalt und weitere digitale Beweismittel, die dieser nicht unterfallen.

Die Grundlage für § 371a ZPO bildet das Signaturgesetz. Das Signaturgesetz ist bislang die einzige rechtliche Infrastrukturregelung für Sicherungsmittel digitaler Beweismittel. Weitere Regelungen, wenn auch weniger grundlegend, sind in Vorbereitung, etwa das Bürgerportalgesetz mit einer Infrastruktur für den sicheren E-Mail Verkehr und den elektronischen Zugangsbeweis.[12] Durch die Einführung des elektronischen Personalausweises[13] könnten die vorhandenen Strukturen außerdem gestärkt und um den elektronischen Identitätsnachweis erweitert werden.

3.2 Beweiswert qualifiziert signierter elektronischer Dokumente ohne Erklärungsinhalt

Bislang ungeklärt ist die Frage, welcher Beweiswert qualifiziert elektronisch signierten Dokumenten zukommt, die keine Erklärung enthalten. Technisch gesehen ist die qualifizierte Signatur geeignet, um nachzuweisen, dass der Dokumenteninhalt ab der Signierung nicht mehr verändert wurde und dass die Signatur mit dem Schlüssel einer bestimmten Person erstellt wurden. Da es bei Erklärungen nicht auf den Prozess des Verfassens ankommt sondern darauf, dass sich der Erklärende die Erklärung durch seine Unterschrift zueigen macht, erfüllt die qualifizierte elektronische Signatur hier vollständig die Anforderungen. Rechtlich wird dies unterstützt, indem nach § 371a Abs. 1 Satz 2 ZPO der Anschein der Echtheit von privaten Erklärungen durch eine einfache Signaturprüfung begründet wird.[14] Da diese Regelung jedoch nur für Erklärungen gilt, hat der Beweisführer jenseits dessen im Bestreitensfall voll zu beweisen, dass die Voraussetzungen des Signaturgesetzes für das Vorliegen einer qualifizierten Signatur erfüllt sind. Bezüglich der technisch-organisatorischen Voraussetzungen an den

---

[10] Hierzu ausführlich [Sc94, 85 ff.].
[11] Eine genaue Analyse der Vorschrift findet sich bei [RF06].
[12] Zu dem Bürgerportalvorhaben s. http://www.buergerportale.de.
[13] Siehe hierzu [RH09].
[14] [Ro08, 25].

Zertifizierungsdiensteanbieter wird ihm das nur bei akkreditierten, also vorab geprüften Anbietern dank der Sicherheitsvermutung des § 15 Abs. 1 S. 4 SigG möglich sein.[15] Liegen diese Voraussetzungen jedoch vor oder können sie angenommen werden, so dürfte bezüglich der Annahme der Unverfälschtheit bei erfolgreicher Dokumentprüfung die Grundlage für einen richterrechtlichen Anscheinsbeweis gelegt sein.[16] Der Erfahrungssatz hierfür wäre wissenschaftlicher Natur und würde auf der Aussage beruhen, dass das verwendete Verfahren zur Bildung eines Hashwertes und sie anschließende Verschlüsselung ein unbemerktes Verändern des Dokuments sicher verhindern. Die Frage, ob die Zuordnung des Schlüssels zuverlässig, ob die alleinige Verfügungsgewalt des Schlüsselinhabers gewahrt ist oder ob die verwendeten technischen Komponenten sicher waren, spielt für die Annahme der Integrität des Dokuments ab der Signierung keine Rolle.

Da sich bislang sämtliche in Deutschland auftretenden Zertifizierungsdiensteanbieter freiwillig der Anbieterakkreditierung unterzogen haben, kommt qualifiziert elektronisch signierten elektronischen Dokumenten auch ohne Erklärungsinhalt soweit ein hoher Beweiswert zu.[17] Abgesehen von der Anwendbarkeit gesetzlicher Beweisregeln bestehen zwischen Erklärungen und anderen Inhalten jedoch weitere grundsätzliche Unterschiede. Bei sonstigen Inhalten geht es regelmäßig nicht um die Zurechnung zu einer Person, der Beweisgegenstand ist ein anderer. Die meisten sonstigen Inhalte wie Fotos, Filme, Audioaufzeichnungen, Protokolldateien oder Messergebnisse sollen direkt bestimmte Vorgänge oder Zustände beweisen. Damit wird die Manipulationsfreiheit einschließlich des Entstehungsprozesses des Inhalts relevant. Durch die qualifizierte Signatur alleine besteht hierüber keine nachweisbare Sicherheit, da sie durch den Signaturschlüsselinhaber regelmäßig erst nach der Dateifertigstellung erfolgt. Der Zeitraum der Herstellung bis zur Signierung ist damit nicht abgedeckt. Da die Zeitangabe der qualifizierten elektronischen Signatur auf der Systemzeit beruht, besteht aus der Signatur selbst heraus kein sicherer Nachweis über die Dauer der Sicherungslücke. Es besteht allerdings die Möglichkeit, sich eines qualifizierten Zeitstempels nach § 2 Nr. 14 SigG zu bedienen. Hier wird sicher mittels einer qualifizierten elektronischen Signatur bestätigt, dass die fraglichen Daten dem Anbieter des Zeitstempeldienstes zu einem bestimmten Zeitpunkt vorgelegen haben. Die Lücke zu dem unter Umständen unklaren Erstellungszeitpunkt schließt jedoch auch dies nicht in jedem Fall. Im Streitfall ist daher der Beweiswert von weiteren Beweismitteln, etwa weiteren gleichartigen Aufzeichnungen über den gleichen Inhalt, Zeugen des Entstehungsvorgangs und der Signierung oder ähnlichen Nachweisen abhängig. Hierdurch wird der hohe Beweiswert durch die Signierung abgeschwächt. Stehen keine weiteren Beweismittel, etwa Zeugen des Erstellungs- und Signierungsprozesses oder Zeugen des zu beweisenden Ereignisses, zur Verfügung und kann die Manipulationsmöglichkeit nicht anderweitig ausgeschlossen oder als unwahrscheinlich verworfen werden, so kann sich der an sich hohe Beweiswert der qualifizierten elektronischen Signatur bei entsprechendem Vortrag des Beweisgegners bei

---

[15] [Ro06, 807].
[16] Zum Erreichen eines Anscheinsbeweises mit Blick auf Photos [Kn08]; zur Anwendbarkeit eines Anscheinsbeweises [Wa77, 280, 283 ff.].
[17] So im Ergebnis wohl auch [MK08, Zimmermann § 371 Rn. 12].

Nichterklärungen als weitgehend wertlos erweisen. Ist das Dokument oder der digitale Inhalt gänzlich unsigniert und ungesichert, so gilt sein Beweiswert in der Regel als sehr gering.

3.3 Digitale Beweismittel und prozessrechtliche Beweisarten

Das Prozessrecht regelt nur bestimmte Beweisarten. Grundsätzlich kennt das Prozessrecht den Zeugenbeweis, den Augenschein, den Urkundenbeweis, den Sachverständigenbeweis und die Parteivernehmung. An die Beweisarten knüpfen bestimmte, nach der Prozessart teilweise differierende, Verfahrensregeln für die jeweilige Beweisführung an, etwa die Auswahl von Sachverständigen oder Regeln zur Rechtsstellung von Zeugen. Da für Urkunden die Verkörperung ein Definitionsmerkmal darstellt und der Zeugenbeweis genau wie die Parteivernahme gänzlich anders geartet ist, bleiben lediglich der Augenschein und der Sachverständigenbeweis für digitale Beweismittel. Der Gesetzgeber hat in § 371 Abs. 1 Satz 2 ZPO eine gesetzliche Zuordnung elektronischer Dokumente zum Augenscheinsbeweis vorgenommen. Außerhalb des Zivilprozesses wird teilweise auf die Zivilprozessordnung ergänzend verwiesen, etwa in § 173 VwGO und spezieller in § 98 VwGO. Da die Verwaltungsgerichtsordnung in § 96 Abs. VwGO lediglich die Beweisarten aufzählt, kommt die Zuordnung der Zivilprozessordnung hier ebenfalls zur Anwendung. Die Strafprozessordnung regelt den Augenschein in § 86 StPO, nimmt auf elektronische Dokumente jedoch keinen Bezug. Dennoch stellt auch hier die Würdigung digitaler Beweismittel zunächst eine in Augenscheinnahme dar.[18]

3.3.1 Augenschein

Trotz der gesetzlichen Festlegung ist der Anscheinsbeweis für digitale Beweismittel nicht frei von Problemen. Digitale Beweismittel können nicht unmittelbar wahrgenommen werden und ihre Vermittlung unterscheidet sich von der Vermittlung durch analoge Wiedergabegeräte wie Schallplattengeräten, Videorecordern oder Diaprojektoren noch einmal erheblich, da neben der Hardware bei digitalen Beweismitteln auch Software zu deren Darstellung eingesetzt werden muss. Rein praktisch ergibt sich das Problem, dass das Gericht über die technischen Mittel verfügen muss, die digitalen Inhalte anzuzeigen.[19] Angesichts der Vielzahl von Formaten und der Bindung von proprietären Formaten an bestimmte Anzeigeprogramme kann das Gericht dies aus eigenen Mitteln praktisch nur für gemeingängige Dateiarten und Inhalte gewährleisten. Handelt es sich nicht um solche, sind entweder Umwandlungen erforderlich, die allerdings die Prüfbarkeit beeinflussen können, oder es sind Mittel des Beweisführers oder Dritter zu nutzen, über deren Funktionsweise sich das Gericht unter

[18] [Ka08, § 86 StPO Rn. 6]
[19] [Fi06, 80].

Umständen kein Bild machen kann. Die notwendige Überzeugungsbildung über die Hilfstatsachen der Unverfälschtheit und Echtheit[20] wird so erschwert.

Mittelbare Augenscheineinnahmen sind nicht ungewöhnlich, der Augenschein kann durch andere Richter eingenommen werden (§ 375 ZPO), durch Sachverständige ergänzt werden (§ 372 ZPO) oder durch Wiedergabegeräte vermittelt werden.[21] Findet eine solche Mittelung statt, muss sich das Gericht aber der ordnungsgemäßen Vermittlung sicher sein. Bei der Beauftragung eines fremden Gerichts oder der Hinzuziehung eines Sachverständigen handelt es sich um vereidigte Personen, die besonderes Vertrauen genießen. Bei analogen Wiedergabegeräten kann die Verlässlichkeit durch das Abspielen anderer Medien geprüft werden. Bei der Verwendung von Hard- und Software besteht diese Vertrauensgrundlage nicht in gleichem Maß und die Prüfung gestaltet sich nicht so einfach. Beweismittel können verdeckten Code enthalten, der Fehler oder bestimmte Eigenschaften gängiger Wiedergabesoftware ausnutzt und so andere Inhalte anzeigt.[22] Dem kann durch die vergleichende Verwendung verschiedener Softwareprodukte begegnet werden, doch hierzu fehlen Verhaltensrichtlinien oder –hilfen für die Gerichte. Kann zur Wiedergabe nur fremde Hard- und Software genutzt werden, besteht noch weniger Kontrolle. Damit das Gericht sich auch bei dieser Form des Augenscheins seiner Wahrnehmung sicher sein kann, sind Maßnahmen erforderlich, um die Sicherheit des Geräts und die Funktionsfähigkeit und Manipulationsfreiheit seiner Software sicherzustellen. Dies gilt umso mehr, wenn die Mittel zur Wahrnehmung von Dritten gestellt werden.

3.3.2 Sachverständigenbeweis

Da das Gericht sich häufig nicht in der Lage sehen wird, die Frage der Manipulationsfreiheit oder der ordnungsgemäßen Darstellung selber zu lösen, kommt als zweite einschlägige Beweisart das Hinzuziehen von Sachverständigen in Betracht (§§ 402 ff. ZPO, §§ 72 ff. StPO). Das Gericht entscheidet über die Erforderlichkeit in freiem Ermessen (§ 286 ZPO).[23] Der Sachverständige begutachtet das Beweismittel und teilt dem Gericht sein Ergebnis und dessen Begründung sowie seine Erläuterungen mit. Das Gericht entscheidet über das Begutachtungsergebnis in freier Beweiswürdigung, d.h. es ist nicht an das Gutachtenergebnis gebunden. Es hat allerdings sein Ergebnis in Auseinandersetzung mit dem Gutachten zu begründen. Auch der Sachverständigenbeweis hat jedoch auf Dauer gesehen Schwächen im Umgang mit digitalen Beweismitteln, die mit Blick auf die künftige Entwicklung zu berücksichtigen sind.

Auch Sachverständige werden zur Beantwortung ihrer Prüfungsaufgaben zunehmend fremde Software einsetzen, sowohl zur Anzeige der Daten als auch zur Untersuchung der Unverfälschtheit und Echtheit. Desto mehr sich das Gutachtenergebnis auf solche

---

[20] [MK08, Zimmermann § 371 Rn.5].
[21] [Mu08, Huber § 371 Rn. 4 ff.].
[22] Mit Beispielen, auch zu nicht erklärungsbezogenen Präsentationsproblemen, [Po03, 54 ff.].
[23] [Ba07, Hartmann, Übers. § 402 Rn. 13].

Software stützt, kommt der Frage, wie die Zuverlässigkeit dieser Software im Rahmen des Gutachtens nachgewiesen wird, Bedeutung zu. Bezüglich der Begutachtung von Digitalphotos wird der Sachverständige bspw. viel aus einer genauen Betrachtung der Wiedergabe ableiten können. Zusätzlich kann er sich aber auch softwarebasierter Detektionsmethoden bedienen.[24] Diese können Hinweise auf Bearbeitungen liefern. Um jedoch die Ergebnisse solcher Untersuchungen zu würdigen, gerade auch wenn sie negativ ausfallen, bedarf es einer zuverlässigen Einschätzung der Leistungsfähigkeit der Software. Über diese aufzuklären, mögliche Fehlerursachen zu erläutern und das Ergebnis zu interpretieren, ist zum einen Aufgabe des Sachverständigen. Solange hier die visuelle Begutachtung im Vordergrund steht, reichen diese Ausführungen aus.

Umso mehr jedoch die Ergebnisse automatisierter Prüfprozesse neben der Fachkompetenz des Sachverständigen in den Mittelpunkt der Untersuchung rückt, desto bedeutsamer wird die Zuverlässigkeit oder die Einschätzung der Software für die Beweiswürdigung. Bei dem Sachverständigen wird die Vertrauenswürdigkeit durch die Vereidigung und den Nachweis der fachlichen Befähigung sichergestellt. Es ist zwar einerseits Teil der Pflichten des Sachverständigen, sich nachweisbar zuverlässiger Mittel zu bedienen, andererseits darf aber auch aus Sicht des würdigenden Gerichts die Prüfung der Software nicht hinter der Prüfung des Sachverständigen selbst zurückbleiben, wenn ihr Einfluss praktisch das Gutachtenergebnis bestimmt. Mit dem Aufkommen digitaler Beweismittel und automatischer Prüfmethoden wird also künftig auch eine objektive, vertrauenswürdige Prüfung der Prüfmethoden und –software benötigt. Soweit es sich bei dem digitalen Beweismittel um das Untersuchungsergebnis zu einem Systemzustand, also bspw. die Untersuchung eines Festplatteninhaltes, handelt, wird von vornherein nur die Einführung über den Sachverständigenbeweis in Frage kommen.

Da der Sachverständigenbeweis regelmäßig hohe Kosten erzeugt, hat seine häufige Erforderlichkeit erhebliche praktische Auswirkungen. Gerade im Bereich des Zivilprozesses kann die Erforderlichkeit der Begutachtung beispielsweise das Prozessrisiko soweit steigern, dass die beweisführende Partei trotz berechtigtem Anlass von der Prozessführung Abstand nimmt. Insgesamt könnte die Zunahme digitaler Beweismittel zu einer erheblichen Verteuerung der Prozesse führen, wenn immer wieder Sachverständige beigezogen werden müssen. Beides ist nicht ohne Folgen für die Rechtsschutzgewährung und hat damit sogar einen grundrechtlichen Bezug. Soweit durch technische Gestaltung eine zu erwartende massenhafte Erforderlichkeit der Sachverständigenbeiziehung vermieden werden kann, sollte dies geschehen.

4 Praxis

Die qualifizierte elektronische Signatur ist derzeit noch nicht sehr verbreitet. Digitale Beweismittel werden daher überwiegend ohne oder nur mit lückenhaften Sicherungsmitteln vorgelegt. Empirische oder statistische Untersuchungen über die Verwendung und Wertung dieser Beweise existieren nicht, auch lassen sich nur wenige

[24] [Gl07]; [PoFa]; [Ki06]; [La08].

einschlägige Urteile finden, die sich eingehend mit den Problemen der Würdigung digitaler Beweismittel auseinandersetzen. Im Rahmen einer Simulationsstudie wurde die Erfahrung gemacht, dass das Abstellen auf die technischen Eigenschaften digitaler Beweismittel gerne vermieden wird, solange weitere Beweismittel, etwa Zeugen, oder Indizien wie vorhandenes technisches Wissen des potentiellen Manipulators oder die Einschätzung des Fälschungsinteresses zur Verfügung stehen und eine Bestätigung oder Widerlegung ermöglichen.[25] Seitens der berufsmäßig mit der Erzeugung von Beweismitteln befassten Personengruppen wird regelmäßig zwar die Erforderlichkeit der Dokumentation der Beweiserzeugung gefordert, ansonsten aber die Notwendigkeit des Vertrauens in den Ersteller betont.[26]

Das bestehende Prozessrecht kann mit digitalen Beweismitteln umgehen, es trägt den Besonderheiten jedoch wenig Rechnung. Vielfach wird es zu einer Verlagerung auf Sachverständige kommen, wenn Gerichte sich des Umgangs mit digitalen Beweismitteln nicht sicher sind. Verlässt sich das Gericht auf sein eigenes technisches Wissen im Rahmen der Allgemein- oder Gerichtskundigkeit, besteht schnell die Gefahr, dass digitale Beweismittel in ihrem Wert verkannt, nicht voll ausgeschöpft oder sogar als für den angestrebten Beweis nicht geeignet abgelehnt werden.[27] Eine vertrauenswürdige Prüf- und Sicherungsinfrastruktur durch Standardisierung und Zertifizierung von Sicherungsmitteln und Prüfsoftware zu schaffen würde hier zu einer verbesserten Rechtssicherheit und Effizienz beitragen.

5 Anhaltspunkte zur Beweiswertermittlung

Die Ausführungen zum Beweiswert signierter elektronischer Dokumente ohne Erklärungsinhalt und der geringe Beweiswert gänzlich ungesicherter digitaler Beweismittel geben Anlass, sich eingehender mit den Voraussetzungen eines hohen Beweiswertes von digitalen Beweismitteln und mit den Anhaltspunkten, anhand derer im Streitfall einem digitalen Beweismittel vertraut wird, auseinanderzusetzen. Letztlich muss das Gericht entscheiden, ob das Beweismittel eine sichere Erkenntnis über den Sachverhalt vermittelt.

5.1 Integrität und Authentizität

An erster Stelle steht hierbei die Integrität der digitalen Daten. Nur wenn diese mit überwiegender Wahrscheinlichkeit nicht manipuliert sind, können sie als Beweis für einen bestimmten Sachverhaltsbestandteil dienen. Zur Integrität gehört auch die Vollständigkeit der digitalen Daten. Die Authentizität, also die sichere Zuordnung einer Datei zu einer bestimmten Person oder Quelle als Ursprung, ist ebenfalls häufig entscheidender Bestandteil einer digitalen Beweisführung. Handelt es sich nicht um

[25] [Ro09, 220].
[26] [Gu04, 582].
[27] Ein Beispiel mit zutreffendem Ergebnis aber eigenwilliger technischer Bewertung s. LG München mit Anmerkung MMR 08, 622.

Erklärungen wird häufig die unverfälschte Zuordnung der Daten zu einer bestimmten Erstellungssoftware oder zu einem bestimmten Gerät von Bedeutung sein.

5.2 Erstellungszeitpunkt, -dokumentation und Dateihistorie

Weitere Bestandteile oder Elemente für die Würdigung ergeben sich jeweils aus dem Beweisgegenstand. Der Zeitpunkt der Dateierstellung oder einer Aufzeichnung wird häufig eine Rolle spielen oder die Nachvollziehbarkeit von Veränderungen einer Datei, also ihre Historie. In diesem Fall müssen wiederum auch diese Angaben zuverlässig sein. Gerade wenn das digitale Beweismittel, beispielsweise ein Photo, ein bestimmtes Ereignis beweisen soll, kommt der Frage, ob das Photo auch zum Zeitpunkt des fraglichen Ereignisses aufgenommen wurde, eine hohe Bedeutung zu. Für die Würdigung des Beweismittels können auch die Umstände seiner Entstehung bedeutsam sein, etwa wenn ein Digitalphoto in eine Serie von Photos eingeordnet werden soll oder wenn das digitale Beweismittel ein Untersuchungsergebnis darstellt.

5.3 Informationen über die Datenquelle

In Bezug auf Protokolle oder Systemzustände wird die Störungsfreiheit und Unbeeinflussbarkeit des aufzeichnenden Systems oder der Mittel zur Zustandsfeststellung eine wichtige Rolle spielen, also die Nachvollziehbarkeit des Entstehungsprozesses des Beweismittels. Zur Beurteilung des Wertes der inhaltlichen Aussage muss Sicherheit darüber bestehen, wie die Aufzeichnung entstanden ist, ob das aufzeichnende System fehlerfrei gearbeitet hat und ob unbemerkte Eingriffe in den Aufzeichnungsvorgang möglich waren. Am zuverlässigsten wird ein Entstehungsprozess dann sein, wenn er gegen Einflussnahmen abgesichert ist, der Inhalt eindeutig auf ihn zurückzuführen ist und seine Funktionstüchtigkeit sicher festgestellt werden kann. Ist die Funktionstüchtigkeit vorab überprüft und bestätigt, stellt dies eine beträchtliche Hilfe bei der Würdigung dar. Dabei muss auch klar sein, wie das Erstellungssystem überhaupt funktioniert, um die entstandenen Daten würdigen zu können. Handelt es sich beispielsweise um ein System zur Erfassung von Raumzutritten und soll bewiesen werden, wer sich wann in dem Raum aufgehalten hat, wäre es von entscheidender Bedeutung zu wissen, ob das System alle Eingänge abdeckt.

Diese Elemente müssen bei einem digitalen Beweismittel je nach Bedarf feststellbar und prüfbar sein. An dem Grad der Sicherheit, mit dem diese Feststellungen erfolgen können, bemisst sich der Beweiswert des Beweismittels, also seine Eignung die Überzeugung des Gerichts zu beeinflussen.[28] Im Nachhinein, ohne Sicherungsmittel als Anhaltspunkte werden diese Feststellungen kaum zu treffen und der Beweiswert regelmäßig niedrig sein.

6 Rolle der digitalen Forensik

[28] [Mu84, Rn. 42].

Die Entwicklung forensischer Hilfsmittel mit Bezug zur Beweisführung hat sich bislang stärker auf die Sicherstellung und das Finden von Beweisen bei der Untersuchung von IT-Geräten konzentriert.[29] Der Bedarf geht aber weiter, denn digitale Beweismittel können auch, wie hier thematisiert, isolierte Dateien sein, deren Eigenschaften unabhängig von der Untersuchung bestimmter Geräte zu würdigen sind. Sofern nachträgliche Untersuchungen immerhin das Fehlen möglicher Veränderungsspuren feststellen können, schaffen sie bereits einen Anhaltspunkt für die Wertung. Selbst bei Textdokumenten werden häufig Metadaten stimmig zu ändern oder wenigstens zu entfernen sein. Unter Umständen kann das Gericht bei entsprechender Ausstattung und Anleitung eine Reihe von Veränderungsspuren eigenständig prüfen. Forensische Software, die für bestimmte Inhalte Veränderungsspuren feststellen kann, könnte in Verbindung mit bestimmten Prüfroutinen, die die erkennenden Gerichte bei der Würdigung bestimmter digitaler Beweismittel anleiten, hilfreich sein. Diese Software für die Gerichte eigenständig verwendbar und auswertbar zu gestalten, stellt jedoch eine große Herausforderung dar. Fehlen standardmäßig prüfbare und für das jeweilige digitale Beweismittel typische Manipulationshinweise deutet dies immerhin darauf hin, dass eine gewisse Kundigkeit und ein gewisser Aufwand notwendig waren, sollte es sich um ein manipuliertes Beweismittel handeln. Dies gilt allerdings nur solange nicht gleichzeitig Software existiert, die Veränderungen unter Vermeidung solcher Spuren für den Laien handhabbar automatisiert. Kann der zur Veränderung und ihrer „Tarnung“ erforderliche Aufwand anhand weiterer Informationen ausgeschlossen werden, können auch nachträgliche Untersuchungsmethoden ein Beweismittel aufwerten, selbst wenn der vollständige Nachweis der Manipulationsfreiheit regelmäßig nicht möglich sein wird. Würden Gerichte in die Lage versetzt, routinemäßig bestimmte Prüfungen an vorgelegten Beweismitteln vorzunehmen, würde dies der Rechtssicherheit zu Gute kommen. Die Rolle multimedialer digitaler Forensik ist also nicht zu unterschätzen.

7 Ansätze zur Erzeugung sicherer digitaler Beweismittel

Die Anhaltspunkte zur Bewertung eines digitalen Beweismittels führen direkt zu der zweiten Perspektive bei der Betrachtung. Um von vornherein sichere Beweismittel zu schaffen, müssen diese Anhaltspunkte durch technische Sicherungsmittel abgesichert werden.

Das derzeit wichtigste Mittel zur Herstellung von Beweissicherheit bei digitalen Beweismitteln ist, wie bereits rechtliche dargestellt, die qualifizierte elektronische Signatur (§ 2 Nr. 2 SigG). In engem Zusammenhang steht die Verwendung von qualifizierten Zeitstempeln i.S.v. § 2 Nr. 14 SigG. Bei der Einführung der heutigen Rechtslage ist deutlich geworden, dass weder die qualifizierte Signatur noch ein qualifizierter Zeitstempel alleine das Führen eines sicheren Beweises mit elektronischen Dokumenten oder Daten ohne Erklärungsinhalt ermöglichen. Ein Beispiel ist die Herstellung einer Filmaufnahme oder von Fotos. Die Signierung kann erst am Ende der

[29] Siehe hierzu [WH07]; hierzu sind eine Reihe von Werkzeugen wie EnCase, FTK oder Forensic Browser verfügbar.

Aufnahme erfolgen. Erfolgt sie zudem etwa nach der Übertragung des Films in ein anderes System als der Kamera für den Signiervorgang, so schließt diese Signatur Verfälschungen, das Unterschieben von Aufnahmen anderer Quellen und ähnliches für den Zeitpunkt vor ihrer Vornahme nicht aus. Aussagen hierüber können zunächst nur über andere Quellen gewonnen werden. Um diese Lücke zu schließen, muss die Signatur also für sonstige Inhalte um weitere Sicherungen ergänzt und mit diesen verbunden werden.

Eine Möglichkeit hierzu liegt in der Zertifizierung manipulationssicherer Systeme, die eine Signatur erzeugen, die das zertifizierte System als Quelle ausweist und damit die Lücke schließt. Rechtlich gesehen handelt es sich bei der so erzeugten Signatur zwar nur um eine fortgeschrittene Signatur, da der Signaturschlüssel keiner Person zugeordnet ist. Umfasst die Zertifizierung aber auch den integrierten Signierungsprozess und orientiert sich dieser an den Anforderungen des Signaturgesetzes, so wäre eine Infrastruktur geschaffen, die eine Grundlage für einen Anscheinsbeweis schaffen würde. Dieser kann durch Richterrecht entstehen, was den Nachteil einer langen Unsicherheitsphase mit sich bringt, bis die Rechtsprechung den Anscheinsbeweis vollständig anerkannt hat. Der Anscheinsbeweis kann aber auch dem Beispiel des § 371a ZPO folgend durch gesetzliche Rechtsanpassung geschaffen werden.

Auch unabhängig von der Signaturverwendung lässt sich ein hoher Beweiswert erzielen, wenn das Beweismittel durch ein vorab zertifiziertes System erzeugt wurde. Das Zertifikat belegt, dass das erzeugende System nach nachvollziehbaren, vorgegebenen Standards auf seine Sicherheit geprüft worden ist. Je nach der Vertrauenswürdigkeit des Zertifikats kann dies die Voraussetzungen für einen Anscheinsbeweis schaffen. Ohne Signaturverwendung ist das Beweismittel an das sichere System gebunden und kann nur innerhalb des Systems gewürdigt werden. Das digitale Beweismittel ist damit nicht verkehrsfähig, was den technischen Prozess der Beweisführung erschwert.

Anknüpfungspunkt ist bei den bisher aufgezeigten Möglichkeiten jeweils die Erfüllung gesetzlich geregelter Sicherheitsanforderungen in Bezug auf die Signatur oder das Vorliegen einer Zertifizierung oder Akkreditierung der Sicherungsmaßnahme bzw. des Anbieters derselben. Gegenstand dieses Weges zur Beweissicherung sind Systeme, die wie eine Photokamera bestimmte Vorgänge oder Zustände aufzeichnen. Eine Akkreditierung oder Zertifizierung erfordert jedoch auch eine Festlegung der Zertifizierungs- oder Akkreditierungsmaßstäbe, wobei diese Maßstäbe gleichzeitig als rechtlich relevanter Anknüpfungspunkt geeignet sein müssen. Mit der Zertifizierung oder Akkreditierung wird ein Teil der sonst durch Sachverständige immer wieder vorzunehmenden Begutachtung vorgezogen und vorab durchgeführt. Auf die Ergebnisse dieser Prüfung kann eine spätere Beurteilung dann in einer Vielzahl von Anwendungsfällen des Beweismittels gestützt werden. Problematisch ist hierbei allerdings, dass die Kontrolle der Einhaltung der Akkreditierungs- oder Zertifizierungsmaßstäbe auch nach der erfolgten Akkreditierung oder Zertifizierung überwacht werden muss, um Grundlage eines Anscheinsbeweises zu werden. Bei zertifizierten Systemen ist zudem sicherzustellen, dass die zertifizierten Eigenschaften nicht verändert werden können ohne dass dies die Funktionen des Systems beeinträchtigt.

Auch nicht zertifizierte oder standardisierte technische Maßnahmen, die bestimmte Eigenschaften des Beweismittels sicherzustellen geeignet sind, können zu einem hohen Beweiswert führen. Sicherungsmittel wie integritätssichernde oder zuordnende Wasserzeichen sind ein Beispiel für Sicherungsmittel, deren Zuverlässigkeit durch einen bestimmten Hersteller oder die verwendende Institution versprochen werden. Bei Bedarf ist hier eine Prüfung dieser Versprechungen erforderlich, um die Zuverlässigkeit im Nachhinein festzustellen. Eine weitere Form der Sicherung – vergleichbar der Erzeugung qualifizierter Zeitstempel – ist die Sicherung durch vertrauenswürdige Dritte. Das Beweismittel wird Dritten vorgelegt, die die Integrität oder weitere Eigenschaften bestätigen. Die Abwicklung eines Geschäfts über einen unabhängigen Dritten, der die Erklärungen und den Ablauf dokumentiert, wäre ein Beispiel. Handlungsabläufe im elektronischen Rechtsverkehr können so gut nachweisbar gemacht werden.

8 Zusammenfassung

Hinsichtlich digitaler Beweismittel jenseits qualifiziert signierter elektronischer Dokumente mit Erklärungsinhalt besteht noch erheblicher Forschungs- und rechtlicher Handlungsbedarf. Alleine durch die steigende Verbreitung von Digitaltechnik wachsen auch die Möglichkeiten und der Bedarf, andere Inhalte als Erklärungen in digitaler Form als Beweismittel zu nutzen. Damit ergibt sich die Notwendigkeit, die für Erklärungen weitgehend vollzogene Entwicklung auch für andere Inhalte in Angriff zu nehmen. Solange zur Verfügung stehende Sicherungsmittel im Vorfeld von Streitigkeiten nur selten genutzt werden und für viele Inhalte noch keine ausreichenden Sicherungsmittel zur Verfügung stehen, kommt technischen Hilfsmitteln für Gerichte und Sachverständige eine erhebliche Bedeutung zu. Forensische Mittel und Verfahren können zu fundierteren und qualitativ besseren Entscheidungsgrundlagen beitragen. Langfristig sollten jedoch die bestehenden Sicherungsinfrastrukturen erweitert und verbreitet werden, um eine verbesserte Rechtssicherheit zu schaffen. Hierzu wird auch das Recht durch die Festlegung von Standards, Sicherheitsmaßstäben und Prüfverfahren beitragen müssen.

Literaturverzeichnis

[Ba99] Bach, W.: Das kriminalistische Potential neuer Technologien, Kriminalistik 1999, 657-672.

[Ba07] Baumbach, A.; Lauterbach, W.; Albers, J.; Hartmann, P.: Zivilprozessordnung, C.H. Beck Verlag, 65. Aufl. München 2007.

[Be05] Berger, C.: Beweisführung mit elektronischen Dokumenten, NJW (Neue juristische Wochenschrift) 2005, 1016-1020.

[Be06] Bergfelder, M.: Der Beweis im elektronischen Rechtsverkehr, Verlag Dr. Kovac, Hamburg 2006.

[Br96] Britz, J.: Urkundenbeweisrecht und Elektroniktechnologie, C.H. Beck Verlag München 1996.

[Dä01] Dästner, C.: Neue Formvorschriften im Prozessrecht, NJW 2001, 3469-3471.

[De07] Deussen, O.: Bildmanipulation – Wie Computer unsere Wirklichkeit verzerren, Spektrum Akademischer Verlag, Berlin 2007.

[Fi02] Fischer-Dieskau, S.; Gitter, R.; Paul, S.; Steidle, R.: Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR (Multimedia und Recht) 2002, 709-713.
[Fi03] Fischer-Dieskau, S.: Der Referentenentwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts, MMR 2003, 701.
[Fi09] Fischer-Dieskau, S.: Das elektronisch signierte Dokument als Mittel zur Beweissicherung, Nomos Verlag, Baden-Baden 2006.
[Gl07] Gloe, T.; Kirchner, M.; Winkler, A.; Böhme, R.: Can we trust Digital Image Forensics?, Proc. of ACM Miltimedia, 2007.
[Gu04] Guggenbühl, H.: Einsatz und Verwertbarkeit multimedialer Bildaufzeichnungen im Strafverfahren, Kriminalistik 2004, 578-582.
[Ja05] Jähne, B.: Digitale Bildverarbeitung, Springer Verlag, 6.Aufl. Berlin 2005
[Ka08] Karlsruher Kommentar zur StPO, C.H. Beck Verlag, 6. Aufl. München 2008.
[Ki06] Kirchner, M.: Digitale Forensik – Spuren in Digitalfotos, abrufbar unter http://events.ccc.de/congress/2006/Fahrplan/attachments/1117-23C3_Kirchner.pdf.
[Kn08] Knopp, M.: Digitalfotos als Beweismittel, ZRP (Zeitschrift für Rechtspolitik) 2008, 156-159.
[Mu84] Musielak, H.-J.; Stadler, M.: Grundfragen des Beweisrechts, C.H. Beck Verlag, München 1984.
[Mu08] Musielak, H.-J. (Hrsg.): ZPO, C.H.Beck Verlag, 6. Aufl. München 2008.
[MK08] Münchner Kommentar zum Zivilprozessrecht, C.H. Beck Verlag, 3. Aufl. München 2008.
[PoFa] Popescu, A.; Farid, H.: Exposing Digital Forgeries by Detecting Traces of Resampling, abrufbar unter http://www.cs.dartmouth.edu/farid/publications/sp05.pdf.
[Po03] Pordesch, U.: Die elektronische Form und das Präsentationsproblem, Nomos Verlag, Baden-Baden 2003.
[RH09] Roßnagel, A.; Hornung, G.: Ein Ausweis für das Internet, DÖV (Die öffentliche Verwaltung) 2009, 301-306.
[Ro98] Roßnagel, A.: Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, 3312-3320.
[Ro01] Roßnagel, A.: Das neue Recht elektronischer Signaturen – Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO, NJW 2001, 1817-1826.
[RF06] Roßnagel, A.; Fischer-Dieskau, S.: Elektronische Dokumente als Beweismittel – Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz, NJW 2006, 806-808.
[Ro08] Roßnagel, A.: Fremderzeugung von qualifizierten Signaturen? – Ein neues Geschäftsmodell und seine Rechtsfolgen, MMR 2008, 22-28.
[Ro09] Roßnagel, A.; Schmidt, A.U.; Wilke, D. (Hrsg.): Rechtssichere Transformation signierter Dokumente, Nomos Verlag, Baden-Baden 2009.
[RP03] Roßnagel, A.; Pfitzmann, A.: Der Beweiswert von E-Mail, NJW 2003, 1209-1214.
[RW06] Roßnagel, A.; Wilke, D.: Die rechtliche Bedeutung gescannter Dokumente, NJW 2006, 2145-2150.
[Sc94] Schneider, E.: Beweis und Beweiswürdigung, Verlag Franz Vahlen, 5. Aufl. München 1994.
[Tr08] Trinkwalder, A.: Pixelsezierer – Digitale Bildforensik: Algorithmus jagt Fälscher, c't 2008, 152-156.
[Tr08a] Trinkwalder, A.: Können diese Pixel lügen – Der schmale Grat zwischen Bildoptimierung und –fälschung, c't 2008, 148-151.
[Vi05] Viefhues, W.: Das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, NJW 2005, 1009-1016.
[Wa77] Walter, G.: Der Anwendungsbereich des Anscheinsbeweises, ZZP (Zeitschrift für Zivilprozess, 90. Band) 1977, 270-284.
[WH07] Willer, C.; Hoppen, P.: Computerforensik – Technische Möglichkeiten und Grenzen, CR (Computer und Recht) 2007, 610-616.