Steffen Kroschwald, Zina Al-Washash, Annalena Secci, Gunther Schiefer, Nadja Kruse, Meike Ullrich, Thomas Schuster

Gerichtsfeste Beweissicherung im Daten- und Verbraucherschutz

DLT-basierte Lösung mit Crowd-Verifikation

Die Verfolgung von Rechtsverstößen im Internet scheitert nicht selten an ihrem Nachweis. Die Autoren stellen das System EVIDENTT zur gerichtsfesten Beweissicherung solcher Verstöße vor, einer Kombination aus Distributed-Ledger-Technologie (DLT) und der verifizierenden Crowd-Absicherung des Verstoßes. Der Beitrag befasst sich im Kern mit der Frage, inwiefern das System eine zuverlässige, datenschutzfreundliche und vor allem gerichtsfeste Dokumentation von Rechtsverstößen im digitalen Raum unterstützen kann.

Prof. Dr. Steffen Kroschwald, LL.M.

lehrt europäisches und internationales Wirtschaftsrecht und ist Direktor des Instituts für Verbraucherforschung und nachhaltigen Konsum (vunk) an der Hochschule Pforzheim.
E-Mail:
steffen.kroschwald@hs-pforzheim.de

Prof. Dr. Thomas Schuster

ist Professor für Datenbanken und Software Technik an der Hochschule Pforzheim und leitet das futureLAB. Wissenschaftlicher Koordinator der Campus IT.
E-Mail:
thomas.schuster@hs-pforzheim.de

Zina Al-Washash, LL.M.

war bis Ende 2025 akademische Mitarbeiterin am Institut für Verbraucherforschung und nachhaltigen Konsum (vunk) an der Hochschule Pforzheim

E-Mail:
zina.al-washash@hs-pforzheim.de

Annalena Secci, LL.M.

ist wissenschaftliche Mitarbeiterin am Institut für Verbraucherforschung und nachhaltigen Konsum (vunk) an der Hochschule Pforzheim.

E-Mail:
annalena.secci@hs-pforzheim.de

1 Einleitung

1.1 Hintergrund und Motivation

Die Beweissicherung im digitalen Raum ist ein wichtiges Problemfeld des modernen Verbraucherschutzes, denn digitale Inhalte sind in hohem Maße flüchtig und manipulierbar. Ein klassisches Beispiel ist die Sicherung durch Screenshots, die auf den ersten Blick als einfache, schnell verfügbare und scheinbar zuverlässige Methode erscheint. Bei näherer Betrachtung zeigt sich jedoch, dass sie erhebliche Schwächen besitzt:

- Manipulationen können vor der Erstellung eines Screenshots erfolgen, indem der zugrunde liegende Quelltext einer Webseite verändert wird.
- Ebenso kann ein Screenshot selbst verändert werden, etwa durch nachträgliche Bildbearbeitung oder durch den Einsatz von KI-basierten Verfahren wie Deepfakes.
- Zusätzlich besteht ein Manipulationsrisiko in der Zeitspanne zwischen der Erstellung und der späteren Verwendung des Screenshots als Beweismittel, da in dieser Phase weder Integrität noch Authentizität zweifelsfrei gewährleistet werden können.

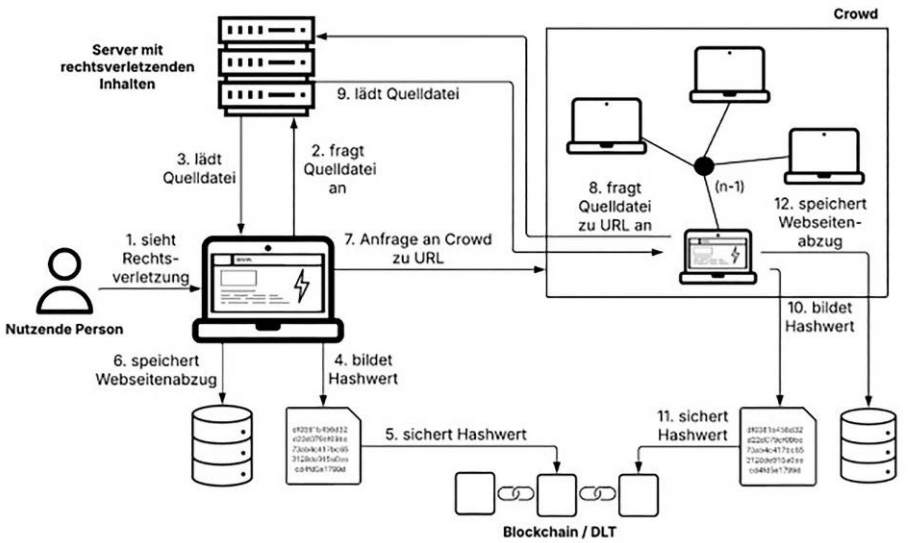
Rechtsprechung und wissenschaftliche Analysen bestätigen diese Einschätzung und weisen auf die geringe Beweiskraft von Screenshots hin.[1]

Im Rahmen der EVIDENTT-Studie[2] wurde die Machbarkeit einer technischen Lösung für eine zuverlässige und gerichtsfes-

1 BGH, Beschluss vom 10.10.2023 – XI ZB 1/23, Rn. 18; OLG Jena, Urt. v. 28.11.2018 – 2 U 524/17, Screenshot, GRUR-RR 2019, 238, Rn. 15; *Zimmermann*, in: MüKo ZPO, 7. A. 2025, § 371, Rn. 8; ausf. *Mankowski* in: Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG, Band 1, 3. A. 2016, S. 12, Rn. 320ff.; *Mankowski*, GRUR-Prax 2019, 123.

2 Machbarkeitsstudie „Einsatz verteilter Technologien zur beweissicheren Dokumentation von Verbraucherschutzverstößen auf Online-Plattformen" des

Abbildung 1 | Prozess der beweissicheren Erfassung und Speicherung von Webseitenabzügen



te Dokumentation von Rechtsverstößen im digitalen Raum untersucht, die sich diesen Herausforderungen stellt. In der Studie wurden ein Lösungsansatz interdisziplinär wissenschaftlich untersucht, ein Demonstrator technisch umgesetzt und praktische Umsetzungsszenarien technisch, wirtschaftlich und juristisch evaluiert.

1.2 Überblick über den Lösungsansatz

Die in EVIDENTT entwickelte Systemarchitektur besteht aus mehreren miteinander verzahnten Komponenten (Abb. 1).

Stellt eine nutzende Person im Internet mit ihrem Webbrowser eine mögliche Rechtsverletzung auf einer Webseite fest (1), kann direkt über ein Browser-Plugin oder über die Client-Anwendung die betreffende Quelldatei vom Quellserver abgerufen und lokal geladen werden (2, 3). Aus dieser Datei erzeugt die Client-Anwendung einen Webseitenabzug und berechnet einen kryptographischen Hashwert (4). Der berechnete Hashwert wird anschließend in einer Distributed-Ledger-Technologie (DLT) gesichert, zum Beispiel einer Blockchain (5), während der eigentliche Webseitenabzug auf einem Speicherserver abgelegt wird (6). Auf diese Weise sind sowohl die Nachvollziehbarkeit als auch die Überprüfbarkeit der Beweise sichergestellt.

Um den Beweiswert weiter zu erhöhen, startet die Client-Anwendung zusätzlich eine Anfrage an die Crowd (7). Mehrere Teilnehmende aus der Crowd rufen daraufhin die Quelldatei unabhängig voneinander erneut vom Quellserver ab (8, 9) und bilden jeweils eigene Webseitenabzüge, die gehasht (10) und in der DLT gesichert werden (11). Die von jedem Crowd-Teilnehmenden erzeugten Webseitenabzüge werden ebenfalls gespeichert (12).

2 Beweisrecht

2.1 Freie richterliche Beweiswürdigung

Sollen infolge von Rechtsverstößen Ansprüche, etwa auf Beseitigung, Unterlassung oder Schadensersatz gerichtlich geltend gemacht werden, sind die Verstöße zu beweisen. Im Zivilprozess zugelassen sind die im Rahmen des sogenannten Strengbeweises gesetzlich vorgesehenen Beweismittel.[3] In Betracht kommen hier insbesondere die Beweismittel Urkunde (§§ 415 ff. ZPO) und Augenschein (§§ 371 ff. ZPO).

In der Praxis werden zur Dokumentation von Rechtsverstößen im Internet häufig Screenshots oder – zur Erfassung beweglicher Inhalte und Abläufe wie Bestellprozesse – Bildschirmvideos erstellt. Einfache Screenshots stellen hierbei ein besonders manipulationsanfälliges Beweismittel dar. Aufgrund der heutigen technischen Möglichkeiten lassen sich Inhalte mit geringem Aufwand verändern, ohne dass dies auf den ersten Blick erkennbar ist. Bereits ein bloßes, durch eigene Beweise substantiiertes

Instituts für Verbraucherforschung und nachhaltigen Konsum (vunk) sowie des Instituts IOS3 der Hochschule Pforzheim sowie des Instituts AIFB des Karlsruher Instituts für Technologie (KIT), gefördert von der Baden-Württemberg Stiftung im Rahmen des *Ideenwettbewerb Blockchain*.

M.Sc. Nadja Kruse

ist Doktorandin am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie (KIT).

E-Mail: nadja.kruse@kit.edu

Dr.-Ing. Meike Ullrich

ist Postdoktorandin am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie (KIT).

E-Mail: meike.ullrich@kit.edu

Dr.-Ing. Gunther Schiefer

forscht in Angewandter Informatik am Karlsruher Institut für Technologie (KIT), insbesondere auf dem Gebiet Digital Privacy. Er ist Fellow der KASTEL Security Research Labs.

E-Mail: gunther.schiefer@kit.edu

3 *Prütting*, in: MüKo ZPO, 7. A. 2025, § 294, Rn. 14.

Bestreiten der Gegenseite kann genügen, um den Beweiswert zu erschüttern.[4]

Unter bestimmten Voraussetzungen können elektronische Dokumente durch die betreffende Vermutung gemäß § 371a ZPO im Sinne eines Anscheinsbeweises eine den privaten Urkunden entsprechende Beweiskraft erlangen. Hierzu müssen die elektronischen Dokumente mit einer qualifizierten elektronischen Signatur (qeS) im Sinne der EU-eIDAS-Verordnung versehen sein. Es wird insofern vermutet, dass eine darin enthaltene Erklärung vom Inhaber des Signaturschlüssels stammt. Zwar kann eine qeS nach § 371a Abs. 1 ZPO eine gesetzliche Vermutung begründen, dass die Erklärung vom Unterzeichner stammt, doch bezieht sich diese Vermutung ausschließlich auf den Erklärenden, nicht auf die inhaltliche Richtigkeit.[5] Wird ein Screenshot bereits in manipulierter Form erstellt und erst danach signiert, bestätigt die Signatur lediglich den (zuvor aber veränderten) Zustand bei Signierung. Damit verfehlt sie in solchen Fällen den Schutzzweck der Signatur, nämlich die Sicherstellung von Integrität und Authentizität, in Bezug auf den Inhalt.

Die EU-eIDAS-Verordnung enthält mit den qualifizierten Siegeln, Archivierungsdiensten und Journalen Regelungen zu technischen und organisatorischen Mitteln, deren Einsatz zu einer beweisrechtlichen Vermutungswirkung führen kann, die sogar über den Anscheinsbeweis hinausgeht. Wie beispielhaft anhand der qeS gezeigt wurde, beziehen diese sich aber stets auf die Unversehrtheit der Angaben seit Einsatz des Dienstes. Vorangehende Manipulationen am Inhalt eines vermeintlichen Beweisobjekts lassen sich mit keinem der Dienste ausschließen. Diese Frage bleibt trotz der Vermutungen zugunsten der eIDAS-Dienste weiter Gegenstand der uneingeschränkten freien richterlichen Beweiswürdigung (§ 371 Abs. 1, § 286 Abs. 1 ZPO).[6] Das Gericht entscheidet insoweit nach freier Überzeugung auch, ob es das als Beweismittel in einer Datei vorgelegte oder übermittelte (§ 371 Abs. 1 Satz 2 ZPO) elektronische Dokument für unverändert und authentisch hält. Das vorliegend angestrebte Ziel der systematischen Beweissicherheit in Bezug auf Rechtsverletzungen im Internet wird insofern weder mit einer qeS noch mit den weiteren eIDAS-Diensten allein vollständig erreicht.

2.2 Folgerungen für die Umsetzung

Die für EVIDENTT konzipierten technischen und organisatorischen Mittel könnten gleichwohl im Rahmen richterlicher Beweiswürdigung beweiswerterhöhend wirken: Im Vergleich zu bloßen Screenshots ermöglicht der Einsatz von Hashmechanismen direkt bei Erfassung der Webseite die Möglichkeit, die Integrität (technisch) sicherzustellen. Dies wird zusätzlich durch die Speicherung in einer DLT (hier: Blockchain) unterstützt: Durch die verteilte Speicherung lassen sich Manipulationen (unter realistischen Annahmen) ausschließen und gleichzeitig der Zeitpunkt der Speicherung unveränderbar dokumentieren.

In der Literatur wird der Blockchain bereits im Zusammenhang mit Bitcoin-Transaktionen[7] ein erhöhter Beweiswert hinsichtlich Authentizität und Integrität zugesprochen.[8] Wird diese Einschätzung auf EVIDENTT übertragen, ließe sich daraus ableiten, dass die eingesetzte Technologie im Vergleich zu reinen, leicht manipulierbaren Screenshots eine deutlich höhere Beweissicherheit bietet, wenngleich diese, mangels entsprechender Beweiskraftvermutungen, freilich nicht an den gesetzlich bestimmten Beweiswert der eIDAS-Dienste bzw. des § 371a ZPO heranreicht.[9]

Perspektivisch ließe sich durch Verwendung einer DLT, welche die Anforderungen an qualifizierte elektronische Journale nach Art. 3 Nr. 53, Art. 45k und l eIDAS-VO erfüllt,[10] auch eine formelle Beweisrechtswirkung zugunsten der DLT erzielen. Hier scheinen aber noch viele (Rechts-)Fragen ungeklärt,[11] insbesondere auch, wie eine entsprechende „Permissioned Blockchain" mit geregeltem Nutzer- und Identitätsmanagement zu gestalten wäre.[12] Auch faktisch ist eine solche Anerkennung eines „Anbieters" einer DLT nicht bekannt.[13]

Eine maßgebend innovative Rolle nimmt sodann auch der Crowd-Mechanismus in EVIDENTT ein. Vorgenannte Mittel – und so auch gängige auf dem Markt befindliche Technologien zur Beweissicherung – können bislang keinen Nachweis bieten, dass die betreffende Darstellung nicht vor der Sicherung künstlich erzeugt oder manipuliert wurde; dass also etwa der Beweispflichtige eine Webdarstellung verändert hat. Neben der Veränderung von Texten wird auch die Manipulation von Bildern und Darstellungen – unter anderem aufgrund der Möglichkeiten der Bildveränderung durch Künstliche Intelligenz – technisch immer einfacher und schwieriger erkennbar. Eine solche Manipulation lässt sich ausschließen, wenn der echte Zustand einer Webseite zeitgleich oder zumindest zeitnah zur Erfassung durch eine Person nochmals von weiterer Stelle durch eigenständigen Zugriff bestätigt wird. Der Crowd-Mechanismus in EVIDENTT sieht vor, dass „Crowd-Teilnehmer" den Verstoß innerhalb kurzer Zeit nach der Ersterfassung bestätigen, indem deren Ansichten ebenfalls durch Erfassung von Screenshots und Webseitendaten sowie der Speicherung eines daraus abgeleiteten Hashwerts dokumentiert werden. Dies kann die Überzeugungsbildung des Gerichts erheblich unterstützen.

EVIDENTT erzeugt insoweit Beweiswert durch technische und organisatorische Mittel. Ihre Auswirkung auf die Beweiswürdigung durch Gerichte hängt weiterhin davon ab, inwiefern der technologische Ansatz einerseits und seine konkrete Umsetzung andererseits Gerichte zu überzeugen vermögen. Dabei kommt es maßgeblich auf die spezifische Gestaltung an. Entsprechende Gestaltungsdeterminanten aus dem Datenschutz- und Urheberrecht sollen nachfolgend erörtert werden.

4 *Mankowski* in: Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG, Band 1, 3. A. 2016, S. 12, Rn. 322ff.

5 Am Beispiel des ersetzenden Scannens: *Roßnagel/Wilke*, NJW 2006, 2145 (2148); *Roßnagel/Nebel*, NJW 2014, 886 (887); *Irskens*, in: Digitalisierung und Zivilverfahren, 2023, S. 445, Rn. 51.

6 So bzgl. der Beurteilung des Beweiswertes angesichts der eIDAS-Dienste i.E. auch *Irskens*, in: Digitalisierung und Zivilverfahren, 2023, 453, Rn. 72.

7 Bitcoin, Gateway, DuD 8/2017, S. 507.

8 S. dazu ausführlich: *Irskens*, in: Digitalisierung und Zivilverfahren, 2023, S. 448, Rn. 59.

9 Darauf weist, völlig zurecht, *Röß*, in: Musielak/Voit, ZPO, 22. A. 2025, § 371a, Rn. 4 hin.

10 *Schwalm/Mueller*, DuD 2024, 227 (250).

11 *Roßnagel*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. A. 2024, Kap. 14, Rn. 77ff.

12 *Brisch/Brisch*, in: Hoeren u. a., Handbuch Multimedia-Recht, 62. A. 2024, Teil 13.3, Rn. 137 verwenden dazu den Begriff „Permissioned Blockchain".

13 *Roßnagel*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. A. 2024, Kap. 14, Rn. 77ff.

3 Datenschutzrecht

Für EVIDENTT ergeben sich datenschutzrechtliche Anforderungen insbesondere im Anwendungsbereich der EU-Datenschutz-Grundverordnung (DSGVO). Bereits in der Entwicklungsphase sind die Vorgaben des Datenschutzrechts zu berücksichtigen, um Gestaltungsanforderungen i. S. d. Art. 25 DSGVO frühzeitig zu verankern.[14] Durch EVIDENTT können dabei auf mehreren Ebenen personenbezogene Daten betroffen sein.

Zur besseren Übersicht werden im Folgenden die in EVIDENTT nach aktueller Einschätzung betroffenen Datenkategorien dargestellt und darauf aufbauend die jeweiligen datenschutzrechtlichen Gestaltungsanforderungen abgeleitet.

3.1 Anwender- und Nutzungsdaten

Der Anwender des Systems als Nutzer oder Crowd-Teilnehmer kann eine natürliche Person sein, die sich – je nach konkreter Umsetzung – registriert und mit Anmeldedaten in das System einloggt. Dabei findet eine Verarbeitung personenbezogener Daten statt, etwa von Namen, (geschäftlichen) Kontaktdaten oder Zugangsdaten. Im Einsatzkontext von Verbraucherzentralen oder ähnlichen Institutionen handelt es sich dabei regelmäßig um geschäftsbezogene, gleichzeitig aber auch personenbezogene Daten i. S. d. DSGVO.

Im Sinne der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) könnte beispielsweise die Verarbeitung im Kontext der Anwenderregistrierung und -anmeldung auf Zugangsdaten beschränkt sein. Ob darüber hinaus eine weitergehende Angabe und entsprechende Verarbeitung von Namen und Kontaktinformationen erforderlich ist, hängt davon ab, ob – je nach konkreter Umsetzung – die betreffende Person zu einem späteren Zeitpunkt (z. B. Zwecks Ladung als Zeuge) identifiziert werden muss.

Im Sinne der Datenminimierung, aber zugleich auch im Einklang mit dem Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f DSGVO und der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO sollten diese Anwender- und Nutzungsdaten nur dem jeweiligen Anwender sowie einem eng begrenzten Personenkreis, etwa direkten Vorgesetzten, funktionalen Vertretern oder für die Prozessführung zuständigen Stellen (sofern eine Zuordnung zur Person als Teil der Beweisführung in der konkreten Umsetzung erforderlich ist) zugänglich sein. Ein Zugriff durch den technischen Anbieter sollte bei einer möglichst datenschutzfreundlichen Lösung in der Standardkonfiguration nicht ohne Weiteres und nicht ohne triftigen Grund möglich sein.

Schließlich ist auch der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO einzuhalten. Technische Metadaten wie IP-Adressen oder Zeitstempel sind nach Abschluss des Beweisverfahrens unverzüglich zu löschen, sofern sie nicht mehr benötigt werden.

Wird EVIDENTT auf den Endgeräten der Crowd-Teilnehmer eingesetzt, stellt sich zudem die Frage, ob dabei weitergehend personenbezogene Daten verarbeitet werden. Zwar speichert die lokale Anwendung selbst keine zusätzlichen personenbezogenen Daten, sondern dient lediglich der Verifizierung und Absicherung der erhobenen Beweise. Gleichwohl kann es mittelbar zu einer Verarbeitung personenbezogener Daten kommen, etwa durch die Erfassung von IP-Adressen, Zeitstempeln, Nutzungsdaten oder Logfiles.

3.2 Daten im Beweisobjekt („Verstoßdaten")

Die im Rahmen von EVIDENTT erfassten Beweisobjekte können ebenfalls personenbezogene Daten enthalten; sie sollen im Folgenden als „Verstoßdaten" bezeichnet werden. Im Rahmen der Beweissicherung erhobene Verstoßdaten können Informationen zu Personen enthalten, die den Verstoß begangen haben, aber auch solche zum Betreiber der Webseite (personenbezogene Daten aus dem Impressum, sofern nicht identisch mit dem Rechtsverletzer) und zu Dritten – letztere zum Beispiel als Abbildungen von Werbegesichtern oder Angaben sonstiger Nutzer der Webseite, z. B. in Kommentarfunktionen und Posts.

Diese Daten dürfen im Sinne des Grundsatzes der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) nur verarbeitet werden, soweit dies für die Beweisführung erforderlich ist. Gerade weil die Verstoßdaten im Rahmen der Beweissicherung erfasst werden und dabei unvermeidbar auch Daten Dritter enthalten können, stellt sich die Frage nach ihrer zulässigen Verarbeitung. Maßgeblich ist hier neben dem Grundsatz der Zweckbindung auch der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO): Die Verarbeitung muss sich auf das für den Beweiszweck Erforderliche beschränken. Technische Maßnahmen zur Reduzierung personenbezogener Inhalte in den Verstoßdaten sind daher grundsätzlich vorzunehmen, soweit sie den Beweiswert und die Integrität der Dateien nicht gefährden.

Ziel der DLT-Lösung ist gerade die Sicherung der Integrität des Beweismaterials. Eine Anonymisierung von Daten Dritter könnte zwar als technische Maßnahme zur Minimierung möglicher Risiken in Betracht gezogen werden, würde jedoch zugleich einen Eingriff in die gesicherte Seite darstellen und damit den Beweiswert sowie den Zweck der DLT-Lösung erheblich schmälern. Da es sich zudem um öffentlich zugängliche Daten handelt, die gezielt und ausschließlich zum Zweck der Beweissicherung erhoben werden, erscheint eine sofortige Schwärzung oder Anonymisierung nicht sachgerecht. Deshalb dürfen die Daten in ihrer ursprünglichen Form so lange gespeichert werden, wie sie für das Verfahren benötigt werden. Zugleich ist durch technische und organisatorische Maßnahmen sicherzustellen, dass die Verarbeitung strikt auf diesen Zweck begrenzt bleibt, eine missbräuchliche Nutzung ausgeschlossen wird und die Speicherung zeitlich auf das notwendige Maß beschränkt ist. Nach Wegfall der Erforderlichkeit sind die Daten umgehend zu anonymisieren oder zu löschen.

Zudem sollte der (weitere) Zugriff auf die Verstoßdaten ausschließlich dem Beweisführer vorbehalten sein. Diese Ausgestaltung entspricht zugleich dem Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO), da durch Zugriffsbeschränkung, Verschlüsselung und zeitliche Begrenzung der Speicherung ein Missbrauch oder eine unbefugte Verarbeitung der Verstoßdaten verhindert wird.

3.3 Daten in der DLT

In der DLT (hier: Blockchain) werden ausschließlich kryptografische Hashwerte gespeichert, die aus einer Kombination von Zeichen bestehen. Ohne Bezug zu den zugrunde liegenden, außerhalb der DLT abgelegten Verstoßdaten lassen diese keinerlei

14 *Baumgartner*, in: Ehmann/Selmayr, DSGVO, 3. A. 2024, Art. 25, Rn. 1.

Rückschlüsse auf den ursprünglichen Inhalt zu.[15] Darüber hinaus werden keine weiteren personenbezogenen Daten an Dritte wie die Crowd oder andere Beteiligte weitergegeben als jene, die einem solchen möglichen Dritten ohnehin vorliegen müssen, um den Hashwert abzugleichen.[16]

4 Urheberrecht

Screenshots sind Abbildungen digitaler Inhalte und können urheberrechtlich relevant sein, wenn sie ein geschütztes Werk abbilden (z. B. ein Video, eine Webseite oder eine Grafik). Auch bei der Speicherung von Webseiten werden möglicherweise urheberrechtlich geschützte Werke wie Grafikdateien technisch kopiert und damit urheberrechtlich relevant.

Neben der Frage, ob die einzelnen Bestandteile einer Webseite urheberrechtlichen Schutz genießen, stellt sich in der Praxis die Frage, ob auch die Webseite als Ganzes urheberrechtlich geschützt sein kann. Die Anforderungen, die hierfür an eine Webseite gestellt werden müssen, sind in Literatur und Rechtsprechung noch nicht vollständig geklärt.[17] Unabhängig davon ist aber von Bedeutung, wie es aus urheberrechtlicher Perspektive zu beurteilen ist, wenn der zu Beweissicherungszwecken angefertigte Screenshot oder die betreffende Webseitenkopie urheberrechtlich geschütztes Material zumindest enthält.

4.1 Screenshots als Werknutzung durch Dritte

Bei der Erstellung von Screenshots oder der Kopie einer Webseite, die ein Werk darstellt oder enthält, kommt es zu einer Vervielfältigung i.S.d. § 16 UrhG. Grundsätzlich steht es ausschließlich dem Urheber zu, über seine Werke zu verfügen und sie gegebenenfalls zu verwerten. Die Person, die den Screenshot zu Beweissicherungszwecken anfertigt, wird i.d.R. nicht Urheber des urheberrechtlich geschützten Materials sein und mithin kein genuines Vervielfältigungsrecht i.S.d. § 16 UrhG haben. Fraglich ist, ob dem ausschließlichen Vervielfältigungsrecht des Urhebers vorliegend sog. „Schranken" gegenüberstehen, die eine Beweissicherung durch Dritte dennoch ermöglichen. Solche, in der Folge erweiterten Nutzungsmöglichkeiten können sich aus einem Vertrag oder dem Gesetz selbst ergeben.

4.2 Verwendung in gerichtlichen Verfahren

Während vorliegend eine vertragliche Einräumung von Nutzungsrechten durch den Urheber (dem ja ein Verstoß vorgeworfen wird) praktisch höchst unrealistisch erscheint, ist denkbar, dass eine Werknutzung im Rahmen des vorliegenden Systems durch §§ 44a ff. UrhG gesetzlich erlaubt ist. So ist es nach § 45 Abs. 1 UrhG zulässig, einzelne Vervielfältigungsstücke von Werken zur Verwendung in Verfahren vor einem Gericht, einem Schiedsgericht oder einer Behörde herzustellen oder herstellen zu lassen. Die Vorschrift hat primär den Zweck, es Beteiligten der Rechtspflege und Verwaltung zu ermöglichen, im Rahmen ihrer Aufgaben erforderliche Vervielfältigungen von verfahrensrelevanten Werken zu erstellen. Der Gesetzesentwurf weist darauf hin, dass das „Werk […] in diesen Fällen nicht um seiner selbst willen, sondern als Beweis oder sonstiges Hilfsmittel für die zu treffende Entscheidung benutzt" wird.[18]

Da der Wortlaut von einer Verwendung *vor* einem Gericht, einem Schiedsgericht oder einer Behörde spricht und der Zweck der Vorschrift die Ermöglichung eines reibungslosen Verfahrensablaufs ist, liegt es entgegen anderslautender Ansicht[19] nahe, dass nicht nur diese, sondern auch weitere am Verfahren Beteiligte von der Schrankenregelung erfasst sind.[20]

Aus Sicht des EVIDENTT-Ansatzes wäre es insofern denkbar, dass zumindest eine Prozesspartei – ein Geschädigter eines Rechtsverstoßes oder Vertreter anderweitig klagebefugter Stellen – mit der EVIDENTT-Technologie entsprechende Vervielfältigungen erstellt. Problematisch ist aber, wie weit im Vorfeld eines Verfahrens Vervielfältigungen durch den § 45 Abs. 1 UrhG privilegiert werden. Auch hier ist mit Blick auf Wortlaut und Zweck naheliegend, nicht in engster Auslegung den Zeitraum der Vervielfältigung auf ein laufendes Verfahren zu beschränken. Es muss davon ausgegangen werden, dass der Gesetzgeber auch Zeiträume im Blick hatte, in denen im Angesicht eines bevorstehenden Verfahrens Beweise gesammelt werden.[21]

Gleichwohl bestehen hier Grenzen: Die Vervielfältigungshandlung muss wohl eine gewisse Verfahrensnähe aufweisen. Das könnte vorliegen, „wenn die vorbereitenden Handlungen bereits für eine zielgerichtete Verwendung in einem konkreten Verfahren beabsichtigt sind"[21] – nach anderer Meinungsnuance aber nicht, wenn eine Vervielfältigung erfolgt, um „erkennbar erst noch zur Klärung der Erfolgsaussichten eines Verfahrens" zu dienen.[22] In noch engerer Auslegung solle die Vorbereitungshandlung derart eng am Verfahren liegen, dass im Gegenzug angenommen werden müsse, die Vervielfältigung sei rechtswidrig, wenn das Verfahren nachfolgend unterbleibe.[23] Auch Handlungen der vorgerichtlichen privaten Rechtsdurchsetzung für Abmahnungen fielen nach einer strengen Lesart nicht unter die Privilegierung.[24]

Für eine eher weite Auslegung spricht vorliegend eine Gesamtwertung. Sofern es in der Praxis bei der Anwendung von EVIDENTT überhaupt zu einer Vervielfältigung von urheberrechtlich geschützten Werken kommt, bezieht sich dies regelmäßig auf ohnehin bereits im Internet veröffentlichte Werke, was deren Schutzbedarf relativiert. Technisch bedingt wird durch den Crowd-Mechanismus ein potenziell auf der betreffenden Webseite enthaltenes Werk durch EVIDENTT zwar gleich von mehreren Stellen für Beweiszwecke vervielfältigt, sodass sich einwen-

15 *Martini*, in: Paal/Pauly, DSGVO, 4. A. 2026, Art. 32, Rn. 34e; *Burghoff*, ZD 2023, 658 (662).

16 *Erbguth*, MMR 2019, 654 (660).

17 *Heckmann/Paschke*, in: Heckmann/Paschke, jurisPK-Internetrecht, 8. A. 2024, Kap. 3.1, Rn. 141.

18 BT-Drucks. VI/270, S. 63 (zu § 45).

19 *Melchiar/Stieper*, in: Loewenheim u. a., Urheberrecht, 3. A. 2021, § 45, Rn. 5; wohl auch Lüft, in: *Wandtke/Bullinger*, UrhR, 6. A. 2025,§ 45, Rn. 1.

20 *Dreier*, in: Dreier u. UrhG, 8. A. 2025, § 45, Rn. 7 *Wiebe*, in: Spindler/Schuster, Recht der elektronischen Medien, 5. A. 2026, § 45 UrhG, Rn. 2; wohl auch *Schulz*, in: Götting u. a., BeckOK Urheberrecht, 48. Ed. 2025, § 45, Rn. 9; zum Vervielfältigungsrecht privat beauftragter Sachverständigen *Ulrich*, DS 2011, 352 (356).

21 LG Düsseldorf, Urteil vom 23. 1. 2007 – 4a O 521/05, GRUR-RR 2007, 139 (194); so wohl auch einhellig die Meinung in der Literatur, etwa *Schulz*, in: Götting/Lauber-Rönsberg/Rauer, UrhG, 2. A. 2019, § 45, Rn. 8ff.; *Dreier*, in: Dreier/Schulze/Raue/Specht-Riemenschneider, UrhG, 8. A. 2025, § 45, Rn. 6; *Melichar/Stieper*, in: Loewenheim/Leistner/Ohly/Schricker, UrhG, 6. A. 2020, § 45, Rn. 6; *Lüft*, in: Wandtke/Bullinger, UrhG, 6. A. 2022. § 45, Rn. 3; *Ulrich*, DS 2011, 352 (356)

22 *Schulz*, in: Götting u. a., BeckOK Urheberrecht, 48. Ed. Stand 01.12.2025, § 45, Rn. 9.

23 *Melchiar/Stieper*, in: Loewenheim u. a., Urheberrecht, 3. A. 2021, § 45, Rn. 5; wohl auch *Lüft*, in: Wandtke/Bullinger, UrhR, 6. A. 2025,§ 45, Rn. 1.

24 *Lüft*, in: Wandtke/Bullinger, UrhR, 6. A. 2022, § 45, Rn. 3.

den ließe, die Grenze von „einzelnen Vervielfältigungsstücken" im Sinne des Wortlauts der Vorschrift würde überschritten.[25] Allerdings ist die Zweckbindung zumindest bei regelgerechter Anwendung gewahrt, da der Einsatz der Technologie und die Speicherung von Vervielfältigungsstücken vorliegend klar auf den Beweiszweck beschränkt ist.[26] Die Vervielfältigungsstücke ihrerseits werden nicht veröffentlicht und auch nicht den teilnehmenden Nutzern oder Crowd-Mitgliedern zur Verfügung gestellt.

Nicht unumstritten, aber möglicherweise noch vertretbar könnte sein, auch – entgegen anderslautender Ansicht[27] – Vervielfältigungen durch EVIDENTT im Rahmen von Verfahren zur Abmahnung auf die Grundlage des § 45 Abs. 1 UrhG zu stützen, wenn diese entsprechend ausgestaltet sind. Grenzen für die Berufung auf § 45 Abs. 1 UrhG sind vermutlich aber dort erreicht, wo sich der Einsatz nicht gezielt auf die Vorbereitung eines Verfahrens, sondern nur auf die Sondierung möglicher Rechtsverstöße und vorsorgliche Beweissicherung bezieht.

4.3 Sui generis-Schranke oder Rechtfertigungstatbestand?

Auch unabhängig von § 45 UrhG liegt es nahe, mögliche, in Einzelfällen vorkommende Vervielfältigungen urheberrechtlich geschützter Werke im Rahmen von EVIDENTT mit Verweis auf das Beweisinteresse und den Vervielfältigungszweck zu begründen. Nicht unbeachtet bleiben darf dabei zunächst ein wohl verbreitet anerkanntes verfassungsrechtlich abgeleitetes Recht auf Beweis und Beweisführung.[28] Demnach muss eine Prozesspartei die Möglichkeit haben, Beweise zugunsten ihrer Tatsachenbehauptung zu führen. Darüber hinaus muss auch der Sinn und Zweck des Urheberrechts berücksichtigt werden.

Vorliegend ließe sich argumentieren, die Erstellung von Screenshots oder anderweitigen Vervielfältigungen im Rahmen der Beweissicherung seien technisch bedingte, auf den Zweck der Beweisführung beschränkte Verwendungshandlungen ohne eigenständige wirtschaftliche Bedeutung. Eine Beweisführung wäre ohne diese Verstoßdaten kaum denkbar und dieser Vorgang insofern urheberrechtlich freizustellen. Entsprechendes wurde wohl auch bisher so gut wie nie beanstandet.[29]

Insgesamt spricht vieles dafür, dass das Sichern von Verstoßdaten, in denen in Einzelfällen auch urheberrechtlich geschützte Werke enthalten sein können, aufgrund des Zusammenspiels des Rechts auf Beweis und des Sinns und Zwecks des Urheberrechts – ggf. im Sinne einer sui generis Schranke – urheberrechtlich zulässig ist. Zumindest als Rechtfertigung zur Abwendung entsprechender Ansprüche aufgrund einer urheberrechtlichen Rechtsgutverletzung ließen sich die vorgenannten Überlegungen nutzbar machen.

5 Offene Herausforderungen

Trotz der entwickelten Architektur zur beweissicheren Dokumentation bestehen weiterhin verschiedene technische und organisatorische Herausforderungen, die in zukünftigen Arbeiten adressiert werden müssen. Diese betreffen insbesondere die Aufnahme dynamischer Inhalte, die Beweisführung in geschützten Bereichen sowie die Vergleichbarkeit von Abzügen, die zwangsläufig Unterschiede aufweisen.

5.1 Dynamische Inhalte

Viele Rechtsverstöße im digitalen Raum manifestieren sich nicht in statischen Momentaufnahmen, sondern über den Verlauf einer Interaktion. Ein typisches Beispiel sind sogenannte Dark Patterns, die erst bei der sukzessiven Navigation durch eine Webseite sichtbar werden, etwa, wenn bestimmte Schaltflächen erst nach mehreren Klicks erscheinen oder Inhalte zeitlich verzögert eingeblendet werden. Klassische Screenshots können diese Abläufe nicht vollständig erfassen.

Mögliche Lösungsansätze:

- Einsatz von Screen-Recording-Technologien, die den gesamten Interaktionsverlauf dokumentieren. Die Aufzeichnungen könnten anschließend segmentiert, gehasht und modular abgespeichert werden.
- Ergänzung durch Metadaten wie Klickpfade, Zeitstempel und Scroll-Positionen, die nachvollziehbar machen, in welchem Nutzungskontext bestimmte Elemente aufgetreten sind.
- Kombination von visuellen Aufnahmen mit DOM[30]-Inspektionen, sodass nicht nur das sichtbare Bild, sondern auch die zugrundeliegende Webseitenstruktur gesichert wird.

5.2 Geschützte Bereiche

Einige Verstöße treten nicht im öffentlich zugänglichen Internet auf, sondern in geschützten Bereichen wie zugangsbeschränkten, benutzerspezifisch dargestellten Webseiten (z. B. Mitgliederportalen) oder hinter Bezahlschranken. In diesen Fällen ist eine Verifikation durch die Crowd nicht möglich, da nur die angemeldete Person selbst Zugriff auf die Inhalte hat. Damit entfällt ein zentrales Element des redundanten Nachweises.

Möglicher Lösungsansatz:

- Einrichtung von vertrauenswürdigen Instanzen (z. B. Verbraucherzentralen oder Ombudsstellen), die nach Vorlage einer Zugangsberechtigung oder über ein Delegationsverfahren den geschützten Bereich im Auftrag der betroffenen Person dokumentieren dürfen.

5.3 Unterschiede in Webseitenabzügen

Ein praktisches Problem liegt darin, dass Webseiten dynamische Inhalte einbinden, beispielsweise Werbung, personalisierte Empfehlungen oder unterschiedliche Darstellungsoptionen. Zwei Nutzer, die zeitgleich denselben Webseitenabzug erstellen, erhalten daher oft leicht unterschiedliche Inhalte. In der Folge unterscheiden sich auch die Hashwerte, obwohl die relevanten Verstöße identisch enthalten sind. Das erschwert den automatisierten Abgleich und mindert die Beweiskraft.

25 *Schulz*, in: Götting u. a., BeckOK Urheberrecht, 48. Ed. Stand 01.12.2025,§ 45, Rn. 5.

26 *Schulz*, in: Götting u. a., BeckOK Urheberrecht, 48. Ed. Stand 01.12.2025,§ 45, Rn. 9.

27 *Lüft*, in: Wandtke/Bullinger, UrhR, 6. A. 2022, § 45, Rn. 3.

28 *Prütting*, in: MüKo ZPO, 7. A. 2025, § 284, Rn. 18 m.w.N.; zum Beweis im Strafverfahren und einer entsprechenden Ableitung aus dem Recht auf ein faires Verfahren siehe auch BVerfG, Beschluss vom 20. 12. 2000 – 2 BvR 591/00, NJW 2001, 2245 (2246).

29 Auf diese offenbare Selbstverständlichkeit weisen, m.w.N., *Melichar/Stieper*, in: Loewenheim u. a., Urheberrecht, 6. A. 2020, § 45, Rn. 1 hin.

30 Document Object Model.

Mögliche Lösungsansätze:

- Entwicklung von Inhaltsvergleichs-Algorithmen, die gezielt einen markierten Rechtsverstoß in den Crowd-Webseitenabzügen suchen, auch wenn sich andere Teile der Seite unterscheiden. Dies könnte z. B. durch KI-gestützte Quelltextanalyse oder Mustererkennung in Screenshots erfolgen.
- Einsatz von Fuzzy Hashing (z. B. ssdeep[31]), bei dem nicht nur exakte Übereinstimmungen, sondern auch Ähnlichkeiten zwischen Dateien berechnet werden können. Auf dieser Grundlage kann eingeschätzt werden, ob auf mehreren Webseitenabzügen mit einer gewissen Wahrscheinlichkeit ein vergleichbarer Rechtsverstoß dokumentiert wurde.

6 Ergebnis

Die Durchsetzung geltenden Rechts im Internet durch Mittel des Rechtsstaats gelingt nur, wenn Verstöße gegen das Recht nachgewiesen werden können. Zwar mag gemeinhin zutreffend sein, dass das Internet „nichts vergisst", in seiner Dynamik sind rechtswidrige Handlungen im Internet gleichwohl häufig flüchtig oder zumindest für Zwecke des späteren Beweises, etwa bei Gerichtsverhandlungen, nicht eindeutig und sicher reproduzierbar. Vorliegend wurde deshalb ein Verfahren auf seine Machbarkeit hin untersucht, das einerseits technisch Webseitenzustände erfasst und durch DLT-Technologie manipulationssicher dokumentiert, andererseits auch bei der Beweissicherung selbst auf verteilte Instanzen durch eine sogenannte „Crowd" setzt. Die Wirksamkeit der Technologie in Bezug auf den angestrebten Zweck der Beweiswerterhöhung hängt stark von der technischen und organisatorischen Umsetzung im Einzelnen ab.

Insgesamt lässt sich gleichwohl auf der Grundlage der Ergebnisse der Machbarkeitsstudie festhalten, dass der vorgestellte Ansatz eine vielversprechende Grundlage für die Entwicklung einer zukunftsfähigen Infrastruktur zur beweissicheren Dokumentation digitaler Inhalte bietet. Die Kombination aus technischer Innovationskraft, rechtlicher Fundierung und partizipativer Ausgestaltung schafft die Basis für eine vertrauenswürdige, skalierbare und gesellschaftlich relevante Lösung zur Stärkung digitaler Rechtsdurchsetzung.

31 *OI, Tsukasa* (Hrsg.), ssdeep Project, online abrufbar unter: https://ssdeep-project.github.io/ssdeep/index.html, zuletzt abgerufen am: 21.01.2026.

Springer

springer.com/informatik

Sachbuch

K. Kersting, C. Lampert, C. Rothkopf (Hrsg.)
Wie Maschinen lernen
Künstliche Intelligenz verständlich erklärt
2019, XIV, 245 S. 71 Abb.,
68 Abb. in Farbe. Brosch.
€ (D) 19,99 | € (A) 20,55 | *CHF 22.50
ISBN 978-3-658-26762-9
€ 14,99 | *CHF 18.00
ISBN 978-3-658-26763-6 (eBook)

M. Donick
Die Unschuld der Maschinen
Technikvertrauen in einer smarten Welt
2019, XXIV, 279 S. 14 Abb. Book + eBook. Brosch.
€ (D) 24,99 | € (A) 26,16 | *CHF 28.00
ISBN 978-3-658-24470-5
€ 19,99 | *CHF 22.00
ISBN 978-3-658-24471-2 (eBook)

Ihre Vorteile in unserem Online Shop:

Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit

€ (D): gebundener Ladenpreis in Deutschland, € (A): in Österreich. * : unverbindliche Preisempfehlung. Alle Preise inkl. MwSt.

Jetzt bestellen auf springer.com/informatik oder in der Buchhandlung

Part of SPRINGER NATURE

A85543