Das E-Evidence-Gesetzespaket: Ein Meilenstein in der grenzüberschreitenden Strafverfolgung in der EU?

*von Juliane Bentler**

Abstract
In vielen der heutigen Strafverfahren spielen digitale Beweismittel eine zentrale Rolle. Der Zugang zu elektronischen Beweismitteln kann für Strafverfolgungsbehörden ein langwieriger und komplizierter Vorgang sein. Auf dieses Problem hat der europäische Gesetzgeber mit der E-Evidence-Verordnung (EU) 2023/ 1543 sowie der dazugehörigen Richtlinie (EU) 2023/ 1544 reagiert, damit die Behörden unabhängig vom Speicherort der Daten einfacher und schneller Zugang zu elektronischen Beweismitteln erhalten. Der Beitrag gibt einen Überblick über das E-Evidence-Gesetzespaket, untersucht die wesentlichen Kritikpunkte und setzt sich kritisch mit dem am 13. März 2026 in Kraft getretenen Elektronischen-Beweismittel-Umsetzungs- und Durchführungsgesetz (EBewMG) auseinander, welches die E-Evidence-Richtlinie in deutsches Recht umsetzt sowie Durchführungsvorschriften zur E-Evidence-Verordnung vorsieht.

In many of today's criminal proceedings, digital evidence plays a crucial role. Accessing electronic evidence can be a lengthy and complicated process for law enforcement agencies. The European legislator has responded to this problem with the E-Evidence Regulation (EU) 2023/1543 and the accompanying Directive (EU) 2023/1544, designed to enable authorities to access electronic evidence more easily and quickly, regardless of where the data is stored. This article provides an overview of the E-Evidence legislative package, examines the main points of criticism and takes a critical look at the Electronic Evidence Implementation and Enforcement Act, which transposes the E-Evidence Directive into German law and provides for implementing provisions for the E-Evidence Regulation.

I. Einleitung

Digitale Beweismittel spielen in vielen der heutigen Strafverfahren in der Europäischen Union als auch weltweit eine zentrale Rolle: von Chat-Verläufen, Emails, Cloud-Daten bis hin zu IP-Adressen. Zudem werden immer mehr Straftaten über das Internet geplant und hinterlassen dabei grenzüberschreitend digitale Spuren, die sowohl zur Identifizierung der Täter als auch zur Sachverhaltsaufklärung unverzichtbar sind. Bei der grenzüberschreitenden Strafverfolgung stellt es die Strafverfolgungsbehörden vor erhebliche Herausforderungen, wenn es um den Zugriff auf Daten als elektronische Beweismittel geht. Denn oftmals ist es zunächst einmal schwierig zu bestimmen, wo genau sich die relevanten Daten überhaupt befinden.

Regelmäßig werden diese Daten von international tätigen Diensteanbietern gespeichert, deren Sitz sich außerhalb des ermittelnden Staates befindet. Ferner sind Strafverfolger, anders als Nutzer und Provider, auch im Internet an nationale Grenzen gebunden.

Die klassischen Rechtsinstrumente sind nicht an die Herausforderungen der digitalen Welt angepasst. So erfolgte der Zugriff auf digitale Beweismittel bisher primär über klassische Rechtshilfeersuchen sowie innerhalb der EU im Wege einer Europäischen Ermittlungsanordnung (Richtline 2014/41 EU des Europäischen Parlaments und des Rates vom 3. April 2014). Beide Verfahren sind regelmäßig mit langen Bearbeitungszeiten verbunden[1], da sie die Mitwirkung der Behörden des Vollstreckungsstaates voraussetzen. Diese Vorgehensweise erweist sich schon bei Ersuchen, bei denen es um analoge Beweismittel geht, also solche die an einem bestimmten Ort belegen sind, als problematisch und erschwert die Strafverfolgung erheblich. Geht es jedoch um Daten oder dynamische Cloud-Strukturen als Beweismittel, offenbart sich deutlich, dass die bisherigen Methoden der transnationalen Ermittlungszusammenarbeit zu langsam und schwerfällig sind. Denn ein Ersuchen um digitale Beweismittel richtet sich nicht direkt an den die Daten speichernden Diensteanbieter, sondern zunächst an die zuständige Strafverfolgungsbehörde im Ausland, die eine Prüfung vornimmt und erst dann die Anordnung an den entsprechenden Diensteanbieter weiterleitet. Letzterer hat die Daten sodann an die Strafverfolgungsbehörde im Vollstreckungsstaat herauszugeben, die diese an die ersuchenden Strafverfolger weiterleitet. Dieses langwierige Prozedere führt häufig zum Verlust der relevanten Daten, da diese gelöscht wurden oder aber ihren Speicherort verändert haben. Auf diese Probleme hat der europäische Gesetzgeber mit dem sogenannten E-Evidence-Gesetzespaket reagiert, bestehend aus der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren – kurz E-Evidence-Verordnung – sowie der dazugehörigen Richtlinie (EU) 2023/1544 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren (E-Evidence-Richtlinie). Die Verordnung ist am 18. August 2023 in Kraft getreten, wird jedoch erst ab dem 18. August 2026 in den EU-Mit-

* *Juliane Bentler* ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Strafrecht, Strafprozessrecht und Kriminalpolitik von *Prof. Dr. Anja Schiemann* sowie Mitarbeiterin im Projekt „MAiDA", das von der Europäischen Union gefördert wird.

[1] Rechtshilfeersuchen benötigen bis zu deren Beantwortung durchschnittlich 10 Monate, der Vollzug einer Europäischen Ermittlungsanordnung bis zu 120 Tage; *Hamel*, in: Hoven/ Kudlich (Hrsg.), Digitalisierung und Strafverfahren, 2020, S. 103, 107 f.

gliedstaaten (mit Ausnahme Dänemarks) verbindlich angewendet.[2] Die Richtlinie galt es bis spätestens 18. Februar 2026 durch die Mitgliedstaaten umzusetzen.[3] In Deutschland ist dies durch das Inkrafttreten des Elektronischen-Beweismittel-Umsetzungs- und Durchführungsgesetzes (EBewMG) geschehen.[4]

II. Das E-Evidence Gesetzespaket

1. Die E-Evidence-Verordnung (EU) 2023/1543

Die E-Evidence-Verordnung (2023/1543) des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren[5] vom 12. Juli 2023 betrifft die Herausgabe und Sicherung elektronischer Beweismittel. Ziel ist es, den grenzüberschreitenden Zugang zu digitalen Daten im Rahmen der Strafverfolgung zu erleichtern und diesen schneller als auch wirksamer zu gestalten, was zu einer Verbesserung der Zusammenarbeit zwischen EU-Staaten führen soll. Der umständliche Behördenweg der internationalen Rechtshilfe in Strafsachen soll zukünftig umgangen werden. Hierzu führt die E-Evidence-VO zwei Instrumente ein: die Europäische Herausgabeanordnung (EPOC[6]) sowie die Europäischer Sicherungsanordnung (EPOC-PR[7]).

a) Die Europäische Herausgabeanordnung

Die Europäische Herausgabeanordnung ist gemäß Art. 5 E-Evidence-VO auf die grenzüberschreitende Herausgabe digitaler Beweismittel gerichtet. Sie kann selbständig durch eine Behörde eines Mitgliedstaates im Rahmen eines Strafverfahrens angeordnet werden oder aber an eine durch die Behörde zuvor ergangene Europäische Sicherungsanordnung anknüpfen (Näheres hierzu sogleich unter *b*).[8] Art. 5 Abs. 2 E-Evidence-VO legt als Voraussetzung für den Erlass einer Herausgabeanordnung fest, dass diese hinsichtlich der Betroffenenrechte notwendig und verhältnismäßig sein muss. Zudem darf die Anordnung nur erfolgen, wenn die ermittelnde Behörde in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen eine ähnliche Anordnung hätte erlassen dürfen. Die weiteren Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung hängen von der Art der zu erhebenden Daten ab. Art. 3 Nr. 8 E-Evidence-VO unterscheidet drei Datenkategorien. Elektronische Beweismittel sind demnach Teilnehmerdaten, Verkehrsdaten oder Inhaltdaten, die von einem Diensteanbieter oder in dessen Auftrag in elektronischer Form gespeichert werden. Bei Teilnehmerdaten (Art. 3 Nr. 9 E-Evidence-VO) handelt es sich um Daten, die sich auf die Teilnahme an einem Dienst beziehen. Sie geben Aufschluss über die Identität des Teilnehmers sowie die Art der Dienstleistung (z.B. Name, Adresse, Anmeldedaten, Rechnungsdaten). Verkehrsdaten (Art. 3 Nr. 11 E-Evidence-VO) dienen dazu, Kontext- oder Zusatzinformationen über eine vom Diensteanbieter angebotene Dienstleistung zu geben; hiervon umfasst sind auch Nutzungsdaten. Die dritte Kategorie der Inhaltsdaten (Art. 3 Nr. 12 E-Evidence-VO) bezieht sich auf Daten in einem digitalen Format wie Text, Sprache, Videos, Bilder oder Tonaufzeichnungen, die nicht Teilnehmer- oder Verkehrsdaten sind. Sozusagen als Sonderkategorie werden in Art. 3 Nr. 10 E-Evidence-VO noch solche Daten erwähnt, die ausschließlich zum Zwecke der Identifizierung des Nutzers angefordert werden (z.B. IP-Adressen). Dabei handelt es sich in der Regel um Verkehrsdaten, die aber in ihrer Schutzbedürftigkeit nur den Teilnehmerdaten gleichwertig sind, weshalb es einer Sonderkategorie bedurfte.[9]

Handelt es sich nun bei den angeforderten Daten um Teilnehmerdaten oder solche, die ausschließlich zum Zweck der Identifizierung des Nutzers angefordert werden, so statuiert Art. 5 Abs. 3 E-Evidence-VO, dass deren Herausgabe beim Verdacht aller Straftaten angeordnet werden kann. Anders bei Verkehrs- und Inhaltsdaten: Deren Herausgabe erfordert den Verdacht von Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden (Art. 5 Abs. 4 lit. a E-Evidence-VO) oder dass es sich um Computer- oder Internetstraftaten handelt, die auf einem Unionsrechtsakt basieren (Art. 5 Abs. 4 lit. b E-Evidence-VO).

Darüber hinaus bestimmt die Art der Daten und folglich die Intensität des Eingriffs – Teilnehmerdaten sind als weniger persönlichkeitsrechtssensibel zu qualifizieren als die eingriffsintensiveren Verkehrs- und Inhaltsdaten[10] – welche Strafverfolgungsbehörde als Anordnungsbehörde zum Erlass einer Europäischen Herausgabeanordnung (vgl. Art. 4 E-Evidence-VO) berechtigt ist. So kann eine

---

2 Art. 34 Abs.2 E-Evidence-VO.

3 Art. 7 Abs. 1 E-Evidence-RL.

4 Das Bundesministerium der Justiz (BMJ) hatte im Oktober 2024 einen Referentenentwurf des EBewMG vorgelegt. Nach dem Regierungswechsel im Mai 2025 wurde das Vorhaben erneut aufgegriffen und im Juni 2025 ein neuer Referentenentwurf durch das nunmehr umbenannte Bundesministerium der Justiz und für Verbraucherschutz (BMJV) veröffentlicht. Im Oktober 2025 legte die Bundesregierung auf dem Referentenentwurf basierend einen Gesetzesentwurf vor. Am 12. Januar 2026 fand hierzu eine öffentliche Sachverständigenanhörung im Ausschuss für Recht und Verbraucherschutz statt. Der Bundestag hat am 29. Januar 2026 den Gesetzentwurf zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren innerhalb der Europäischen Union beschlossen. Am 12. März 2026 wurde das Umsetzungsgesetz (EBewMG) im Bundesgesetzblatt veröffentlicht und trat am darauffolgenden Tag in Kraft.

5 Amtsblatt der Europäischen Union 2023 L 191, S. 118; im folgenden E-Evidence-VO.

6 European Production Order; Es sei darauf hingewiesen, dass EPOC in der Literatur meist synonym für die Europäische Herausgabeanordnung verwendet wird. Genau genommen bezeichnet EPOC jedoch die standardisierte Bescheinigung mittels derer eine Europäische Herausgabeanordnung an den Adressaten übermittelt wird. Das gleiche gilt für die Bezeichnung EPOC-PR und die Europäische Sicherungsanordnung (vgl. Art. 9 Abs. 1 E-Evidence-VO).

7 European Preservation Order.

8 Gem. Art. 1 Abs. 2 E-Evidence-VO kann der Erlass einer Europäischen Herausgabe- oder Sicherungsanordnung auch von einem Verdächtigen, Beschuldigten oder in deren Namen von einem Rechtsanwalt beantragt werden.

9 *Rexin*, CR 2024, 64 (66).

10 *Ambos*, ZfIStw 2025, 204 (208 f.).

Herausgabeanordnung bezüglich Teilnehmerdaten oder solchen, die ausschließlich zum Zweck der Identifizierung des Nutzers dienen, nicht nur von einem Richter, sondern ebenso von einem Staatsanwalt erlassen werden (Art. 4 Abs. 1 lit. a E-Evidence-VO). Wird sie von einer anderen im Anordnungsstaat zuständigen Ermittlungsbehörde erlassen, hat eine richterliche oder staatsanwaltschaftliche Validierung zu erfolgen (Art. 4 Abs. 1 lit. b E-Evidence-VO). Im Fall einer Europäischen Herausgabeanordnung Inhalts- und Verkehrsdaten (mit Ausnahme ausschließlich zum Zweck der Identifizierung des Nutzers angeforderter Daten) betreffend, kann diese nur von einem Richter erlassen werden (Art. 4 Abs. 2 lit. a E-Evidence-VO). Bei Erlass durch eine andere Ermittlungsbehörde ist die Prüfung und Validierung durch einen Richter erforderlich (Art. 4 Abs. 2 lit. b E-Evidence-VO).

Elektronische Daten eines Berufsgeheimnisträgers unterliegen besonderen Schutzmechanismen. Art. 5 Abs. 9 E-Evidence-VO regelt, dass im Hinblick auf Berufsgeheimnisträger Inhaltsdaten sowie nicht ausschließlich zur Identifizierung des Nutzers angeforderte Verkehrsdaten nur unter bestimmten Voraussetzungen mittels Europäischer Herausgabeanordnung herausverlangt werden können: wenn der Berufsgeheimnisträger im Anordnungsstaat wohnhaft ist, die Ermittlungen durch eine direkte Adressierung des Berufsgeheimnisträgers gefährdet werden würden oder das Berufsgeheimnis im Einklang mit dem anwendbaren Recht aufgehoben würde.

Ferner unterliegen Verkehrs- und Inhaltsdaten, die durch Immunitäten, Vorrechte oder durch die Presse- und Meinungsfreiheit geschützt sind, restriktiven Anordnungsvoraussetzungen (Art. 5 Abs. 10 E-Evidence-VO). Hier hat die Anordnungsbehörde ein Ermessen hinsichtlich der Sachverhaltsaufklärung. Sie „kann" den Sachverhalt vor Erlass der Herausgabeanordnung klären. Stellt die Anordnungsbehörde fest, dass die geschützten Rechte betroffen sind, darf sie die Anordnung nicht erlassen (Art. 5 Abs. 10 UAbs. 2 E-Evidence-VO).

Der Betroffene, dessen Daten angefordert werden, ist von der Anordnungsbehörde – nicht jedoch vom Diensteanbieter grundsätzlich – unverzüglich zu informieren (Art. 13 Abs. 1 E-Evidence-VO). Art. 13 Abs. 2 E-Evidence-VO sieht vor, dass die Information durch die Anordnungsbehörde aufgeschoben, eingeschränkt oder unterlassen werden kann, soweit diese Maßnahme notwendig und verhältnismäßig ist, etwa zum Schutz der öffentlichen oder nationalen Sicherheit, um die Strafverfolgung nicht zu gefährden oder die Rechte und Freiheiten anderer zu schützen.[11] Eine entsprechende Informationspflicht gegenüber dem Betroffenen besteht nicht hinsichtlich einer Sicherungsanordnung.

b) Die Europäische Sicherungsanordnung

Die Europäische Sicherungsanordnung im Sinne des Art. 6 E-Evidence-VO ermöglicht Strafverfolgungsbehörden eines EU-Mitgliedstaates, die Aufbewahrung digitaler Beweismittel gegebenenfalls bis zum Vorliegen einer Herausgabeanordnung zu verlangen, damit relevante Daten nicht gelöscht werden oder verloren gehen. Sie kann für alle Straftaten erlassen werden, wenn sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können. Außerdem kann eine Sicherungsanordnung zur Vollstreckung von in Strafverfahren ergangenen, mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehender Sicherungsmaßregeln erlassen werden (Art. 6 Abs. 3 E-Evidence-VO). Auf diese Weise können Daten gesichert werden, anhand derer der Aufenthaltsort eines Flüchtigen bestimmt werden kann, um so die Vollstreckung der Freiheitsstrafe zu ermöglichen. Des Weiteren ist sicher zu stellen, dass die Sicherungsanordnung hinsichtlich des Sicherungszwecks – der späteren Herausgabe der Daten – als auch der Beschuldigtenrechte notwendig und verhältnismäßig ist (Art. 6 Abs. 2 E-Evidence-VO).

Anders als bei der Europäischen Herausgabeanordnung wird bei der Sicherungsanordnung nicht nach der Art der Daten differenziert. Sie kann für alle Datenkategorien sowohl durch einen Richter als auch einen Staatsanwalt erlassen werden bzw. muss bei Erlass durch eine andere vom Anordnungsstaat bezeichnete zuständige Behörde richterlich oder staatsanwaltlich geprüft und validiert werden (Art. 4 Abs. 3 E-Evidence-VO).

c) Diensteanbieter als Adressaten

Die E-Evidence-Verordnung richtet sich gemäß Art. 2 Abs. 1 an Diensteanbieter, die ihre Dienste in der Europäischen Union anbieten (Marktortprinzip). Der Sitz oder Speicherort des Diensteanbieters ist irrelevant. Mit dem E-Evidence-Gesetzespaket wurde mithin ein unilaterales Datenzugangsmodell unabhängig vom tatsächlichen Speicherort, der häufig in Drittstaaten wie den USA liegt, gewählt.[12]

Art. 3 Nr. 3 E-Evidence-VO definiert Diensteanbieter als jede natürliche und juristische Person, die eine oder mehrere der in der Verordnung aufgeführten Dienste anbietet. Zu den Dienstleistungskategorien gehören elektronische Kommunikationsdienste (gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste), Internetdomänenamen- und IP-Nummerierungsdienste sowie andere Dienste der Informationsgesellschaft. Letztere Kategorie umfasst auch Diensteanbieter, die zwar nicht als Anbieter elektronischer Kommunikationsdienste

---

11 Art. 13 Abs. 3 RL (EU) 2016/680.

12 *Krumwiede*, ZfIStw 2024, 202 (213); Die E-Evidence-VO kann dabei in einen Konflikt mit dem Recht des Belegenheitsorts der Daten geraten. Geht es bspw. um in den USA gespeicherte Inhaltsdaten, droht eine Normenkollision zwischen unionsrechtlichen Herausgabepflichten und US-amerikanischen Offenlegungsverboten. Denn nach US-Recht ist es amerikanischen Diensteanbietern grundsätzlich untersagt, Daten, die auf Servern in den USA gespeichert sind, an ausländische Strafverfolgungsbehörden herauszugeben. Selbst wenn dies in Zukunft auf Basis einer Europäischen Herausgabeanordnung verlangt wird. Der CLOUD-Act sieht eine Ausnahme von diesem Verbot für den Fall vor, dass ein entsprechendes bilaterales Abkommen mit einer ausländischen Regierung geschlossen wurde. Die Verhandlungen zwischen der EU-Kommission und der amerikanischen Administration zu einem EU-US E-Evidence Abkommen liegen derzeit auf Eis (*Rexin*, CR 2025, 554 [559 f.]; *Krumwiede*, ZfIStw 2024, 202 [213 f.]; *Hüttemann*, NZWiSt 2024, 81 [88]).

gelten, die es den Nutzern aber ermöglichen, miteinander zu kommunizieren, oder die ihnen Dienste anbieten, die für die Speicherung oder anderweitige Verarbeitung von Daten in ihrem Namen genutzt werden können (Art. 3 Abs. 3 lit. c E-Evidence-VO).

Entscheidend ist, dass sowohl die Herausgabe- als auch die Sicherungsanordnung durch eine Anordnungsbehörde in einem EU-Mitgliedstaat unmittelbar an den Diensteanbieter zu richten ist (Art. 7 Abs. 1 E-Evidence-VO), der nach Art. 5 Abs. 6 E-Evidence-VO als Verantwortlicher gilt. Dies markiert einen Paradigmenwechsel, da die grenzüberschreitende Beweiserhebung *„aus der Logik staatlicher Rechtshilfe herausgelöst und in ein hybrides, teilweise privat vermitteltes Vollzugsmodell überführt“*[13] wird. Letztendlich wird die Verantwortung auf private Akteure verlagert. *Hüttemann* fasst treffend zusammen: *„Eine transnational wirksame Verpflichtung ausländischer privater Wirtschaftsteilnehmer ist ein rechtliches Novum im Bereich der justiziellen Zusammenarbeit in Strafsachen. Es ist […] ein weiterer Paradigmenwechsel, weil keine Anerkennung durch justizielle Zusammenarbeit erfolgt, sondern ein Hoheitsakt mit Wirkung auf Territorien anderer Staaten möglich ist.“*[14]

Art. 7 der E-Evidence-VO schreibt vor, dass die Diensteanbieter einen festen Adressaten in der Europäischen Union benennen müssen, an den sich Ermittlungsbehörden zwecks Europäischer Herausgabe- oder Sicherungsanordnung wenden können. Soweit ein Diensteanbieter Niederlassungen innerhalb der EU hat, ist eine davon als Adressat schriftlich zu benennen; andernfalls ist ein gesetzlicher Vertreter in einem EU-Mitgliedstaat zu bestellen.[15] Auf diese Weise kann sichergestellt werden, dass eine Herausgabe- oder Sicherungsanordnung auf Grundlage der E-Evidence-VO zugestellt werden kann. Die Kommunikation zwischen Adressaten und Ermittlungsbehörden soll über ein *„sicheres und zuverlässiges dezentrales IT-System“* (Art. 19 Abs. 2 E-Evidence-VO) erfolgen. Dabei haben die EU-Mitgliedstaaten zu gewährleisten, dass die in dem jeweiligen Mitgliedstaat ansässigen Adressaten Zugang zum dezentralen IT-System über das jeweilige nationale IT-System erhalten (Art. 19 Abs. 2 E-Evidence-VO).

Nach Erhalt einer Europäischen Herausgabeanordnung hat der Adressat sodann sicherzustellen, dass die angeforderten Daten innerhalb von 10 Tagen an die Anordnungsbehörde übermittelt werden, soweit keine Unterrichtung der Vollstreckungsbehörde erforderlich ist[16] (Art. 10 Abs. 3 E-Evidence-VO). In Notfällen beträgt die Übermittlungsfrist maximal acht Stunden (Art. 10 Abs. 4 E-Evidence-VO). Bei einer Sicherungsanordnung ist der Adressat nach Art. 11 E-Evidence-VO dazu verpflichtet, die entsprechenden Daten zunächst für 60 Tage zu sichern. Die Anordnungsbehörde kann die Sicherungsdauer um weitere 30 Tage verlängern, wenn dies für ein anschließendes Herausgabeersuchen erforderlich ist.

Ist der Adressat der Ansicht, die Vollstreckung einer Herausgabe- bzw. Sicherungsanordnung könnte Immunitäten, Vorrechte oder Vorschriften über die Feststellung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Presse- und Meinungsfreiheit in anderen Medien nach dem Recht des Vollstreckungsstaates beeinträchtigen, hat er dies der zuständigen Behörde im Anordnungsstaat als auch im Vollstreckungsstaat mitzuteilen (Art. 10 Abs. 5, Art. 11 Abs. 4 E-Evidence-VO). Zudem kann der Adressat eine Herausgabe- oder Sicherungsanordnung zurückverweisen, wenn sie unvollständig ist, offensichtliche Fehler enthält oder keine ausreichenden Informationen zur Ausführung enthält (Art. 10 Abs. 6 bzw. Art. 11 Abs. 5 E-Evidence-VO). Verletzt der Diensteanbieter die ihn aus der Verordnung treffenden Pflichten, sind gemäß Art. 15 E-Evidence-VO finanzielle Sanktionen vorgesehen. Die Mitgliedstaaten haben Vorschriften zu erlassen, die sicherstellen, dass entsprechende Sanktionen in Höhe von bis zu 2 % des im vorhergehenden Geschäftsjahr weltweit erzielten Jahresgesamtumsatzes des Diensteanbieters verhängt werden können. In Deutschland obliegt es dem Bundesamt für Justiz als zentrale Behörde, die Erfüllung der Pflichten, die sich für die Diensteanbieter ergeben, zu überwachen.[17] Das Bundesamt für Justiz kann von den Diensteanbietern sowohl Auskünfte als auch Nachweise anfordern, insbesondere hinsichtlich der Ausstattung der Adressaten mit den erforderlichen Befugnissen und Ressourcen (§ 6 Abs. 1 S.3 EBewMG).

Wie unter *a)* und *b)* dargestellt, ist Voraussetzung sowohl für den Erlass einer Europäischen Herausgabeanordnung als auch einer Sicherungsanordnung, dass sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können. Art. 5 Abs. 2 E-Evidence-VO schwächt diese Voraussetzung hinsichtlich der Europäischen Herausgabeanordnung etwas ab, indem eine *„ähnliche Anordnung“* hätte erlassen werden dürfen. Zwei Probleme werden in diesem Zusammenhang ersichtlich. Zum einen stellt sich die Frage, was sich der europäische Gesetzgeber unter *„ähnlich“* vorstellt. Eine Definition findet sich hierzu nirgends. Die Formulierung ist derart unpräzise, dass sie den ermittelnden Behörden einen weiten Spielraum lässt, da nicht eindeutig festgelegt wird, was für Fallkonstellationen umfasst werden sollen. Zum anderen bedarf es einer Rechtsgrundlage in den nationalen Strafverfahrensordnungen der Anordnungsstaaten, wenn Voraussetzung für den Erlass einer Europäischen Herausgabe- bzw. Sicherungsanordnung ist, dass dieser in einem vergleichbaren innerstaatlichen Fall zulässig wäre.[18] Für die innerstaatlichen Zuständigkeiten in Deutschland gelten die §§ 94 ff. StPO sowie insbesondere §§ 100j Abs.1 S.1, 100k Abs. 3 StPO im Hinblick auf Herausgabe von Teilnehmerdaten; bei Verkehrs- und Inhaltsdaten ist neben §§ 94 ff. StPO insbesondere auf § 110g

13 *Sinn*, Ausschussdrucksache 21(6)49e, S. 3.
14 *Hüttemann*, NZWiSt 2024, 81 (85).
15 Vgl. auch Art. 3 Abs. 1 E-Evidence-RL.
16 Zur Einbindung und Unterrichtung der Vollstreckungsbehörde sogleich unter *d)*.
17 § 6 Abs. 1 S. 1 EBewMG RefE 2025 zit.: EBewMF-E.
18 *Rexin*, CR 2024, 64 (68).

StPO zu verweisen.[19]

Komplizierter gestaltet sich der Fall hinsichtlich einer Rechtsgrundlage für eine nationale (deutsche) Sicherungsanordnung. Es fehlt an einer Rechtsgrundlage in der StPO, die es deutschen Behörden erlaubt, Sicherungsanordnungen gegenüber Diensteanbietern mit Sitz in Deutschland zu erlassen. Ohne nationales Instrument einer Sicherungsanordnung ist der Erlass einer solchen in Deutschland ausgeschlossen.[20]

Nach dem *„Doppeltürmodell"* des *BVerfG* bedarf es neben einer Ermächtigungsgrundlage für die anordnende Behörde gleichzeitig einer Erlaubnisnorm auf Seiten der Diensteanbieter zur Datenübermittlung bzw. -speicherung. Deshalb sieht das deutsche Umsetzungsgesetz EBewMG die Einfügung zweier neuer Regelungen vor, die er Anbietern von Telekommunikationsdiensten bzw. digitalen Diensten erlauben, Daten im Sinne der E-Evidence-Verordnung zu verarbeiten, soweit dies zur Erfüllung einer Europäischen Herausgabe- oder Sicherungsanordnung erforderlich ist (Näheres hierzu sogleich unter *III. 1.)*.

d) (Fehlende) Einbindung der Vollstreckungsbehörde

Grundsätzlich werden die Behörden im Vollstreckungsstaat in die Abläufe hinsichtlich einer Europäischen Herausgabe- oder Sicherungsanordnung nicht eingebunden. Lediglich bei der Anordnung von Verkehrs-[21] und Inhaltsdaten sieht Art. 8 Abs. 1 der E-Evidence-VO eine Unterrichtung der Vollstreckungsbehörde[22] zeitgleich mit dem Adressaten durch die Anordnungsbehörde vor. Die Unterrichtung der Vollstreckungsbehörde hat – außer in Notfällen – aufschiebende Wirkung (Art. 8 Abs. 4 E-Evidence-VO). Somit erhält die Vollstreckungsbehörde Zeit für eine Überprüfung der Anordnung und kann ggfs. Ablehnungsgründe aus Art. 12 Abs. 1 E-Evidence-VO geltend machen, und zwar innerhalb von 10 Tagen nach Erhalt der Unterrichtung bzw. innerhalb von 96 Stunden in Notfällen.

Zu den möglichen Ablehnungsgründen gehört neben dem Schutz der Daten durch Vorrechte, Immunitäten sowie die Presse- und Meinungsfreiheit auch, dass die Anordnung dem Grundsatz „ne bis in idem" zuwiderlaufen würde, eine Verletzung der europäischen Grundrechte (Art. 6 EUV, Charta) zur Folge hätte oder keine Strafbarkeit im Vollstreckungsstaat besteht[23]. Macht die Vollstreckungsbehörde nicht innerhalb von 10 Tagen nach Erhalt einer Herausgabeanordnung einen der in Art. 12 E-Evidence-VO aufgeführten Ablehnungsgründe geltend, muss der Adressat die angeforderten Daten an die Anordnungsbehörde übermitteln.

Auch bei Verkehrs- und Inhaltsdaten bestehen jedoch Ausnahmen, was die Notifizierung der Vollstreckungsbehörde betrifft. So ist diese dann nicht zu unterrichten, wenn die Anordnungsbehörde zum Zeitpunkt des Anordnungserlasses hinreichende Gründe zu der Annahme hat, dass die Straftat im Anordnungsstaat begangen wurde (oder wahrscheinlich begangen werden wird)[24] und die betroffene Person im Anordnungsstaat ansässig ist (Art. 8 Abs. 2 E-Evidence-VO).

e) Kompetenzgrundlage für die E-Evidence-Verordnung

Es stellt sich bei dem in der E-Evidence-VO vorgesehenen Verfahren die Frage, auf welche Kompetenzgrundlage dieses gestützt wird. Als Ermächtigungsgrundlage zieht die E-Evidence-VO Art. 82 Abs. 1 AEUV heran *(„gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 82 Absatz 1")*[25]. Art. 82 Abs. 1 AEUV erlaubt der Europäischen Union, Maßnahmen zur Förderung der justiziellen Zusammenarbeit in Strafsachen zu erlassen, insbesondere auf Grundlage des Prinzips der gegenseitigen Anerkennung gerichtlicher Entscheidungen.

Die Heranziehung des Art. 82 Abs. 1 AEUV ist in der Literatur nicht unumstritten und teils auf Ablehnung gestoßen. Denn die Norm ist auf Kooperationsmechanismen zwischen Staaten zugeschnitten. Art. 82 Abs. 1 AEUV gilt also lediglich zwischenstaatlich und beruht auf dem Gedanken staatlicher Anerkennung. Private kommen hingegen nicht vor.[26] *Petersen* betrachtet das Verfahren nach der E-Evidence-VO als grundsätzlich unvereinbar mit dem Grundsatz gegenseitiger Anerkennung und folglich Art. 82 Abs. 1 AEUV als nicht taugliche Ermächtigungsgrundlage.[27] Der Vollstreckungsstaat werde *„daran gehindert, seiner Schutzpflicht, die durch die territoriale Beziehung des Diensteanbieters zum Hoheitsstaat ausgelöst wird, gegenüber den von der Anordnung Betroffenen […] im Einzelfall nachzukommen"*.[28] Es bedürfe einer Kontrollmöglichkeit des Vollstreckungsstaates, die zur Ablehnung einer Ermittlungsmaßnahme auf dessen Territorium führen könne. Dieser Kontrollmöglichkeit könne der Vollstreckungsstaat aufgrund der Beschränkung der Unterrichtung auf Verkehrs- und Inhaltsdaten sowie auf bestimmte Vollstreckungshindernisse wie beispielsweise Immunitäten nur sehr eingeschränkt nachkommen.[29] Da-

---

19 *Ambos*, ZfIStw 2025, 204 (208 f.).
20 *Rexin*, CR 2025, 554 (559).
21 Ausgenommen Verkehrsdaten, die ausschließlich zum Zweck der Identifizierung des Nutzers angefordert werden.
22 Als Vollstreckungsbehörde ist gem. Art. 3 Nr. 17 E-Evidence-VO die Behörde im Vollstreckungsstaat zu verstehen, die im Einklang mit dem nationalen Recht dieses Staates für die Entgegennahme einer Europäischen Herausgabeanordnung/ Sicherungsanordnung zuständig ist; In Deutschland soll dies die Staatsanwaltschaft sein (§ 11 Abs. 1 EBewMG-E).
23 Es sei denn, es betrifft eine Katalogstraftat (Anhang IV), die im Anordnungsstaat mit einer Freiheitsstrafe von mindestens drei Jahren bedroht ist (Art. 12 Abs. 1 lit. d E-Evidence-VO).
24 Die Formulierung „wird oder wahrscheinlich begangen werden wird" in Art. 8 Abs. 2 lit. a E-Evidence-VO ist bedenklich, da es um digitale Beweismittel im Rahmen eines Strafverfahrens und folglich um eine bereits konkret begangene Tat geht, nicht aber um präventive Maßnahmen. *Ambos* bezeichnet deshalb die Erweiterung auf zukünftige Taten als „systemwidrig"; *Ambos*, ZfIStw 2025, 204 (213).
25 Amtsblatt der Europäischen Union 2023 L 191, S. 118 oben.
26 *Ambos*, ZfIStw 2025, 204 Fn. 8.
27 *Petersen*, Probleme des transnationalen Zugriffs, 2024, S. 307.
28 *Petersen*, Probleme des transnationalen Zugriffs, S. 306.
29 *Petersen*, Probleme des transnationalen Zugriffs, S. 306f.

mit reduziert die E-Evidence-VO die Rolle des Vollstreckungsstaates und verschiebt die Kompetenzen einseitig zugunsten des Anordnungsstaates. Aus einem System gegenseitiger Anerkennung zwischen Staaten wird nach dieser Auffassung ein Anordnungsmodell gegenüber privaten Diensteanbietern, an welche eine Herausgabe- oder Sicherungsanordnung direkt gerichtet wird – und Art. 82 Abs. 1 AEUV passt infolgedessen nur schwerlich als Kompetenzgrundlage.

Andere Stimmen in der Literatur plädieren für eine flexible Auslegung des Art. 82 Abs. 1 AEUV. Es sei zwar richtig, dass laut der Vorschrift das Prinzip der gegenseitigen Anerkennung als Grundlage für die justizielle Zusammenarbeit in Strafsachen diene. Dabei könne die justizielle Kooperation schon begrifflich Private nicht einbeziehen: *„judicial cooperation, a term that does not suggest the involvement of private parties"*.[30] Das Prinzip der gegenseitigen Anerkennung erlaube gleichwohl eine flexible Auslegung: *„[I]t should be interpreted in a flexible way and that, in this context, there is room for taking into consideration the latest technological developments, including but not limited to the growing importance of cross-border access to e-evidence."*[31] Nach dieser Lesart ist Art. 82 Abs. 1 AEUV weit genug gefasst, um auch neue Formen der Beweisgewinnung zu erfassen. Befürworter einer solchen flexiblen Auslegung der Vorschrift verknüpfen mit der zunehmenden Digitalisierung das Erfordernis einer Weiterentwicklung des Prinzips der gegenseitigen Anerkennung unter digitalen Bedingungen, was durchaus konsequent und nachvollziehbar erscheint.[32] Ferner sehe die Verordnung nicht vollständig von einer Involvierung der Behörden im Vollstreckungsstaat ab und sei damit noch mit dem Grundsatz gegenseitiger Anerkennung vereinbar.[33]

2. Die E-Evidence-Richtline (EU) 2023/1544

Ergänzt wird die E-Evidence-Verordnung durch die E-Evidence-Richtlinie (2023/1544) zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren vom 12. Juli 2023.[34] Gemäß Art. 7 Abs. 1 E-Evidence-RL hat deren Umsetzung in den Mitgliedstaaten bis zum 18. Februar 2026 zu erfolgen: *„Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie bis zum 18. Februar 2026 nachzukommen."*

Zu den zentralen Regelungsinhalten der Richtlinie gehört die Verpflichtung der Diensteanbieter zur Benennung eines gesetzlichen Vertreters in der Europäischen Union (Art. 3 E-Evidence-RL). Dieser Vertreter fungiert als rechtlich verantwortlicher Ansprechpartner für die Entgegennahme, Bearbeitung und Befolgung von Anordnungen nach der Verordnung. Die Richtlinie zielt damit nicht primär auf die inhaltliche Ausgestaltung von Ermittlungsbefugnissen, sondern auf die organisatorische Absicherung ihrer praktischen Wirksamkeit. Sie bewirkt, dass in den EU-Mitgliedstaaten einheitliche Regeln für die Bestellung solcher Vertreter bestehen und dass europäische Ermittlungsbehörden Adressaten für ihre Anordnungen innerhalb der EU haben, selbst wenn es sich um Anbieter aus Drittstaaten handeln sollte.

Des Weiteren regelt Art. 5 der E-Evidence-RL Sanktionen bei Nichtbefolgung und Haftungsregelungen. Die Richtlinie überlässt die konkrete Ausgestaltung der Sanktionen den Mitgliedstaaten, verpflichtet diese jedoch zur Gewährleistung effektiver Durchsetzungsmechanismen. Die von den Mitgliedstaaten festgelegten Sanktionen haben wirksam, verhältnismäßig und abschreckend zu sein. Sie sind für den Fall vorgesehen, dass ein Vertreter gegen seine Pflicht verstößt, im Namen des Diensteanbieters Anordnungen entgegenzunehmen und ihre Einhaltung zu gewährleisten.

Zusammenfassend kann man sagen, die E-Evidence-VO regelt das „Wie" des Zugangs zu digitalen Beweismitteln, während die Richtlinie festlegt, wie die Zuständigkeit („Wer") ausgestaltet werden soll. Die Verordnung schafft somit die Instrumente zur Datenherausgabe und -sicherung. Die Richtlinie hingegen komplettiert die Verordnung, indem sie die effektive Durchsetzbarkeit dieser Instrumente gegenüber Diensteanbietern sicherstellt.

3. Kritische Anmerkungen zum E-Evidence-Gesetzespaket

a) Rechtbehelfe und Grundrechtsschutz

Das E-Evidence-Gesetzespaket hat nicht nur Zustimmung, sondern auch zahlreiche Kritik erfahren. Einer der zentralen Kritikpunkte bezieht sich auf den mit der Verordnung gewährten Rechtsschutz. Art. 47 GRCh statuiert das Recht auf einen wirksamen Rechtsbehelf. Es ist indessen fraglich, ob die E-Evidence-VO den Anforderungen an die Effektivität des Rechtsschutzes nach Art. 47 GRCh gerecht wird. Überdies wirft das neue Verfahren zur digitalen Beweisgewinnung grundrechtliche bzw. datenschutzrechtliche Fragen auf.

Digitale Daten enthalten regelmäßig personenbezogene Informationen und ermöglichen die Preisgabe tiefgreifender Persönlichkeits- und Bewegungsprofile. Sie können soziale Netzwerke, Kommunikationsverhalten sowie individuelle Präferenzen offenlegen. Der Zugriff staatlicher Behörden auf solche personenbezogenen Daten bedeutet einen unmittelbaren Eingriff in das Grundrecht auf Datenschutz und der Eingriffsgehalt ist regelmäßig hoch. Geschützt wird das Grundrecht auf Datenschutz auf europäischer Ebene vor allem durch Art. 8 GRCh (Schutz perso-

30 *Sachoulidou*, NJECL 2024, 256 (265f.).
31 *Sachoulidou*, NJECL 2024, 256 (266).
32 Art. 82 Abs. 2 AEUV kann als Kompetenzgrundlage nicht herangezogen werden, da er sekundärrechtlich nur Richtlinien zulässt, auch wenn die Norm auf den ersten Blick passender erscheinen mag, da sie sich auf die Erleichterung gegenseitiger Anerkennung u.a. in Bezug auf die Zulässigkeit von Beweismitteln bezieht.
33 *Hamel*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 103, 112.
34 Amtsblatt der Europäischen Union 2023 L 191, S. 181; im Folgenden E-Evidence-RL.

nenbezogener Daten) und Art. 7 GRCh (Achtung des Privat- und Familienlebens) sowie die Datenschutz-Grundverordnung (DSGVO, (EU) 2016/679) und die Richtlinie (EU) 2016/680. Infolge der mit der E-Evidence-VO intendierten Effizienzsteigerung in der Strafverfolgung entsteht zwischen dieser und den geschützten Rechtspositionen aus den Art. 7 und 8 GRCh[35] ein Spannungsverhältnis. Insbesondere stellt sich die Frage, inwieweit durch die Einbindung der Diensteanbieter in das Rechtshilfeverfahren und damit der Privatisierung der Rechtshilfe noch ein effektiver Grundrechtsschutz durch die Mitgliedstaaten gewährleistet werden kann. Von zentraler Bedeutung in diesem Zusammenhang ist, welche Rechtsschutzmöglichkeiten den Betroffenen zustehen für den Fall, dass sie sich durch die Datenanforderung bzw. -herausgabe in ihren Grundrechten verletzt sehen.

Gemäß Art. 18 E-Evidence-VO stehen Personen, deren Daten im Wege einer Europäischen Herausgabeanordnung angefordert wurden, wirksame Rechtsbehelfe gegen diese Anordnung zur Verfügung. Verdächtige oder Beschuldigte haben das Recht, während des Strafverfahrens, in welchem die Daten verwendet wurden, wirksame Rechtsbehelfe einzulegen (Art. 18 Abs. 1 E-Evidence-VO). Nach Art. 13 Abs. 3 der Verordnung ist der Betroffene auf die nach Art. 18 verfügbaren Rechtsbehelfe hinzuweisen. Art. 18 Abs. 2 E-Evidence-VO zufolge umfasst das Recht auf Einlegung eines wirksamen Rechtbehelfs die Möglichkeit, die Rechtmäßigkeit der Maßnahme, einschließlich ihrer Notwendigkeit und Verhältnismäßigkeit, anzufechten. Rechtsbehelfe gegen die Europäische Sicherungsanordnung sieht die E-Evidence-VO hingegen nicht vor.

Art. 18 E-Evidence-VO nennt keine formellen oder materiellen Voraussetzungen, sondern verweist vielmehr auf das nationale Recht (*„werden rechtzeitig Informationen über die nach nationalem Recht bestehenden Möglichkeiten zur Einlegung von Rechtsbehelfen bereitgestellt“*, Art. 18. Abs. 3 E-Evidence-VO). Dies wird zur Folge haben, dass die Rechtsbehelfe zwischen den EU-Mitgliedstaaten variieren. Der Rechtsschutz des Betroffenen ist zudem auf Einlegung eines Rechtsbehelfs vor einem Gericht des Anordnungsstaats nach dessen nationalem Recht beschränkt (Art. 18 Abs. Abs. 2 E-Evidence-VO). Dies bedeutet faktisch eine große Hürde für den Betroffenen, der unter Umständen keine Bezüge zum Anordnungsstaat hat. Dass die Verordnung versucht, dem entgegen zu wirken, indem sie den Anordnungsstaat verpflichtet, den Betroffenen (soweit er überhaupt informiert wurde) über die zur Verfügung stehenden Rechtsbehelfe aufzuklären, kann letztlich nicht darüber hinwegtäuschen, dass das Recht auf effektiven Rechtsschutz durch die Verordnung deutlich beschnitten wird.[36] Denn es hängt rein vom Zufall ab, ob dem Betroffenen in dem Staat, in dem er lebt oder in dem seine Daten gespeichert sind, ein Rechtsbehelf zur Verfügung gestellt wird – nämlich dann, wenn es sich zufällig um den Anordnungsstaat handelt.

Die Konzentration des Rechtschutzes primär auf den Anordnungsstaat hat indes auch systematische Gründe, da in der Regel außer dem Anordnungsstaat kein anderer Staat tätig wird, gegen dessen Entscheidung Rechtsbehelfe eingelegt werden könnten. Die E-Evidence-VO *„verabschiedet sich ja gerade von der Notwendigkeit eines Anerkennungsaktes durch den Vollstreckungsstaat wie sonst bei Rechtsakten der gegenseitigen Anerkennung üblich“*[37]. Es geht vielmehr um direkte Rechtshilfe des Diensteanbieters ohne Beteiligung des Vollstreckungsstaates.[38]

Es obliegt auch alleine dem Anordnungsstaat zu prüfen, ob die Anordnung notwendig und verhältnismäßig ist sowie bei der Verhältnismäßigkeitsprüfung die Grundrechte des Beschuldigten zu berücksichtigen (Art. 5 Abs. 2 E-Evidence-VO; vgl. auch *II.1. a)*). In gewissem Umfang ist auch der Diensteanbieter verpflichtet, Grundrechte der Betroffenen zu berücksichtigen (Immunitäten und Vorrechte sowie die Grundrechte auf Meinungs- und Pressefreiheit, Art. 10 Abs. 5 E-Evidence-VO). Das alles mag folgerichtig und in der Verordnung so angelegt sein. Dennoch verbleiben Bedenken angesichts des fehlenden Rechtschutzes im Vollstreckungsstaat und der Kompetenzverlagerung von der klassischen territorialen Schutzfunktion hin zu einem europaweit harmonisierten Modell. Denn der Vollstreckungsstaat ist dazu verpflichtet, *„die Grundrechte der auf seinem Gebiet befindlichen Personen zu achten und zu schützen und auch im Rahmen der grenzüberschreitenden Zusammenarbeit in Strafsachen dafür Sorge zu tragen, dass menschenrechtliche und rechtsstaatliche Mindeststandards gewahrt werden“*[39]. Bereits infolge der automatischen Anerkennung einer Europäischen Herausgabe- oder Sicherungsanordnung kann der Vollstreckungsstaat seiner Verantwortung für den Grundrechtsschutz nicht mehr nachkommen.[40] Verstärkt wird dies durch die Verlagerung des Rechtsschutzes auf den Anordnungsstaat sowie die Verlagerung des Grundrechtsschutzes auf den Anordnungsstaat und private Akteure. Die den Vollstreckungsstaat treffende und aus der Gebietshoheit folgende grundrechtliche Schutzpflicht wird aufgegeben.[41] *Petersen* erwartet ein Absinken des Grundrechtschutzes innerhalb der Europäischen Union als Folge der E-Evidence-VO.[42]

Ebendiese staatliche Schutzpflicht kann weder durch den Anordnungsstaat noch den Diensteanbieter vollständig übernommen werden.[43] So dominiert beim Anordnungsstaat die Ermittlungspflicht und damit ein großes Interesse an der Vollstreckung, was die Grundrechte und den Rechtsschutz des Betroffenen möglicherweise in den Hintergrund treten lassen. Die Diensteanbieter wiederum erhalten keine substantiellen Informationen, die eine Grundrechtsprüfung ermöglichen würden. Außerdem handelt es sich bei den Diensteanbietern um Unternehmen, bei denen vornehmlich wirtschaftliche Interessen im Vordergrund

35 Vergleichbare Garantien finden sich in Art. 6, 8, 13 EMRK.
36 *Hüttemann*, NZWiSt 2024, 81 (91).
37 *Hüttemann*, NZWiSt 2024, 81 (91).
38 *Ambos*, ZfIStw 2025, 204 (216).
39 *Böse*, KriPoZ 2019, 140 (143); ähnlich auch: *Krumwiede*, ZfIStw 2024, 202 (210).
40 *Böse*, KriPoZ 2019, 140 (143).
41 *Hüttemann*, NZWiSt 2024, 81 (92).
42 *Petersen*, Probleme des transnationalen Zugriffs, S. 318.
43 *Petersen*, Probleme des transnationalen Zugriffs, S. 317.

stehen und nicht mögliche Grundrechtsbeeinträchtigungen derjenigen, deren Daten herausgegeben oder gesichert werden sollen. Unternehmen wird es in erster Linie darum gehen, finanzielle Sanktionen zu vermeiden.[44] *Ambos* fasst das Dilemma der Diensteanbieter zutreffend wie folgt zusammen:

„Was die Geltendmachung möglicher Grundrechtsverletzungen durch den privaten Diensteanbieter angeht […], so unterliegt die darin liegende Verlagerung des Grundrechtsschutzes auf einen privaten Akteur („Privatisierung") zunächst grundsätzlichen Bedenken, weil sich einerseits private Akteure grundsätzlich nicht von öffentlichen (sondern eben privaten, geschäftlichen) Interessen leiten lassen und sich andererseits grundrechtliche Schutzpflichten ausschließlich an den Staat richten und sich dieser der daraus erwachsenden Verpflichtung nicht durch Delegation auf Private entziehen kann."[45]

Problematisch ist zudem, dass die Benachrichtigung der betroffenen Person aufgeschoben oder sogar komplett unterlassen werden kann (Art. 13 Abs. 2 E-Evidence-VO, s.o. *II.1. a)*). Erfolgt keinerlei Benachrichtigung, kann der Betroffene keinen Rechtsschutz geltend machen. Erfolgt sie so spät, dass die Maßnahme bereits vollzogen wurde und der Grundrechtseingriff damit irreversibel ist, kommt lediglich ein ex-post-Rechtsschutz infrage, welcher kaum noch korrigierende Wirkung entfalten kann. Es besteht das Risiko eines zwar formal bestehenden, faktisch aber erschwerten Rechtsschutzes.

Art. 47 GRCh verlangt zwar keinen optimalen Rechtsschutz, aber einen effektiven. Dafür genügt die bloße Existenz eines Rechtsbehelfs wie in Art. 18 E-Evidence-VO normiert nicht. Voraussetzung effektiven Rechtsschutzes ist es, dass Betroffene auch tatsächlich in die Lage versetzt werden, ihre Rechte auszuüben. Die E-Evidence-VO schränkt durch die fehlende Transparenz gegenüber betroffenen Personen für diese einen effektiven Rechtsschutz sowie damit einhergehend den Schutz von Grundrechten ein. Zu beachten ist jedoch, dass die Rechtsbehelfe der Verordnung für den Betroffenen nicht abschließend sind, sondern Art. 18 Abs. 1 E-Evidence-VO weitergehende nationale Rechtsbehelfe zulässt (*„Unbeschadet weiterer Rechtsbehelfe, die nach dem nationalen Recht zur Verfügung stehen"*). Somit sind die einzelnen Mitgliedstaaten berufen, im Rahmen ihrer gesetzgeberischen Durchführungsvorschriften einen adäquaten (Grund)Rechtsschutz sicherzustellen.[46]

Wie bereits erwähnt gibt es indes weder einen Rechtsbehelf gegen Sicherungsanordnungen noch einen Verweis auf etwaige nationale Rechtsbehelfe, um die Rechtmäßigkeit einer Europäischen Sicherungsanordnung zu überprüfen. Art. 18 E-Evidence-VO erwähnt lediglich die Europäische Herausgabeanordnung. Zwar haben Sicherungsanordnungen im Vergleich zu Herausgabeanordnungen keine vergleichbare Eingriffsintensität. Nichtdestotrotz handelt es sich um Eingriffe, weshalb *Hüttemann* den generellen Verzicht auf Rechtsbehelfe gegen Europäische Sicherungsanordnungen als primärrechtswidrig erachtet.[47] Ferner sollte einer missbräuchlichen Nutzung der Sicherungsanordnung durch die Strafverfolgungsbehörden vorgebeugt werden, was ebenfalls ein Argument für die Erforderlichkeit ist, *„einen Rechtsbehelf für die Sicherungsanordnung oder zumindest eine inzidente Überprüfung in der anschließenden Herausgabeanordnung vorzusehen"*[48].

Diensteanbietern räumt die E-Evidence-VO lediglich gegen die Sanktionsbeschlüsse bei Nicht-Befolgung einer Herausgabe- oder Sicherungsanordnung Rechtsbehelfe ein (*„Gegen einen Beschluss zur Verhängung einer finanziellen Sanktion muss ein wirksamer Rechtsbehelf eingelegt werden können"*, Art. 16 Abs 10 E-Evidence-VO). Gegen die Anordnung an sich (gegenüber der Anordnungsbehörde) oder ihre Vollstreckung (gegenüber der Vollstreckungsbehörde) steht den Diensteanbietern jedoch kein effektiver Rechtsbehelf zu. Dass für die Diensteanbieter gegen das Vollstreckungsverlangen kein Rechtsbehelf vorgesehen ist, ist kritisch zu betrachten. Denn die Unternehmen sind selbst Adressaten einer belastenden Anordnung und haben als solche ein Grundrecht auf effektiven Rechtsschutz gemäß Art. 47 GRCh. Ein Rechtsbehelf lediglich gegen eventuelle finanzielle Sanktionen ist insoweit nicht ausreichend.[49]

Abschließend sei noch darauf hingewiesen, dass Mitbetroffenen bzw. unbeteiligten Dritten, deren Daten beiläufig mitübermittelt wurden, keinerlei Rechtsbehelfe durch die E-Evidence-VO zur Verfügung gestellt werden.[50] Werden also Daten von Personen herausgegeben, deren Daten nicht angefordert wurden, die aber Bestandteil der angeforderten Daten sind, so besteht für diese mitbetroffenen Personen nach der E-Evidence-VO keine Rechtsschutzmöglichkeit.

b) Beweisverwertungsverbote

Ein weiterer bedeutender Kritikpunkt an der E-Evidence-VO ist das Fehlen von Beweisverwertungsverboten. Der Bereich der Beweisverwertung wird von der Verordnung im Wesentlichen ausgeklammert. Es existiert keine Regelung zur Zulässigkeit bzw. Verwertung rechtswidrig erlangter Daten als Beweismittel; in Bezug auf bestehende Aussage- und Zeugnisverweigerungsrechte sowie Daten anderer schützenswerter Personengruppen wie Journalisten, Rechtsanwälte, Therapeuten etc. ist folglich kein effektiver Grundrechtsschutz gewährleistet.[51] Lediglich Art. 4 Abs. 5 sowie Art. 10 Abs. 4 E-Evidence-VO erwähnen selektive Fälle, bei denen Daten gelöscht werden oder deren Verwendung beschränkt wird. Im Zusammenhang mit den Rechtsbehelfen statuiert Art. 18 Abs. 5 E-Evidence-VO die Verpflichtung der Mitgliedstaaten bei der

44 *Sachoulidou*, NJECL 2024, 256 (268).
45 *Ambos*, ZfIStw 2025, 204 (215).
46 *Hüttemann*, NZWiSt 2024, 81 (92).
47 *Hüttemann*, NZWiSt 2024, 81 (91).
48 *Petersen*, Probleme des transnationalen Zugriffs, S. 329.
49 *Hüttemann*, NZWiSt 2024, 81 (92).
50 *Krumwiede*, ZfIStw 2024, 202 (213).
51 *Thomae*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 139, 143.

Bewertung der ihnen herausgegebenen digitalen Beweismittel, die Verteidigungsrechte zu wahren und ein faires Verfahren zu gewährleisten. Wie genau dies zu geschehen hat, wird nicht präzisiert. Die Verordnung führt hierzu keine Vorgaben oder gar Schutzmaßnahmen an.[52] Hier sind die Mitgliedstaaten aufgerufen, nationale Regelungen, die der praktischen Realisierung dieser Garantien dienen, zu etablieren.

Da sich in der E-Evidence-VO keine konkreten rechtlichen Vorgaben zu Verwertungsverboten finden, sind der Beschuldigte und Betroffene weiterer schützenswerter Personenkreise letztlich auf die ihnen nach dem jeweiligen nationalen Recht zustehenden Einwände beschränkt.[53] Die Verordnung selbst liefert keine Harmonisierung relevanter strafprozessualer Aspekte. An einigen Stellen der Verordnung wird auf das nationale Strafverfahrensrecht (Art. 1 Abs. 2 E-Evidence-VO) oder einen *„vergleichbaren nationalen Fall“* (Art. 5 Abs. 2, Art. 6 Abs. 3 E-Evidence-VO) verwiesen. *Ambos* vertritt die Ansicht, dadurch werde eine Anpassung nationalen Rechts impliziert. Es würden Mindestbestimmungen festgelegt, die einer faktischen Harmonisierung gleichkämen.[54] Ob hierin tatsächlich erste Harmonisierungsversuche in Form von Mindestbestimmungen zu erblicken sind, bleibt fraglich. Zu bedenken ist in diesem Kontext außerdem, dass eine solche Harmonisierung nur durch Richtlinien herbeigeführt werden kann, wie Art. 82 Abs. 2 AEUV festlegt.

Auch *Sachoulidou* vertritt im Gegensatz zu *Ambos* eine eher kritische Sichtweise und betrachtet das Fehlen einheitlicher Regelungen hinsichtlich von Beweisverwertungsverboten als großes Manko: *„This provision, however, may be turned into empty words in the absence of specific regulation that takes into account the particularities of e-evidence, given, inter alia, the real risk of tampering with such evidence and the strong interference with the rights of suspects and accused persons or third parties that communicate with them, as well as in the absence of harmonised rules on the admissibility of evidence in general and e-evidence in particular.”*[55]

Es bleibt abschließend festzuhalten, dass das Fehlen expliziter Beweisverwertungsverbote eine Schutzlücke entstehen lässt, da die Folgen rechtswidriger digitaler Beweiserhebung nicht unionsweit einheitlich geklärt sind. Die damit verbundene Verlagerung von Verwertungsentscheidungen auf die nationalen Rechtsordnungen kann zu divergierenden Standards führen und wirft Fragen auf hinsichtlich der effektiven Gewährleistung der Verteidigungsrechte und des fairen Verfahrens aus Art. 18 Abs. 5 E-Evidence-VO. Um ein ausgewogenes Verhältnis zwischen effektiver Strafverfolgung und Grundrechtsschutz sicherzustellen, wäre eine stärkere Harmonisierung in diesem Bereich begrüßenswert.[56]

III. Das Elektronische-Beweismittel-Umsetzungs- und Durchführungsgesetz (EBewMG)

1. Allgemeines zum EBewMG

Gem. Art. 7 E-Evidence-RL waren die EU-Mitgliedstaaten dazu angehalten, die zur Umsetzung der Richtlinie erforderlichen Vorschriften bis zum 18. Februar 2026 zu erlassen. Zur Umsetzung der E-Evidence-RL und Durchführung der E-Evidence-VO hat das Bundesministerium der Justiz und für Verbraucherschutz zunächst im Juni 2025 einen Referentenentwurf vorgelegt. Dieser basiert auf dem der Diskontinuität unterfallenen Referentenentwurf der vergangenen Legislaturperiode und berücksichtigt Forderungen der Justizministerkonferenz aus dem Herbst 2024. Auf Grundlage des Referentenentwurfs hat die Bundesregierung am 8. Oktober 2025 einen Gesetzesentwurf für das geplante Stammgesetz vorgelegt.[57] Der Gesetzentwurf zum EBewMG wurde am 29. Januar 2026 vom Bundestag verabschiedet und am 12. März mit Veröffentlichung im Bundesgesetzblatt verkündet. Gem. Art. 4 Abs. 1 EBewMG trat das Gesetz am Tag nach der Verkündung, dem 13. März 2026, in Kraft, womit die in der E-Evidence-RL vorgegebene Umsetzungsfrist nicht eingehalten wurde. Darüber hinaus statuiert Art. 4 Abs. 2 EBewMG für die §§ 7 bis 17, 18 Abs. 2, 3 Nr. 1 b) und Nr. 2, Abs. 4 bis 7 sowie 8 Nr. 2 und § 19 des Art. 1 und Art. 3 das Inkrafttreten am 18. August 2026 – dem Tag, an dem die E-Evidence-VO in den EU-Mitgliedstaaten verbindlich wird.

Mit dem Stammgesetz erfolgt die Integration des E-Evidence-Mechanismus in das deutsche Recht. Neben der Schaffung des Elektronischen-Beweismittel-Umsetzungs- und Durchführungsgesetzes (EBewMG) sieht der Gesetzesentwurf Änderungen im Telekommunikationsgesetz (TKG) sowie im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) vor.

Das EBewMG gliedert sich in insgesamt vier Teile. Der erste Teil beinhaltet allgemeine Regelungen, die für das gesamte Stammgesetz geltende Begriffsbestimmungen festlegen. Teil 2 betrifft die Umsetzung der Richtlinie 2023/1544 und damit die Umsetzung der europäischen Vorgaben in das nationale Recht. In Teil 3 finden sich Durchführungsvorschriften, mit Hilfe derer die E-Evidence-VO 2023/1543 in das bestehende deutsche Regelungsgerüst eingebettet wird. Der vierte Teil schließlich umfasst Bußgeldvorschriften sowie die Einschränkung eines Grundrechts. Die Bußgeldvorschriften geben vor, wie Zuwiderhandlungen der Diensteanbieter gegen die ihnen auferlegten Pflichten aus dem Stammgesetz sowie der E-Evidence-VO zu ahnden sind. § 19 in Teil 4 legt die Einschränkung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG nach Maßgabe des Gesetzes fest.

---

52 *Okunrobo Perez*, EJCCLJ 2025, 187 (195).
53 *Hüttemann*, NZWiSt 2024, 81 (92).
54 *Ambos*, ZfIStw 2025, 204 (212).
55 *Sachoulidou*, NJECL 2024, 256 (272f.).
56 Ansonsten müsste eine präzisierende Auslegung durch die Rechtsprechung erfolgen.
57 Der Gesetzentwurf der Bundesregierung stimmt weitestgehend mit dem Referentenentwurf 2025 überein. Es sind jedoch kleinere Änderungen wie die Einfügung des § 19 (Einschränkung eines Grundrechts) in Teil 4 erfolgt.

Art. 2 des EBewMG sieht Änderungen im TKG vor. Da die Regelungen des TKG im Widerspruch zu Art. 1 Abs. 4 der E-Evidence-RL stehen, indem sie über die Vorgaben der Richtlinie hinausgehende Verpflichtungen für Diensteanbieter statuieren, werden in einem dem TKG einzufügenden § 170 Abs. 12 die Regelungen des § 170 Abs. 1 Nr. 3 b) als auch Abs. 2 Nr. 2 c) im Anwendungsbereich der E-Evidence-RL für unanwendbar erklärt.

Im Gegensatz zum Referentenentwurf aus dem Jahr 2024 hat der Entwurf von 2025 und damit das letztlich verkündete Gesetz einige Neuerungen erfahren. So wurde mit § 8 eine Zuordnung der in der E-Evidence-VO definierten Arten der elektronischen Beweismittel zu den Datenkategorien des deutschen Rechts eingefügt. Ziel dieser Zuordnung ist es, für Anwendungssicherheit zu sorgen. Diese besteht für Diensteanbieter darin, dass sie eine bestehende Klassifizierung ihres Datenbestands nach nationalen Kategorien nun systematisch auf die Datenkategorien der E-Evidence-VO übertragen können. Für Behörden ist die Zuordnung insofern hilfreich, als sie vor Erlass einer Europäischen Herausgabe- oder Sicherungsanordnung zu prüfen haben, ob eine vergleichbare Anordnung auch nach nationalem Recht zulässig wäre (vgl. Art. 5 Abs. 2, Art. 6 Abs. 3 E-Evidence-VO). Die Zuordnung der Datenkategorien erleichtert es den Behörden insoweit, die einschlägige nationale Rechtsgrundlage zu identifizieren.[58] Keine Berücksichtigung finden allerdings die in der E-Evidence-VO ebenfalls definierten Inhaltsdaten.

Überdies sieht das neue Stammgesetz die Einfügung zweier neuer Regelungen im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) vor, wie Art. 3 zu entnehmen ist.[59] Durch die geplante Erweiterung des TDDDG um zwei spezifische datenschutzrechtliche Befugnisnormen – §§ 13a, 24a TDDDG – wird es den Anbietern von Telekommunikationsdiensten sowie von digitalen Diensten ermöglicht, personenbezogene Daten im Zusammenhang mit der Ausführung einer Europäischen Herausgabe- oder Sicherungsanordnung gemäß der E-Evidence-VO rechtmäßig zu verarbeiten. Diese Ergänzung geht das unter *II.1.c)* identifizierte Problem einer in Deutschland fehlenden, aber vor dem Hintergrund der *„Doppeltür-Rechtsprechung"* des *BVerfG* erforderlichen Rechtsgrundlage, für die Datenübermittlung durch die Diensteanbieter an.[60] Die Erweiterung des TDDDG verfolgt demnach das Ziel, eine klare Grundlage für die Mitwirkung privater Diensteanbieter an unionsweit harmonisierten Maßnahmen im digitalen Kontext zu schaffen.[61]

Abschließend sei noch darauf hingewiesen, dass das EBewMG sich auf die Europäische Herausgabeanordnung beschränkt und keine speziellen Regelungen zur Europäischen Sicherungsanordnung enthält. Es sind keine Vorschriften für den Erlass von Sicherungsanordnungen durch deutsche Behörden gegenüber Adressaten im EU-Ausland vorgesehen.[62] Grund hierfür dürfte sein, dass es weiterhin an einer deutschen Rechtsgrundlage fehlt, die es deutschen Behörden erlaubt, Sicherungsanordnungen gegenüber Diensteanbietern mit Sitz in Deutschland zu erlassen (Vgl. *II.1.c)*). Eine solche Rechtsgrundlage wäre aber gem. Art. 6 Abs. 3 E-Evidence-VO unionsrechtlich erforderlich. Somit werden deutsche Behörden keine Europäischen Sicherungsanordnungen erlassen dürfen, wohingegen ein solcher Erlass anderen europäischen Strafverfolgungsbehörden gegenüber deutschen Adressaten möglich ist.[63]

2. Kritik am EBewMG

Das EBewMG bzw. vorab der Gesetzentwurf ist, ähnlich wie die E-Evidence-VO, in der Literatur Kritik ausgesetzt gewesen. Nochmals besonders deutlich zum Ausdruck gekommen sind die maßgeblichen Kritikpunkte insbesondere in der Anhörung verschiedener Sachverständiger[64] im Ausschuss für Recht und Verbraucherschutz vom 12. Januar 2026, bevor der Gesetzentwurf am 29. Januar 2026 in den Bundestag zur Abstimmung eingebracht wurde. Deren Ausführungen haben etwaige Schwächen des EBewMG verdeutlicht.

Einer der zentralen Kritikpunkte am Gesetz ist die Verkürzung des Rechtsschutzes. Wie unter *II.3.a)* dargelegt, sieht Art. 18 der E-Evidence-VO zwar ausdrücklich einen Rechtsbehelf vor. Der Betroffene wird dabei aber auf den Rechtsweg im Anordnungsstaat verwiesen. Eine Kompensation des fehlenden Rechtsschutzes im Vollstreckungsstaat wird durch das EBewMG nicht erreicht. Im Übrigen beschränkt das Umsetzungsgesetz in §§ 13,14 den Rechtsschutz, wie auch Art. 18 E-Evidence-VO, auf Herausgabeanordnungen. Der Referentenentwurf von 2024 hatte noch die Europäische Sicherungsanordnung einbezogen. Dies wurde im Gesetzentwurf 2025 aufgegeben, da es in Deutschland derzeit an einer Rechtsgrundlage für eine Sicherungsanordnung fehlt.[65]

§ 13 EBewMG sieht abgestufte Überprüfungsmöglichkeiten durch Gerichte vor, wobei nach Datentyp differenziert und jeweils auf die Regelungen der StPO verwiesen wird.

---

58 *Rexin*, CR 2025, 554 (555); Die Regelung des § 8 EBewMG wird auch kritisch gesehen: „So dürfte es unionsrechtlich unzulässig sein, Datenkategorien der E-Evidence-Verordnung unter Verweis auf Legaldefinitionen des nationalen Rechts zu bestimmen." (*Holling*, Ausschussdrucksache 21[6]49b, S. 8).

59 Der Referentenentwurf von 2024 sah die Einfügung dieser Rechtsnormen noch nicht vor.

60 *Rexin*, CR 2025, 554 (556).

61 *Rexin* wendet hinsichtlich der geplanten Rechtsgrundlagen ein, die Erlaubnis zur Datenverarbeitung würde im Grunde an die falschen Akteure erteilen. Es seien nicht die Diensteanbieter, die der Erlaubnis zur Verarbeitung der Daten bedürften, sondern die Adressaten. Die für das TDDDG geplanten §§13a und 24a würden jedoch für die Adressaten lediglich „dann eine taugliche Übermittlungsgrundlage darstellen, wenn Diensteanbieter und Adressat personenidentisch sind – was regelmäßig nicht der Fall sein wird" (*Rexin*, CR 2025, 554 [556]). Es ist aber sicherlich davon auszugehen, dass man beim Entwurf der entsprechenden Normen mit der Bezeichnung „Anbieter für Telekommunikationsdienste" sowie „Anbieter für digitale Dienste" letztendlich auch die Adressaten im Sinn hatte.

62 Die im Entwurf von 2024 enthaltene Regelung für Sicherungsanordnungen (§ 9) wurde gestrichen.

63 *Rexin*, CR 2025, 554 (559).

64 Zu den Sachverständigen gehörten *Prof. Dr. Dr. Kai Ambos* (Universität Göttingen), *Leonora Holling* (BRAK), *Kai Kempgens* (DAV), *Sven Kurenbach* (BKA) *Sebastian Murer* (GenStA München), *Dr. Anna Oemichen* (Freie Universität Berlin), *Prof. Dr. Arndt Sinn* (Universität Osnabrück).

65 *Ambos*, Ausschussdrucksache 21(6)49f, S. 18

Gegen Herausgabeanordnungen zu Teilnehmerdaten und Daten, die ausschließlich der Identifizierung des Nutzers dienen, soll die gerichtliche Entscheidung nach § 98 Abs. 2 S. 2 StPO beantragt werden können. Ferner verweist § 13 Abs. 1 EBewMG auf die Beschwerde nach § 304 StPO, die grundsätzlich schon vor dem tatsächlichen Vollzug einer Maßnahme eröffnet ist. Für Verkehrs- und Inhaltsdaten hingegen normiert § 13 Abs. 2 und 3 EBewMG nur nachträglichen Rechtsschutz. Für diese Datenkategorien wird der Rechtsschutz im EBewMG an die Regelungen angelehnt, die für verdeckte Ermittlungsmaßnahmen wie die Telekommunikationsüberwachung konzipiert wurden und in der Regel einen nachträglichen Rechtschutz vorsehen. Folglich knüpft die Umsetzung nicht primär an die Eingriffsintensität der Maßnahme an, sondern an die betroffenen Datenkategorien.[66] Und genau in diesem Punkt zeigt sich ein strukturelles Defizit des Gesetzes: *„Die grundrechtsintensivsten Maßnahmen – namentlich die Herausgabe von Inhaltsdaten aufgrund einer ausgehenden Anordnung – unterliegen nach dem deutschen Entwurf lediglich einem nachträglichen Rechtsschutz."*[67] Entsprechend greift der in § 13 Abs. 2 und 3 vorgesehene Rechtschutz erst, *„nachdem der zentrale Grundrechtseingriff – die Offenbarung und Kenntnisnahme der Inhalte – bereits erfolgt ist. Ein nachträglicher Rechtsbehelf kann diese Kenntnisnahme nicht verhindern und den Eingriff nicht rückgängig machen, sondern lediglich ex post bewerten. Der Rechtsschutz verliert damit seine präventive Schutzfunktion und reduziert sich faktisch auf eine nachträgliche Feststellung, ohne den Eingriff in dem Zeitpunkt abwehren zu können, in dem der Grundrechtsschutz praktisch wirksam sein müsste."*[68]

In diesem Zusammenhang wird weiterhin kritisiert, das deutsche Umsetzungsgesetz stehe im Widerspruch zum erklärten Ziel der E-Evidence-VO, Grundrechte zu wahren und betroffenen Personen einen wirksamen Rechtsbehelf zur Verfügung zu stellen.[69] Denn die E-Evidence-VO differenziert in Art. 18 nicht nach Datenkategorien, während das EBewMG den stärksten Rechtsschutz bei der geringsten Eingriffsintensität gewährt und ihn bei Inhaltsdaten auf eine nachgelagerte Kontrolle beschränkt. Kritiker sehen hierin einen Widerspruch zum unionsrechtlichen Effektivitätsgebot aus Art. 47 GRCh.[70] Allerdings wird schon die E-Evidence-VO den Anforderungen an die Effektivität des Rechtsschutzes nach Art. 47 GRCh nicht gerecht angesichts der in der Verordnung vorgesehenen Konzentration des Rechtsschutzes primär auf den Anordnungsstaat sowie die fehlende Transparenz gegenüber betroffenen Personen (vgl. *II.3.a)*). Der Forderung von *Hüttmann*,[71] die Mitgliedsstaaten mögen das Defizit der Verordnung beheben, indem sie in ihren nationalen Durchführungsvorschriften einen adäquaten Rechtsschutz sicherstellen, kommt Deutschland mit dem EBewMG nicht nach.

Ein weiterer Kritikpunkt in Bezug auf den Rechtsschutz betrifft den Verzicht auf einen Rechtsbehelf zur Überprüfung von Ermessensentscheidungen der Vollstreckungsbehörde. Dies könne zur Rechtsunsicherheit führen.[72] Hatte der Referentenentwurf von 2024 noch einen moderaten Rechtsbehelf vorgesehen, mit dem nach Übermittlung der Daten an den Anordnungsstaat eine gerichtliche Überprüfung stattfinden können sollte, ob die Nichtgeltendmachung von Ablehnungsgründen rechtskonform war, sieht das EBewMG keine gerichtliche Entscheidung über ermessensfehlerhaft nicht von der Vollstreckungsbehörde geltend gemachte Ablehnungsgründe nach Art. 12 E-Evidence-VO mehr vor. Nach Ansicht von *Weiß* wäre ein entsprechender Rechtsbehelf jedoch rechtsstaatlich geboten.[73] Sie führt in ihrer kritischen Bewertung weiter aus: *„Ein klar normierter Rechtsbehelf gegen eine behördliche Untätigkeit im Falle drohender elementarer Grundrechtsverletzung würde angesichts der erforderlichen Überprüfbarkeit im Hinblick auf Art. 19 IV GG für Rechtssicherheit sorgen, und es deutschen Gerichten ermöglichen, etwaige Streitfragen im Hinblick auf den Anwendungsbereich des Art. 12 VO (EU) 2023/1543 dem EuGH vorzulegen."*[74]

Ferner wird in der Literatur sowie von einigen Sachverständigen kritisch eingewandt, dass auch für Daten von Berufsgeheimnisträgern eine Regelung zu deren Schutz im EBewMG wünschenswert wäre.[75] Zwar finden sich in Art. 5 Abs. 9 E-Evidence-VO Schutzmechanismen für Daten von Berufsgeheimnisträgern. Diese sind jedoch an enge Voraussetzungen geknüpft und beziehen sich lediglich auf Fälle, in denen gemäß dem Recht des Anordnungsstaates Daten vom Berufsgeheimnis geschützt sind. Eine Regelung für Daten von Berufsgeheimnisträgern im Vollstreckungsstaat existiert nicht. Nach allgemeiner Ansicht unterfällt auch der Schutz von Kommunikation von Berufsgeheimnisträgern dem Art. 12 Abs. 1 lit. a E-Evidence-VO.[76] Da ein Rechtsbehelf zur Überprüfung von Ermessensentscheidungen der Vollstreckungsbehörde im EBewMG fehlt, ist nicht einmal die Möglichkeit gegeben, im Vollstreckungsstaat nachträglich gerichtlich überprüfen zu lassen, ob durch den Datenzugriff ein Grundrechtsverstoß vorliegt. Um einen ausreichenden Schutz gegen die Erlangung vom Berufsgeheimnis geschützter Daten zu gewährleisten, müssten auf nationaler Ebene mit dem EBewMG effektive Kontrollmöglichkeiten für Betroffene eingeführt werden, was nicht der Fall ist.[77]

66 *Sinn*, Ausschussdrucksache 21(6)49e, S. 5.
67 *Sinn*, Ausschussdrucksache 21(6)49e, S. 5.
68 *Sinn*, Ausschussdrucksache 21(6)49e, S. 5.
69 *Oemichen*, Ausschuss für Recht und Verbraucherschutz, Wortprotokoll der 20. – öffentlichen – Sitzung vom 12. Januar 2026, S. 15, online abrufbar unter: https://bit.ly/41TrFIr (zuletzt abgerufen am 27.4.2026).
70 *Sinn*, Ausschussdrucksache 21(6)49e, S. 5 f.; *Oemichen*, Ausschuss für Recht und Verbraucherschutz, Wortprotokoll der 20. – öffentlichen – Sitzung vom 12. Januar 2026, S. 14 f.
71 *Hüttemann*, NZWiSt 2024, 81 (92).
72 *Holling*, Ausschussdrucksache 21(6)49b, S. 5.
73 *Weiß*, ZRP 2025, 218 (220).
74 *Weiß*, ZRP 2025, 218 (220).
75 *Weiß*, ZRP 2025, 218 (220); *Holling*, Ausschussdrucksache 21(6)49b, S. 6.
76 *Holling*, Ausschussdrucksache 21(6)49b, S. 6.
77 *Weiß,* ZRP 2025, 218 (220).

Aufgrund der Tatsache, dass der Vollzug einer Europäische Herausgabeanordnung regelmäßig ohne vorgelagerte Kontrolle des Vollstreckungsstaates erfolgt, kommt der gerichtlichen Entscheidung im Anordnungsstaat besondere Bedeutung zu. Die E-Evidence-VO trägt dem in Art. 4 und 5 Rechnung, indem sie dort materielle und formelle Voraussetzungen für den Erlass einer Herausgabeanordnung normiert und diese einer gerichtlichen Überprüfung unterstellt.[78] Das deutsche Umsetzungsgesetz greift diese Vorgaben in § 14 EBewMG auf. Mit Blick auf § 14 Abs. 2 EBewMG wird deutlich, dass das neue Stammgesetz – anders als noch der Entwurf von 2024 – keine Löschung der erlangten Daten sowie ein Verwendungsverbot vorsieht, für den Fall der gerichtlich festgestellten Rechtswidrigkeit und Aufhebung der Herausgabeanordnung. Vor allem das Fehlen eines Verwendungsverbotes ist bedenklich, da die Kenntnisnahme rechtswidrig erlangter Daten faktisch irreversibel ist. Insofern bleibt der Gesetzentwurf hinter den Vorgaben der E-Evidence-VO zurück, die zumindest stellenweise Löschungsvorschriften (Art. 4 Abs. 5, 10 Abs. 4) bestimmt. Diese Reduktion der Rechtsfolgen rechtswidrig erlangter Daten wird als problematisch erachtet. Die gerichtliche Entscheidung bleibe in ihren praktischen Wirkungen unbestimmt und reduziere sich normativ auf eine deklaratorische Feststellung, indem die Rechtswidrigkeit der Datenherausgabe ohne Konsequenzen bleibe und die herausgegebenen Daten weiterhin verwendbar seien. Rechtsunsicherheit sei die Folge.[79]

Überdies wird in diesem Zusammenhang eingewandt, dass das EBewMG keine Regelung für solche Fälle vorsehe, in denen über eine Europäische Herausgabeanordnung erlangte Daten für andere Verfahren relevant sein könnten. Für den Fall solcher Zufallsfunde sei eine Umwidmung der Beweismittel immer grundrechtsrelevant.[80]

Weitere Kritikpunkte betreffen den Mehraufwand für die Staatsanwaltschaften sowie die Frage, ob die Staatsanwaltschaften geeignete Vollstreckungsbehörden sind. Auf die Staatsanwaltschaften komme ein erheblicher zusätzlicher Arbeitsaufwand bei der Durchführung und Umsetzung des E-Evidence-Pakets zu. Dieser betreffe die Prüfung von eigenen Herausgabeanordnungen als auch die Prüfung von Ablehnungsgründen bei aus dem Ausland eingehenden Anordnungen im Rahmen der Unterrichtung der Vollstreckungsbehörde. Zudem seien die Staatsanwaltschaften als Vollstreckungsbehörden für die Vollstreckung bei Verletzung der Mitwirkungspflichten durch den Diensteanbieter, insbesondere bei den Bußgeldern nach § 18 EBewMG zuständig. Ohne erhöhte Unterstützung sei dies kaum zu bewältigen.[81]

Es sei ferner zweifelhaft, ob die Staatsanwaltschaften grundsätzlich, wie § 11 EBewMG festlegt, als geeignete Vollstreckungsbehörden anzusehen seien. Da der Gesetzentwurf keinen Rechtsbehelf hinsichtlich der (Nicht-)Geltendmachung von Ablehnungsgründen nach Art. 12 E-Evidence-VO enthalte, sei es „bedenklich, wenn ausschließlich die Staatsanwaltschaft zur Entscheidung berufen ist, wenn ein derart schwerwiegender Grundrechtseingriff, wie z.B. der Eingriff in privilegierte Inhaltsdaten von Anwälten und Journalisten, im Raum steh[e]. Eine derart schwerwiegende Entscheidung […] erfordert die gerichtliche Beteiligung“[82].

IV. Schlussbemerkungen

Zusammenfassend lässt sich feststellen, dass das E-Evidence-Paket einerseits einen bedeutenden Fortschritt für die grenzüberschreitende Strafverfolgung in der Europäischen Union darstellt und eine Effizienzsteigerung bei der Bekämpfung grenzüberschreitender Kriminalität erzielt. Der neue rechtliche Rahmen für den grenzüberschreitenden Zugriff auf digitale Beweismittel in Strafverfahren kann zur nachhaltigen Bekämpfung von Straftaten beitragen. Denn durch die Schaffung einheitlicher Verfahren zum Datenzugriff innerhalb der EU werden Ermittlungen in Strafverfahren effizienter, schneller und weniger abhängig von langwierigen Rechtshilfeverfahren. Das E-Evidence-Gesetzespaket ist somit eine konsequente Reaktion auf technische Veränderungen im digitalen Zeitalter, in dem es kaum noch Strafverfahren gibt, in welchen keine elektronischen Beweismittel relevant sind.

Gleichzeitig wirft das E-Evidence-Paket wichtige Fragen auf hinsichtlich Grundrechtsschutz, Datenschutz und Rechtsschutz insbesondere für betroffene Personen, deren Daten gesichert oder herausgegeben werden. Es erscheint fraglich, ob die in der Verordnung vorgesehenen Schutzmechanismen ausreichen, ein Absinken des Grundrechtsschutzes in der EU zu verhindern. In diesem Zusammenhang weist die E-Evidence-Verordnung zu viele Defizite auf. Das betrifft einmal die Einbindung der Diensteanbieter in das Verfahren und die daraus folgende Privatisierung der Rechtshilfe. Die grundrechtliche Schutzpflicht obliegt dem Staat und kann nicht auf private Akteure, die von wirtschaftlichen Interessen geleitet werden, übertragen werden. Im Übrigen sind diese privaten Akteure nicht einmal verpflichtet, die Voraussetzungen für den Erlass einer Anordnung umfassend zu prüfen oder individualschützende Ablehnungsgründe geltend zu machen. Grundrechte der Betroffenen sind durch die Diensteanbieter lediglich in eingeschränktem Umfang zu berücksichtigen (vgl. Art. 10 Abs. 5 E-Evidence-VO). Überdies sind die Diensteanbieter dem Druck unterworfen, Sanktionen zu vermeiden, weshalb sie im Zweifel den Herausgabeverlangen nachkommen dürften. Auf der anderen Seite erfordert die Erhebung digitaler Beweismittel aufgrund der Flüchtigkeit der Daten die Einbindung privater Diensteanbieter in das Rechtshilfeverfahren. Die teilweise Privatisierung der Rechtshilfe ist insoweit unumgänglich.

---

78 Eine Herausgabeanordnung zur Erlangung von Teilnehmerdaten oder Daten, die ausschließlich der Identifizierung des Nutzers dienen, kann jedoch auch von einem Staatsanwalt erlassen bzw. validiert werden (vgl. auch *II.1.a*).

79 *Sinn*, Ausschussdrucksache 21(6)49e, S. 7; *Ambos*, Ausschussdrucksache 21(6)49f, S. 18; *Kempgens*, Ausschussdrucksache 21(6)49a, S. 3; *Weiß*, ZRP 2025, 218 (220).

80 *Kempgens*, Ausschussdrucksache 21(6)49a, S. 3.

81 *Murer*, Ausschussdrucksache 21(6)49d, S. 6.

82 *Holling*, Ausschussdrucksache 21(6)49b, S. 5.

Verstärkt wird das Problem des Grundrechtsschutzes auch durch die Verlagerung der Kontrollkompetenz vom Vollstreckungsstaat auf den Anordnungsstaat, wodurch der Vollstreckungsstaat seiner Verantwortung für den Grundrechtsschutz nicht mehr nachkommen kann. Andererseits soll gerade die eingeschränkte Einbindung der Behörden des Vollstreckungsstaates die langen Bearbeitungszeiten für Rechtshilfeersuchen deutlich verkürzen.

Ebenso sind Nachbesserungen im Rechtsschutz erforderlich. Zur Wahrung der Betroffenenrechte sind hinreichende Rechtsbehelfe und Beweisverwertungsverbote erforderlich.

Hier hätte der deutsche Gesetzgeber mit dem EBewMG ansetzen und mittels nationaler Vorschriften einen adäquaten Rechtsschutz sicherstellen können, was nicht überzeugend gelungen ist. Die Problematik der Verwendung rechtswidrig erlangter Daten wurde mit dem neuen Umsetzungsgesetz ebenso wenig angegangen. § 14 EBewMG müsste ergänzt werden, um zu gewährleisten, dass Daten, die mittels eine rechtswidrigen Herausgabeanordnung erlangt wurden, in einem Strafverfahren nicht verwendet werden dürfen.[83]

Insgesamt wurde mit dem E-Evidence-Paket ein entscheidender Schritt in die richtige Richtung eingeschlagen, da es den rechtlichen Rahmen an die digitale Realität anpasst und die Zusammenarbeit zwischen den Mitgliedstaaten stärkt. Die klassische zwischenstaatliche Rechtshilfe ist den Anforderungen von Strafverfahren, bei denen digitale Beweismittel im Vordergrund stehen, nicht mehr gewachsen. Dennoch wäre es verfrüht bei dem E-Evidence-Gesetzespaket von einem Meilenstein der grenzüberschreitenden Strafverfolgung in der Europäischen Union zu sprechen. Derzeit existieren noch zu zahlreiche Kritikpunkte, die das E-Evidence-Paket von einem wirklichen Meilenstein trennen. Letztlich ist aber ungewiss, ob das Spannungsverhältnis zwischen einer schnellen und effizienten Strafverfolgung auf der einen Seite sowie einem optimalen Grundrechts-, Daten- und Rechtsschutz auf der anderen Seite überhaupt vollständig aufgelöst werden kann. Vielmehr werden am Ende auf einer der beiden Seiten wohl Zugeständnisse notwendig sein.

[83] Es sei noch angemerkt, dass weder die E-Evidence-VO noch das EBewMG auf den Aspekt der Integrität digitaler Beweismittel eingehen. In Zeiten von KI und „Deepfakes“ wird sich zunehmend die Frage stellen, ob Daten authentisch und nicht in irgendeiner Weise manipuliert sind. Weiterführend hierzu: *Okunrobo Perez*, EJCCLJ 2025, 187.