



Anlagenkonvolut

zum Wortprotokoll der 20. Sitzung vom 12. Januar 2026

	Seite
Stellungnahme Kai Kempgens	1
Stellungnahme Leonora Holling	6
Stellungnahme Sven Kurenbach	25
Stellungnahme Sebastian Murer	32
Stellungnahme Prof. Dr. Arndt Sinn	38
Stellungnahme Prof. Dr. Kai Ambos	47



Ausschussdrucksache 21(6)49a
vom 8. Januar 2026, 16:02 Uhr

Schriftliche Stellungnahme
des Sachverständigen Kai Kempgens

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes 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
BT-Drucksache 21/3192

Stellungnahme

zum Referentenentwurf eines Gesetzes 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

Der Deutsche Anwaltverein hat bereits Stellungnahmen zu den zwei Referentenentwürfen des Gesetzes zur Umsetzung des sog. E-Evidence-Pakets des Europäischen Parlaments und des Rates vom 12. Juli 2023 abgegeben. Nachfolgend sollen in Vorbereitung der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz am Montag, den 12. Januar 2026 zentrale Punkte präzisiert und hervorgehoben werden. Die Stellungnahme erfolgt in Hinblick auf die Kurzfristigkeit durch den Verfasser persönlich.

I. Einleitung

Die mit dem E-Evidence-Paket und dem nationalen Umsetzungsgesetz geschaffenen Ermittlungsinstrumente werden in der Praxis der deutschen Ermittlungsbehörden ganz erhebliche Auswirkungen haben. Die grenzüberschreitende innereuropäische Beschaffung von elektronischen Beweismitteln wird für die hiesigen Ermittlungsbehörden vereinfacht und beschleunigt. Die Ermittlungsarbeit erfährt dadurch einen deutlichen Effizienzgewinn. Ermittler erhalten ein mächtiges Werkzeug, direkt auf Daten zuzugreifen, die in Händen privater Diensteanbieter in europäischen Mitgliedsstaaten liegen.

Auf der anderen Seite geht die Bundesrepublik erhebliche unionsinterne Verpflichtungen ein, wenn im Gegenzug anderen Mitgliedsstaaten ein solcher direkter Abruf von Daten bei hiesigen Diensteanbieter gewährt und die Verpflichtung zur gegenseitigen Anerkennung von Rechtsakten anderer innereuropäischer Jurisdiktionen erweitert wird.

II. Hohe Grundrechtsrelevanz

Beides – sowohl die Anforderung als auch die Herausgabe elektronischer Beweismittel – hat für die jeweils Betroffenen in vielen Fällen eine hohe Grundrechtsrelevanz und bedarf daher eines sicheren und verlässlichen Rechtsrahmens. In der Regel wird sich es dabei zudem um Maßnahmen handeln, die heimlich und unter ohne Benachrichtigung der Betroffenen umgesetzt werden.

III. Ausgehende Herausgabeersuchen an Mitgliedsstaaten

Der vorliegende Referentenentwurf verfolgt hinsichtlich ausgehender Herausgabeersuchen durch seine Orientierung an den bestehenden Regelungen der Strafprozessordnung einen konsequenten und aus meiner Sicht sehr begrüßenswerten Ansatz. Sowohl Zuständigkeitsregelungen und Anordnungsvoraussetzungen als auch die Eröffnung von Rechtsbehelfen sind dem bestehenden und bewährten Regelungskonzept der StPO nachgebildet.

Zwei Punkte sind indes ergänzungsbedürftig:

[1] Löschungspflicht und Verwendungsverbot

Zum einen sollte die im ursprünglichen Referentenentwurf noch vorgesehene Löschungspflicht im Falle der gerichtlichen Feststellung der Herausgabe ebenso beibehalten werden wie das damals noch vorgesehene Verwendungsverbot im Falle der Rechtswidrigkeitsfeststellung. Nur so sind die Rechtsfolgen eines gerichtlich rechtskräftig festgestellten Rechtsverstoßes klar geregelt und eine drohende Rechtsgefährdung ausgeschlossen.

[2] Verwendungsbeschränkung auf Anordnungsverfahren

Zum anderen sollte ein klarer Rechtsrahmen geschaffen werden, wie mit Fällen umzugehen ist, in denen über eine europäische Herausgabeordnung erlangte Daten für andere Verfahren relevant sein könnten (z.B. im Falle von sog. Zufallsfunden). Eine solche Umwidmung der Beweismittel ist immer grundrechtsrelevant. Da die Strafprozessordnung nach ihrem Regelungskonzept immer auf den Gewinnungsweg von Beweismitteln und nicht etwa auf deren Gegenstand abstellt, sollte klar und deutlich geregelt werden, dass über eine EPOC bezogene elektronische Beweismittel nur für das Verfahren Verwendung finden dürfen, für welche die entsprechende Anordnung erfolgte. Soll eine Verwertung für andere Zwecke erfolgen, kann ohne weiteres erneut der effiziente neu eröffnete Gewinnungsweg beschritten werden – auch um den jeweils vollstreckenden Mitgliedsstaaten die Wahrnehmung ihrer Prüfungspflichten für die angedachte Verwertung zu ermöglichen.

III. Eingehende Herausgabeersuchen von Mitgliedsstaaten

Überarbeitungsbedürftig ist aber insbesondere die Ausgestaltung der Vorgaben für eingehende Herausgabeordnungen. Die Entscheidungsmacht über die Geltendmachung von Vorbehalten wird in § 11 des Entwurfes ausschließlich den Staatsanwaltschaften überantwortet, ohne dass eine gerichtliche Beteiligung in der Regel vorgesehen wäre. Dies kombiniert sich mit dem Umstand, dass im Referentenentwurf keinerlei Individualrechtsbehelf gegen die unterlassene Geltendmachung von Ablehnungsgründen vorgesehen ist. Damit stehen Betroffene, auf deren Daten im Rahmen einer eingehenden Anforderung eines Mitgliedsstaats zugegriffen wurde, im

hiesigen Rechtssystem weitgehend schutzlos dar. Dies ist vor dem Hintergrund von Art. 47 EUGrCh, Art. 13 EMRK und Art. 19 Abs. 4 GG nicht hinnehmbar.

Die Anwaltschaft hat daher zurecht drei Nachbesserungserfordernisse formuliert:

[1] Einbindung der Gerichte im Vollstreckungsverfahren

Erforderlich ist eine Beteiligung der Gerichte bereits im Vollstreckungsverfahren. Klassischerweise liegen solche Genehmigungsvorbehalte bei diesbezüglich über hohes Erfahrungswissen verfügenden Judikative. Zudem kann nur eine Einbindung der Gerichte eine einheitliche Entscheidungs- und Spruchpraxis und eine fundierte Rechtsfortwicklung hinsichtlich der zu erwartenden komplexen Rechtsfragen der Anwendungspraxis gewährleisten werden.

[2] Rechtsschutz bei unterlassener Geltendmachung von Ablehnungsgründen

Dringend vorzusehen sind zudem aber auch gerichtliche Rechtsschutzmöglichkeiten gegen die Entscheidung der Vollstreckungsbehörde, keine Ablehnungsgründe geltend zu machen. Angesichts der Tragweite und der Eingriffstiefe muss auch eine Beschwerdemöglichkeit und damit die Herbeiführung einer Entscheidung auf Landgerichtsebene vorgesehen werden.

Offenbar maßgeblicher Grund, wieso dieser zunächst noch vorgesehene – und aus hiesiger Sicht unbedingt notwendige – Rechtsbehelf auf Druck der Justizministerkonferenz aus dem Gesetzesentwurf gestrichen wurde, soll in der Steigerung der Effizienz der Strafverfolgung begründet sein. Eine solche Sichtweise halte ich dem Grunde nach für verfehlt. Zum kann ein solcher nachträglicher Rechtsschutz wohl kaum die Verfahrensabläufe im empfangenden Anordnungsstaat beeinträchtigen. Entsprechende Rechtsbehelfe dürften ohnehin eher selten zu erwarten sein. Ein Fehlen würde Anträge gem. § 23ff. EGGVG notwendig machen und zur Befassung der Verwaltungsgerichte und der Verfassungsgerichte führen. Zum anderen dürfen Effizienzgründe kein tragfähiger Grund sein, beschwerten Personen keine rechtsstaatliche Interventionsmöglichkeit nach hiesigem Recht zuzugestehen. Nur durch Gewährleistung eines effektiven Rechtsschutzes lässt sich in dem – auch kontradiktorisch zu betrachtenden – Strafverfahren gewährleisten, dass die europäischen Vorgaben des E-Evidence-Pakets sorgfältig eingehalten werden und die Verfahrenspraxis dieser mächtigen und für sich bereits effizienten Ermittlungsbefugnis allgemein als rechtsstaatlich und angemessen akzeptiert wird. Dieses hohe Gut der Rechtsstaatsakzeptanz sollte aus meiner Sicht nicht durch Versagung von Rechtsschutzmöglichkeiten gefährdet werden.

[3] Verpflichtung der Vollstreckungsbehörde zur Ermittlung eventueller Ablehnungsgründe

Es liegt in der Natur der Sache, dass Anordnungsstaaten in vielen Fällen nur mangelnde Kenntnis etwaiger Ablehnungsgründe wie Immunitäten, Vorrechte, Schutz der Pressefreiheit und dem Schutz von Berufsgeheimnisträgern haben werden. Daher dürften die mit der EPOC übermittelten Informationen im Unterrichtsfall oft nicht

ausreichen, um das Fehlen von Ablehnungsgründen des Artikel 12 der Verordnung verlässlich feststellen zu können.

Dies begründet die Notwendigkeit, dass hiesige Vollstreckungsbehörden eigene Ermittlungen vorzunehmen haben werden, um die jeweilige Sachkonstellation so weit zu erhellen, dass ein Vorliegen von Ablehnungstatbestände sicher ausgeschlossen werden kann. Angesichts der nur sehr kurzen Prüfungsfrist, der fehlenden Einbindung der Betroffenen und der sich anschließenden irreversiblen Herausgabe personenbezogener Daten an eine andere Jurisdiktion steht die Vollstreckungsbehörde dabei in hoher Verantwortung.

Das Gesetz sollte und muss daher ausdrücklich eine Ermittlungsverpflichtung im Unterrichtsfall konstituieren und das diesbezüglich erforderliche Prüfungsprogramm ausdrücklich festlegen.

Berlin, 08. Januar 2026



Ausschussdrucksache 21(6)49b
vom 9. Januar 2026, 11:33 Uhr

Schriftliche Stellungnahme
der Sachverständigen Leonora Holling

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes 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
BT-Drucksache 21/3192



BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 29/2025

Juli 2025

Registernummer: 25412265365-88

Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz – Gesetz 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

Mitglieder des AS Strafrecht (Strauda)

RAin Dr. Carolin Arnemann

RA Prof. Dr. Jan Bockemühl

RA Prof. Dr. Alfred Dierlamm

RA Prof. Dr. Björn Gercke

RA Dr. Mayeul Hiéramente (Berichterstatter)

RA Thomas C. Knierim

RA Dr. Daniel M. Krause

RAin Theres Kraußlach

RA Prof. Dr. Holger Matt (Vorsitzender und Berichterstatter)

RA Prof. Dr. Ralf Neuhaus,

RA Prof. Dr. Tido Park

RAin Dr. Hellen Schilling

RA Dr. Jens Schmidt

RAin Dr. Annette von Stetten

Prof. Dr. Dominik Brodowski (Ständiger Gast und Berichterstatter)

RAin Leonora Holling, Schatzmeisterin, Bundesrechtsanwaltskammer

Mitglieder des AS Europa

RA Dr. Sebastian Cording

RA Dr. Hans-Joachim Fritz

RA Marc André Gimmy

RAin Dr. Margarete Gräfin von Galen (Vorsitzende und Berichterstatterin)

RA Andreas Max Haak

RA Dr. Frank J. Hospach

RA Dr. Christian Lemke

RA Maximilian Müller

RAin Dr. Kerstin Niethammer-Jürgens

RA Dr. Hans-Michael Pott

RA Jan K. Schäfer, LL.M.

RAin Stefanie Schott (Berichterstatterin)

Prof. Dr. Gerson Trüg

RA Andreas von Máriássy

RA Dr. Christian Lemke, Vizepräsident, Bundesrechtsanwaltskammer

RAin Astrid Gamisch, LL.M., Bundesrechtsanwaltskammer, Brüssel

Ass. jur. Nadja Wietoska, Bundesrechtsanwaltskammer, Brüssel

Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel

Ass. jur. Sarah Pratscher, Bundesrechtsanwaltskammer, Brüssel

Verteiler:

Bundesministerium der Justiz

Bundesministerium des Innern und für Heimat

Justizministerien der Länder

Innenministerien der Länder

Rechtsausschuss des Deutschen Bundestages

Arbeitskreise Recht der Bundestagsfraktionen

Rechtsanwaltskammern

Der Generalbundesanwalt beim BGH

Bundesgerichtshof

Bundesverband der Freien Berufe

Bundesnotarkammer

Bundessteuerberaterkammer

Deutscher Steuerberaterverband

Wirtschaftsprüferkammer

Institut der Wirtschaftsprüfer

Deutscher Anwaltverein

Deutscher Notarverein

Deutscher Richterbund

Deutscher Juristinnenbund

Bundestag Neue Richtervereinigung

Strafverteidigervereinigungen

Deutsche Strafverteidiger e.V.

Neue Richtervereinigung e.V.

Bund Deutscher Kriminalbeamter

Redaktionen der NJW, Beck Verlag, Deubner Verlag, Jurion, Juris, LexisNexis, Otto Schmidt Verlag, Strafverteidiger, Neue Zeitschrift für Strafrecht, ZAP Verlag, Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht, wistra - Zeitschrift für Wirtschafts- und Steuerstrafrecht, Zeitschrift HRR-Strafrecht, Kriminalpolitische Zeitschrift
FAZ, Süddeutsche Zeitung, Die Welt, Handelsblatt, Tagesspiegel, LTO, Der Spiegel, Focus, Die ZEIT

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten¹ gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

I. Einführung

Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) hat mit Datum vom 04. Juni 2025 einen überarbeiteten Referentenentwurf zur Durchführung der Verordnung (EU) 2023/1543 (fortan: E-Evidence-Verordnung) sowie weiterer unionsrechtlicher Vorgaben vorgelegt. Dieser berücksichtigt u.a. Forderungen der 96. JuMiKo zur Überarbeitung des „ersten“ Referentenentwurfs vom Oktober 2024 und beschränkt sich darüber hinaus darauf, **Durchführungsvorschriften für den Erlass Europäischer Herausgabeanordnungen** zu schaffen. Durchführungsvorschriften für den Erlass von Sicherungsanordnungen sieht der Referentenentwurf, anders als der vorherige Referentenentwurf, nicht mehr vor.²

Die Bundesrechtsanwaltskammer hatte zu dem Ende Oktober 2024 vorgelegten ersten Referentenentwurf des damaligen Bundesministeriums der Justiz (BMJ) bereits ausführlich Stellung genommen (BRAK-Stellungnahme Nr. 88/2024) und hält an den dortigen Ausführungen grundsätzlich fest, soweit im aktuellen Referentenentwurf die Regelungen unverändert geblieben sind und daher die gleichen Kritikpunkte greifen. Hinsichtlich der schon damals vorgeschlagenen Regelungen zu Teil 3 (Durchführung der E-Evidence-Verordnung) besteht aus Sicht der Bundesrechtsanwaltskammer in einzelnen Punkten nach wie vor Änderungsbedarf. Bedauerlich war bereits im ersten Referentenentwurf, dass dieser den europarechtlich zulässigen und zum Antragsrecht der Verteidigung notwendigen Umsetzungsspielraum nicht genutzt hat, um einige notwendige Anpassungen

¹ Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden gewählte männliche Form schließt alle Geschlechter gleichberechtigt ein.

² Der Strafrechtsausschuss der BRAK (Strauda) hat auf seiner 252. Sitzung, zugleich 7. Gemeinsame Sitzung mit der StraKo des ÖRAK, Ende Juni 2025 in Wien nochmals die Spielräume zur Durchführung der E-Evidence-Verordnung intensiv diskutiert, die diesbezüglichen österreichischen Überlegungen des dortigen Justizministeriums reflektiert sowie den konkret ergänzenden Stellungnahmebedarf zum aktuellen Referentenentwurf eruiert und nunmehr gemeinsam mit dem Europaausschuss der BRAK umgesetzt.

vorzunehmen. Diese wichtige Kritik bleibt unverändert gültig auch für den aktuellen Referentenentwurf. Zudem bleibt zu erwägen, die rechtshilferechtlichen Regelungen in die Neufassung des – dringend reformbedürftigen – IRG³ zu integrieren, ebenso wie die Umsetzung der Europäischen Ermittlungsanordnung im IRG zu finden ist (§§ 91 a ff. IRG a.F., §§ 258 ff. IRG-RefE).

Die Bundesrechtsanwaltskammer kritisiert ausdrücklich die von der 96. JuMiKo geforderte und im neuen Referentenentwurf vorgenommene Einschränkung der Rechtsbehelfe. Der Verzicht auf einen **Rechtsbehelf zur (nachträglichen) Überprüfung von Ermessensentscheidungen der Vollstreckungsbehörde** im Hinblick auf die (Nicht-) Geltendmachung von unionsrechtlichen Ablehnungsgründen nach Art. 12 E-Evidence-Verordnung kann zur Rechtsunsicherheit führen und gefährdet fundamentale Unionsgrundrechte, u.a. das Recht auf Vertraulichkeit der Kommunikation zwischen Mandanten und Berufsgeheimnisträgern (dazu unter II.). Darüber hinaus erinnert die Bundesrechtsanwaltskammer an den mit der BRAK-Stellungnahme Nr. 88/2024 ausführlich dargelegten Regelungsbedarf zur Ermöglichung eines **effektiven Antragsrechts der Verteidigung**⁴ sowie einen datenschutzrechtlichen Anpassungsbedarf bei strafprozessualen Regelungen zur Zweckänderung und Löschung.⁵ Die im Referentenentwurf vorgeschlagenen **Zuständigkeitsregelungen** sind aus Sicht der Bundesrechtsanwaltskammer im Grundsatz zu begrüßen. Im Lichte der vorgesehenen Streichung eines Rechtsbehelfs zur Feststellung von Ermessensfehlern bei Anwendung des Art. 12 E-Evidence-Verordnung sollte indes die in § 11 Abs. 1 EBewMG-E vorgesehene Definition der Vollstreckungsbehörde iSd Art. 3 Nr. 17 E-Evidence-Verordnung überdacht werden. Hier bietet sich aus zahlreichen Gründen eine Einbindung des Gerichts an (dazu unter III.). Ferner wäre es zielführend, wenn der Gesetzgeber einen Kommunikationskanal zwischen Diensteanbieter und Vollstreckungsbehörde schafft, um die Entscheidungsgrundlage der Vollstreckungsbehörde zu optimieren (dazu unter IV.). Darüber hinaus erlaubt sich die Bundesrechtsanwaltskammer auf weitere ausgewählte Aspekte hinzuweisen, die zu Rechtsunsicherheit in der Praxis führen könnten (dazu unter V.).

II. Effektiver Rechtsschutz

Nach der Konzeption der E-Evidence-Verordnung soll der Vollstreckungsstaat nur beim besonders eingriffsintensiven Zugriff auf Verkehrsdaten oder Inhaltsdaten über eine Europäische Herausgabeanordnung in Kenntnis gesetzt werden (vgl. Art. 8 Abs. 1 E-Evidence-Verordnung). Der Vollstreckungsstaat kann nur in äußerst eingeschränktem Umfang intervenieren, wenn aus Sicht der Vollstreckungsbehörde ein Ablehnungsgrund iSd Art. 12 Abs. 1 E-Evidence-Verordnung vorliegt. Hierbei handelt es sich um die folgenden Gründe:

*a) die angeforderten Daten sind durch **Immunitäten oder Vorrechte** geschützt, die nach dem Recht des Vollstreckungsstaats gewährt werden, wodurch die Ausführung oder Vollstreckung der Anordnung verhindert wird, oder die angeforderten Daten unterliegen Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die **Freiheit der Presse und das Recht auf freie Meinungsäußerung** in anderen Medien, wodurch die*

³ Referentenentwurf des Bundesministeriums der Justiz eines Gesetzes zur Neuregelung des Rechts der internationalen Rechtshilfe in Strafsachen (IRG); siehe hierzu die BRAK-Stellungnahmen Nr. 50/2024 und 83/2024.

⁴ Vgl. dazu ausführlich BRAK Stellungnahme Nr. 88/2024, S. 6 ff.

⁵ Vgl. dazu BRAK Stellungnahme Nr. 88/2024, S. 10.

Ausführung oder Vollstreckung der Anordnung verhindert wird;

*b) in Ausnahmefällen bestehen aufgrund genauer und objektiver Belege berechnete Gründe zu der Annahme, dass die Ausführung der Anordnung unter den besonderen Umständen des Falles eine **offensichtliche Verletzung eines einschlägigen in Artikel 6 EUV und der Charta verankerten Grundrechts** zur Folge hätte;*

*c) die Ausführung der Anordnung würde dem Grundsatz „**ne bis in idem**“ zuwiderlaufen;*

*d) die Handlung, aufgrund deren die Anordnung erlassen wurde, stellt nach dem Recht des Vollstreckungsstaats **keine Straftat** dar, es sei denn, sie betrifft eine Straftat, die unter den in Anhang IV aufgeführten Kategorien von Straftaten – wie von der Anordnungsbehörde im EPOC angegeben – genannt wird, und sofern die Straftat im Anordnungsstaat mit einer Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist.*

Nach allgemeiner, vom BMJ geteilter Auffassung fällt unter Art. 12 Abs. 1 a) E-Evidence-Verordnung auch der Schutz von Kommunikation mit Berufsgeheimnisträgern.⁶

Die E-Evidence-Verordnung räumt dem Vollstreckungsstaat mithin nur bei drohenden – äußerst gewichtigen – Verstößen ein Ablehnungsrecht ein. Eine Einbindung der betroffenen Person bei der Entscheidung über die (Nicht-) Geltendmachung dieser Ablehnungsgründe ist weder in der E-Evidence-Verordnung noch im Referentenentwurf vorgesehen.

Der erste **Referentenentwurf aus dem Jahr 2024** sah einen äußerst moderaten (!) Rechtsbehelf vor, mit dem – *post facto*, d.h. nach Übermittlung der Daten an den Anordnungsstaat – gerichtlich geprüft werden können sollte, ob die Nichtgeltendmachung von Ablehnungsgründen rechtskonform war. Eine gerichtliche Feststellung der Rechtswidrigkeit (z.B. wegen Verstoßes gegen §§ 97, 148, 160a StPO durch Zugriff auf Akten oder Verbindungsdaten deutscher Journalisten) hätte zunächst einmal keine unmittelbaren Rechtswirkungen. Es würde den Betroffenen jedoch in die Lage versetzen, diese gerichtliche Feststellung durch ein deutsches Gericht im Anordnungsstaat vorzulegen, um dort auf eine Heilung bzw. Berücksichtigung eines gravierenden Grundrechtsverstoßes hinzuwirken.

Sofern die 96. JuMiKo befürchtet, ein solcher Rechtsbehelf [konterkariere] „*die mit dem Vorhaben intendierte Steigerung der Effizienz der Strafverfolgung [...], weil er – neben vermeidbaren Mehrkosten – erhebliche Verfahrensverzögerungen besorgen lässt*“, zeugt dies von einem offensichtlichen Fehlverständnis des vom BMJ zunächst vorgeschlagenen Rechtsbehelfs. Ein solcher Rechtsbehelf wäre angesichts des eingeschränkten Anwendungsbereichs der Art. 8 Abs. 1, Art. 12 Abs. 1 E-Evidence-Verordnung nur in Ausnahmefällen zu erwarten und würde das in einem anderen (!) Mitgliedstaat geführte Strafverfahren in keiner Weise verzögern. Die Belastung für die deutsche Strafjustiz wäre äußerst gering.

Die Einführung eines solchen – (s.o.) äußerst moderaten (!) – Rechtsbehelfs ist **im Interesse eines effektiven Grundrechtsschutzes geboten**. Sofern eine deutsche Vollstreckungsbehörde trotz einer drohenden Verletzung elementarer Grundrechte untätig bleiben sollte und sich – trotz der in Art. 12 E-Evidence-Verordnung vorgesehene Möglichkeit – gegen die Geltendmachung von Ablehnungsgründen

⁶ RefE 2024, S. 22, 50; BRAK Stellungnahme Nr. 88/2024, S. 6.

entscheiden sollte, muss ein solch rechtswidriges Unterlassen im Hinblick auf **Art. 19 Abs. 4 GG** gerichtlich überprüfbar sein. Der Verzicht auf einen klar normierten Rechtsbehelf im EBewMG-E dürfte in der Praxis daher dazu führen, dass ein etwaiges Fehlverhalten der Vollstreckungsbehörde im aufwendigeren Verfahren nach §§ 23 ff. EGGVG oder vor den Verwaltungsgerichten überprüft werden wird. Insoweit würde die Schaffung eines Rechtsbehelfs im EBewMG prozessualer Rechtsunsicherheit vorbeugen. Hinzukommt, dass ein eigenständiger Rechtsbehelf es deutschen Gerichten ermöglichen würde, etwaige Streitfragen im Hinblick auf den Anwendungsbereich des Art. 12 E-Evidence-Verordnung dem EuGH vorzulegen und auf diese Weise zu Rechtssicherheit innerhalb der Europäischen Union beizutragen.

III. Zuständigkeitsregelungen

Der Referentenentwurf orientiert sich sowohl hinsichtlich des Erlasses von Europäischen Herausgabebeanordnungen (§§ 9, 10 EBewMG-E) als auch hinsichtlich der insoweit maßgeblichen Rechtsbehelfe (§ 13 EBewMG-E) an den für vergleichbare Maßnahmen im innerstaatlichen Verfahren maßgeblichen Zuständigkeiten. Dieser Regelungsansatz ist nachvollziehbar.⁷ Es ist insoweit zu begrüßen, dass im Interesse der Anwendungsfreundlichkeit parallele Zuständigkeiten normiert worden sind.

Sofern der Referentenentwurf an der Streichung eines Rechtsbehelfs hinsichtlich der (Nicht-) Geltendmachung von Ablehnungsgründen nach Art. 12 Abs. 1 E-Evidence-Verordnung festhalten sollte, wäre allerdings zu überdenken, ob die Staatsanwaltschaft eine geeignete Vollstreckungsbehörde ist (vgl. § 11 Abs. 1 EBewMG-E). Es ist 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 steht. Eine derart schwerwiegende Entscheidung, die zudem aufgrund der im Regelfall vorgenommenen Übertragung der Daten vor Anhörung des Betroffenen im Anordnungsstaat nicht immer revidierbar ist, erfordert eine **gerichtliche Beteiligung**. Eine Beteiligung der Gerichte als „Vollstreckungsbehörde“ wäre zudem durchaus kohärent. So sieht § 10 EBewMG-E für Europäische Herausgabebeanordnungen zur Herausgabe von Verkehrsdaten und Inhaltsdaten eine Anordnungszuständigkeit der Gerichte vor. Es liegt insoweit nahe, für die Vollstreckungszuständigkeit nach Art. 12 Abs. 1 E-Evidence-Verordnung, die sich ebenfalls ausschließlich auf diese Datenkategorien bezieht, ebenfalls eine gerichtliche Zuständigkeit anzunehmen.

Eine derart umfassende gerichtliche Zuständigkeit hätte auch gewichtige **praktische Vorteile**:

So könnte auf Ebene der zuständigen Gerichte ein besonderes **Erfahrungswissen** aufgebaut werden. Zudem kann die bei Gerichtsentscheidungen übliche – bei staatsanwaltschaftlichen Verfügungen hingegen sehr unübliche – **Praxis der Veröffentlichung wichtiger Entscheidungen** einen Beitrag zur Rechtsfortbildung und -vereinheitlichung leisten. Darüber hinaus sind nach Art. 267 AEUV ausschließlich Gerichte zur **Vorlage an den EuGH** befugt. Auch insoweit wäre eine Einbindung deutscher Gerichte vorzugswürdig, um eine einfache Klärung wichtiger unionsrechtlicher Fragen herbeiführen zu können.

⁷ Vgl. dazu auch BRAK Stellungnahme Nr. 88/2024, S.3 f.

IV. Kommunikationskanal zwischen Diensteanbieter und Vollstreckungsbehörde

Nach der Konzeption der E-Evidence-Verordnung informiert die (ausländische) Anordnungsbehörde im Fall der Anwendung des Art. 8 Abs. 1 E-Evidence-Verordnung sowohl den Adressaten (vgl. Art. 9 Abs. 1 iVm Anhang I, Abschn. C) als auch die Vollstreckungsbehörde (vgl. Art. 8 Abs. 1 E-Evidence-Verordnung). Eine Kommunikation mit dem Diensteanbieter wird durch die Verordnung vorgeschrieben, wenn die Vollstreckungsbehörde eine Entscheidung zur (Nicht-) Geltendmachung von Ablehnungsgründen getroffen hat (vgl. Art. 10 Abs. 2, Art. 10 Abs. 4 E-Evidence-Verordnung). Darüber hinaus ist eine direkte Kommunikation des Diensteanbieters an die Vollstreckungsbehörde vorgesehen, wenn diese aufgrund der vorliegenden Erkenntnisse von der Anwendbarkeit (ausgewählter) Ablehnungsgründe Kenntnis hat (vgl. Art. 10 Abs. 5 1. UA E-Evidence-Verordnung). Der Verordnungsgeber geht augenscheinlich davon aus, dass der Diensteanbieter im Einzelfall über Informationen verfügen kann, die für die Bewertung der Ablehnungsgründe nach Art. 12 Abs. 1 E-Evidence-Verordnung von Bedeutung sein können (vgl. auch Art. 10 Abs. 5 2. UA, 3. UA E-Evidence-Verordnung).

Es wäre aus Sicht der (anwaltlichen) Praxis zu begrüßen und im Lichte des Regelungsgefüges der E-Evidence-Verordnung auch zulässig, wenn der deutsche Gesetzgeber für den Fall einer Prüfung von Ablehnungsgründen einen Kommunikationskanal zwischen Vollstreckungsbehörde und Diensteanbieter öffnen würde, so dass es der Vollstreckungsbehörde – zumindest bei Anhaltspunkten für das Vorliegen von Ablehnungsgründen – ermöglicht würde, den Diensteanbieter hierzu anzuhören. Insbesondere spezialisierte Anbieter (z.B. Anbieter von ausgewählten IT-Dienstleistungen für Berufsgeheimnisträger) könnten, wie die Existenz von Art. 10 Abs. 5 E-Evidence-Verordnung belegt, einen wesentlichen Beitrag dazu leisten, dass die Vollstreckungsbehörde bei den äußerst grundrechtssensiblen Entscheidungen iSd Art. 12 E-Evidence-Verordnung über eine bessere Entscheidungsgrundlage verfügt.

V. Ergänzende Anmerkungen

Abschließend erlauben wir uns den Hinweis auf Regelungen, die zu Rechtsunsicherheit in der Praxis führen könnten.

Zunächst regen wir an, die Regelung des **§ 8 EBewMG-E** zu überdenken und auf **Unionsrechtskonformität** hin zu überprüfen. So dürfte es unionsrechtlich unzulässig sein, Datenkategorien der E-Evidence-Verordnung unter Verweis auf Legaldefinitionen des nationalen Rechts zu bestimmen.

Ferner regen wir an, eine weitergehende Klarstellung hinsichtlich der Regelung des **§ 13 Abs. 4 EBewMG-E** vorzunehmen. Der Absatz lautet:

„Die Rechtsbehelfe nach den Absätze 1 bis 3 stehen nur Personen zur Verfügung, deren Daten im Wege einer Europäischen Herausgabeanordnung nach der Verordnung (EU) 2023/1543 angefordert wurden.“

In der Gesetzesbegründung ist klargestellt, dass die Beschränkung des Rechtsbehelfs auf bestimmte Personen (ausschließlich) dazu dienen soll, ein Beschwerderecht des Diensteanbieters

auszuschließen.⁸ Insoweit dürfte vorzugswürdig sein, ein solches Beschwerderecht des Diensteanbieters ausdrücklich auszuschließen. So birgt die Formulierung, ein Beschwerderecht stehe nur Personen zu, „deren Daten [...] angefordert werden“, Auslegungsunsicherheiten. Insbesondere ist unklar, ob der Formulierung ein datenschutzrechtliches Verständnis (personenbezogene Daten) oder eine andere Form der Datenzuordnung zugrunde liegt.

- - -

⁸ RefE 2025, S. 51.



BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 88/2024

Dezember 2024

Registernummer: 25412265365-88

Referentenentwurf des BMJ – Gesetz zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel im Strafverfahren innerhalb der Europäischen Union

Mitglieder des AS Strafrecht (Strauda)

RAin Dr. Carolin Arnemann

RA Prof. Dr. Jan Bockemühl

RA Prof. Dr. Alfred Dierlamm

RA Prof. Dr. Björn Gercke

RA Dr. Mayeul Hiéramente (Berichterstatter)

RA Thomas C. Knierim

RA Dr. Daniel M. Krause

RAin Theres Kraußlach

RA Prof. Dr. Holger Matt (Vorsitzender und Berichterstatter)

RA Prof. Dr. Ralf Neuhaus

RA Prof. Dr. Tido Park

RAin Dr. Hellen Schilling

RA Dr. Jens Schmidt

RAin Dr. Annette von Stetten

Prof. Dr. Dominik Brodowski (Berichterstatter)

RAin Leonora Holling, Schatzmeisterin, Bundesrechtsanwaltskammer

Mitglieder des AS Europa

RA Dr. Sebastian Cording

RA Dr. Hans-Joachim Fritz

RA Marc André Gimmy

RAin Dr. Margarete Gräfin von Galen (Vorsitzende und Berichterstatterin)

RA Andreas Max Haak

RA Dr. Frank J. Hospach

RA Dr. Christian Lemke

RA Maximilian Müller

RAin Dr. Kerstin Niethammer-Jürgens

RA Dr. Hans-Michael Pott

RA Jan K. Schäfer, LL.M.

RAin Stefanie Schott (Berichterstatte(rin))

Prof. Dr. Gerson Trüg

RA Andreas von Máriássy

RA Dr. Christian Lemke, Vizepräsident, Bundesrechtsanwaltskammer

RAin Astrid Gamisch, LL.M., Bundesrechtsanwaltskammer, Brüssel

Ass. jur. Nadja Wietoska, Bundesrechtsanwaltskammer, Brüssel

Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel

Ass. jur. Sarah Pratscher, Bundesrechtsanwaltskammer, Brüssel

Verteiler:

Bundesministerium der Justiz

Bundesministerium des Innern und für Heimat

Justizministerien der Länder

Innenministerien der Länder

Rechtsausschuss des Deutschen Bundestages

Arbeitskreise Recht der Bundestagsfraktionen

Rechtsanwaltskammern

Der Generalbundesanwalt beim BGH

Bundesgerichtshof

Bundesverband der Freien Berufe

Bundesnotarkammer

Bundessteuerberaterkammer

Deutscher Steuerberaterverband

Wirtschaftsprüferkammer

Institut der Wirtschaftsprüfer

Deutscher Anwaltverein

Deutscher Notarverein

Deutscher Richterbund

Deutscher Juristinnenbund

Bundesvorstand Neue Richtervereinigung

Strafverteidigervereinigungen

Deutsche Strafverteidiger e.V.

Neue Richtervereinigung e.V.

Bund Deutscher Kriminalbeamter

Redaktionen der NJW, Beck Verlag, Deubner Verlag, Jurion, Juris, LexisNexis,

Otto Schmidt Verlag, Strafverteidiger, Neue Zeitschrift für Strafrecht, ZAP Verlag,

Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht,

Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht,

wistra - Zeitschrift für Wirtschafts- und Steuerstrafrecht, Zeitschrift HRR-Strafrecht,

Kriminalpolitische Zeitschrift

FAZ, Süddeutsche Zeitung, Die Welt, Handelsblatt, Tagesspiegel, LTO, Der Spiegel,

Focus, Die ZEIT

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten¹ gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

I. Einführung

Die Bundesrechtsanwaltskammer begrüßt, dass das Bundesministerium der Justiz (BMJ) bereits frühzeitig den Schritt zur Umsetzung bzw. Ergänzung europarechtlicher Vorgaben unternommen und hierfür einen, aus Sicht der Bundesrechtsanwaltskammer ausgewogenen Entwurf vorgelegt hat. Hinsichtlich der vorgeschlagenen Regelungen des Teils 3 („Durchführung der Verordnung (EU) 2023/1543“; fortan: E-Evidence-Verordnung) besteht aus Sicht der Bundesrechtsanwaltskammer in einzelnen Punkten Änderungsbedarf. Bedauerlich ist, dass der Referentenentwurf den europarechtlich zulässigen und zum Antragsrecht der Verteidigung notwendigen Umsetzungsspielraum nicht genutzt hat, um einige notwendige Anpassungen vorzunehmen.

Zudem sollte erwogen werden, die rechtshilferechtlichen Regelungen in die Neufassung des – dringend reformbedürftigen – IRG² zu integrieren, ebenso wie die Umsetzung der Europäischen Ermittlungsanordnung im IRG zu finden ist (§§ 91 a ff. IRG a.F., §§ 258 ff. IRG-RefE).

II. Zuständigkeitsregelung

Der Referentenentwurf definiert in § 7 EBewMG-RefE die Zuständigkeit für den Erlass Europäischer Herausgabeanordnungen und in § 8 EBewMG-RefE die Zuständigkeit für etwaige Validierungen. In § 9 EBewMG-RefE wird die Zuständigkeit für den Erlass Europäischer Sicherungsanordnungen definiert. Dabei orientiert sich der Referentenentwurf an der Zuständigkeit für den Erlass vergleichbarer Maßnahmen im rein nationalen Kontext und stellt sicher, dass bei eingriffsintensiven Maßnahmen eine Einbindung der Gerichte erfolgt. Insoweit hat der Referentenentwurf eine nachvollziehbare und überzeugende Zuständigkeitsregelung getroffen. Da bei Erlass der Anordnungen eine Prüfung nach nationalem Recht zu erfolgen hat,³ ist es zielführend, eine einheitliche Zuständigkeitsregelung vorzunehmen.

Aus Perspektive der Praxis ist indes bedenklich, dass der Referentenentwurf pauschal auf den „Achten Abschnitt des Ersten Buch der Strafprozessordnung“ verweist. Dieser enthält u.a. Vorschriften zur Beschlagnahme (§§ 94 ff. StPO), die §§ 100 a ff. StPO sowie die Regelungen zur Durchsuchung (§§ 102 ff. StPO). Dies führt zu Anwendungsschwierigkeiten. Zum einen ist für den Rechtsanwender unklar, welche Vorschriften zu der gebotenen Prüfung nach dem nationalen Recht heranzuziehen sind. Zum anderen folgt aus dieser Unklarheit auch eine Unsicherheit hinsichtlich der Zuständigkeit. Dies mag bei Anordnungen zur Sicherung und Herausgabe von Teilnehmerdaten⁴ und Verkehrsdaten

¹ Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden gewählte männliche Form schließt alle Geschlechter gleichberechtigt ein.

² Referentenentwurf des Bundesministeriums der Justiz eines Gesetzes zur Neuregelung des Rechts der internationalen Rechtshilfe in Strafsachen (IRG); siehe hierzu die BRAK-Stellungnahmen Nr. 50/2024 und 83/2024.

³ RefE, S. 49: „Das Gericht hat also nach einem doppelten Maßstab zu prüfen: Zum einen anhand der Verordnung (EU) 2023/1543, zum anderen anhand des nationalen Rechts.“

⁴ Im Sprachgebrauch der StPO: Bestandsdaten und Nutzungsdaten, vgl. RefE, S. 43.

vertretbar sein. Hinsichtlich des Zugriffs auf Inhaltsdaten dürfte es in der Praxis jedoch zu beträchtlichen Rechtsunsicherheiten kommen.⁵ Es wäre daher zu prüfen, ob bei der Zuständigkeitsregelung im EBewMG-RefE auf die *konkreten* Zuständigkeitsregelungen in der StPO verwiesen werden sollte.

III. Effektiver Rechtsschutz

Die Bundesrechtsanwaltskammer begrüßt, dass der Referentenentwurf für einen effektiven Rechtsschutz Sorge tragen will und die dazu erforderlichen Rechtsbehelfe vorsieht. Da die Vollstreckung der Herausgabeanordnungen einerseits auf maximale Beschleunigung ausgerichtet ist und die betroffene Person andererseits in der Praxis in aller Regel erst nachträglich über die bereits erfolgte Herausgabe von Daten informiert werden wird, wird die Herausgabe der Daten im Zeitpunkt der gerichtlichen Entscheidung in aller Regel bereits erfolgt sein. Die Bundesrechtsanwaltskammer hält es daher für geboten und begrüßt dementsprechend, dass für Fälle ausgehender Europäischer Herausgabeanordnungen in § 15 Abs. 2 EBewMG-RefE die Löschung der rechtswidrig erlangten Daten angeordnet wird.

1. Rechtsschutz gegen Europäische Herausgabeanordnungen (Deutschland als Anordnungsstaat)

In § 14 Abs. 1 EBewMG-RefE werden Rechtsschutzmöglichkeiten gegen die Anordnung Europäischer Herausgabeanordnungen definiert. Insoweit ist es überzeugend, dass sich der Referentenentwurf am Rechtsschutz gegen vergleichbare Maßnahmen im nationalen Recht orientiert und daher auf die Regelungen des § 98 Abs. 2 S. 2 ff. StPO sowie die Beschwerdevorschriften der §§ 304 ff. StPO verweist. Es ist sachgerecht, dass für diese Maßnahmen im Grundsatz die Amts- und Landgerichte zuständig sind. Dieses Rechtsschutzkonzept steht auch im Einklang mit dem Ansatz des IRG-Referentenentwurfs. Die Bundesrechtsanwaltskammer hat allerdings bereits darauf hingewiesen, dass bei besonders eingriffsintensiven Maßnahmen eine Einbindung der mit Rechtshilfethemen vertrauten Oberlandesgerichte als weitere Instanz zur Klärung von Rechtsfragen wünschenswert wäre, um eine einheitlichere Rechtsprechung zu gewährleisten.⁶ Eine derartige Einbindung wäre auch beim EBewMG-RefE zu begrüßen.

Darüber hinaus sollte in § 14 Abs. 1 EBewMG-RefE klargestellt werden, dass gegen Europäische Herausgabeanordnungen der Staatsanwaltschaft⁷ nicht nur ein Antrag auf gerichtliche Entscheidung nach § 98 Abs. 2 S. 2 StPO gestellt werden kann, sondern eine Beschwerdemöglichkeit zum Landgericht besteht. Eine solche ließe sich zwar aus § 13 EBewMG-RefE herleiten. Eine Beschwerdemöglichkeit dürfte zwar intendiert sein, da selbst für die Europäische Sicherungsanordnung eine Möglichkeit der Anrufung des Landgerichts vorgesehen ist (§ 14 Abs. 2 EBewMG-RefE).⁸ Der Wortlaut des § 14 EBewMG-RefE könnte jedoch unterschiedlich ausgelegt werden. Im Interesse der Rechtsklarheit sollte die **Beschwerdemöglichkeit** unbedingt auch in § 14 Abs. 1 EBewMG-RefE klargestellt werden.

Die Bundesrechtsanwaltskammer begrüßt, dass in § 15 Abs. 2 EBewMG-RefE die Folgen einer Feststellung der Rechtswidrigkeit ausdrücklich geregelt werden.

⁵ Vgl. z. B. dem Meinungsstreit hinsichtlich des Zugriffs auf „Alt-E-mails“ BT-Drs. 18/12785, S. 50 f.; *Oppermann*, juris PraxisReport StrafR 22/2024, Anm. 3; *Grözingner* NSTZ 2021, 358-360; *Hiéramente* WiJ 2021, 19; aA BGH, Beschl. v. 14.10.2020, 5 StR 229/19; im Ergebnis zustimmend *Abraham*, HRRS 2021, 356. Begrüßenswert der Hinweis, RefE, S. 44, auf die möglicherweise zu erfolgende Prüfung anhand von § 100b StPO.

⁶ Vgl. dazu BRAK-Stellungnahme 83/2024, S. 9 f.

⁷ Oder bei Validierung durch die Staatsanwaltschaft, vgl. RefE, S. 48.

⁸ RefE, S. 48.

2. Rechtsschutz gegen Europäische Herausgabebeanordnungen (Deutschland als Vollstreckungsstaat)

Begrüßenswert im Hinblick auf die Gewährung von Rechtsschutz gegen in Deutschland zu vollstreckende Europäische Herausgabebeanordnungen ist, dass der Referentenentwurf in §§ 16, 17 EBewMG-RefE ein gerichtliches Verfahren vorsieht, in dem betroffene Personen oder deren gesetzliche Vertreter antragsberechtigt sind (§ 16 Abs. 3 EBewMG-RefE). Der Prüfungsmaßstab richtet sich nach Art. 12 E-Evidence-Verordnung. Maßgeblich ist, ob die Vollstreckungsbehörde ermessensfehlerhaft auf die Geltendmachung von Ablehnungsgründen verzichtet hat. Da sich aus der E-Evidence-Verordnung aus dem Zusammenspiel von Art. 12 und den Erwägungsgründen, insbesondere aus Erwägungsgrund 62, ein Ermessen der Vollstreckungsbehörde ergibt, erkennt die Bundesrechtsanwaltskammer an, dass der nationale Gesetzgeber europarechtlich verpflichtet ist, (nur) eine Überprüfung der Ermessensausübung zu ermöglichen. Allerdings dürfte angesichts der Ausgestaltung der Ablehnungsgründe zumeist von einer Ermessensreduktion auf Null auszugehen sein.

Zuständig für die gerichtliche Prüfung ist das Amtsgericht. Die Zuweisung an die ordentlichen Gerichte überzeugt. Ebenso ist es überzeugend, wenn man die Prüfung zunächst dem Amtsgericht zuweist. Angesichts der besonderen Grundrechtsrelevanz der in Art. 12 E-Evidence-Verordnung normierten Ablehnungsgründe sowie der (möglichen) Bedeutung einer Ablehnungsentscheidung für den weiteren Umgang mit den Daten im Anordnungsstaat⁹ ist allerdings die **Einbindung des Landgerichts dringend geboten**. Insbesondere einer Entscheidung über die Reichweite der in der StPO zum Schutz von Berufsgeheimnisträgern vorgesehenen Vorschriften kommt eine fundamentale Bedeutung für ein faires und rechtsstaatliches Verfahren zu,¹⁰ der mit der Beschwerdemöglichkeit zum Landgericht Rechnung zu tragen ist. Darüber hinaus kann durch eine Beschwerdemöglichkeit zum Landgericht vermieden werden, dass sich eine schier unübersehbare Kasuistik deutscher Amtsgerichte herausbildet. Schließlich entspricht die Möglichkeit der Beschwerde (§§ 304 ff. StPO)¹¹ oder sofortigen Beschwerde (§ 311 StPO)¹² der Systematik der StPO – auch bei der nachträglichen Feststellung der Rechtswidrigkeit einer (sonstigen) Ermittlungsmaßnahme. Ein Ausschluss der Beschwerde wäre daher eine systemwidrige Ausnahme.

IV. Schutz von Berufsgeheimnisträgern

Der Gesetzestext verhält sich nicht ausdrücklich zur Thematik des Schutzes von Berufsgeheimnisträgern. Die Begründung des Referentenentwurfs betont jedoch an verschiedenen Stellen die Bedeutung des Schutzes von Berufsgeheimnisträgern.

1. Deutschland als Anordnungsstaat

In der Begründung des Referentenentwurfs wird klargestellt, dass der Schutz von Berufsgeheimnisträgern aus zweierlei Weise erfolgt. Zum einen wird erläutert, dass sich aus der E-Evidence-Verordnung spezifische Pflichten zum Schutz von Berufsgeheimnisträgern ergeben.¹³ Darüber hinaus wird explizit darauf hingewiesen, dass die Schutzvorschriften des nationalen Rechts – der Referentenentwurf nennt Beschlagnahmeverbote – zu beachten sind.¹⁴ Auf diese Weise wird sichergestellt, dass bei einer Anordnung durch eine deutsche Behörde die Schutzvorschriften der StPO (insb. §§ 53, 97, 100 d Abs. 5, 100 g Abs. 4, 148 StPO) Anwendung finden. Aus Sicht der Praxis wäre

⁹ Vgl. z. B. Art. 10 Abs. 4 E-Evidence-VO für Übermittlung in Notfallkonstellationen.

¹⁰ Vgl. z. B. BVerfG NJW 2005, 1917.

¹¹ Vgl. LG Lübeck, Beschl. v. 29.09.2022 – 6 Qs 21/22.

¹² Vgl. dazu § 101 Abs. 7 S. 3 StPO.

¹³ RefE, S. 22.

¹⁴ RefE, S. 22.

wünschenswert, wenn sich diese Prüfvorgaben auch im Text des EBewMG-RefE niederschlagen würden, damit eine regelmäßige Anwendung sichergestellt ist.

2. Deutschland als Vollstreckungsstaat

Die Begründung des Referentenentwurfs stellt auch insoweit klar, dass die Vollstreckungsbehörde im Rahmen einer Prüfung der Ablehnungsgründe nach Art. 12 E-Evidence-Verordnung im Rahmen der Prüfung der Vorrechte (Art. 12 Abs. 1 a) E-Evidence-Verordnung) auch die deutschen Vorschriften zum Schutz von Berufsgeheimnisträgern zu prüfen hat.¹⁵ Auch hier wäre es wünschenswert, wenn das in der Begründung geschilderte Prüfprogramm sich auch im Gesetzestext niederschlagen würde.

Angezeigt wäre darüber hinaus eine Ergänzung, z. B. des § 6 Abs. 1 EBewMG-RefE. Hierin sollte eine Verpflichtung niedergelegt werden, die Verpflichteten nach § 3 EBewMG-RefE über die in Deutschland maßgeblichen Ablehnungsgründe (Immunitäten, Vorrechte, Schutz der Pressefreiheit) und deren gesetzlicher Grundlage in Kenntnis zu setzen, damit diese im Interesse ihrer, von der Maßnahme betroffenen Vertragspartner Hinderungsgründe nach Art. 10 Abs. 8 E-Evidence-Verordnung iVm Abschnitt D von Annex III zur E-Evidence-Verordnung geltend machen¹⁶ oder – in einem späteren Stadium – auf eine Ablehnung der Vollstreckung einer Anordnung hinwirken können.¹⁷ Dies ist indes nur auf Grundlage ausreichender Kenntnis der maßgeblichen Rechtslage möglich.

V. Antragsrecht für die Verteidigung

Der Referentenentwurf setzt das in Art. 1 Abs. 2 der E-Evidence-Verordnung vorgegebene Antragsrecht des Beschuldigten bzw. seines Rechtsanwalts nicht um. Vielmehr verweist er lediglich in den §§ 13, 14 EBewMG-RefE auf die Vorschriften der StPO. Diese sehen aber jedenfalls im Stadium des Ermittlungsverfahrens kein Antragsrecht des Beschuldigten bzw. seines Verteidigers im Hinblick auf die Beweiserhebung vor.¹⁸ Die Entscheidung darüber, welche Beweise erhoben werden, liegt im Ermessen der Staatsanwaltschaft. Eine Möglichkeit zu einer (gerichtlichen) Überprüfung der Entscheidung der Staatsanwaltschaft ist im nationalen Strafprozessrecht ebenfalls nicht vorgesehen.

Dem Referentenentwurf liegt offenbar ein Verständnis zugrunde, wonach dem Beschuldigten und seiner Verteidigung das Antragsrecht nur dann einzuräumen wäre, wenn ein solches Recht nach nationalem Strafprozessrecht ohnehin bereits besteht. Dass der Standpunkt des Referentenentwurfs hierzu nicht richtig sein kann, folgt bereits daraus, dass bei einem solchen Verständnis die Normierung des Antragsrechts in der Verordnung entbehrlich gewesen wäre. Dem europäischen Gesetzgeber war es aber offensichtlich sehr wichtig, das Antragsrecht gleich im ersten Artikel der Verordnung zu verankern. Der Verweis auf das nationale Recht bezieht sich demgegenüber lediglich auf die Frage, wie dieses Recht konkret ausgestaltet ist. Statt das Antragsrecht selbst in der Verordnung zu regeln, überlässt der europäische Gesetzgeber die Umsetzung den Mitgliedstaaten, damit diese es in das nationale Prozessrecht einpflegen können. Insofern bleibt der Referentenentwurf die nähere Ausgestaltung des in Art. 1 Abs. 2 der E-Evidence-Verordnung verankerten Antragsrechts schuldig. Damit wird der Referentenentwurf einer europarechtlichen Überprüfung durch den EuGH aller Voraussicht nach nicht standhalten, zumal das Argument des „*effet utile*“ aus Art. 4 Abs. 3 EUV bei der Anwendung des

¹⁵ RefE, S. 22, 50.

¹⁶ Vgl. so auch die Forderung von CCBE, Draft CCBE recommendations for Bars on the implementation of the e-Evidence Regulation, S. 4.

¹⁷ Art. 16 Abs. 3 a), Abs. 4 f) der E-Evidence-Verordnung erlaubt es den Adressaten einer Anordnung derartige Einwände gegen die Vollstreckung einer Anordnung vorzubringen.

¹⁸ Vgl. zum Antragsrecht bei der Europäischen Ermittlungsanordnung (EEA) bereits BRAK-Stellungnahme 83/2024, S. 21 ff., wobei es bei der EEA nicht um die Durchführung einer VO, sondern um die Umsetzung einer Richtlinie geht.

europäischen Rechts eine große Rolle spielt. Mit der auf der Grundlage des Referentenentwurfs vorgesehenen neuen Gesetzeslage würde in Deutschland „*die unmittelbare Geltung [der Verordnung zu diesem Punkt, d.h. das Antragsrecht der Verteidigung] aufs Spiel gesetzt*“.¹⁹ Unionsrecht geht dem nationalen Recht vor und es geht um die Frage, wie sich das Unionsrecht am besten und wirkungsvollsten durchsetzt.

1. Wortlaut, Systematik und Entstehungsgeschichte von Art. 1 Abs. 2 der E-Evidence-Verordnung

Diese Auslegung der Verordnung ist nach europäischem Recht zwingend, sie ergibt sich aus dem Wortlaut der Norm sowie ihrer Entstehung. Nach dem Wortlaut des Art. 1 Abs. 2 der E-Evidence-Verordnung kann der Erlass einer Europäischen Sicherungs- oder Herausgabeanordnung auch „*von einem Verdächtigen oder Beschuldigten oder in dessen Namen von einem Rechtsanwalt im Rahmen der geltenden Verteidigungsrechte im Einklang mit dem nationalen Strafverfahrensrecht beantragt werden*.“

Der erste Verweis auf die „*geltenden Verteidigungsrechte*“ bezieht sich systematisch auf die Ebene des europäischen Rechts²⁰ und dort insbesondere auf das **Recht auf ein faires Verfahren** und den **Grundsatz der Waffengleichheit** (Art. 6 EMRK und Art. 47, 48, 53 GRCh). Diese europaweit anerkannten Garantien gebieten es, Verdächtigen oder Beschuldigten sowie deren Verteidigung die gleiche Möglichkeit des Zugriffs auf die – in Form elektronischer Daten besonders flüchtigen – Beweismittel zu gewähren, wie den staatlichen Stellen. Zentrales Anliegen der E-Evidence-Verordnung ist es, für eine effektive Sicherung von elektronischen Beweismitteln Sorge zu tragen (s. Art. 11 Abs. 1 E-Evidence-Verordnung) und Handlungsinstrumente zu schaffen, die dem besonderen Charakter derartiger Beweismittel Rechnung trägt (vgl. Erwägungsgrund 9 d. E-Evidence-Verordnung). Die in Rede stehenden Daten unterliegen regelmäßig (teils sehr kurzen) Speicherfristen (Teilnehmerdaten, Verkehrsdaten) oder können von den Dateninhabern im Handumdrehen gelöscht werden (Inhaltsdaten). Daher liefe ein Antragsrecht der Verteidigung erst in der (stets öffentlichen und daher auch Dritten bekannten) Hauptverhandlung regelmäßig ins Leere. Es bedarf daher eines **Antragsrechts in jedem Verfahrensstadium**, um dem in Art. 1 Abs. 2 der E-Evidence-Verordnung gemachten Vorgaben effektiv Geltung zu verschaffen. Für die **spezifische Fallkonstellation der Sicherung- und Herausgabe elektronischer Beweismittel** besteht ein dringendes Bedürfnis für ein normiertes Antragsrecht der Verteidigung, um dringende Maßnahmen der Beweissicherung durchsetzen zu können und Waffengleichheit herzustellen.

Zur näheren Erläuterung ist kurz auf den Hintergrund der Einfügung des Antragsrechts in der E-Evidence-Verordnung einzugehen:

Im ersten Entwurf der Kommission²¹ war ein Antragsrecht des Beschuldigten bzw. der Verteidigung noch nicht vorgesehen, was von diversen Stakeholdern mit fundierter Begründung kritisiert wurde.

So führte etwa der CCBE aus: „*The proposal does not take properly into account the **requirement of equality of arms in criminal proceedings, which is a concept recognized by the ECtHR in the context of the right to a fair trial. Whereas prosecutors can issue production and preservation***

¹⁹ dazu EuGH v. 28. März 1985 Rs. 272/83, erster Leitsatz und Rn. 26.

²⁰ Es heißt nicht „nach den nationalen Verteidigungsrechten“ oder „nach den Verteidigungsrechten nach nationalem Recht“.

²¹ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vom 17.4.2018, COM/2018/225 final - 2018/0108 (COD).

orders, no provisions exist enabling defendants or their representatives to access or request electronic evidence."²²

Ähnlich kritisierte das europäische Netzwerk EDRI²³: *"The (1) lack of early access to the casefile and (2) to evidence-gathering tools for the defence weakens the right to a fair trial and the principle of equality of arms. Yet, the principle of equality of arms is an essential guarantee of an accused's right to defend themselves. It ensures that the accused has a genuine opportunity to prepare and present their case, and to contest the arguments and evidence put before the court, on a footing equal to that of the prosecution. ...*

2. In practice, it is extremely difficult, if not impossible, for the defence to use the cross-border evidence gathering mechanisms to gather evidence abroad. It can only trust the objectivity of law enforcement authorities to gather both incriminatory and exculpatory information.

Therefore, the future Regulation should (1) give early access to the casefile and (2) empower the defence to request a production or preservation order on behalf of a suspected or accused person in order to gather evidence on equal terms with the prosecution. Member States or service providers receiving such requests should have the obligation to process them with the same urgency as requests received from law enforcement authorities."²⁴

Die Forderung lautete übersetzt ins Deutsche, die **künftige Verordnung müsse ... (2) die Verteidigung ermächtigen, im Namen einer verdächtigen oder beschuldigten Person eine Anordnung zur Vorlage oder Sicherung von Beweismitteln zu beantragen, um auf Augenhöhe mit der Staatsanwaltschaft Beweise zu sammeln.**

Diese Bedenken berücksichtigend, fügte das Europäische Parlament daraufhin das Antragsrecht in seinen Vorschlag für die Verordnung mit dem heute geltenden Wortlaut ein.²⁵

Es ist folglich neben dem Wortlaut und seiner Systematik auch aus der Entstehungsgeschichte ersichtlich, dass dem Beschuldigten und seinem Verteidiger das Antragsrecht aufgrund der allgemeinen Verteidigungsrechte zu gewähren ist. Das Verständnis der Bundesrechtsanwaltskammer deckt sich insoweit mit der Auslegung durch den CCBE. Dieser führt in seinen Empfehlungen zur Umsetzung der Verordnung im Hinblick auf Art. 1 Abs. 1 der Verordnung aus: *"While it is clear that the Regulation intends to grant a lawyer the right to make such a request, the right is phrased as being granted 'within the framework of applicable defence rights in accordance with national criminal procedural law'."*²⁶

²² CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters vom 19.10.2018 (abrufbar unter: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf, zuletzt abgerufen am 6.12.2024).

²³ EDRI - European Digital Rights ist ein europäischer Zusammenschluss von Nichtregierungsorganisationen, dem u.a. der CCBE, Fair Trials und der DAV angehören, die auch an der hier zitierten Publikation Demonstrating gaps in the e-Evidence Regulation mitgewirkt haben.

²⁴ Die Publikation ist abrufbar unter: <https://www.cpme.eu/api/documents/adopted/2021/9/cpme.2021-116.eEvidence-Scenarios.pdf>, siehe dort S. 28 (zuletzt abgerufen am 6.12.2024).

²⁵ Die Regelung fand sich damals noch in Art. 1 Abs. 1a. Geändert wurde nachträglich lediglich eine Ergänzung, wonach auch der Beschuldigte selbst einen solchen Antrag stellen kann.

²⁶ CCBE, Draft CCBE recommendations for Bars on the implementation of the e-Evidence Regulation, S. 2 f.

2. Vorschläge für die Integration des Antragsrechts in das deutsche Recht

Die Bundesrechtsanwaltskammer erachtet die **Einführung eines entsprechenden Antragsrechts** auf Beweiserhebung als zwingend notwendig. Der Antrag wäre in den Fällen des § 7 Abs. 1 RefE (Herausgabe von Teilnehmerdaten und zur Erlangung von ausschließlich zum Zweck der Identifizierung des Nutzers erforderlichen Daten) an die Staatsanwaltschaft zu stellen. Zu verbinden wäre das Antragsrecht mit einem – nach der Systematik der StPO üblichen – Antrag auf gerichtliche Entscheidung und einer Beschwerdemöglichkeit zum Gericht der nächsthöheren Instanz. In den Fällen des § 7 Abs. 2 RefE (Erlangung von Verkehrsdaten mit Ausnahme von ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten und zur Erlangung von Inhaltsdaten nach Artikel 4 Absatz 2 Buchstabe a der E-Evidence-Verordnung) bestünde insoweit eine Zuständigkeit des Gerichts, die mit einer Beschwerdemöglichkeit zum Gericht der nächsthöheren Instanz zu verbinden wäre. Aufgrund der Flüchtigkeit von elektronischen Beweismitteln, wäre das Antragsrecht zu flankieren durch die Möglichkeit, einen Eilantrag zu stellen. Bei Zweifeln wäre zunächst eine Sicherungsanordnung zu erlassen, um die Löschung der begehrten Daten vor Ergehen der abschließenden Entscheidung zu verhindern.

Ein entsprechendes Eilverfahren müsste auch für das gerichtliche Verfahren eingeführt werden, da insoweit zwar grundsätzlich ein Beweisantragsrecht besteht, dieses aber nach der StPO aktuell nicht kurzfristig überprüfbar ist. Eine Geltendmachung der Verletzung des Antragsrechts erst im Rahmen der Revision würde dieses Recht hinfällig machen.

3. Kein Verstoß gegen das Doppelregelungsverbot

Da der europäische Gesetzgeber die konkrete Ausgestaltung des Antragsrechts ausdrücklich den Mitgliedstaaten überlassen hat, verstößt eine entsprechende Regelung durch den nationalen Gesetzgeber selbsterklärend auch nicht gegen das europarechtliche Doppelregelungsverbot. Das prinzipielle Verbot nationaler Parallelgesetzgebung bezieht sich auf die bloße Wiederholung einer Bestimmung, die bereits durch die unmittelbar geltende Verordnung selbst getroffen wurde. Das Doppelregelungsverbot verbietet jedoch nicht, dass nationale Bestimmungen anlässlich ihrer Anpassung an die neue, durch die Verordnung geschaffene Gesetzeslage *„im Interesse ihres inneren Zusammenhangs und ihrer Verständlichkeit für die Adressaten bestimmte Punkte der (Unions-) Verordnungen wiederholen“*²⁷. Kann ein bestimmtes System von Regelungen nur durch *„das Zusammentreffen einer ganzen Reihe“* unionsrechtlicher und einzelstaatlicher Vorschriften²⁸ verwirklicht werden, darf der nationale Gesetzgeber eine zersplitterte Rechtslage ausnahmsweise durch den Erlass eines zusammenhängenden Gesetzeswerks bereinigen, auch wenn dadurch punktuelle Normwiederholungen nötig sind.²⁹ Verweist eine Verordnung für die Ausgestaltung des Antragsrechts gerade auf das nationale Recht, so steht eine solche Regelung ersichtlich nicht im Konflikt mit den Vorgaben der Verordnung, sondern die Verordnung verlangt umgekehrt die nähere Ausgestaltung (des bisher nicht existenten Antragsrechts) *„im Interesse ihres inneren Zusammenhangs und ihrer Verständlichkeit für die Adressaten“*³⁰, auch wenn es zu diesem Zweck einer „Wiederholung“ des Antragsrechts bedarf.

²⁷ EuGH v. 28. März 1985 Rs. 272/83 zweiter Leitsatz und Rn. 27.

²⁸ Nochmals: EuGH v. 28. März 1985 Rs. 272/83 zweiter Leitsatz und Rn. 27.

²⁹ W. Schroeder in: Streinz, EUV/AEUV 3. Aufl. 2018 Rn. 50.

³⁰ EuGH v. 28. März 1985 Rs. 272/83 Rn. 27.

VI. Löschungspflichten, Zweckbindung, Mitteilungspflichten (Deutschland als Anordnungsstaat)

Der Referentenentwurf stellt in begrüßender Klarheit fest, dass im Falle einer gerichtlichen Feststellung der Rechtswidrigkeit einer Herausgabeanordnung etwaig bereits übermittelte Daten unverzüglich zu löschen sind, vgl. § 15 Abs. 2 S. 2 EBewMG-RefE. Diese, für sich genommen zu begrüßende Regelung sollte ergänzt werden durch einen weiteren Satz, der § 161 Abs. 2 StPO für entsprechend anwendbar erklärt. Diese Regelung stellt klar, dass für **Löschungspflichten** nach der StPO § 58 Abs. 3 BDSG keine Anwendung findet. Da der Referentenentwurf die Regelungen zur E-Evidence-Verordnung jedoch nicht in die StPO integriert hat, sondern ein eigenes Stammgesetz bevorzugt,³¹ findet § 161 Abs. 2 StPO nach dem Wortlaut zunächst keine Anwendung. Allerdings unterscheidet sich die Interessenlage nicht von einer in der StPO selbst normierten Löschungspflicht, weshalb eine entsprechende Anwendung des § 161 Abs. 2 StPO angezeigt ist.

Ein vergleichbarer Klarstellungsbedarf besteht hinsichtlich des in § 479 Abs. 2 S. 1 StPO und § 100 e Abs. 6 StPO geregelten **Zweckbindungsgrundsatzes**. Die Vorschrift regelt, dass Daten, die durch besonders eingriffsintensive Maßnahmen generiert werden, nur unter bestimmten Bedingungen („hypothetischer Ersatzeingriff“³²) zur Verfolgung anderer Straftaten genutzt werden dürfen. § 479 Abs. 2 S. 1 StPO stellt insoweit allerdings auf „Maßnahmen nach diesem Gesetz“ ab. § 100 e Abs. 6 StPO verweist auf „Maßnahmen nach den §§ 100 b und 100 c StPO“. Der Referentenentwurf stellt zwar ausdrücklich klar, dass bei einer (ausgehenden) Herausgabeanordnung eine Prüfung nach den Vorschriften des nationalen Rechts zu erfolgen hat.³³ Dennoch handelt es sich bei der Herausgabeanordnung nach strenger Lesart um eine Maßnahme nach EBewMG-RefE iVm der E-Evidence-Verordnung. Ein mehrstufiges System (wie z. B. bei Haftbefehl und EU-Haftbefehl) ist nach dem EBewMG-RefE nicht vorgesehen, so dass es an der der Herausgabeanordnung zugrundeliegende nationale Entscheidung fehlt. Daher sollte auch hier klargestellt werden, dass die Zweckbindungsregelungen der StPO entsprechende Anwendung finden.

Darüber hinaus hat der Bundesgesetzgeber in der Strafprozessordnung an verschiedenen Stellen **Bekanntmachungs- bzw. Mitteilungspflichten** normiert (vgl. z. B. § 35 Abs. 2 StPO,³⁴ § 101 Abs. 4 StPO). Auch diese Regelungen beziehen sich bei strenger Lesart auf Maßnahmen nach der StPO. Auch hier ist sicherzustellen, dass diese Pflichten auch bei vergleichbaren Maßnahmen nach dem EBewMG-RefE iVm der E-Evidence-Verordnung bestehen. Eine Unterrichtung des Betroffenen ist auch deshalb dringend geboten, um den Weg zum gerichtlichen Rechtsschutz nach §§ 14 f. EBewMG-RefE zu öffnen. Zudem ist nach Art. 13 Abs. 1, Abs. 3 E-Evidence-Verordnung eine Information der betroffenen Person (Dateninhaber) sicherzustellen. Da Art. 13 Abs. 2 E-Evidence-Verordnung die Ausgestaltung dem nationalen Gesetzgeber ermöglicht, ist eine klare Regelung im deutschen Recht vorzunehmen.

Jedenfalls hinsichtlich dieser fundamentalen Regelungen sollte im Interesse der Praxisfreundlichkeit nicht auf die „Generalverweisklausel“ des § 13 EBewMG-RefE zurückgegriffen werden müssen.

³¹ Vgl. RefE, S. 1, 27.

³² Vgl. dazu Gieg, in: KK-StPO, 9. Aufl. 2023, § 479, Rn. 3 mwN.

³³ RefE, S. 49.

³⁴ Vgl. dazu z. B. BGH, Beschl. v. 24.11.2009 - StB 48/09 (a) zur Bekanntmachungspflichten bei Beschlagnahmen beim Provider.



Ausschussdrucksache 21(6)49c
vom 9. Januar 2026, 12:02 Uhr

Schriftliche Stellungnahme
des Sachverständigen Sven Kurenbach

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes 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
BT-Drucksache 21/3192



Bundeskriminalamt, 65173 Wiesbaden

Per E-Mail
Deutscher Bundestag
Ausschuss für Recht und Verbraucherschutz
Paul Löbe Haus
Berlin

Am Treptower Park 5-8
12435 Berlin

Zentrale Postanschrift:
65173 Wiesbaden

Tel. +49 611 55-0
Fax +49 611 55-26003

bearbeitet von:
Leitungsstab 4

LS4-2025-0037217910

www.bka.de

Gesetzentwurf der Bundesregierung 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 (BT-Drs. 21/3192)

hier: Stellungnahme Bundeskriminalamt

Bezug: Öffentliche Anhörung am 12.01.2026, 15:00 Uhr

Berlin, 08.01.2026
Seite 1 von 5

Sehr geehrte Damen und Herren,

das Bundeskriminalamt (BKA) nimmt zu dem o. g. Gesetzentwurf auf BT-Drs. 21/3192 wie folgt Stellung:

1. Vorbemerkung

Mit dem vorliegenden Gesetz zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 (nachfolgend e-Evidence-VO - eEVO) werden die europäischen Vorgaben zur grenzüberschreitenden Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren in nationales Recht überführt und die organisatorischen und verfahrensrechtlichen Voraussetzungen geschaffen, um die e-Evidence-Instrumente in der Praxis rechtssicher anwenden zu können. Ein zentraler Baustein der Richtlinie ist hierbei die Pflicht zur Benennung von Zustellungsbevollmächtigten (bzw. Ansprechpartnern/Vertretern) durch Diensteanbieter, um Zustellungen grenzüberschreitender Anordnungen innerhalb der EU sicherzustellen.

Für die polizeiliche Praxis sind insbesondere die Europäische Herausgabee-Anordnung und die Europäische Sicherungsanordnung - zwei Instrumente der eEVO - von zentraler Bedeutung. Beide Instrumente adressieren den praktischen Kernbedarf der Strafverfolgung: Anfragen zu Teilnehmer- und Identifizierungsdaten sowie Anfragen zu Inhalts- und Verkehrsdaten direkt an ausländische Anbieter stellen zu können, ohne auf



Seite 2 von 6

eine freiwillige Kooperation der Anbieter angewiesen zu sein oder den zuweilen langwierigen Weg der justiziellen Rechtshilfe über die zuständigen Behörden im EU-Mitgliedsstaat zu beschreiten, in dem der Anbieter seinen Sitz (Zustellungsbevollmächtigung) hat.

Es werden daher aus polizeilicher Sicht die Verfahrenserleichterungen zur Erlangung digitaler Beweismittel innerhalb der EU und die Schaffung rechtsstaatlich verbindlicher Regelungen begrüßt. Weiterhin wird auf praktische Herausforderungen hingewiesen, welche die aktuell geplante Umsetzung der eEVO und der hier gegenständliche Gesetzesentwurf für die Strafverfolgungsbehörden in Deutschland, insbesondere für die Polizeien des Bundes und der Länder, mit sich bringen dürften.

2. Rechtliche Aspekte

a) Strafverfolgung

Die eEVO bedeutet für Strafverfahren einen maßgeblichen Fortschritt. Sie schafft ein einheitliches, verbindliches Instrument zur grenzüberschreitenden Direkterlangung elektronischer Beweismittel, das gerade bei dynamischen Sachverhalten und einem hohen Zeitdruck die Abläufe spürbar beschleunigen sollte.

Dabei werden die Anordnungen in der Regel von der Polizei, von Finanzbehörden oder von Behörden der Zollverwaltung erstellt und vor der Weiterleitung an ausländische Anbieter durch die jeweils zuständige Justizbehörde validiert. Bei dem Vorliegen einer unmittelbaren Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person oder für eine kritische Infrastruktur können Herausgabeanordnungen ausnahmsweise direkt durch Polizeibehörden erlassen werden (siehe Art. 4 Abs. 5 eEVO). In diesen Fällen ist innerhalb von 48 Stunden eine Validierung durch die Staatsanwaltschaft oder ein Gericht nachzuholen. Für die Praxis bedeutet dies, dass die Abläufe so aufzustellen sind, dass Anordnungen fristgerecht – auch an Wochenenden, Feiertagen und außerhalb der Regeldienstzeiten – und in der Sprache des Ziellandes zeitnah an die Anbieter übermittelt werden können.

Aus den Transparenzberichten großer Anbieter ergibt sich für Deutschland im Zeitraum 01/2024 bis 12/2024 eine Größenordnung von mehr als 160.000 behördlichen Anfragen zu Nutzerdaten allein bei Apple, Google, Meta, Microsoft und TikTok. Wenngleich in den Berichten keine Unterscheidung zwischen Anfragen in Strafverfahren, Gefahrenabwehr- oder Zentralstellenvorgängen vorgenommen wird, entfällt ein nicht unerheblicher Anteil der übersandten Anfragen aus Deutschland auf Strafverfahren.

Seite 3 von 6

Bundesweit ist daher nach Inkrafttreten der eEVO mit einer niedrigen bis mittleren sechsstelligen Zahl pro Jahr an zeitnah zu validierenden Anfragen in Strafverfahren zu rechnen. Angesichts der sich weiter beschleunigenden Digitalisierung der Kriminalität dürfte deren Anzahl in den Folgejahren weiter ansteigen. Vor diesem Hintergrund kommt aus polizeifachlicher Sicht nicht der Anordnungserstellung durch die Polizei, die einen mit bisherigen Bestandsdatenabfragen vergleichbaren Aufwand mit sich bringen wird, sondern der Validierung durch die Justiz, einem neuen und damit zusätzlichen Verfahrensschritt, eine entscheidende Rolle im e-Evidence-Prozess zu. Aufgrund der zu erwartenden Mengenvolumina und der erforderlichen Implementierung dieses zusätzlichen Verfahrensschritts ist mit einem justiziellen Mehraufwand zu rechnen.

b) Zentralstelle und Gefahrenabwehr

Zu begrüßen ist weiterhin, dass das nationale Umsetzungsgesetz außerhalb von Strafverfahren keine zusätzlichen, neuen Durchführungsmechanismen etabliert und die rechtlichen Grundlagen für Auskunftersuchen – insbesondere zu Teilnehmer- und Identifizierungsdaten – für die Aufgabenwahrnehmung des BKA als Zentralstelle (§ 2 BKAG) sowie im Kontext der Abwehr von Gefahren des internationalen Terrorismus (§ 5 BKAG) fortbestehen:

- Bestandsdatenabfragen nach § 10 BKAG (Zentralstelle) und § 40 BKAG (Gefahrenabwehr)
- Auskunftsverlangen zu Nutzungsdaten bei Digitalen Diensten gemäß § 10a BKAG (Zentralstelle) und § 52 Abs. 2 BKAG (Gefahrenabwehr)
- Erheben von Verkehrsdaten bei Telekommunikationsdiensten gemäß § 52 Abs. 1 BKAG (Gefahrenabwehr)

Die Polizeigesetze der Länder sowie der Bundespolizei enthalten gleichlautende Regelungen für Bestandsdatenabfragen und Auskunftsverlangen zu Nutzungsdaten und die Erhebung von Verkehrsdaten.

Spiegelbildlich hierzu regeln die Parallelvorschriften der §§ 170 ff. TKG (Telekommunikationsgesetz) und §§ 22 ff. TDDDG (Telekommunikations-Datenschutz-Diensteanbieter-Gesetz) die (Herausgabe-)Verpflichtungen und Verarbeitungsbefugnisse der Anbieter. Für die diesbezüglichen Herausgabeverpflichtungen gilt aus Sicht des BKA dabei im Kontext von Strafverfahren nach wie vor das Marktortprinzip¹. Dies bedeutet, dass die entsprechenden Vorschriften bei Auskunftsverlangen in grenzüberschreitenden Sachverhalten und auch für Anbieter mit Sitz außerhalb Deutschlands unverändert rechtlich verbindlich sind, sofern sie im Bundesgebiet Niederlassungen haben oder Dienstleistungen erbringen.

¹ siehe hierzu § 1 Abs. 2 TKG und § 1 Abs. 3 TDDDG.
Ausschussdrucksache 21(6)49c



Seite 4 von 6

Gleichwohl zeigt die Praxis, dass die Verbindlichkeit dieser Verpflichtungen von einzelnen ausländischen Anbietern nicht immer anerkannt wird, sofern den Anfragen kein Rechtshilfeersuchen oder eine justizielle Anordnung zugrunde liegt. Auskunftersuchen, insbesondere zu Bestandsdaten, werden daher oft nur im Rahmen einer „freiwilligen“ Kooperation beantwortet oder mit Verweis auf angeblich fehlende Zuständigkeiten zurückgewiesen. Gerade im Aufgabenbereich des BKA als Zentralstelle (§ 2 BKAG) sowie in Gefahrenabwehrvorgängen (§ 5 BKAG) und beim Schutz von Mitgliedern der Verfassungsorgane (§ 6 BKAG) werden jedoch regelmäßig Antworten Bestands- und Nutzungsdatenanfragen benötigt, um Tatverdächtige zu identifizieren, örtliche Zuständigkeiten festzustellen und Sachverhalte zur weiteren Bearbeitung zu verdichten. Allein im Jahr 2024 hat das BKA in diesem Kontext Anfragen an ausländische Anbieter in niedriger fünfstelliger Höhe gestellt. Vergleichbare Anforderungen zu Auskünften aus Bestands- und Nutzungsdatenanfragen im polizeirechtlichen Kontext bestehen für die Polizeien der Länder und die Bundespolizei.

Aus polizeilicher Sicht besteht daher die Sorge, dass Anfragen außerhalb von Strafverfahren nach Inkrafttreten der eEVO – mit Ausnahme von Notfalleinfragen² (sog. Emergency-Requests) – vermehrt nicht mehr beantwortet werden. Dies würde eine insbesondere bei Gefährdungshinweisen im Phänomenbereich der Politisch Motivierten Kriminalität sowie bei der Bekämpfung von zum Teil schweren Sexualdelikten eine erhebliche Einschränkung bedeuten. Gleiches dürfte für die Aufgabenwahrnehmung der Polizeien der Länder im Bereich der Gefahrenabwehr gelten.

Vor diesem Hintergrund ist es angezeigt, bestehende Auskunftspflichten gegenüber ausländischen Anbietern und das Marktortprinzip für Telekommunikationsanbieter und Anbieter Digitaler Dienste sowie die hieran anknüpfenden Verpflichtungen auch nach Inkrafttreten der eEVO als verbindlichen Maßstab abzusichern. Es ist daher zu begrüßen, dass dies in der Gesetzesbegründung klar herausgestellt wird. Auch die Pflichten des Art. 10 DSA (Digital Services Act) sind seitens der Anbieter weiterhin zu beachten. Dies findet sich in der Gesetzesbegründung jedoch noch nicht hinreichend wieder, so dass eine klarstellende Ergänzung empfohlen wird.

Darüber hinaus bedarf es aus polizeilicher Sicht der Möglichkeit einer konsequenten Durchsetzung dieser Auskunftspflichten und einer spürbaren Sanktionierung bei Nichtbefolgung, damit die Auskunftspflichten nicht als eine freiwillige Kooperationsbereitschaft wahrgenommen werden. In diesem Zusammenhang regt das BKA an, existierende Bußgeldtatbestände und deren Höhe anzupassen.

² gem. 18 U. S. Code § 2702 (b)(8) und (c)(4) ist eine Notfalleinfrage zu stellen, wenn eine gegenwärtige und konkrete Gefahr für Leib und Leben vorliegt.

Seite 5 von 6

c) Sicherungsanordnung

Das Umsetzungsgesetz bleibt aus polizeifachlicher Sicht bei der Befugnis zur Sicherungsanordnung hinter den Vorgaben der eEVO zurück. Der Gesetzgeber hat mit dem Entwurf eines „Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“ verdeutlicht, dass er beabsichtigt, eine Befugnis zur Sicherungsanordnung gegenüber den Telekommunikationsanbietern bei Verkehrsdaten in das Strafprozessrecht einzuführen. Dadurch ist sichergestellt, dass in deutschen Strafverfahren das Instrument der Europäischen Sicherungsanordnung bezogen auf diese Daten genutzt werden kann.

Allerdings ist bislang nicht sichergestellt, dass das in der eEVO vorgesehene Instrument der Sicherungsanordnung auch für die gespeicherten Inhaltsdaten bei Telekommunikationsanbietern (z. B. E-Mail-Anbieter) oder Inhalts- und Nutzungsdaten bei den Anbietern Digitaler Dienste ins nationale Strafverfahrensrecht eingeführt wird. Dieses wäre aus Sicht der Strafverfolgungsbehörden jedoch fachlich sinnvoll, um z. B. in einem deutschen Strafverfahren gegenüber einem französischen Anbieter eine entsprechende Sicherungsanordnung über den E-Evidence-Mechanismus aussprechen zu können.

Auf Basis des derzeitigen Entwurfs wäre es denkbar, dass für ein Strafverfahren eines anderen EU-Mitgliedsstaates ein deutscher E-Mail-Anbieter (etwa GMX) gespeicherte Inhaltsdaten und zugehörige Verkehrsdaten sichern muss, dies aber für ein deutsches Strafverfahren zwar bezogen auf Verkehrsdaten, nicht jedoch für die ermittlungsrelevanten Inhaltsdaten angeordnet werden kann. Die eEVO sieht in diesen Fällen vor, dass Inhalts- und zugehörige Verkehrsdaten gesichert werden, um einen Beweismittelverlust zu verhindern, bevor Täter diese Daten aus dem Account löschen und die eigentliche Datenerhebung stattfinden konnte. Aus polizeilicher Sicht wären daher entsprechende Befugnisnormen in der StPO zu empfehlen, da ansonsten nur auf die allgemeinen Datenerhebungsbefugnisse der §§ 94 ff. StPO verwiesen werden könnte.

3. Technik und Erfüllungsaufwand

Nach derzeitiger Planung wird die Umsetzung der Europäischen Herausgabeanordnung und der Europäischen Sicherungsanordnung über eine Referenzimplementierung der EU-Kommission (e-Evidence Digital Exchange System - eEDES) erfolgen. Diese Umsetzung wird kurz- bis mindestens mittelfristig in der polizeilichen Praxis für Medienbrüche sorgen, da die Weboberfläche von eEDES bislang nur über das Internet und damit nicht aus den polizeilichen und justiziellen Systemen heraus erreichbar ist.

Die angekündigte Bereitstellung zentraler technischer Spezifikationen und eines Testsystems durch die EU im März 2026 sowie eines Produktivsystems wenige Wochen vor dem Start ist als ambitioniert anzusehen und ermöglicht wenig Raum für belastbare Tests und Prozessstabilisierungen.



Seite 6 von 6

Da die Realisierung der technischen Lösungen über die polizeiliche Umgebung vor dem Hintergrund offener technischer Fragen bis August 2026 unsicher ist, wird das BKA als Rückfalloption zunächst die Übermittlung von Anfragen nach der eEVO über die Weboberfläche von eEDES einplanen. Hier sind Medienbrüche und zusätzliche personelle Aufwände absehbar, da Anfragen außerhalb der polizeilichen Informationssysteme händisch in die vorgegebenen Formulare eingegeben werden müssen. Medienbrüche aufgrund der bisherigen Größenbeschränkung der EU-Schnittstelle für die zu übermittelnden Dateien sind ebenfalls erwartbar.

Nach aktuellem Stand ist für das BKA mit einmaligen Kosten in Höhe von ca. 500.000 Euro für die initiale Implementierung sowie jährlichen Kosten in Höhe von ca. 350.000 Euro für den Betrieb zu rechnen. Gleichmaßen entstehenden in den Ländern Aufwände für die dortige Anbindung der Polizeien an die eEDES. Betriebliche Zusatzaufwände werden weiterhin bei den Staatsanwaltschaften entstehen, die jährlich Anfragen im mittleren sechsstelligen Bereich gemäß der eEVO validieren müssen.



Ausschussdrucksache 21(6)49d
vom 9. Januar 2026, 09:42 Uhr

Schriftliche Stellungnahme
des Sachverständigen Sebastian Murer

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes 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
BT-Drucksache 21/3192

Deutscher Bundestag Rechtsausschuss

Öffentliche Anhörung

zum 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 (E-Evidence)

Bundestagsdrucksache 21/3192

Schriftliche Stellungnahme

Sachverständiger:

Name: Sebastian Murer
Institution: Generalstaatsanwaltschaft München
Funktion: Oberstaatsanwalt

Datum der Anhörung: 12.01.2026

München, den 09.01.2026

Stellungnahme zum Gesetzentwurf zur Umsetzung und Durchführung des europäischen E-Evidence-Pakets

I. Einleitung

Grundlage dieser Stellungnahme sind die praktischen Erfahrungen eines langjährigen Strafverfolgers. Ziel ist es, **eine effektive Strafverfolgung** auch im digitalen Zeitalter sicherzustellen.

II. Ermittlungsrealität

Elektronische Beweismittel sind heute in nahezu allen Ermittlungsverfahren von zentraler Bedeutung. Kindesmissbrauch, Organisierte Kriminalität, Terrorismus und andere Kriminalitätsformen (Cybercrime) hinterlassen regelmäßig **grenzüberschreitend** digitale Spuren wie Inhalts-, Bestands-, Nutzungs- und Verkehrsdaten, die zur Identifizierung der Täter und Aufklärung des Sachverhalts unerlässlich sind. Regelmäßig werden diese Daten von **international tätigen Diensteanbietern** gespeichert, deren Sitz sich häufig außerhalb des Hoheitsgebiets des ermittelnden Mitgliedstaates befindet. Die bisherigen Instrumente der internationalen Rechtshilfe haben sich für diese Realität gerade bei **flüchtigen Daten** als unzureichend erwiesen. Die entsprechenden Ersuchen dauern zum Teil mehrere Monate und dies führt nicht selten zum endgültigen Verlust relevanter Beweise. Auch verweisen Diensteanbieter des Öfteren darauf, dass die betreffenden Daten auf Servern in Drittstaaten gespeichert seien und sich die Ermittler dorthin wenden sollen. Mangels Erfolgsaussichten werden entsprechende Rechtshilfeersuchen von den Staatsanwaltschaften daher teilweise erst gar nicht gestellt.

III. Bewertung des E-Evidence-Pakets

Das europäische E-Evidence-Paket, bestehend aus der Richtlinie (EU) 2023/1544 und der Verordnung (EU) 2023/1543 (letztere im Folgenden: Verordnung), wird daher **ausdrücklich begrüßt**. Die Einführung von Herausgabe- und Sicherungsanordnungen ermöglicht erstmals einen schnellen, direkten und unionsweit durchsetzbaren grenzüberschreitenden Zugriff auf elektronische Beweismittel bei in der EU tätigen

Diensteanbietern. Eine mangelhafte Auskunftserteilung der Diensteanbieter kann zudem sanktioniert werden. Das E-Evidence-Paket kann damit zur **nachhaltigen Bekämpfung von Straftaten** beitragen.

IV. Anforderungen an die nationale Durchführung der Verordnung

Die unionsrechtlichen Vorgaben der unmittelbar geltenden Verordnung, beispielsweise zur Prüfung von Ablehnungsgründen im Rahmen der Notifizierung, sind für die Praxis herausfordernd, das Verfahren aufwendig. Um das Instrument in der **Praxis dennoch zum Erfolg** zu führen, sind bei den gesetzlichen Vorschriften zur Durchführung im Bundesgebiet aus meiner Sicht folgende Punkte in den Blick zu nehmen:

1. Sicherungsanordnung

Sowohl die Europäische Herausgabeordnung als auch die Europäische Sicherungsanordnung dürfen nur erlassen werden, wenn in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen eine ähnliche Anordnung hätte erlassen werden können, Art. 5 Abs. 2, 6 Abs. 3 der Verordnung. Das setzt **entsprechende nationale Instrumente in der StPO voraus**. Bisher fehlt es in der StPO jedoch an einer entsprechenden Sicherungsanordnung. Ob der Weg über die Beschlagnahme nach §§ 94, 98 StPO insoweit aus Sicht des Unionsrechts ausreicht, dürfte mit Unsicherheiten behaftet sein.

Daher ist die möglichst schnelle Einführung einer **umfassenden Sicherungsanordnung** in der StPO erforderlich. Eine entsprechende Initiative des Gesetzgebers sollte rasch umgesetzt werden, um nicht bei Geltung der Verordnung ab 18. August 2026 ein deutsches Vollzugsdefizit zu riskieren.

2. Dreimonatige Speicherung von IP-Adressen

Zur praktischen Wirksamkeit der Herausgabe- und Sicherungsanordnung ist eine nationale Verpflichtung von Internetzugangsanbietern zur **Speicherung von IP-Adressen** für einen Zeitraum von drei Monaten erforderlich. IP-Adressen sind in vielen Verfahren, insbesondere bei sexuellem Missbrauch von Kindern im Internet, Kinderpornografie, Terrorfinanzierung, Drogenhandel im Darknet, Cybercrime (u.a. Betrug mit Fake-Shops, betrügerische Anlageplattformen, Phishing mit virtuellen Debit-

karten, Phishing mit QR-Codes) und strafbarer Hatespeech regelmäßig der einzige Anknüpfungspunkt **zur Identifizierung des Täters**. Bislang werden relevante IP-Adressen, Logfiles oder Kommunikationsdaten häufig automatisiert gelöscht, bevor ein richterlicher Beschluss oder ein Rechtshilfeersuchen um Herausgabe vorliegt.

Die Speicherung von IP-Adressen stellt einen vergleichsweise geringen Eingriff dar, ist zeitlich begrenzt und unterliegt strenger Zweckbindung. Sie ist nach der Rechtsprechung des EuGH unter bestimmten Voraussetzungen unionsrechtlich zulässig und auch verfassungsrechtlich verhältnismäßig.

Um Anordnungen **nicht leerlaufen zu lassen**, ist daher auch unter diesem Gesichtspunkt eine rasche Umsetzung des **Gesetzentwurfs zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren** von großer Bedeutung. Da viele Diensteanbieter ihren Sitz oder Ansprechpunkt im Ausland haben (werden), erscheint es zudem erforderlich, **unionsrechtlich zu harmonisieren** und eine EU-weite Regelung zur Speicherung zu schaffen.

3. Zuständigkeit auch der Staatsanwaltschaft für die Übermittlung der Bescheinigung einer Herausgabeanordnung, § 10 Abs. 3 Satz 1 EBewMG-E

Der Gesetzentwurf sieht in § 10 Abs. 3 Satz 1 des neuen Stammgesetzes (Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetz/EBewMG) bislang nur das Gericht als zuständig für die Übermittlung der Bescheinigung an den Diensteanbieter an. Diese Regelung sollte aus Sicht der Praxis ergänzt werden. **Auch die Staatsanwaltschaft** sollte – neben dem Gericht – bei Bedarf die Bescheinigung selbst übermitteln und damit bestimmen können, zu welchem konkreten Zeitpunkt sie die Anordnung – ggf. in Abstimmung mit weiteren Ermittlungsmaßnahmen oder anderen Ermittlungsbehörden – vollzieht. Als **Leiterin des Ermittlungsverfahrens** (§§ 152, 160 StPO) trägt sie die Verantwortung für Rechtmäßigkeit, Zweckmäßigkeit und Zeitpunkt der Maßnahme.

Zwar erfolgt die Übermittlung der Bescheinigung ausschließlich über ein dezentrales IT-System und kann daher grundsätzlich auch durch das Gericht erfolgen. In der Praxis gibt es jedoch vielfältige Fallkonstellationen, in denen die Staatsanwaltschaft **mit gutem Grund** selbst über den Vollzug von gerichtlich angeordneten Maßnahmen entscheidet.

So können etwa zwischen Erlass und Vollzug **Umstände eintreten**, die den Vollzug der (rechtmäßig angeordneten) Maßnahme untersagen, jedoch nur der Staatsanwaltschaft bekannt sind. Auch kann es bei **konzertierten Aktionen** zum Schutz des gesamten Verfahrenskomplexes erforderlich sein, einen **gemeinsamen Vollzugszeitpunkt** zu wählen. Bei **besonderer Eilbedürftigkeit** könnte es im richterlichen Breitschaftdienst insbesondere am Wochenende oder an Feiertagen außerdem zu Übermittlungsschwierigkeiten kommen, wenn mit dem IT-System nicht gleichermaßen geübtes Personal im Dienst ist.

Durch die Rückleitung vom Gericht zur Staatsanwaltschaft entsteht aufgrund Einführung der **eAkte** im Übrigen kein wesentlicher Zeitverzug.

V. Schlussbemerkung - Mehraufwand für die Staatsanwaltschaft

Die Umsetzung und Durchführung des E-Evidence-Pakets führt zu einem erheblichen **zusätzlichen Arbeitsaufwand** für die Staatsanwaltschaften. Dieser Mehraufwand betrifft nicht nur die Prüfung **von eigenen Herausgabe- und Sicherungsanordnungen**, sondern auch die Prüfung von Ablehnungsgründen bei aus dem Ausland eingehenden Anordnungen im Rahmen der **Notifizierung** und auch die **Vollstreckung** bei Verletzung der Mitwirkungspflichten durch den Diensteanbieter, insbesondere **bei Bußgeldern** nach § 18 EBewMG-E.

Diese Bußgeldverfahren werden eine eigenständige rechtliche Prüfung, eine Dokumentation der Versäumnisse sowie eine belastbare Beweisführung gegenüber häufig im Ausland ansässigen Unternehmen erfordern. Die Verfahren werden regelmäßig komplex, zeitaufwendig und mit erheblichem Kommunikationsaufwand verbunden sein. Sie binden qualifiziertes Personal und erfordern spezialisiertes Know-how im europäischen Verfahrensrecht sowie im Unternehmens- und Datenschutzrecht.

Gerade diese Vollstreckungsaufgaben gegenüber Diensteanbietern könnten grundsätzlich auch zentral durch eine Bundesbehörde, zum Beispiel durch das Bundesamt für Justiz, durchgeführt werden. Davon hat der Gesetzgeber jedoch abgesehen. Daher sollte im Gegenzug die **Unterstützung der Länder** und damit auch der Staatsanwaltschaften, beispielsweise über den **Pakt für den Rechtsstaat**, erhöht werden.



Ausschussdrucksache 21(6)49e
vom 9. Januar 2026, 14:50 Uhr

Schriftliche Stellungnahme
des Sachverständigen Prof. Dr. Arndt Sinn

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes 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
BT-Drucksache 21/3192

Fachbereich Rechtswissenschaften

Prof. Dr. Arndt Sinn
(Prof. h.c. National University
Kaohsiung)

Lehrstuhl für Deutsches und
Europäisches Straf- und Strafprozess-
recht, Internationales Strafrecht
sowie Strafrechtsvergleichung

Vors. Der Ethikkommission

Direktor des



Heger-Tor-Wall 14
49069 Osnabrück
Telefon: (0541) 969-6133 DW 6135
Fax: (0541) 969-4852
LS-Sinn@uos.de
zeis@uos.de

Osnabrück, 9. Januar 2026

Stellungnahme
zur Anhörung im Rechtsausschuss
des Deutschen Bundestages zum
Entwurf eines
Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der
Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Heraus-
gabe elektronischer Beweismittel (E-Evidence)

I. Einleitung und Erkenntnisinteresse

Der Gesetzentwurf zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 verfolgt das unionsrechtlich vorgegebene Ziel, die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren effizienter und schneller zu gestalten. Die Initiative reagiert auf eine seit Jahren diagnostizierte strukturelle Dysfunktion klassischer Rechtshilfeinstrumente, die für digitale Beweismittel – aufgrund ihrer Volatilität, ihrer häufigen Cloud-Verteilung und der kurzen Speicherfristen – vielfach ungeeignet sind. Elektronische Kommunikations-, Verkehrs- und Inhaltsdaten spielen heute in nahezu allen Bereichen schwerer und mittlerer Kriminalität eine zentrale Rolle; Verzögerungen bei ihrer Sicherung führen nicht selten zum endgültigen Beweisverlust.

Die vorliegende Stellungnahme nimmt den Gesetzentwurf nicht zum Anlass, die unionsrechtliche Grundentscheidung für ein E-Evidence-System in Frage zu stellen. Diese Entscheidung ist getroffen und für die Mitgliedstaaten verbindlich. Gegenstand der Stellungnahme ist vielmehr die Qualität der nationalen Durchführung: Es geht um die Frage, ob

und inwieweit der deutsche Gesetzgeber den verbleibenden Gestaltungsspielraum genutzt hat, um Effizienzgewinne mit den verfassungs-, unions- und konventionsrechtlichen Anforderungen an ein faires, grundrechtskonformes Strafverfahren in Einklang zu bringen. Der Schwerpunkt dieser Stellungnahme liegt auf dem Rechtsschutzsystem

II. Normativer und systematischer Hintergrund des E-Evidence-Pakets

Die Verordnung (EU) 2023/1543 führt mit der Europäischen Sicherungsanordnung und der Europäischen Herausgabeanordnung ein unmittelbares Zugriffsmodell gegenüber Diensteanbietern ein.

Anders als bei der klassischen Rechtshilfe oder der Europäischen Ermittlungsanordnung wird der Vollstreckungsstaat grundsätzlich nicht mehr als vorgelagerte Kontrollinstanz tätig. Stattdessen richtet sich die Anordnung direkt an den Anbieter, der die angeforderten Daten vorhält oder technisch kontrolliert. Flankiert wird dieses Modell durch die Richtlinie (EU) 2023/1544, die Diensteanbieter verpflichtet, innerhalb der Europäischen Union erreichbare Niederlassungen oder Vertreter zu benennen. Erst diese organisatorische Anbindung ermöglicht die praktische Durchsetzung der Verordnung. Beide Instrumente zusammen markieren einen Paradigmenwechsel: Die grenzüberschreitende Beweiserhebung wird aus der Logik staatlicher Rechtshilfe herausgelöst und in ein hybrides, teilweise privat vermitteltes Vollzugsmodell überführt. Diese Systementscheidung hat erhebliche rechtsstaatliche Implikationen. Sie verlagert Verantwortung auf private Akteure, reduziert die Souveränitätskontrolle des Vollstreckungsstaates und verändert die zeitliche Lage von Rechtsschutz. Daraus folgt, dass die nationale Durchführung nicht lediglich technisch-administrativ, sondern zwingend auch grundrechtlich sensibel ausgestaltet sein muss.

III. Gesetzgebungstechnik und Grundkonzeption des deutschen Entwurfs

Der Entwurf sieht vor, die unionsrechtlichen Vorgaben in Form eines eigenständigen Stammgesetzes umzusetzen. Diese Entscheidung ist systematisch überzeugend. Sie vermeidet eine Zersplitterung der Regelungen in der Strafprozessordnung, im IRG und in datenschutzrechtlichen Nebengesetzen und schafft für Praxis und Wissenschaft einen klar identifizierbaren Rechtsrahmen.

Positiv hervorzuheben ist ferner, dass der Entwurf die unionsrechtliche Kategorisierung der Datenarten in § 8 EBewMG-E übernimmt. Allerdings verweist § 8 EBewMG-E auf nationale Vorschriften. Dennoch begegnet § 8 EBewMG-E unionsrechtlich keinen durchgreifenden Bedenken, soweit die dortigen Verweisungen auf nationale Vorschriften lediglich beispielhaften Charakter haben. Die Verwendung des Begriffs „insbesondere“ stellt klar, dass die unionsrechtlichen Legaldefinitionen in Art. 3 der Verordnung (EU) 2023/1543 maßgeblich bleiben. Gleichwohl besteht die Gefahr, dass durch die Anknüp-

fung an sektorspezifische nationale Begriffe der autonome unionsrechtliche Bedeutungsgehalt der Datenkategorien in der Praxis faktisch verengt wird. Um eine faktische Verkürzung der unionsrechtlichen Datenkategorien zu vermeiden, wäre entweder ein unmittelbarer Verweis auf die Legaldefinitionen des Art. 3 der Verordnung ausreichend oder – noch praktikabler – eine deklaratorische Klarstellung in § 8 EBewMG-E, dass die nationalen Verweisungen lediglich Regelbeispiele darstellen und die unionsrechtlichen Definitionen maßgeblich bleiben.

Die institutionelle Einbindung des Bundesamts für Justiz als zentrale Koordinationsstelle ist grundsätzlich geeignet, Transparenz, Statistik und unionsweite Abstimmung zu verbessern. Diese Stärken ändern jedoch nichts daran, dass die Kernfragen der rechtsstaatlichen Absicherung weniger in der Gesetzgebungstechnik als in der konkreten Ausgestaltung von Rechtsschutz, Geheimnisschutz und Verfahrensbalance liegen.

IV. Rechtsschutz

1. Rechtsbehelfe gegen ausgehende Anordnungen, § 13 EBewMG-E

Der Entwurf ist in seiner Grundanlage geeignet, die von der EU verfolgte Beschleunigung und Standardisierung der grenzüberschreitenden Beweiserhebung zu unterstützen, und er trifft mit dem Stammgesetzansatz sowie mit einer prinzipiell klaren Zuständigkeitsarchitektur mehrere richtige Weichenstellungen. Zugleich erscheint der Entwurf dort ausbaufähig, wo er Rechtsbehelfe limitiert und damit eine ohnehin schwache Kontrollarchitektur weiter ausdünnert. Gerade im Kontext elektronischer Beweise, in dem Eingriffsintensität, Streubreite und Missbrauchsrisiken strukturell erhöht sind, ist ein „dünner“ Rechtsschutz nicht nur ein abstraktes Grundrechtsproblem, sondern ein Risiko für die Verwertbarkeit und für die Legitimität strafprozessualer Ergebnisse. Normative Stabilität entsteht hier nicht durch maximale Geschwindigkeit, sondern durch die Kopplung von Geschwindigkeit an überprüfbare, dokumentierte und rechtsschutzfähige Verfahren.

Die unionsrechtliche Vorgabe zu wirksamen Rechtsbehelfen bei Europäischen Herausgabeanordnungen (Art. 18 Verordnung (EU) 2023/1543) verfolgt erkennbar das Ziel, den tiefgreifenden Grundrechtseingriff, der mit der grenzüberschreitenden Herausgabe elektronischer Beweismittel verbunden ist, durch einen effektiven gerichtlichen Rechtsschutz abzusichern. Die Verordnung statuiert dabei kein bloß formales Beschwerderecht, sondern ein subjektives Recht der betroffenen Person auf wirksame Rechtsbehelfe, die die Rechtmäßigkeit der Maßnahme einschließlich ihrer Notwendigkeit und Verhältnismäßigkeit erfassen und praktisch ausübbar sein müssen. Maßgeblich ist nicht allein die Existenz eines Rechtsbehelfs, sondern dessen Effektivität unter den tatsächlichen Bedingungen der Maßnahme. Dieses Verständnis wird durch die Bezugnahme auf Art. 47 der Grundrechtecharta mit der Garantie der Wahrung der Verteidigungsrechte und eines fairen Verfahrens bestätigt.

Im Entwurf werden diese Vorgaben in § 13 EBewMG-E dadurch aufgegriffen, dass er für Rechtsbehelfe gegen Europäische Herausgabebeanordnungen auf bestehende strafprozessuale Rechtsschutzmechanismen verweist. Die Ausgestaltung erfolgt dabei abgestuft nach Datenkategorien: Für Herausgabebeanordnungen zu Teilnehmerdaten und zu Daten, die ausschließlich der Identifizierung des Nutzers dienen, wird auf die klassische Beschwerde nach §§ 304 ff. StPO verwiesen, die regelmäßig vor Vollzug der Maßnahme eröffnet ist. Für Verkehrsdaten und Inhaltsdaten hingegen wird der Rechtsschutz an die Regelungen angelehnt, die für verdeckte Ermittlungsmaßnahmen wie die Telekommunikationsüberwachung konzipiert wurden und typischerweise einen nachträglichen Rechtsschutz vorsehen. Die Umsetzung knüpft damit nicht primär an die Eingriffsintensität der Maßnahme an, sondern an eine formale Kategorisierung der betroffenen Datenarten.

Genau an diesem Punkt zeigt sich jedoch ein strukturelles Problem der Umsetzung. Die grundrechtsintensivsten Maßnahmen – namentlich die Herausgabe von Inhaltsdaten aufgrund einer ausgehenden Anordnung – unterliegen nach dem deutschen Entwurf lediglich einem *nachträglichen* Rechtsschutz. Dieser Ansatz mag im innerstaatlichen Kontext verdeckter Überwachungsmaßnahmen nachvollziehbar sein. Bei Europäischen Herausgabebeanordnungen ist die Situation jedoch grundlegend anders als bei klassischen innerstaatlichen Überwachungsmaßnahmen. Zwar werden die angeforderten Daten bei ausgehenden Anordnungen für ein deutsches Strafverfahren erhoben und unterliegen anschließend der deutschen Verfahrensherrschaft. Der nach § 13 Abs. 2 und 3 EBewMG-E vorgesehene Rechtsschutz greift jedoch erst nach Vollzug der Maßnahme und damit 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 Grundrechtsschutz praktisch wirksam sein müsste.

Auch innerstaatlich setzt Rechtsschutz häufig erst nach Kenntnisnahme ein. Er ist dort jedoch in ein enges System staatlicher Vorhersehbarkeit, Begrenzung und nachträglicher Korrekturmöglichkeiten eingebettet. Bei Europäischen Herausgabebeanordnungen fehlt es an dieser strukturellen Eingriffskontrolle, sodass ein ausschließlich nachträglicher Rechtsschutz bei besonders eingriffsintensiven Daten seine Schutzwirkung deutlich verliert.

Daraus ergibt sich ein deutlicher Widerspruch sowohl zur Systematik der Verordnung als auch zur inneren Logik des Grundrechtsschutzes. Während die Verordnung auch für tiefgreifende Eingriffe einen wirksamen Rechtsbehelf fordert, gewährt die nationale Umsetzung den stärksten Rechtsschutz ausgerechnet bei der geringsten Eingriffsintensität und beschränkt ihn bei Inhaltsdaten auf eine zeitlich nachgelagerte Kontrolle. Diese Umkeh-

rung der Schutzlogik steht zudem in Spannung zu dem unionsrechtlichen Effektivitätsgebot: Ein Rechtsbehelf, der strukturell zu spät greift, ist kein wirksamer Rechtsbehelf im Sinne des Unionsrechts, auch wenn er formal existiert. Hinzu tritt ein innerer Widerspruch zur eigenen Gesetzesbegründung, die die besondere Grundrechtsrelevanz von Verkehrs- und Inhaltsdaten ausdrücklich anerkennt.

Der deutsche Gesetzgeber ist dabei keineswegs unionsrechtlich gezwungen, sich auf dieses minimale Rechtsschutzniveau zu beschränken. Die Verordnung regelt den Rechtsschutz nicht in seinen Details, sondern überlässt seine konkrete Ausgestaltung ausdrücklich dem nationalen Recht, solange die unionsrechtlichen Mindestanforderungen an Effektivität und Praktikabilität gewahrt bleiben. Dass ein weitergehender Rechtsschutz möglich ist, zeigt bereits der frühere Referentenentwurf (2024), der einheitlich die Beschwerde gegen gerichtliche oder validierte Herausgabeanordnungen vorsah. Der spätere Verzicht auf diesen Ansatz beruht daher nicht auf unionsrechtlichen Zwängen, sondern auf einer bewussten nationalen Entscheidung. Der Umsetzungsspielraum umfasst insbesondere die Möglichkeit, bei grundrechtsintensiven Herausgabeanordnungen einen vorgelagerten gerichtlichen Rechtsschutz mit aufschiebender Wirkung vorzusehen.

Ein solcher Ansatz wäre nicht nur unionsrechtlich zulässig, sondern unionsrechtlich gut begründbar. Er würde dem in der Verordnung angelegten Effektivitätsgebot Rechnung tragen, Art. 47 der Grundrechtecharta praktisch zur Geltung bringen und die in der Verordnung ausdrücklich geforderte Wahrung der Verteidigungsrechte sichern. Zugleich ist er verfassungsrechtlich geboten. Das Grundgesetz verlangt bei besonders schweren Eingriffen in das Telekommunikationsgeheimnis und in das allgemeine Persönlichkeitsrecht einen effektiven, möglichst vorgelagerten Rechtsschutz. Ein Rechtsschutz, der aufgrund der Irreversibilität der Maßnahme leerläuft, genügt diesem Maßstab nicht. Der Gesetzgeber sollte sich nicht darauf beschränken, innerstaatliche Rechtsschutzmodelle schematisch auf grenzüberschreitende Konstellationen zu übertragen, wenn sich deren tatsächliche Wirkungen grundlegend unterscheiden.

2. Gerichtliche Entscheidung § 14 EBewMG-E:

Die Verordnung (EU) 2023/1543 verortet die gerichtliche Kontrolle von Europäischen Herausgabeanordnungen bewusst als zentrales rechtsstaatliches Korrektiv eines Systems, das den Vollzug von der klassischen zwischenstaatlichen Rechtshilfe auf eine unmittelbare Adressierung privater Diensteanbieter verlagert. Gerade weil die Maßnahme regelmäßig ohne vorgelagerte Kontrolle des Vollstreckungsstaats erfolgt, kommt der gerichtlichen Entscheidung im Anordnungsstaat eine besondere Bedeutung zu. Der Verordnungstext trägt dem Rechnung, indem er in Art. 4 und 5 detaillierte materielle und formelle Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung normiert und diese ausdrücklich der gerichtlichen Prüfung unterstellt. Ziel ist es, sicherzustellen, dass der erhebliche Grundrechtseingriff nur dann erfolgt, wenn die unions-

rechtlichen Schranken eingehalten sind, und dass diese Einhaltung effektiv justiziell überprüfbar ist.

Der Entwurf greift diese Vorgaben in § 14 EBewMG-E auf. Nach Absatz 1 prüft das Gericht im Fall Europäischer Herausgabebeanordnungen, ob die Voraussetzungen des Erlasses nach Art. 4 Abs. 1, 2, 4 und 5 sowie Art. 5 der Verordnung (EU) 2023/1543 erfüllt sind. Der Prüfungsmaßstab wird damit unionsrechtskonform an die materiellen Anforderungen der Verordnung angebunden. § 14 Abs. 2 EBewMG-E regelt sodann die Rechtsfolge einer negativen Prüfung: Liegen die Voraussetzungen nicht vor, stellt das Gericht die Rechtswidrigkeit fest und hebt die Europäische Herausgabebeanordnung auf. Weitergehende Rechtsfolgen sieht die Vorschrift nicht vor.

Gerade diese Beschränkung der Rechtsfolgen auf die Feststellung der Rechtswidrigkeit und die Aufhebung der Anordnung markiert jedoch einen zentralen Punkt der Umsetzung. Während frühere Entwurfsfassungen noch ausdrücklich weitergehende Konsequenzen in den Blick nahmen, verzichtet der aktuelle Entwurf bewusst auf eine solche Regelung. Eine ausdrückliche gesetzliche Anordnung der Löschung rechtswidrig erlangter Daten enthält § 14 Abs. 2 EBewMG-E gerade nicht mehr. Die gerichtliche Entscheidung bleibt damit in ihren praktischen Wirkungen unbestimmt und reduziert sich normativ auf eine deklaratorische Feststellung.

Diese Reduktion der Rechtsfolgen ist problematisch. Die Gesetzesbegründung (S. 46) stellt darauf ab, dass im Hinblick auf bereits erlangte Daten und daraus gezogene Erkenntnisse im Einzelfall nach den allgemeinen strafprozessualen und datenschutzrechtlichen Grundsätzen zu prüfen sei, ob sich aus der Rechtswidrigkeit der Europäischen Herausgabebeanordnung ein Erfordernis der Datenlöschung oder ein strafprozessuales Verwertungs- oder Verwendungsverbot ergebe. Maßgeblich sollen dabei das Gewicht des Verfahrensverstößes und zugleich das Gewicht der verfolgten Straftat sein. Damit verlagert der Gesetzgeber die Entscheidung über die prozessualen Folgen rechtswidriger Maßnahmen vollständig in eine nachgelagerte Abwägung im Einzelfall. Zwar ist zutreffend, dass das Bundesverfassungsgericht und der Bundesgerichtshof Verwertungsverbote nicht schematisch, sondern im Wege einer Abwägung entwickelt haben. Nach der Rechtsprechung des Bundesverfassungsgerichts ist ein Verwertungsverbot insbesondere dann geboten, wenn es sich um schwerwiegende, bewusste oder objektiv willkürliche Rechtsverstöße handelt, bei denen grundrechtliche Sicherungen planmäßig oder systematisch außer Acht gelassen wurden.

Gerade im Kontext der Europäischen Herausgabebeanordnung verschärft sich dieses Problem. Die Kenntnisnahme rechtswidrig erlangter Daten – insbesondere bei Inhaltsdaten oder bei berufsgeheimnisgeschützter Kommunikation – ist faktisch irreversibel. Eine nachträgliche Abwägung, die sich auf die bereits gezogenen Erkenntnisse stützt, kann den eingetretenen Grundrechtseingriff nicht mehr verhindern, sondern nur noch ex post

bewerten. Damit droht die gerichtliche Kontrolle auf eine bloß deklaratorische Ebene reduziert zu werden, ohne eine effektive präventive oder kompensatorische Schutzwirkung zu entfalten.

Aus rechtsstaatlicher Sicht wäre daher eine klarere normative Vorstrukturierung geboten. Die vollständige Verlagerung der Frage von Löschungs-, Verwendungs- und Verwertungsverboten in eine offene Einzelfallabwägung birgt erhebliche Risiken für Rechtsklarheit, Vorhersehbarkeit und effektiven Grundrechtsschutz. Dies gilt umso mehr, als mit dem E-Evidence-System ein Verfahren etabliert wird, das besonders intensive und zugleich grenzüberschreitend irreparable Grundrechtseingriffe ermöglicht. In einer solchen Konstellation reicht es nicht aus, auf die allgemeine Abwägungsdogmatik zu verweisen; vielmehr bedarf es klarer gesetzlicher Leitplanken, die sicherstellen, dass schwerwiegende Verstöße gegen die unions- und verfassungsrechtlichen Sicherungen nicht folgenlos bleiben.

Unionsrechtlich besteht für eine weitergehende Ausgestaltung kein Hindernis. Die Verordnung legt zwar die Voraussetzungen und den Prüfungsmaßstab für den Erlass europäischer Herausgabeanordnungen fest, trifft jedoch keine abschließenden Regelungen zu den nationalen Rechtsfolgen rechtswidriger Maßnahmen. Insbesondere enthält sie kein Verbot, zusätzliche prozessuale Sicherungen wie Verwendungs- oder Verwertungsverbote vorzusehen. Im Gegenteil sprechen die in der Verordnung ausdrücklich verankerten Garantien wirksamer Rechtsbehelfe, der Wahrung der Verteidigungsrechte und eines fairen Verfahrens dafür, dass nationale Regelungen, die der praktischen Effektuierung dieser Garantien dienen, unionsrechtlich zulässig und systemgerecht sind.

Verfassungsrechtlich ist der nationale Gesetzgeber sogar gehalten, diesen Spielraum zu nutzen. Wo ein Verfahren eröffnet wird, das besonders intensive und zugleich faktisch irreversible Grundrechtseingriffe ermöglicht, genügt es nicht, die Rechtswidrigkeit lediglich festzustellen. Erforderlich sind klare und vorhersehbare Regelungen zu den prozessualen Folgen solcher Rechtsverstöße. Die vollständige Verlagerung der Frage von Verwendungs- und Verwertungsverboten in die ungeschriebene Einzelfallrechtsprechung wird den Anforderungen an Rechtsklarheit und effektiven Grundrechtsschutz im Kontext des E-Evidence-Systems nicht gerecht.

Eine sachgerechte Lösung bestünde daher darin, § 14 EBewMG-E ausdrücklich zu ergänzen. Denkbar wäre eine Regelung, die klarstellt, dass bei schwerwiegenden Rechtsverstößen – insbesondere bei Verletzungen von Berufsgeheimnissen oder bei Missachtung der unionsrechtlichen Erlassvoraussetzungen – die mittels einer rechtswidrigen Europäischen Herausgabeanordnung erlangten Daten im weiteren Verfahren nicht verwendet werden dürfen. Eine solche Normierung würde weder die unionsrechtlichen Vorgaben unterlaufen noch die verfassungsgerichtliche Abwägungsdogmatik suspendieren. Sie würde vielmehr die gerichtliche Kontrolle nach § 14 EBewMG-E mit realen verfahren-

rensrechtlichen Konsequenzen verknüpfen und damit sicherstellen, dass die richterliche Prüfung nicht auf eine folgenlose Rechtswidrigkeitsfeststellung reduziert wird, sondern den ihr zugedachten rechtsstaatlichen Schutz tatsächlich entfaltet.

Prof. Dr. Prof. h.c. Arndt Sinn



Ausschussdrucksache 21(6)49f
vom 9. Januar 2026, 11:33 Uhr

Schriftliche Stellungnahme
des Sachverständigen Prof. Dr. Dr. Kai Ambos

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes 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
BT-Drucksache 21/3192

Prof. Dr. Dr. h.c. Kai Ambos
Platz der Göttinger Sieben 5 • 37073 Göttingen

Prof. Dr. Dr. h.c. Kai Ambos
Richter Kosovo Specialist Chambers

Lehrstuhl für Straf- und Strafprozessrecht,
Rechtsvergleichung, internationales Strafrecht
und Völkerrecht

Forschungsstelle für lateinamerikanisches
Straf- und Strafprozessrecht (CEDPAL)

Platz der Göttinger Sieben 5
37073 Göttingen

lehrstuhl.ambos@jura.uni-goettingen.de

Tel. +49 (0) 551 39-27430

URL: <https://uni-goettingen.de/de/697726.html>

Stellungnahme*

zur Anhörung des Rechtsausschusses des Deutschen Bundestags

zum

**Entwurfs eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544
und zur Durchführung der Verordnung (EU) 2023/1543 über die grenz-
überschreitende Sicherung und Herausgabe elektronischer Beweismit-
tel in Strafverfahren innerhalb der Europäischen Union („E-Evidence“),
BT-Drucksache 21/3192.**

12. Januar 2026

* Die Stellungnahme beruht auf meinem – überarbeiteten und aktualisierten – Beitrag in Zeitschrift für Internationale Strafrechtswissenschaft, 2025, 204, abrufbar hier: https://www.zfistw.de/dat/artikel/2025_2_1672.pdf.

I. Vorbemerkungen

Ein zentrales Problem grenzüberschreitender Strafverfolgung ist der Zugriff auf Daten als elektronische Beweismittel. Im Bereich der EU wird in mehr als der Hälfte der Ermittlungen um grenzüberschreitenden Zugriff auf elektronische Beweismittel ersucht.¹ Solche Ersuchen müssen schnell erledigt werden, da die Daten flüchtig und regelmäßig nicht – wie analoge Beweismittel – an einem bestimmten Ort belegen sind; sie sind in diesem Sinne „unterritorial“ („a-territorial“)² und befinden sich häufig in einer „cloud“. Die klassische zwischenstaatliche Rechtshilfe erweist sich meist als zu langsam und zu schwerfällig;³ dies gilt auch für die Europäische Ermittlungsanordnung (EEA).⁴ Verzögerungen können zu einem Datenverlust führen, sei es, weil die Daten gelöscht werden, oder weil sie ihren Speicherort verändern („wandern“).⁵ Allerdings wenden sich schon heute die Strafverfolgungsbehörden direkt an die privaten Diensteanbieter und diese geben freiwillig eine große Mengen an Daten („user information“)⁶ heraus.⁷

¹ Das ergibt sich aus der Kombination von zwei Datensätzen: elektronische Beweismittel seien für 85 % der strafrechtlichen Ermittlungen bedeutsam und in 65 % der Ermittlungsverfahren seien die maßgeblichen elektronischen Beweismittel im europäischen Ausland gespeichert, vgl. Europäische Kommission, Arbeitspapier, SWD (2018) 119 final, S. 14, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118>. Zur Europäischen Staatsanwaltschaft insoweit s. *Frunza-Nicolescu*, eucrim 2023, 210 ff.

² Grdl. *Daskal*, The Yale Law Journal 2015, 326 („un-territoriality“); krit. *Burchard*, ZIS 2018, 249; *Hüttemann*, NZWiSt 2024, 82 (93).

³ Vgl. e-evidence Verordnung (u. Fn. 10), Erwägungsgrund (‘ErwGr’) 8; *Burchard*, ZIS 2018, 190 (196); *Tosza*, CLR 2024, 139 (143).

⁴ Nach Art. 12 Abs. 3, 4 EEA (Richtlinie 2014/41/EU v. 3.4.2014) beträgt die Anerkennungs- und Vollstreckungsfrist grundsätzlich 120 Tage. Krit. auch *Babucke*, wistra 2024, 57 (auch EEA „zeitintensiv“, so dass Daten oft schon gelöscht); *Topalnakos*, eucrim 2023, 200 (201); skeptisch *Tosza*, CLR 2024, 144 f. (Ineffizienz von EEA „more an assumption than a proven fact“).

⁵ Vgl. e-evidence Verordnung (u. Fn. 10), ErwGr 8; BMJ, Fragen und Antworten zum Thema E-Evidence, https://www.bmjv.de/SharedDocs/FAQ/DE/FAQ_Database/E-Evidence/FAQ-E-Evidence-Liste.html?nn=18816 („... können relevante digitale Daten längst gelöscht oder veraltet sein. Hinzu kommt, dass die Diensteanbieter die Daten in der Regel dezentral und flexibel nach wirtschaftlichen Kriterien speichern, weswegen sich deren Speicherort ständig ändern kann – im Extremfall etwa zehntelsekundlich.“).

⁶ Bei den US-Anbietern geht es um Teilnehmer- und Verkehrsdaten („user information“), keine Inhaltsdaten, s. die Statistiken bei Google, Meta und Amazon.

⁷ Vgl. *Petersen*, Probleme des transnationalen Zugriffs auf elektronische Beweismittel im Lichte der europäischen Beweisrechtshilfe in Strafsachen, 2024, S. 134 f.; vorher *Burchard*, ZIS 2018, 249 (257 ff.); zum Konflikt mit Persönlichkeits- und Datenschutzrechten *Tosza*, CLR 2024, 144; zur fragmentarischen mitgliedstaatlichen Rechtslage und der unklaren Verwertbarkeit *Sachoulidou*, NJECL 2024, 256 (258).

Vor diesem Hintergrund hat die EU – auf der Grundlage des Grundsatzes gegenseitiger Anerkennung⁸ und dem daraus abgeleiteten Grundsatz der Verfügbarkeit⁹ – am 12.7.2023 die e-evidence Verordnung¹⁰ und zeitgleich die Richtlinie zur Benennung von Adressaten (RL-Vertreter)¹¹ verabschiedet, wobei die RL bis zum 18.2.2026 umzusetzen ist¹² und die VO ab 18.8.2026 gelten wird.¹³ Mit Blick auf den vorliegenden Gesetzentwurf¹⁴ (insbesondere das „Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetz“, EBewMG)¹⁵ ist zu berücksichtigen, dass die die wesentlichen (und ggf. problematischen) e-evidence Regelungen enthaltende VO „in allen ihren Teilen verbindlich“ ist und „unmittelbar“ gilt,¹⁶ der nationale Gesetzgeber also allenfalls Durchführungsvorschriften erlassen kann; hinsichtlich der RL hat der innerstaatliche Gesetzgeber zwar einen Ermessensspielraum hinsichtlich der „Wahl der Form und der Mittel“,¹⁷ sie ist aber in ihrem Regelungsziel – Bestimmung eines empfangsberechtigten Vertreters eines Diensteanbieters (Adressaten) im EU-Raum – unproblematisch. Aus europarechtlicher Sicht scheint der Regelungsspielraum des nationalen Gesetzgebers also denkbar gering, obgleich eine lückenhafte VO gesetzgeberische Handlungsoptionen eröffnen dürfte. Wir kommen darauf zurück.

II. Verordnung, Richtlinie und Gesetzentwurf (2025)

⁸ Die VO wird auf Art. 82 Abs. 1 AEUV gestützt (u. Fn. 10, S. 118 oben), dieser gilt aber nur zwischenstaatlich und beruht auf dem Gedanken staatlicher Anerkennung, Private kommen nicht vor (u.a. deshalb ablehnend Esser, in: Sosnitzer et al., Digitalisierung im Europäischen Recht, 2022, 45; Burchard, ZIS 2018, 197, 261 ff., 266 f.; Petersen, StraFo 2023, 426 (429); ders. (Fn. 7), S. 305 ff.; krit. auch Topalnakos, eucrim 2023, 200 (201); i.E. zust. aber Tosza, CLR 2024, 156 ff. auf lit. (a) und (d) abstellend und ein flexibles Verständnis ggs. Anerkennung proklamierend; für eine flexible Auslegung auch Sachoulidou, NJECL 2024, 256 (266); der von der Lit. präferierte Art. 82 Abs. 2 passt zwar in der Sache besser („Erleichterung der gegenseitigen Anerkennung...“, insbesondere bezüglich „Zulässigkeit von Beweismitteln“; i.E. auch Burchard, ZIS 2018, 249 (267); ders., ZRP 2019, 166 [„wenn überhaupt“]; Esser, a.a.O., 45), lässt aber sekundärrechtlich nur Richtlinien zu (deshalb generell ablehnend Petersen, StraFo 2023, 426 (429)). Ausführlich zu den in Betracht kommenden Kompetenzgrundlagen und deren Grenzen, s. Petersen (Fn. 7), S. 163 ff., 305 ff., wobei er insbesondere den kaum beachteten Art. 89 AEUV anführt (S. 181, 310). Dessen Anwendbarkeit mit Blick auf die grenzüberschreitende Wirkung der Herausgabe- und Sicherungsanordnung ablehnend Tosza, CLR 2024, 159 („... the proposal clearly disregards the existence of Article 89, and rightly so. It is convincing to claim that Article 89 does not apply to situations foreseen in the Regulation, as the issuing authority does not “operate” in the territory of another Member State“).

⁹ Grdl. Böse, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der EU, 2007; jüngst dazu Brodowski, ZStW 2024, 659 (670 ff.).

¹⁰ VO (EU) 2023/1543 (e-evidence Verordnung) 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, ABI L 191, S. 118. Zur Entstehungsschicht ausführlich Burchard, ZIS 2018, 190 (193 ff.); auch Esser (Fn. 8), 42 ff.; Forlani, eucrim 2023, 174 (175 ff.).

¹¹ RL (EU) 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, ABI L 191, S. 181. Die RL muss bis 18.2.2026 umgesetzt werden (Art. 7), eine Evaluierung soll zum 18.8.2029 erfolgen (Art. 8). Als primärrechtliche Grundlage gibt die RL Art. 53, 62 EUV an, also Regelungen zur Niederlassungsfreiheit. Art. 2 Abs. 2 und ErwGr 6 der RL stellen klar, dass die aufgrund der RL benannten Niederlassungen und Vertreter nur als Adressaten von Anordnungen nach der e-evidence VO, der RL-EEA und bei entsprechenden rein innerstaatlichen Fällen fungieren sollen. Diese klare Begrenzung des Anwendungsbereichs auf die justizielle Zusammenarbeit spricht für die Anwendbarkeit der Art. 82 ff. AEUV, die damit wohl unter Verweis auf Art. 53, 62 EUV umgangen werden sollten, vgl. Petersen (Fn. 7), S. 296 ff, 311 f.

¹² Art. 7 Abs. 1 RL.

¹³ Art. 34 Abs. 2 e-evidence Verordnung [„VO“]. Eine Evaluierung soll es – wie bei der RL – zum 18.8.2029 geben (Art. 33). Die VO gilt nicht für Dänemark wegen dessen opt-out bezüglich Teil III, Titel V AEUV (Raum der Freiheit, der Sicherheit und des Rechts; s. ErwGr 101). Irland hat dagegen vom opt-in Recht Gebrauch gemacht, ErwGr 100.

¹⁴ Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel im Strafverfahren innerhalb der Europäischen Union [„GesE“], 8.10.2025, <https://www.bmfv.de/Shared-Docs/Downloads/DE/Gesetzgebung/RegE/RegE_E_Evidence_2025.pdf?__blob=publicationFile&v=2>

¹⁵ Art. 1 GesE (Fn. 14).

¹⁶ Art. 288 UA 2 AEUV.

¹⁷ Art. 288 UA 3 AEUV.

1. Anwendungsbereich, Begrifflichkeiten, Datenarten

Die VO betrifft die Herausgabe und Sicherung (zum Zweck eines späteren Herausgabeersuchens) von elektronischen Beweismitteln (*Daten*¹⁸, Art. 3 Nr. 8¹⁹) mittels einer „Europäischen Herausgabe-anordnung“ („European Production Order Certificate“, „EPOC“) oder „Europäischen Sicherungsanordnung“ („European Preservation Order Certificate-Preservation Request“, „EPOC-PR“)²⁰ und zwar „unabhängig davon [!], wo sich die Daten befinden“ (Art. 1 Abs. 1). Diese Anordnungen dürfen im Rahmen von Strafverfahren²¹ und zur Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Maßregeln (Mindestdauer vier Monate bei Verkehrs- und Inhaltsdaten),²² die in einem Urteil in Anwesenheit des Betroffenen ergangen sind,²³ erlassen werden; sie dürfen auch in Strafverfahren gegen juristische Personen im Anordnungsstaat erlassen werden (Art. 2 Abs. 2).

Die Herausgabe bzw. Sicherung wird durch eine Anordnungsbehörde des Mitgliedstaats (Anordnungsstaat) bewirkt (Art. 3 Nr. 1, 2), doch sieht Art. 1 Abs. 2 – anders als die bisherigen Sekundärrechtsakte der europäischen Beweisrechtshilfe²⁴ – immerhin ein ausdrückliches Antragsrecht des Verdächtigen oder Beschuldigten bzw. deren rechtlicher Vertreter vor.²⁵ Die Anordnung wird – das ist entscheidend – **unmittelbar an den Diensteanbieter** (Art. 7 Abs. 1), der als Verantwortlicher handelt (Art. 5 Abs. 6), gerichtet (Art. 7 Abs. 1).²⁶ Als Diensteanbieter gilt jede natürliche oder juristische Person, die „elektronische Kommunikationsdienste“,²⁷ Registrierungsdienste sowie „andere Dienste der Informationsgesellschaft“ (zur Kommunikation, Datenspeicherung)²⁸ erbringt (Art. 3 Nr. 3).²⁹ In Deutschland sind ca. 10.000 Diensteanbieter betroffen, davon sind 10% auslandskontrolliert.³⁰

Die Dienste müssen in der Union angeboten werden (s. schon Art. 2 Abs. 1, Marktortprinzip),³¹ d.h. in einem Mitgliedstaat in Anspruch genommen werden können, zu dem der Diensteanbieter eine „wesentliche Verbindung“ hat, also (gesetzliche Vermutung) dort niedergelassen ist oder seine

¹⁸ Es handelt sich um schon existierende Daten, Echtzeitdaten sind nicht erfasst, vgl. auch *Babucke*, wistra 2024, 57 (61); *Beukelmann*, NJW-Spezial 2023, 568.

¹⁹ Art. ohne Bezeichnung beziehen sich auf die e-evidence VO (Fn. 10)

²⁰ Bestimmung der Abkürzungen in ErwGr. 50 und Art. 9.

²¹ Zur Notwendigkeit einer Regelung für („punitive“) Verwaltungsverfahren (insbesondere von OLAF) s. *Tosza*, eucrim 2023, 216 ff.

²² Art. 2 Abs. 2 differenziert nicht nach Datenart, aus ErwGr 40 und Art. 5 Abs. 3 ergibt sich aber, dass die Mindeststrafe nur bei Verkehrs- und Inhaltsdaten, nicht aber bei hier sog. Identifikationsdaten (u. Fn. 37 mit Haupttext) gelten soll; krit. zu dieser unvollständigen Regelung und im Übrigen niedrigen Anwendungsschwelle *Sachoulidou*, NJECL 2024, 256 (269 f.); s. auch ErwGr 41 mit Nennung bestimmter Straftaten, bei denen in der Regel nur e-evidence zur Verfügung steht.

²³ Die Erweiterung auf Fahndung im Rahmen der Strafvollstreckung erfolgte auf Bestreben des Rats, krit. *Hüttemann*, NZWiSt 2024, 82 (89).

²⁴ Das Fehlen eines solchen Antragsrechts in der RL-EEA ist vielfach kritisiert worden, s. etwa *Karas et al.*, in: Ambos et al., *The European Investigation Order*, 2023, S. 45 („[...] does not create a binding European rule which would create a right for the defence to request the issuing of an EIO“); *Scomparin et al.*, ebd. S. 83; *Barata et al.*, ebd., S. 100.

²⁵

²⁶ Es handelt sich um den Verantwortlichen i.S.v. Art. 4 Nr. 7 DSGVO (VO 2016/679), also „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet ...“. Das dürfte in der Regel der Kunde (Unternehmen oder Privatperson) des Diensteanbieters sein, vgl. *Weiß/Brinkel*, RD 2023, 522 (527).

²⁷ Näher RI. (EU) 2018/1972, Art. 2 Nr. 4.

²⁸ Näher RI. (EU) 2015/1535, Art. 1 Abs. 1 lit b.

²⁹ Näher zum Diensteanbieter *Weiß/Pradel*, CCZ 2024, 102 (105 ff.); zu den erfassten Dienstleistungen Eidgenössisches Justiz und Polizeidepartement (EJPD)/Bundesamt für Justiz (BJ), Bericht zur e-evidence-Vorlage der EU, 24.10.2023, 5 ff.

³⁰ GesE (Fn. 14), 33.

³¹ *Esser* (Fn. 8), S. 45; *Brodowski*, ZStW 2024, 659 (675).

Dienste in einem oder mehreren Mitgliedstaaten durch „eine erhebliche Zahl von Nutzern“ in Anspruch genommen wird oder seine Tätigkeit auf eine oder mehrere Mitgliedstaaten ausgerichtet ist (Art. 3 Nr. 4). Ein Diensteanbieter muss mindestens einen³² im Unionsgebiet ansässigen Adressaten zur Entgegennahme etc. von Herausgabe- und Sicherungsanordnungen benennen (Art. 3 Abs. 1 RL-Vertreter³³). In der Union niedergelassene Diensteanbieter müssen insoweit eine Niederlassung benennen (Art. 3 Abs. 1(a)); außerhalb der Union oder in einem nicht teilnehmenden Mitgliedstaat³⁴ niedergelassene Diensteanbieter müssen einen Vertreter benennen, der sich in einem teilnehmenden Mitgliedstaat befindet (Art. 3 Abs. 1(b)(c)). In der Sache verpflichtet die RL-Vertreter den Diensteanbieter damit zur Schaffung (mindestens) eines territorialen Anknüpfungspunkts im Unionsgebiet, mittels dessen zugleich die Ausübung von Hoheits- und Strafgewalt gegenüber dem Diensteanbieter – unabhängig, wie schon oben erwähnt, von der Belegenheit der Daten (Art. 1 Abs. 1) – legitimiert wird.³⁵ § 3 GesE regelt die unterschiedlichen Konstellationen zur Benennung einer Niederlassung oder eines Vertreters. Kommt der Diensteanbieter dieser Verpflichtung nicht nach, so droht ein Bußgeld³⁶ aufgrund der entsprechenden Ordnungswidrigkeit (§ 18 Abs. 1 GesE). Das Bundesamt für Justiz überwacht die Pflichterfüllung des Diensteanbieters (§ 6 GesE).

Was die *Daten* angeht, so wird zwischen drei Arten unterschieden: Teilnehmer-, Verkehrs- und Inhaltsdaten (Art. 3 Nr. 9-12). *Teilnehmerdaten* betreffen die Identität, einschließlich Adresse, Telefonnummer, E-Mail Adresse (Nr. 9), sowie weitere „ausschließlich zum Zwecke der Identifizierung“ angeforderte Daten, z.B. IP-Adressen (Nr. 10, im Folgenden ‘Identifikationsdaten’).³⁷ Im Kern geht es – in telekommunikationsrechtlicher Begrifflichkeit – um Bestandsdaten i.w.S.³⁸ *Verkehrsdaten* betreffen die Interaktion (Ursprung und Ziel einer Nachricht, Zeitpunkt und Dauer der Nutzung) sowie sonstige Metadaten (Nr. 11).³⁹ *Inhaltsdaten* beziehen sich auf den Inhalt der Interaktion, also Daten in Form von Text, Sprache, Videos, Bildern und Tonaufzeichnungen (Nr. 12). Die Zugriffsanforderungen sind im Fall von Verkehrs- und Inhaltsdaten höher als im Fall von Identifikationsdaten, weil in jenem Fall die Eingriffsintensität (allgemeines Persönlichkeitsrecht) grundsätzlich höher ist; allerdings ist es nicht völlig ausgeschlossen, dass auch aus entsprechend aggregierten Teilnehmerdaten, ggf. in Verbindung mit Verkehrsdaten (die allerdings höheren Eingriffsvoraussetzungen unterliegen), persönlichkeitsensible Information generiert werden, indem etwa ein Bewegungsprofil erstellt oder ein bestimmtes Nutzerverhalten identifiziert wird.⁴⁰

2. Herausgabe-/Sicherungsanordnung, Voraussetzungen, Unterrichtung Vollstreckungsbehörde

Der Begriff der Anordnungsbehörde (Art. 4) ist weit zu verstehen und erfasst grundsätzlich auch polizeiliche Ermittlungspersonen. Entscheidend ist, um welche Art von Daten es geht, und ob um

³² Die alternative Benennung von Adressaten in *jedem* Mitgliedstaat würde gerade kleine bis mittlere Diensteanbietern überfordern; insoweit ist die Beschränkung auf einen Adressaten für das gesamte Unionsgebiet vorzugswürdig.

³³ O. (Fn. 11).

³⁴ Das betrifft Dänemark (Fn. 13).

³⁵ Petersen, StraFo 2023, 426 (427); ausführlich dazu Petersen (Fn. 7), S. 256 ff.

³⁶ Gemäß § 18 Abs. 3 Nr. 1 a) GesE (Fn. 14) bis zu € 500.000.

³⁷ Damit wird zwar vordergründig begrifflich an den drei etablierten Datenkategorien festgehalten, zugleich aber die darin liegende klare Unterscheidung verwässert. Die Voraussetzungen für die Erhebung der Daten bestimmt sich nicht mehr nur nach den Datenkategorien, sondern auch nach der Eingriffsintensität der Ermittlungsmaßnahme, vgl. dazu Warken, Klassifizierung elektronischer Beweismittel für strafprozessuale Zwecke, 2019, S. 103; Petersen (Fn. 7), S. 82 f.

³⁸ Vgl. § 3 Nr. 6 TKG sowie § 2 Abs. 2 Nr. 2 Telekommunikation-Digitale-Dienste-Datenschutzgesetz (TDDDG).

³⁹ Ungenauer insofern § 3 Nr. 70 TKG: „Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind.“

⁴⁰ Krit. auch Burchard, ZIS 2018, 190 (202) mit (Fn. 94); ZRP 2019, 164 (165) (in Abgrenzung zu Inhaltsdaten); Krumwiede, ZfIStw 2024, 202 (211).

Herausgabe oder Sicherung ersucht wird. Bei den weniger persönlichkeitsrechtssensiblen *Identifikationsdaten* kann eine *Herausgabe*anordnung nicht nur von einem Richter, sondern auch von einem Staatsanwalt erlassen werden (Art. 4 Abs. 1 lit. a)); wird sie von einer „anderen“ (polizeilichen) Ermittlungsbehörde erlassen, muss sie richterlich oder staatsanwaltschaftlich validiert werden (Art. 4 Abs. 1 lit. b)). Für die innerstaatlichen Zuständigkeiten gelten die strafprozessualen Vorschriften zu den Ermittlungsmaßnahmen (§ 9 Abs. 1 GesE, §§ 94 ff. StPO),⁴¹ insbesondere §§ 100j Abs. 1 S. 1, 100k Abs. 3 StPO. Zuständige Polizeibehörden sind grundsätzlich die Ermittlungspersonen der Staatsanwaltschaft i.S.v. § 152 GVG im Rahmen der StPO-Zuständigkeiten (§ 9 Abs. 2 GesE), also insbesondere aufgrund § 100j Abs. 1 S. 1, nicht aber etwa aufgrund § 100k Abs. 3 StPO;⁴² jedenfalls sind deren Anordnungen staatsanwaltschaftlich zu validieren (§ 9 Abs. 3 GesE).⁴³

Bei eingriffsintensiveren *Verkehrs- und Inhaltsdaten* kann die Herausgabeanordnung grundsätzlich nur von einem Richter erlassen werden (Art. 4 Abs. 2 lit. a)); bei Erlass durch eine andere (polizeiliche) Ermittlungsbehörde muss eine Validierung durch einen Richter erfolgen (Art. 4 Abs. 2 lit. b)). Innerstaatlich gelten auch insoweit §§ 94 ff. StPO, insbesondere § 100g (Richtervorbehalt nach 101a Abs. 1 S. 1 i.V.m. § 100e Abs. 1 S. 1 StPO), wobei die VO allerdings die staatsanwaltschaftliche Eilkompetenz gemäß § 100e Abs. 1 S. 2 StPO blockiert: Eine Notfallzuständigkeit anderer Ermittlungsbehörden ohne *vorherige* richterliche Validierung existiert nur bezüglich Identifikationsdaten (Art. 4 Abs. 5 VO), die deutsche *nachträgliche* gerichtliche Bestätigung (§ 100e Abs. 1 S. 3 StPO) bei Verkehrsdaten ist von der VO nicht gedeckt.⁴⁴ Zuständiger Richter ist der Ermittlungsrichter (§§ 162 Abs. 1, 169 StPO); zuständige Behörde i.S.v. Art. 4 Abs. 2 lit. b ist aber nur die Staatsanwaltschaft (nicht die Polizei), deren Anordnung allerdings richterlich validiert werden muss (Art. 4 Abs. 2 lit. b VO, § 10 Abs. 2, 3 GesE).⁴⁵

Bei der *Sicherungsanordnung* wird nicht zwischen der Art der Daten differenziert: sie kann immer durch einen Richter oder Staatsanwalt erlassen werden (Art. 4 Abs. 3 lit. a)) bzw. muss bei Erlass durch eine (polizeiliche) Ermittlungsbehörde richterlich oder staatsanwaltschaftlich validiert werden (Art. 4 Abs. 3 lit. b)). Innerstaatlich soll die Erlasszuständigkeit – nach dem Ende des RefE quick freeze⁴⁶ – nun über einen neuen § 10a EBewMG geregelt werden, der wiederum im Rahmen des

⁴¹ Grundlegend zur Zuständigkeit nach nationalem Recht s. EuGH, Urt. v. 16.12.2021 – Rs. C-724/19, ECLI:EU:C:2021:1020, *HP*, Rn. 45; Urt. v. 8.12.2020 – Rs. C-584/19, ECLI:EU:C:2020:1002, Staatsanwaltschaft Wien, Rn. 57 ff.

⁴² Nach § 100j Abs. 3 StPO besteht ein Richtervorbehalt nur bezüglich Abs. 1 S. 2 und 3, ein Auskunftsverlangen nach Abs. 1 S. 1 kann die Polizei danach im Rahmen der Ermittlungsgeneralklausel (§ 163 Abs. 1 StPO: „Ermittlungen jeder Art“) stellen, vgl. *Bär*, ZIS 2011, 53 (54); *Petersen* (Fn. 7), S. 134. Demgegenüber ist nach § 100k Abs. 3 allein die Staatsanwaltschaft ermächtigt.

⁴³ S. auch GesE (Fn. 14), Begründung, S. 45 ff. („gestufte[r] Ansatz“ je nach Eingriffsintensität).

⁴⁴ S. auch GesE (Fn. 14), Begründung, S. 48 („... aufgrund der Systematik der Verordnung in diesen Fällen ausgeschlossen ...“); expliziter vorher RefE, Begründung, S. 44 („Das auf nachträglicher gerichtlicher Bestätigung basierende deutsche Modell wird folglich von der Verordnung ... blockiert“).

⁴⁵ Die im Zusammenhang mit dem EuHB aufgeworfene Frage der Staatsanwaltschaft als (unabhängige) Justizbehörde, die für die deutsche Staatsanwaltschaft wegen der ministeriellen Aufsichts- und Leitungsbefugnis (§ 147 Nr. 1, 2 GVG) zu verneinen ist (EuGH NJW 2019, 2145, 2150: „... ‘ausstellende Justizbehörde’ iSv Art. 6 Absatz I des Rahmenbeschlusses 2002/584 dahin auszulegen ..., dass darunter nicht die Staatsanwaltschaften eines Mitgliedstaats fallen, die der Gefahr ausgesetzt sind, im Rahmen des Erlasses einer Entscheidung über die Ausstellung eines Europäischen Haftbefehls unmittelbar oder mittelbar Anordnungen oder Einzelweisungen seitens der Exekutive, etwa eines Justizministers, unterworfen zu werden“; anders zur EEA EuGH NJW 2021, 1373), stellt sich hier nicht, denn die Staatsanwaltschaft darf ohnehin nur bei Identifikationsdaten selbständig tätig werden (Art. 4 Abs. 1 lit. a und schon oben im Haupttext) und zwar unabhängig davon, ob und wie unabhängig sie ist (s. auch ErwGr 36, der alleine auf die objektive Entscheidungsfindung der Staatsanwaltschaft abstellt). Bedenken aber bei DRiB, Stellungnahme, August 2025, 4.

⁴⁶ Vgl. § 9 RefE 2024 mit Fn. 3.

(neuen) Gesetzes zur IP-Adressenspeicherung und Weiterentwicklung der Befugnisse im Strafverfahren⁴⁷ (dort Art. 3) eingeführt werden soll. Danach sind für den Erlass zum Zweck der Strafverfolgung Gerichte und Staatsanwaltschaften (§ 10a Abs. 1), zum Zwecke der Strafvollstreckung die Staatsanwaltschaft (§ 10a Abs. 2) zuständig.

Was die *materiellen Voraussetzungen* des Erlasses einer *Herausgabeanordnung* angeht, so muss diese, insbesondere mit Blick auf die Beschuldigtenrechte, notwendig und verhältnismäßig⁴⁸ und nach nationalem Recht in einem vergleichbaren Fall zulässig sein (Art. 5 Abs. 2). Bei Identifikationsdaten kann die Anordnung für alle Straftaten oder zur Vollstreckung von mindestens viermonatigen Freiheitsstrafen oder Maßregeln (sofern diese nicht in Abwesenheit ergangen sind) erlassen werden (Art. 5 Abs. 3). Bei Verkehrs- und Inhaltsdaten ist die Anordnung bei Straftaten mit einem Mindesthöchstmaß von 3 Jahren Freiheitsstrafe⁴⁹ und einer Reihe sekundärrechtlich geregelter Taten zulässig (Art. 5 Abs. 4). Verkehrs- und Inhaltsdaten eines Berufsgeheimnisträgers dürfen nur (sofern sie in einer spezifischen Infrastruktur abgelegt sind) unter bestimmten (alternativen) Voraussetzungen mittels Europäischer Herausgabeanordnung angefordert werden (Art. 5 Abs. 9). Auch bei durch Immunitäten oder Vorrechte oder durch Presse- und Meinungsfreiheit geschützte Verkehrs- oder Inhaltsdaten gelten restriktive Anordnungsvoraussetzungen (Art. 5 Abs. 10), jedoch hat die ermittelnde Behörde – wenig verständlich⁵⁰ – ein Ermessen („kann“) bezüglich der Sachverhaltsklärung. Stellt sie aber fest, dass die geschützten Rechte betroffen sind, darf sie die Anordnung nicht erlassen (Art. 5 Abs. 2 Unterabs. 2).

Eine *Sicherungsanordnung* kann für alle Daten und für alle Straftaten (Art. 6 Abs. 3) erlassen werden, wenn sie mit Blick auf den Sicherungszweck (spätere Herausgabe der Daten) und unter besonderer Berücksichtigung der Beschuldigtenrechte notwendig und verhältnismäßig ist (Art. 6 Abs. 2) und in einem vergleichbaren Fall auch im nationalen Recht hätte erlassen werden können (Art. 6 Abs. 3). Diese, dem hypothetischen Ermittlungseingriff (§ 161 Abs. 3 S. 1 StPO) ähnliche Regelung setzt eine nationale Rechtsgrundlage zur Verpflichtung privater Diensteanbieter zur Datensicherung voraus. Ob eine solche in Deutschland existiert, ist umstritten.⁵¹ Selbst wenn sie existieren würde, würde es an einer – nach dem „Doppeltürmodell“ erforderlichen⁵² – Erlaubnisnorm für Diensteanbieter zur Datenspeicherung fehlen.⁵³ Deshalb soll eine Rechtsgrundlage zur Erfüllung der Pflichten gem. Art. 10 und 11 VO im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz

⁴⁷ RefE abrufbar hier: https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_IP_Speicherung.pdf?__blob=publicationFile&v=2

⁴⁸ Krit. insoweit *Sachoulidou*, NJECL 2024, 256 (270) (keine Konkretisierung der Verhältnismäßigkeit bezüglich bestimmter Straftat und bestimmten Tatverdächtigen i.S.d. Vorschlags des Ausschusses für „Civil Liberties, Justice and Home Affairs“, „LIBE“).

⁴⁹ Krit. insoweit *Hüttemann*, NZWiSt 2024, 82 (85) („Alltagskriminalität“).

⁵⁰ Krit. auch *Hüttemann*, NZWiSt 2024, 82 (86).

⁵¹ Die insoweit einschlägigen telekommunikationsrechtlichen Regelungen zur Vorratsdatenspeicherung (§§ 175 Abs. 1, 176 TKG) hat das Bundesverwaltungsgericht am 14.8.2023 (6 C 7.22, Rn. 19 ff.) – infolge der EuGH-Entscheidung zur Vorratsdatenspeicherung vom 20.9.2022 (C-793/19, C-794/19) – für unanwendbar erklärt. Die Ermittlungsgeneralklausel (§§ 161 Abs. 1, 163 Abs. 1 StPO) kann eine Verpflichtung Privater zur Datenspeicherung nicht begründen. Die Anwendbarkeit der §§ 94 ff. (insbesondere § 94 Abs. 2, Abs 1 Alt. 2), 100g Abs. 1, 100j Abs. 1 StPO ist ebenfalls umstritten. Vgl. *Rexin*, CR 2024, 64 (67 f.).

⁵² Danach bedarf es einer Rechtsgrundlage sowohl für die Übermittlung also auch den Abruf/die Abfrage von Daten: „Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten“ (BVerfG, Beschluss v. 27.1.2020, 1 BvR 1873/13, 1 BvR 2618/13, Rn. 93). Es bedarf also nicht nur einer Rechtsgrundlage zur Übermittlung an die Strafverfolgungsbehörden, sondern auch zur Speicherung/den Abruf auf Seiten des Diensteanbieters.

⁵³ *Rexin*, CR 2024, 64 (68 ff.) (mit einem Regelungsvorschlag und einem grenzüberschreitenden Blick nach Österreich, Portugal, Irland, Italien und Frankreich).

(TDDDG) geschaffen werden.⁵⁴ Zur Vollstreckung kann eine Sicherungsanordnung schließlich aus den gleichen Gründen wie eine Herausgabeanordnung ergehen (Art. 6 Abs. 3).

Wie schon gesagt, werden Herausgabe- und Sicherungsanordnung unmittelbar an den Diensteanbieter gerichtet, doch ist die *Vollstreckungsbehörde*⁵⁵ des Vollstreckungsstaats (in dem sich Niederlassung oder Vertreter des Diensteanbieters befindet, Art. 3 Nr. 16, 17) bei einer Herausgabeanordnung bezüglich Verkehrs- und Inhaltsdaten (zeitgleich) zu *unterrichten* (Art. 8 Abs. 1). Dies ist allerdings dann nicht erforderlich, wenn die Anordnungsbehörde hinreichende Gründe zu der Annahme hat, dass die Straftat im Anordnungsstaat begangen wurde/wird und die betroffene Person im Anordnungsstaat ansässig ist (Art. 8 Abs. 2). Die Unterrichtung hat aufschiebende Wirkung für den betreffenden Diensteanbieter (Art. 8 Abs. 4, außer in Notfällen, dazu sogleich) bis zum Ablauf der maximal 10-tägigen Überlegungsfrist der Vollstreckungsbehörde (Art. 10 Abs. 2). Die Unterrichtungs- bzw. Notifizierungspflicht war Gegenstand heftiger Kontroversen. Sie war im ursprünglichen Kommissionsentwurf nicht vorgesehen⁵⁶ und wurde erst (nicht zuletzt auf Druck Deutschlands, aber vor allem des Europäischen Parlaments⁵⁷) in fortgeschrittenem Verhandlungsstadium als Grundidee eingeführt. Ihre nun vorliegende Form erhielt sie im Rahmen der Trilogverhandlungen.⁵⁸ Ob damit ein ausreichend „robustes“ Unterrichtsverfahren⁵⁹ in grundrechtlicher Hinsicht etabliert wurde, wird unten (4.a)) zu bewerten sein.

Sofern keine Unterrichtung erforderlich ist, hat der Diensteanbieter die angeforderten Daten umgehend zu sichern (Art. 10 Abs. 1) und spätestens innerhalb von 10 Tagen an die Anordnungsbehörde zu übermitteln (Art. 10 Abs. 3); in „Notfällen“⁶⁰ spätestens innerhalb von 8 Stunden (Art. 10 Abs. 4 S. 1).⁶¹ Die Sicherungspflicht endet grundsätzlich nach 60 Tagen, sofern bis dahin kein Herausgabeersuchen gestellt oder beantragt wurde, die Sicherungsdauer mit Blick auf ein Herausgabeersuchen um 30 Tage zu verlängern (Art. 11 Abs. 1). Wurde ein Herausgabeersuchen gestellt, so hat der Diensteanbieter die Daten aber „so lange“ zu sichern, „wie dies erforderlich ist“ (Art. 11 Abs. 2). Ist die Sicherung nicht mehr erforderlich, so ist der Diensteanbieter von der Anordnungsbehörde davon zu unterrichten und die Sicherungsverpflichtung erlischt (Art. 11 Abs. 3).

3. Ablehnungsgründe, Rechtsschutz, Vollstreckung, Sanktionen

Wird die Vollstreckungsbehörde unterrichtet, so hat sie „so bald wie möglich“, spätestens innerhalb von 10 Tagen bzw. in Notfällen innerhalb von 96 Stunden, die Geltendmachung von Ablehnungsgründen zu prüfen (Art. 12 Abs. 1). Als solche kommen (abschließend) in Betracht:⁶²

⁵⁴ GesE (Fn. 14), Art. 3, S. 16 f., 61 ff. (auf die „Doppeltür“ Bezug nehmen).

⁵⁵ In Deutschland soll dies die Staatsanwaltschaft sein, § 11 GesE (Fn. 14). Nur nebenbei sei gesagt, dass der deutsche Verordnungstext weiterhin an dem Begriff der Vollstreckungsbehörde festhält, während im Englischen zutreffend von „enforcing“ (statt „executing“) „authority“ gesprochen wird, vgl. *Petersen* (Fn. 7), (Fn. 17), S. 304.

⁵⁶ Krit. *Esser* (Fn. 8), S. 48 ff.

⁵⁷ S. *Sippel* (EP-Berichterstatlerin), *eu crim* 2023, 109 (guest editorial).

⁵⁸ GesE (Fn. 14), S. 20 f. Zur Verhandlungsgeschichte auch *Burchard*, *ZIS* 2018, 249 (255 f.); *Hüttemann*, *NZWiSt* 2024, 82 (86); *Basar*, *jurisPR-StrafR* 14/2023, 2; *Petersen* (Fn. 7), S. 302 ff.; *Sachoulidou*, *NJECL* 2024, 256 (270 f.).

⁵⁹ GesE (Fn. 14), S. 21.

⁶⁰ Als „Notfall“ definiert Art. 3 Nr. 18 VO eine Situation unmittelbarer Gefahr für Leben, körperliche Unversehrtheit oder Sicherheit oder für eine kritische Infrastruktur, wenn deren Störung zu den genannten Gefahren oder einer schweren Beeinträchtigung der Grundversorgung der Bevölkerung oder der Wahrnehmung der Kernfunktionen des Staates führen würde.

⁶¹ Instruktive Unterscheidung der drei Konstellationen bei *Krumwiede*, *ZfIStw* 2024, 202 (206 ff.) (Unterrichtung Vollstreckungsbehörde, keine Unterrichtung, Notfalleinordnung).

⁶² Krit. insoweit zum RefE BRAK (Fn. 25), S. 6 („wünschenswert, wenn das... Prüfprogramm sich auch im Gesetzestext niederschlagen würde“).

- Schutz der angeforderten Daten durch Immunitäten und Vorrechte (z.B. Beschlagnahmeverbot von Berufsgeheimnisträger gemäß § 97 Abs. 1 StPO)⁶³ oder durch strafrechtliche Haftungsbeschränkung aufgrund Presse- und Meinungsfreiheit;
- offensichtliche Verletzung der europäischen Grundrechte (Art. 6 EUV, Charta) durch Herausgabe;
- Verstoß gegen „ne bis in idem“;
- fehlende beiderseitige Strafbarkeit: keine Strafbarkeit im Vollstreckungsstaat bei Nicht-Vorliegen einer Katalogtat (Anhang IV)⁶⁴ mit Mindesthöchststrafe von drei Jahren im Anordnungsstaat.

Die Vollstreckungsbehörde soll diese Ablehnungsgründe aber nur „gegebenenfalls“ geltend machen (Art. 12 Abs. 1); wir kommen darauf zurück (4.a)). Sollte eine Konsultation zwischen Anordnungs- und Vollstreckungsbehörde nicht zu einer Einigung führen (etwa Anpassung der Herausgabeanordnung), macht die Vollstreckungsbehörde die Ablehnungsgründe geltend⁶⁵ und unterrichtet Diensteanbieter und Anordnungsbehörde (Art. 12 Abs. 3). Dann beendet der Diensteanbieter die Vollstreckung und darf die Daten nicht übermitteln und die Anordnungsbehörde widerruft die Anordnung (Art. 12 Abs. 2).

Mögliche Ausführungshindernisse aufgrund von Immunitäten und Vorrechten oder Presse- und Meinungsfreiheit – die sich mangels europarechtlicher Vorgaben alleine nach dem (innerstaatlichen) Recht des Vollstreckungsstaats richten⁶⁶ – können auch vom Diensteanbieter gegenüber Anordnungs- und Vollstreckungsbehörde vorgebracht werden (Art. 10 Abs. 5 UA 1, Art. 11 Abs. 4 UA 1). Die Anordnungsbehörde muss dann entscheiden, ob sie die Herausgabe- oder Sicherungsanordnung zurücknehmen, anpassen oder aufrechterhalten will, die Vollstreckungsbehörde kann ggf. den entsprechenden Ablehnungsgrund geltend machen (Art. 10 Abs. 5 UA 2, 3, Art. 11 Abs. 4 UA 2). Ferner kann der Diensteanbieter bei einem unvollständigen Ersuchen um Klarstellung bitten (Art. 11 Abs. 5) und eine faktische Unmöglichkeit der Ausführung geltend machen (Art. 11 Abs. 6). Schließlich kann ein Diensteanbieter auch – detailliert und innerhalb von 10 Tagen – *gegenläufige Verpflichtungen* aus dem Recht eines *Drittlands* vorbringen (Art. 17 Abs. 1, 2). Dies kann zu einer gerichtlichen Überprüfung im Anordnungsstaat bei Aussetzung der Ausführung führen (Art. 17 Abs. 3-8). In Deutschland soll insoweit das OLG zuständig sein (§ 15 Abs. 2 GesE); es entscheidet durch unanfechtbaren Beschluss (§ 16 GesE).

Art. 18 gewährt **Rechtsschutz** gegen die Herausgabeanordnung vor einem Gericht des Anordnungsstaats, das die Rechtmäßigkeit, einschließlich Notwendigkeit und Verhältnismäßigkeit, zu prüfen hat (Abs. 1, 2). Fristen und sonstige Voraussetzungen sollen vergleichbaren Fällen des nationalen Rechts entsprechen (Abs. 4). Bei der „Bewertung“ der eingeholten Beweismittel ist sicherzustellen, dass die Verteidigungsrechte gewahrt und ein faires Verfahren gewährleistet sind (Abs. 5). Rechtsschutz gegen eine Sicherungsanordnung wird nicht ausdrücklich gewährt. Der GesE regelt nun in §§ 13, 14 den Rechtsschutz bei ausgehenden (Herausgabe-)Anordnungen (vorher §§

⁶³ S. auch GesE (Fn. 14), S. 50.

⁶⁴ E-evidence VO, S. 175 f.

⁶⁵ Ggf. auf bestimmte Daten beschränkt und mit Bedingungen versehen, Art. 12 Abs. 4.

⁶⁶ S. auch *Babucke*, wistra 2024, 57 (60).

14, 15 RefE) – der noch im RefE (§ 14 Abs. 2) vorgesehene Rechtsschutz gegen Sicherungsanordnungen⁶⁷ ist entfallen – und differenziert nach der Art der angeforderten Daten. Bei Herausgabeanordnungen bezüglich Identifikationsdaten gelten, jeweils entsprechend, die §§ 98 Abs. 2 S. 2, § 304 Abs. 1 sowie §§ 306 bis 310 StPO, bezüglich Verkehrsdaten § 101a Abs. 6 S. 2 i.V.m. § 101 Abs. 7 S. 2 sowie § 311, bezüglich Inhaltsdaten § 95a Abs. 5 S. 1, 2, § 101 Abs. 7 S. 2, 3, § 304 Abs. 2, §§ 306, 310 Abs. 2 sowie § 311 StPO (§ 13 Abs. 1-3 GesE). In der Sache muss das Gericht die (materiellen) Voraussetzungen zum Erlass der jeweiligen Herausgabeanordnung gemäß Art. 4, 5 VO (§ 14 Abs. 1 GesE) und damit auch die Zulässigkeit des Erlasses nach deutschem Recht (Art. 5 Abs. 2 letzter HS) prüfen; es gilt also ein doppelter (europarechtlicher und nationaler) Maßstab.⁶⁸ Liegen die Voraussetzungen nicht vor, ist die Herausgabeanordnung rechtswidrig und aufzuheben (§ 14 Abs. 2 GesE). Die noch im RefE 2024 (§ 15 Abs. 2) enthaltene Rechtsfolge einer Löschung der erlangten Daten und eines Verwendungsverbots bezüglich darauf beruhender Erkenntnisse, ist im GesE nicht mehr vorgesehen. Wir kommen unten (4. b) bb)) darauf zurück.

Sollte ein Diensteanbieter eine (wirksame) Herausgabe- oder Sicherungsanordnung nicht vollstrecken, kann die Anordnungsbehörde die Vollstreckungsbehörde um *Vollstreckung* ersuchen (Art. 16 Abs. 1, 2). Dabei informiert die Vollstreckungsbehörde den Diensteanbieter über die Möglichkeit, Einwände (dazu Art. 16 Abs. 4, 5) vorzubringen und über anwendbare Sanktionen (Art. 16 Abs. 3). Die Vollstreckungsbehörde entscheidet über die Stichhaltigkeit vorgebrachter Einwände (Art. 16 Abs. 6) und konsultiert ggf. die Anordnungsbehörde, falls sie Zweifel an der Vollstreckbarkeit hat (Art. 16 Abs. 7). Bestätigt die Vollstreckungsbehörde die Vollstreckbarkeit, wird bei Nichtbefolgung eine Sanktion verhängt (Art. 16 Abs. 10 S. 1). Der dagegen erforderliche Rechtsbehelf (Art. 16 Abs. 10 S. 2) richtet sich innerstaatlich nach §§ 67 ff. OWiG (§ 17 GesE).

Die Mitgliedstaaten müssen wirksame, verhältnismäßige und abschreckende *Sanktionen* für Fälle der Nichtbefolgung von Herausgabe- oder Sicherungsanordnungen vorsehen (Art. 15 Abs. 1 S. 1, 2). Sie sollen sich auf maximal 2% des Jahresgesamturnsatzes des Diensteanbieters belaufen (Art. 15 Abs. 1 S. 3). § 18 RefE sieht insoweit bußgeldbewehrte Ordnungswidrigkeiten vor (Abs. 1, 2) und zwar – differenzierend nach der Schwere der Zuwiderhandlung – bis zu € 100.000, € 500.000 oder bis zu 2% des Jahresumsatzes, sofern dieser mehr als 5 Mio. beträgt (Abs. 3-6). Bußgeldbehörde ist das Bundesamt für Justiz oder die Staatsanwaltschaft als Vollstreckungsbehörde (Abs. 8).⁶⁹

4. Weitere (spezifische) Kritik

Die VO sieht keine umfassende Regelung zur Zulässigkeit bzw. Verwertung rechtswidrig erlangter Beweise, sondern nur selektive Verwendungsverbote⁷⁰ vor.⁷¹ Sie liefert auch keine (sonstige) Harmonisierung relevanter strafprozessualer Aspekte, insbesondere bezüglich Grad des Tatverdachts und beweisrechtlicher Substantiierungsanforderungen (etwa zur Eingrenzung der Datenabfrage).⁷² Allerdings ist zu bedenken, dass eine solche Harmonisierung nur durch Richtlinien herbeigeführt werden kann (Art. 82 Abs. 2 AEUV).⁷³ In der Sache könnte man eine faktische Harmonisierung in der Bestimmung von Mindestbedingungen (Art. 5 Abs. 4 lit. a: Mindesthöchststrafe drei Jahre) und,

⁶⁷ Dazu Begründung RefE, S. 48 f. sowie Ambos, ZfStW 2025, 211.

⁶⁸ S. auch GesE (Fn. 14), S. 52.

⁶⁹ S. dazu auch GesE (Fn. 14), S. 54 ff.

⁷⁰ Vgl. Art 4 Abs. 5 a.E., 10 Abs. 4 a.E. und 12 Abs. 4 (Löschung von Daten und Verwendungsbeschränkung).

⁷¹ Krit. Sachoulidou, NJECL 2024, 256 (272 f.); ungenau Basar, jurisPR-StrafR 14/2023, 4; Krumwiede, ZfStw 2024, 202 (212) (keine Verwendungsverbote). Zum Vorschlag des European Law Institute (ELI) für Mindestanforderungen zur gegenseitigen Zulässigkeit von Beweisen s. Bachmaier, eucrim 2023, 223 ff.

⁷² Burchard, ZRP 2019, 164 (166); auch Petersen (Fn. 7), S. 322.

⁷³ Zur Rechtsgrundlage der VO s. schon (Fn. 8).

jedenfalls faktisch, darin sehen, dass die VO an mehreren Stellen auf das nationale Verfahrensrecht (Art. 1 Abs. 2) oder einen „vergleichbaren nationalen Fall“ verweist (Art. 5 Abs. 2, Art. 6 Abs. 3), weil dadurch eine Anpassung des nationalen Rechts impliziert wird.⁷⁴ Hinsichtlich des weiteren Anpassungsbedarfs stellt sich insoweit die Frage, wie nach Inkrafttreten der VO in Konfliktfällen zwischen dieser und dem nationalen Recht zu verfahren sein wird. Beispielhaft: Kann eine Herausgabe- oder Sicherungsanordnung auf Antrag eines Beschuldigten erlassen werden (Art. 1 Abs. 2), wenn das nationale Strafverfahrensrecht⁷⁵ eine solche Möglichkeit nicht vorsieht? Dafür spricht die unmittelbare Anwendbarkeit der VO (Art. 288 UA 2 AEUV) und der *effet utile* Grundsatz, dagegen die fehlende (formale) Harmonisierung durch Richtlinien (Art. 82 Abs. 2 AEUV). Tatsächlich fordert die VO in zahlreichen Fällen eine nationale Umsetzung, also mehr als nur eine bloße Durchführung, wie es der GesE insinuiert; sie ähnelt insoweit in der Sache einer Richtlinie.

Die VO führt zu einer Teilprivatisierung⁷⁶ der Rechtshilfe, weil die – auch im EU-System gegenseitiger Anerkennung – *staatlich* erledigte Vollstreckung eines Rechtshilfeersuchens einem *privaten* Diensteanbieter übertragen wird. Darin kann man einen qualitativen Sprung der eigentlich zwischenstaatlichen gegenseitigen Anerkennung sehen,⁷⁷ doch wird dieser teilweise durch die oben beschriebene Einbindung der Vollstreckungsbehörde per Unterrichtung und vor allem durch deren Rolle bei der Vollstreckung einer Anordnung wieder zurückgenommen.⁷⁸ Zugleich ändert das Schlagwort der „Teilprivatisierung“ nichts daran, dass die Kooperation Privater im Bereich elektronischer Beweismittel unentbehrlich ist,⁷⁹ allerdings muss, wie oben schon angedeutet, die mit der fehlenden Beteiligung des (ersuchten) Vollstreckungsstaats einhergehende Rechtsschutzverkürzung irgendwie ausgeglichen werden, sei es durch seine Beteiligung (per Unterrichtung) und/oder durch die Eröffnung effektiven Rechtsschutzes für den Diensteanbieter und/oder Betroffenen. Beide Ansätze finden sich in der Verordnung, doch wird, wie im Folgenden gezeigt wird (*infra* a) und b)), nur sehr begrenzter Rechtsschutz gewährt. Ferner gerät der Diensteanbieter in ein pflichtenkollisionsrechtliches Dilemma, das letztlich nur durch zwischenstaatliche Abkommen aufgelöst werden kann (*infra* c)).

a) Unterrichtungsverfahren

Mit der Einbindung der Vollstreckungsbehörde durch das Unterrichtungsverfahren soll umfassender Rechtsschutz gewährleistet werden,⁸⁰ die Unterrichtungspflicht ist aber mehrfach eingeschränkt und wird damit eher zur Ausnahme als zur Regel.⁸¹ Zum einen gilt sie nur bei einer Herausgabeordnung, zum anderen nur bezüglich Verkehrs- und Inhaltsdaten (Art. 8 Abs. 1). Damit

⁷⁴ S. auch *Petersen* (Fn. 7), S. 314, der eine Harmonisierung der nationalen Ermittlungsmaßnahmen durch die Vorgaben an die EPOC und EPOC-PR sieht.

⁷⁵ Zur dt. Rechtslage s. schon (Fn. 25).

⁷⁶ Entgegen der in der Lit. geäußerten Kritik (*Brodowski*, ZStW 2024, 659 (675); *Burchard*, ZIS 2018, 249 (265); *Tosza*, CLR 2024, 141 f., 156; auch *EJPD/BJ*, Fn. 29, 21) handelt es sich nicht um eine *vollständige* Privatisierung, denn die Herausgabe bzw. Sicherung wird ja von einem (Anordnungs-)Staat verlangt.

⁷⁷ *Tosza*, CLR 2024, 139, 156 („paradigm shift“, „quantum leap“); ebenso *Sachoulidou*, NJECL 2024, 256 (259, 267).

⁷⁸ *Tosza*, CLR 2024, 153.

⁷⁹ Sie ist auch im nationalen Recht vorgesehen, s. etwa § 100a Abs. 4 StPO; dazu *Basar*, jurisPR-StrafR 14/2023, 4; *Beukelmann*, NJW-Spezial 2023, 568; *Petersen* (Fn. 7), S. 124. Im Übrigen bleiben die nationalen Befugnisse unberührt (Art. 1 Abs. 1 UA 2), die der VO und Richtlinie zugrundeliegenden Prinzipien dürfen aber nicht umgegangen werden (RL-Vertreter, ErwGr 9; dazu auch *Weiß/Brinkel*, RD 2023, 522 (525), die sogar – wohl zu weitgehend – eine „Sperrwirkung“ der VO gegenüber den nationalen Befugnisnormen annehmen). Zur Privatisierung der Kooperation in anderen Bereichen (etwa Geldwäsche) s. *Sachoulidou*, NJECL 2024, 256 (259, 266 f.).

⁸⁰ GesE (Fn. 14), S. 20 f.

⁸¹ EDRI, e-Evidence compromise blows a hole in fundamental rights safeguards, 7.2.2023 („exception rather than the rule“), abrufbar unter <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/>;

muss weder bei einer auf jegliche Daten gerichteten Sicherungsanordnung, noch bei einer Herausgabeanordnung bezüglich Identifikationsdaten unterrichtet werden.⁸² Selbst im Fall einer Herausgabeanordnung bezüglich Verkehrs- und Inhaltsdaten gilt die Unterrichtungspflicht nicht, wenn die betreffende Straftat im Anordnungsstaat begangen wurde, „wird“ oder „wahrscheinlich ... werden wird“ (Art. 8 Abs. 2 (a)) und die betroffene Person im Anordnungsstaat ansässig ist (Art. 8 Abs. 2 (b)).⁸³ Ob dafür „hinreichende Gründe“ bestehen, hat alleine die – möglicherweise befangene – Anordnungsbehörde zu entscheiden (Art. 8 Abs. 2).⁸⁴ Besonders schutzbedürftige Gruppen, etwa Journalisten, Dissidenten oder Whistleblower, die ein legitimes Interesse haben, ihre Daten im Ausland zu sichern, sehen sich somit ggf. einem direkten Zugriff ihres Heimatstaats auf ihren Diensteanbieter/seinen Vertreter ausgesetzt, ohne dass der „zuständige“ Vollstreckungsstaat (oder der Wohnsitzstaat des Betroffenen)⁸⁵ unterrichtet werden müsste (Beispielhaft: die ungarische Regierung kann sich ggf. direkt an den in Deutschland ansässigen Vertreter des Diensteanbieters wenden, um auf die von diesem gesicherten Daten missliebiger ungarischer Journalisten zuzugreifen, ohne Deutschland zu unterrichten). Diese Personen müssen dann darauf hoffen, dass der Diensteanbieter Einwände geltend macht (dazu III. b) aa)).

Der Begehungsort richtet sich nach dem nationalen Recht des Anordnungsstaats, wobei dem Wohnsitz des Opfers indizielle Bedeutung zukommt.⁸⁶ Systemwidrig ist insoweit die Erweiterung auf zukünftige Taten in Art. 8 Abs. 2 (a) Alt. 2 und 3 („wird oder wahrscheinlich begangen werden wird“), denn es geht um e-evidence „im Rahmen eines Strafverfahrens“ mit Blick auf „eine konkrete, bereits begangene Straftat“,⁸⁷ nicht aber um präventiv-polizeiliche Straftatverhütung.⁸⁸ Hinsichtlich der „Ansässigkeit“ des Tatverdächtigen im Anordnungsstaat (Art. 8 Abs. 2 (b)) reichen – jenseits einer Registrierung (Meldung) dort – auch bestimmten Bindungen aus;⁸⁹ das ist unbestimmt weit.⁹⁰

Praktisch bedeutet die Ausnahme von der Unterrichtung der Vollstreckungsbehörde (bzw. das faktische Unterlassen der Unterrichtung⁹¹), dass Verkehrs- und Inhaltsdaten von einem Diensteanbieter/seinem Vertreter – per Herausgabeanordnung – herausverlangt werden können, ohne dass der Sitzstaat des Vertreters (ggf. Vollstreckungsstaat) davon erfährt und – wichtiger noch – ohne dass das inkriminierte Verhalten in diesem Staat überhaupt strafbar sein müsste. Beispielhaft: Deutsch-

krit. auch *Petersen*, StraFo 2023, 426 (432) (kläglicher Rest eines effektiven Rechtsbehelfs im Vollstreckungsstaat); *Topalnakos*, eucrim 2023, 200 (201); *Tosza*, CLR 2024, 148, 150 f.

⁸² Vgl. GesE (Fn. 14), S. 21: laut Protokollerklärung „sei es unter rechtsstaatlichen Gesichtspunkten unerlässlich, dass Rechtsschutz nicht nur gegen Herausgabeanordnungen und im Anordnungsstaat bestehe, sondern ebenso gegen Sicherungsanordnungen und im Vollstreckungsstaat.“

⁸³ Krit. *Krumwiede*, ZfStw 2024, 202 (210 f.); *Basar*, jurisPR-StrafR 14/2023, 4; *Juszcak/Sason*, eucrim 2023, 182 (193).

⁸⁴ Krit. auch EDRI („considerable interests in avoiding the notification procedure“; zust. EJPB/BJ (Fn. 29), 12 („beachtliches Interesse an der Vermeidung der Notifizierung“).

⁸⁵ So der nicht angenommene Vorschlag des LIBE-Ausschusses, dazu *Sachoulidou*, NJECL 2024, 256 (271) mit (Fn. 124).

⁸⁶ Vgl. e-evidence VO, ErwGr 52.

⁸⁷ Vgl. ErwGr 24 und Art. 1 Abs. 1.

⁸⁸ Krit. auch *Hüttemann*, NZWiSt 2024, 82 (85) („systemwidrig“, „Risiko einer missbräuchlichen Datenerhebung durch den Anordnungsstaat“).

⁸⁹ Vgl. e-evidence VO, ErwGr 53 („bestimmte Bindungen“, konkretisiert durch objektive Faktoren wie Dauer, Art und Umstände des Aufenthalts sowie „familiäre und wirtschaftliche Bindungen“).

⁹⁰ Krit. auch *Hüttemann*, NZWiSt 2024, 82 (86); *Krumwiede*, ZfStw 2024, 202 (211); *Basar*, jurisPR-StrafR 14/2023, 4; EDRI.

⁹¹ Insoweit geben die Erfahrungen mit der EEA Anlass zur Sorge, vgl. insoweit zur Missachtung der Notifizierungspflicht *Petersen* (Fn. 7), S. 240 (Fn. 494) unter Verweis auf Eurojust, Meeting on the EIO, 19 – 20 September 2018, Outcome Report, S. 13, https://www.ejn-crimjust.europa.eu/ejnupload/News/Outcome-Report_Eurojust-meeting-on-EIO-Sept-2018_EN.pdf („most participants believed that [...] the intercepting authorities have simply not notified them“).

land müsste nicht über eine – an einen in Deutschland ansässigen Vertreter eines Diensteanbieters gerichtete – polnische Herausgabeanordnung bezüglich Verkehrs- und Inhaltsdaten unterrichtet werden, wenn es sich bei der zugrundeliegenden Tat um eine von einem polnischen Staatsbürger in Polen vorgenommene Abtreibung handelt, die dort zwar strafbar, aber hier straflos wäre.⁹² Damit wird faktisch der (ohnein stark eingeschränkte)⁹³ Grundsatz der beiderseitigen Strafbarkeit ausgehebelt,⁹⁴ denn dessen Verletzung kann nur von der Vollstreckungsbehörde geltend gemacht werden (Art. 12 Abs 1(d)), die ja aber überhaupt keine Kenntnis von dem Herausgabeverlagen hat. Selbst ein innerstaatlicher Rechtsbehelf, wie er noch von § 16 RefE vorgesehen war, kann hier – mangels Kenntnis der Vollstreckungsbehörde – nicht greifen. Schließlich gilt die grundsätzlich aufschiebende Wirkung der Unterrichtung (Art. 10 Abs. 2: 10 Tage) bei Notfällen nicht (Art. 8 Abs. 4). Die 10 Tagefrist (Art. 10 Abs. 2) wird dann auf 96 Stunden verkürzt (Art. 10 Abs. 4 S. 2, Art. 12 Abs. 1). Allerdings findet hier wieder eine Vermischung repressiver und präventiver Zwecke statt, weil Notfälle präventiv – auf unmittelbar bevorstehende Gefahren – ausgerichtet sind⁹⁵ und schon begangene Straftaten überhaupt nicht betreffen.⁹⁶

Die ebenfalls schon o.g. möglichen Ablehnungsgründe muss die Vollstreckungsbehörde nur „gegebenenfalls“ („where appropriate“, Art 12 Abs. 1) geltend machen.⁹⁷ Die Bundesregierung fordert insoweit – nach wie vor – zu Recht, dass „im Rahmen des Unterrichtungsverfahrens die individualrechtsschützenden Zurückweisungsgründe obligatorisch zu prüfen seien, was in den Erwägungsgründen [und eben auch in Art. 12, K.A.] der Verordnung nicht hinreichend klar zum Ausdruck komme.“⁹⁸ Der hier in Bezug genommenen Erwägungsgrund 62 ist in der Tat scheinbar widersprüchlich: Einerseits „sollte“ die Vollstreckungsbehörde das „Recht haben ...“, die in der Anordnung angegebenen Informationen zu bewerten und diese gegebenenfalls abzulehnen“, andererseits soll diese Entscheidung aber auf einer „obligatorischen und pflichtgemäßen Prüfung“ beruhen. Während also der erste Satzteil ein Ermessen („sollte“) anzuordnen scheint,⁹⁹ indiziert der zweite Satzteil eine pflichtgemäße Prüfpflicht. Deshalb dürfte eine Ermessensreduzierung auf Null in der Regel dann anzunehmen sein, wenn einer der Ablehnungsgründe vorliegt, also dessen Geltendmachung dann „appropriate“ sein.¹⁰⁰ Eine Prüfpflicht folgt im Übrigen nicht nur aus dem Wortlaut von Art. 12 Abs. 1 („prüft“), sondern logisch auch daraus, dass die Vollstreckungsbehörde überhaupt erst nach vorangegangener Prüfung entscheiden kann, ob sie einen Ablehnungsgrund geltend macht; die Ermessungsausübung setzt also die Prüfung voraus. Bei alledem darf aber nicht das praktische Problem übersehen werden, dass die Vollstreckungsbehörden von Vollstreckungsstaaten, in denen sich Vertreter zahlreicher Diensteanbieter befinden und die damit mit einem erhöhten Aufkommen von Herausgabe- und Sicherungsanordnungen zu rechnen haben, gar nicht in der Lage sein werden, alle Anordnungen (von denen sie Kenntnis haben) gründlich zu prüfen.¹⁰¹

⁹² Bsp. nach *Babucke*, wistra 2024, 57 (60 f.) (leicht geändert).

⁹³ S. zur Ausnahme bei Katalogtaten laut Anhang IV der VO und Mindesthöchststrafe schon (o. Fn. 64 mit Haupttext).

⁹⁴ Krit. auch *Topalnakos*, eucrim 2023, 200 (202) (auch zum überhaupt nicht erwähnten Spezialitätsgrundsatz).

⁹⁵ Zur Def. schon o. Fn. 60.

⁹⁶ Näher *Hüttemann*, NZWiSt 2024, 82 (87).

⁹⁷ Krit. *Hüttemann*, NZWiSt 2024, 82 (87).

⁹⁸ RefE 2024, S. 20 f. und nun GesE (Fn. 14), S. 21. Der EuGH stellte in der EncroChat Entscheidung ausdrücklich klar, dass der Unterrichtungspflicht aus Art. 31 Abs. 1 RI-EEA (grenzüberschreitende TKÜ) individualschützender Charakter zukommt, EuGH, Urt. v. 30.4.2024 – C-670/22, NJW 2024, 1723 (1731) Rn. 124. Zum individualschützenden Charakter s. auch *Petersen*, StV 2022, 679 (680 ff.); *Böse*, JZ 2022, 1048 (1054 f.); *Schmidt*, ZStW 2022, 982 (1000 f.).

⁹⁹ Ganz im Sinne des auch im letzten Satz von ErwGr 62 betonten Ermessensspielraums der (unabhängigen) Justizbehörden.

¹⁰⁰ In diesem Sinne noch überzeugend RefE 2024, S. 50, 51; i.E. ebenso BRAK (Fn. 25), S. 5.

¹⁰¹ Vgl. *Tosza*, CLR 2024, 151, 159 (wo er zusätzlich den „real effect“ hinsichtlich des Grundrechtsschutzes einer „additional bureaucracy“ schaffenden obligatorischen Unterrichtung anzweifelt), 160 („administrative burden“).

Was die Ablehnungsgründe selbst angeht, so existiert kein allgemeiner Grundrechtsvorbehalt, sondern eine Grundrechtsverletzung kann nur „in Ausnahmefällen“ und „aufgrund genauer und objektiver Belege“ mit Blick auf die „besonderen Umstände[n] des Falles“ bei einer „offensichtliche[n] Verletzung“ geltend gemacht werden (Art. 12 Abs. 1 (b), auch Art. 16 Abs. 4 (g)). Es ist fraglich, ob mit dieser komplizierten und restringierenden Formulierung dem politisch motivierten Einsatz des Instruments gegen Dissidenten und Regierungskritiker ausreichend entgegengewirkt werden kann.¹⁰²

b) Rechtsschutz

aa) Diensteanbieter

Was die Geltendmachung möglicher Grundrechtsverletzungen durch den privaten Diensteanbieter angeht (Art. 10 Abs. 5 UA 1, Art. 11 Abs. 4 UA 1), so unterliegt die darin liegende Verlagerung des Grundrechtsschutzes auf einen privaten Akteur („Privatisierung“) zunächst grundsätzlichen Bedenken.¹⁰³ Denn einerseits lassen sich private Akteure grundsätzlich nicht von öffentlichen (sondern eben von privaten, geschäftlichen) Interessen leiten¹⁰⁴ und andererseits richten sich grundrechtliche Schutzpflichten ausschließlich an den Staat richten und dieser kann sich der daraus erwachsenden Verpflichtung nicht durch Delegation auf Private entziehen. Ob und inwieweit Anordnungs- und Vollstreckungsbehörden in einem solchen Szenario noch ihren Schutzpflichten gerecht werden können und/oder der Diensteanbieter – trotz der angesprochenen Interessenkonflikte (geschäftliche Interessen vs. Daten-/Grundrechtsschutz) – zum „Wächter der Grundrechte“ werden kann,¹⁰⁵ wird erst die Praxis zeigen und diese wird, soviel wird man prognostizieren können, in den Mitgliedstaaten unterschiedlich sein. Bezüglich der Vollstreckungsstaaten wird insoweit die schon oben erwähnte ungleiche mitgliedstaatliche Verteilung von Vertretern der Diensteanbieter zu einer Beschränkung der Prüfungskapazität führen.

In der Sache regelt die VO den Rechtsschutz nur rudimentär und überlässt Einzelheiten der innerstaatlichen Umsetzung.¹⁰⁶ Dem Diensteanbieter steht ein effektiver Rechtsbehelf nur gegen die finanzielle Sanktionierung bei Nicht-Befolgung einer Herausgabe- oder Sicherungsanordnung zu (Art. 16 Abs. 10), nicht aber gegen die Anordnung (gegenüber der Anordnungsbehörde) oder gar ihre Vollstreckung (gegenüber der Vollstreckungsbehörde) an sich.¹⁰⁷ Bezüglich der Anordnung hat der Diensteanbieter lediglich eine beschränkte Prüfungsbefugnis mit Blick auf bestimmte (Grund-)Rechte (Immunitäten, Vorrechte, Presse- und Meinungsfreiheit) mit etwaiger In-Kennntnis-Setzung von Anordnungs- und Vollstreckungsbehörde (Art. 10 Abs. 5 UA 1, Art. 11 Abs. 4 UA 1), der in Bezug genommene Anhang III enthält aber einen weitergehenden Prüfungskatalog.¹⁰⁸ Zwar kann er auch auf anderen Gründen beruhende Einwände geltend machen (Art. 10 Abs. 8), doch

¹⁰² Krit. insoweit EDRI; auch EJPB/BJ (Fn. 29), 12; *Tosza*, CLR 2024, 154 f. (insbes. krit. zum einschränkenden Adjektiv „manifest“ [„offensichtlich“]).

¹⁰³ Krit. auch *Esser* (Fn. 8), S. 50; *Burchard*, ZIS 2018, 249 (265 f.); *Hüttemann*, NZWiSt 2024, 82 (90); *Petersen* (Fn. 7), S. 117, 139; *Sachoulidou*, NJECL 2024, 256.

¹⁰⁴ Dazu *Tosza*, CLR 2024, 162 ff., 166; folgend *Sachoulidou*, NJECL 2024, 256 (268); zu möglichen Interessenkonflikten zutreffend *Juszcak/Sason*, eucrim 2023, 182 (192 f.).

¹⁰⁵ So tendenziell *Tosza*, CLR 2024, 162, 166; ebenso *Sachoulidou*, NJECL 2024, 256 (269).

¹⁰⁶ Krit. *Tosza*, CLR 2024 160; *Juszcak/Sason*, eucrim 2023, 182 (192 f.), 200 mit (Fn. 126) (Verweise auf Kritik von Staaten, insbesondere Deutschland); *Topalnakos*, eucrim 2023, 200 (202).

¹⁰⁷ S. auch *Basar*, jurisPR-StrafR 14/2023, 3; *Rexin*, CR 2024, 64 (72).

¹⁰⁸ Art. 10 Abs. 5 UA 1, Art. 11 Abs. 4 UA 1 verweisen auf das Formular in Anhang III (e-evidence Verordnung, (Fn. 10), S. 172 ff.), das in Abschnitt D eine Liste von Gründen für die Unmöglichkeit der Ausführung enthält. Krit. auch *Tosza*, CLR 2024, 162.

obliegt das weitere Verfahren der Vollstreckungsbehörde, insbesondere hat sie mögliche Grundrechtsverletzungen – ggf. immerhin auf der Grundlage der Einwände des Diensteanbieters (Art. 10 Abs. 8) – zu prüfen (Art. 16 Abs. 2 lit. a, Abs. 4).¹⁰⁹

Ob all dies mit dem Grundrecht auf effektiven Rechtsschutz (Art. 47 GRCh) vereinbar ist, darf bezweifelt werden, denn der Diensteanbieter ist ja selbst Adressat einer belastenden Anordnung (auf Herausgabe oder Sicherung), gegen die er sich wehren können sollte.¹¹⁰ Überdies setzt er sich datenschutzrechtlichen Haftungsansprüchen aus der Datenschutzgrundverordnung aus,¹¹¹ etwa wenn er Daten ohne innerstaatliche Rechtsgrundlage (Art. 6 Abs. 3) speichert.¹¹² Was die genannte Prüfungsbefugnis angeht, so ist der Diensteanbieter „allein“ auf die im EPOC bzw. EPOC-PR Formular enthaltenen Informationen angewiesen (Art. 10 Abs. 5 UA 1, Art. 11 Abs. 4 UA 1), wobei die im EPOC-Formular enthaltenen substantiellen Informationen zu Notwendigkeit und Verhältnismäßigkeit der EPOC, zum zugrundeliegenden Sachverhalt und möglichen Straftaten (Abschnitt M) ausdrücklich „nicht an den Adressaten“ übermittelt werden dürfen.¹¹³ Der Diensteanbieter erhält damit überhaupt keine substantiellen Informationen, die ihm die beschränkte Grundrechtsprüfung ermöglichen würden und er darf sich diese Informationen auch nicht beschaffen, weil alleine die Anordnungsbehörde mit der betroffenen Person in Kontakt treten darf (Art. 13 sowie Abschnitt H EPOC-Formular¹¹⁴).¹¹⁵ Hält der Diensteanbieter gleichwohl eine Grundrechtsbeeinträchtigung für möglich, so kann er nicht selbst über mögliche Konsequenzen entscheiden, sondern muss die Anordnungs- und Vollstreckungsbehörde informieren, die dann über eine Rücknahme, Anpassung oder Aufrechterhaltung der EPOC zu entscheiden hat (Art. 10 Abs. 5 UA 2, 3; ähnlich Art. 11 Abs. 4 UA 2 bezüglich EPOC-PR). Ist sie anderer Auffassung, sieht also keine Rechtsverletzung, setzt sich der Diensteanbieter dem Risiko einer finanziellen Sanktion aus (Art. 15 Abs. 1), während er bei gutgläubigem Vollzug einer Anordnung von Haftung freigestellt ist (Art. 15 Abs. 2); der Diensteanbieter befindet sich also in einem „compliance or punishment“ Dilemma.¹¹⁶

Insgesamt kann der private Rechtsschutz durch den Diensteanbieter die Umgehung des Vollstreckungsstaats bei Nicht-Unterrichtung also nicht kompensieren.¹¹⁷ Deshalb hätte die Unterrichtungspflicht nicht a limine auf Verkehrs- und Inhaltsdaten und Herausgabeanordnungen beschränkt (Art. 8 Abs. 1) werden sollen.¹¹⁸ Auch ist die Ausnahme von der Unterrichtung gemäß Art. 8 Abs. 2 kritisch zu sehen; zumindest hätte man die Entscheidung über die Ausnahmetatbestände nicht alleine der Anordnungsbehörde überlassen dürfen. Nur bei umfassender und ausnahmsloser Unterrichtung der Vollstreckungsbehörde kann man tatsächlich von einem „robusten“ Unterrichtungsverfahren¹¹⁹ sprechen. Eine darüberhinausgehende „aktive Prüf- und Validationspflicht des

¹⁰⁹ Insbesondere Art. 16 Abs. 4 lit. g (auf Grundrechte Bezugnehmend), auf den aber eben Art. 16 Abs. 3 lit. a – Hinweis der Vollstreckungsbehörde an Diensteanbieter (Adressaten) auf mögliche Einwände – gerade nicht verweist.

¹¹⁰ Ebenso *Hüttemann*, NZWiSt 2024, 82 (92).

¹¹¹ Vgl. Art. 15 Abs. 2 VO: „Unbeschadet ihrer Datenschutzpflichten...“. Dazu *Rexin*, CR 2024, 64 (70 f.).

¹¹² Vgl. schon o. Fn. 51 ff. mit Haupttext.

¹¹³ Vgl. das EPOC-Formular als Anhang I der e-evidence VO.

¹¹⁴ Laut Abschnitt H EPOC-Formular darf der „Adressat ... die Person, deren Daten angefordert werden, hiervon in keinem Fall in Kenntnis setzen“.

¹¹⁵ Krit. auch *Hüttemann*, NZWiSt 2024, 82 (89); *Krumwiede*, ZfIStw 2024, 202 (211).

¹¹⁶ *Sachoulidou*, NJECL 2024, 256 (268); s. auch *Tosza*, CLR 2024, 166; *Topalnakos*, eucrim 2023, 200 (201).

¹¹⁷ Krit. auch *Hüttemann*, NZWiSt 2024, 82 (90) („häufig wirkungslos“, „Rechtsschutzlücke“).

¹¹⁸ Für eine Ausweitung und Verallgemeinerung der Unterrichtung auch *Krumwiede*, ZfIStw 2024, 202 (210 f.); ebenso *Petersen* (Fn. 7), S. 331 unter Verweis auf den Verordnungsentwurf des LIBE-Ausschusses, der eine weitergehende Unterrichtungspflicht mit einem zweistufigen Ablehnungsmechanismus vorsah (S. 303 f.).

¹¹⁹ S. o. Fn. 59 und Haupttext.

Vollstreckungsstaats“¹²⁰ wäre dann entbehrlich. Sie würde auch zu weit gehen, weil sie dem Zweck der e-evidence VO – eines grundsätzlich direkten Zugriffs auf den privaten Diensteanbieter – zuwiderliefe.

bb) Betroffener

Wie schon oben erwähnt, sieht die VO (Art. 1 Abs. 2) ein explizites Antragsrecht des Betroffenen vor, im GesE wird dies aber nicht umgesetzt, sondern nur auf die StPO verwiesen (§ 7 GesE). Dies lässt sich zwar damit rechtfertigen, dass Art. 1 Abs. 2 VO das Antragsrecht (nur) „im Einklang mit dem nationalen Strafverfahrensrecht“ vorsieht, der GesE sollte aber zumindest in der Begründung – schon aus Klarstellungsgründen – auf die – allerdings nicht erzwingbare – Beweisantragsrechte im Ermittlungsverfahren in §§ 136 Abs. 1 S. 5, 163a Abs. 2, 166 StPO verweisen.¹²¹

Der Betroffene muss von der Anordnungsbehörde grundsätzlich „unverzüglich“ informiert werden (Art. 13 Abs. 1); dem Diensteanbieter ist dies allerdings, wie schon oben gesehen,¹²² verwehrt. Überdies kann auch die Information durch die Anordnungsbehörde aus bestimmten Gründen (etwa zum Schutz der öffentlichen oder nationalen Sicherheit) aufgeschoben, eingeschränkt oder unterlassen werden (Art. 13 Abs. 2), solange dies „in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird“ (so der in Bezug genommene Art. 13 Abs. 3 RL 2016/680).¹²³ Im Übrigen muss diese Einschränkung „im Einklang mit dem nationalen Recht“ (s. z.B. § 95a oder § 101 Abs. 4 Nr. 4, Abs. 5-7 StPO) geschehen.

Art. 18 Abs. 1 sieht ausdrücklich einen Rechtsbehelf vor und verweist nicht, wie noch Art. 14 Abs. 1 RI-EEA, nur auf das innerstaatliche Recht. Der Rechtsschutz ist allerdings auf die Anordnung „vor einem Gericht des Anordnungsstaats“ (Art. 18 Abs. 2) beschränkt.¹²⁴ Das kann man kritisch sehen,¹²⁵ ist aber insofern folgerichtig, als es vom Grundsatz her ja um direkte Rechtshilfe des Diensteanbieters ohne Beteiligung des Vollstreckungsstaats gehen soll. Im Übrigen bleiben die Grundrechtsgarantien im Vollstreckungsstaat „hiervon unberührt“ (Art. 18 Abs. 2 letzter HS), was aber Auslegungsfragen aufwirft.¹²⁶ Im Ergebnis liegt im fehlenden Rechtsschutz im Vollstreckungsstaat eine empfindliche Rechtsschutzverkürzung, weil der Betroffene auf den Rechtsweg im Anordnungsstaat verwiesen wird.¹²⁷ Das sollte der deutsche Gesetzgeber kompensieren, durch den GesE wird dies aber nicht gelingen.

Zunächst stellt schon die fehlende Information des Betroffenen über den Umfang des Datenzugriffs ein gravierendes grundrechtliches Problem dar. Nach aktueller Rechtslage würde ein Datenzugriff (z.B. auf emails) regelmäßig mittels einer Durchsuchung nach §§ 102 ff. StPO erfolgen. Dies ermöglicht dem Betroffenen eine gewissen Kontrolle, sei es durch Anwesenheit bei der offenen Durchsuchungsmaßnahme (§ 106 StPO) und/oder durch Durchsicht sichergestellter Daten (§ 110 StPO), die jedenfalls dem Berufsgeheimnisträger aus verfassungsrechtlicher Sicht zu gewähren ist. Eine vergleichbare Kontrollmöglichkeit hat der Betroffene beim e-evidence Verfahren nicht. Der

¹²⁰ Krumwiede, ZfIStw 2024, 202 (211).

¹²¹ Dafür auch DAV (Fn. 139), 13; BRAK (Fn. 139), 3 f.; ungenau vorher BRAK, Stellungnahme Nr. 88/2024, Dezember 2024, S. 6, wonach die StPO ein solches Antragsrecht nicht vorsehe (mit eigenem Regelungsvorschlag, ebd., S. 9); krit. auch Beukelmann, NJW-Spezial 2023, 568.

¹²² Vgl. schon o. Fn. 114 mit Haupttext.

¹²³ Krit. Tosza, CLR 2024, 161; Sachoulidou, NJECL 2024, 256 (272); auch Juszcak/Sason, eucrim 2023, 182 (193).

¹²⁴ In der Sache entspricht dies der Rechtsschutzregelung bei der EEA, vgl. Art. 14 Abs. 2 RI-EEA.

¹²⁵ Hüttemann, NZWiSt 2024, 82 (91); Topalnakos, eucrim 2023, 200 (202 f.); Sachoulidou, NJECL 2024, 256 (272).

¹²⁶ Krit. zu dieser unklaren Formulierung Sachoulidou, NJECL 2024, 256 (272).

¹²⁷ Krit. insbesondere zu Mitbetroffenen, die auf einen ggf. „fernen Anordnungsstaat“ verwiesen werden Brodowski, ZStW 2024, 659 (676).

Gesetzgeber könnte ihm aber ein § 102 ff. (§ 110) StPO analoges Anwesenheits- und Informationsrecht bezüglich der betroffenen Daten und ihrer Auswertung geben.¹²⁸

Wie schon oben erwähnt, beschränkt Art. 18 den Rechtsschutz auf Herausgabeanordnungen;¹²⁹ insoweit war es zu begrüßen, dass der RefE 2024 (§ 14 Abs. 2, § 15 Abs. 1 S. 2) auch Sicherungsanordnungen einbezogen hatte; der GesE (§§ 13, 14) hat das aber aufgegeben, weil es mit dem Ende des RefE quick freeze¹³⁰ derzeit an einer Rechtsgrundlage fehlt. Weiter beschränkt der GesE den Rechtsschutz bei (ausgehenden) Herausgabeanordnungen insoweit, als nur noch bei Identifikationsdaten eine (vorherige) Beschwerde und ansonsten (bei Verkehrs- und Inhaltsdaten) nur nachträglicher Rechtsschutz möglich ist.¹³¹ Bei Verkehrs- und Inhaltsdaten ist damit Rechtsschutz erst möglich, wenn sich die Daten bereits im Hoheitsbereich eines anderen (die Daten herausfordernden) Mitgliedstaates befinden, was den Rechtsschutz praktisch wirkungslos macht.¹³²

Außerdem ist die noch im RefE 2024 (§ 15 Abs. 2) vorgesehene Löschung der erlangten Daten und das Verbot der Verwendung darauf beruhender Erkenntnisse bei gerichtlicher Feststellung der Rechtswidrigkeit und Aufhebung der Herausgabeanordnung nun entfallen (§ 14 Abs. 2 GesE). Die Rechtswidrigkeit der Herausgabe bleibt damit also u.U. ohne Konsequenzen, die herausgegebenen Daten bleiben praktisch weiter verwendbar.¹³³ Nach der Gesetzesbegründung soll über Löschung und Verwendungsverbot „im Einzelfall“ entschieden werden und zwar „nach den allgemeinen, strafprozessualen und datenschutzrechtlichen Grundsätzen unter Berücksichtigung des Gewichts des Verfahrensverstößes und des Gewichts der verfolgten Straftat“.¹³⁴ Das führt zu Rechtsunsicherheit und es ist fraglich, ob es mit den verfassungsrechtlichen Anforderungen vereinbar ist;¹³⁵ selbst die VO sieht ja Löschungsvorschriften und Verwendungsbeschränkungen vor.¹³⁶

Last but not least wurde der noch im RefE 2024 (§§ 16, 17) enthaltene Rechtsbehelf gegen die unterlassende Geltendmachung von Ablehnungsgründen durch die Vollstreckungsbehörde (bezüglich einer Herausgabeanordnung) – auf Betreiben der 96. JuMiKo, die einen Effizienzverlust befürchtet – gestrichen. Danach konnte das Amtsgericht gegebenenfalls die Rechtswidrigkeit der unterlassenen Geltendmachung – durch unanfechtbaren Beschluss (§ 17 Abs. 2 RefE) – feststellen (§ 17 Abs. 1 RefE). Dieser nachträgliche – nicht in der VO vorgesehene – Rechtsschutz ist eigentlich zu begrüßen und wegen Art. 19 IV GG (und Art. 47 GRCh) wohl auch gefordert. Jedenfalls trägt er dem Umstand Rechnung, dass nach dem in der e-evidence VO vorgesehenen Verfahren eine Beteiligung des Vollstreckungsstaates grundsätzlich entbehrlich ist, aber aus rechtsstaatlicher Sicht gefordert sein mag.¹³⁷ Deshalb hätte schon die VO einen solchen Rechtsbehelf vorsehen

¹²⁸ S. auch DAV (Fn. 139), 10 f.

¹²⁹ Krit. *Hüttemann*, NZWiSt 2024, 82 (91) („primärrechtswidrig“); krit. auch *Juszcak/Sason*, eucrim 2023, 182 (188) („so-mehow unsatisfactory“); *Topalnakos*, eucrim 2023, 200 (202).

¹³⁰ Vgl. schon o. Fn. 46

¹³¹ Das ergibt sich aus den in § 13 Abs. 1 einerseits und § 13 Abs. 2, 3 andererseits in Bezug genommenen StPO Vorschriften. S. z.B. § 98 Abs. 2 S. 2 („jederzeit ... gerichtliche Entscheidung“) versus § 101 Abs. 7 S. 2 („nach Beendigung der Maßnahme“). Zu berücksichtigen ist allerdings, dass eine Herausgabeanordnung bezüglich Verkehrs- und Inhaltsdaten (§ 13 Abs. 2, 3 GesE) nur durch den Richter erlassen werden kann, insoweit also ex ante eine richterliche Beteiligung (ohne Geltendmachung eines Rechtsbehelfs) gegeben ist.

¹³² Krit. auch DAV (Fn. 139), 6 f.

¹³³ Schon die BRAK (Fn. 25), 4 hielt die Löschung und Nicht-Verwendung für geboten; krit. zum Wegfall nun auch DAV (Fn. 139), 7; gg. Lösungsverpflichtung aber DRiB (Fn. 45), 4.

¹³⁴ GesE (Fn. 14), S. 53.

¹³⁵ Dagegen DAV (Fn. 139), 7.

¹³⁶ O. Fn. 70 mit Haupttext.

¹³⁷ Vgl. *Petersen* (Fn. 7), S. 324.

müssen.¹³⁸ Wenn nun nicht einmal mehr ein innerstaatlicher Rechtsbefehl vorgesehen ist, so kann das praktisch – schon aus den genannten Effizienzgründen – dazu führen, dass Ablehnungsgründe schon deshalb nicht geltend gemacht werden.¹³⁹ Ein eventuelles Fehlverhalten bleibt i.Ü. nach §§ 23 ff. EGGVG oder verwaltungsgerichtlich überprüfbar,¹⁴⁰ so dass sich der Verzicht auf den spezifischen Rechtsbehelf als – im Hinblick auf Effizienz und Verfahrensverzögerung – als kontraproduktiv erweisen kann. Sollte es bei dem Verzicht auf diesen Rechtsbehelf bleiben, wäre auch zu überlegen, ob eine gerichtliche Beteiligung in anderer Form sichergestellt werden kann, etwa durch Genehmigung der Entscheidung der Staatsanwaltschaft (als Vollstreckungsbehörde, § 11 GesE), Ablehnungsgründe nicht geltend zu machen.¹⁴¹ Auch könnte eine Anhörung des Diensteanbieters vor dieser Entscheidung der Vollstreckungsbehörde wichtige Informationen liefern.¹⁴²

c) Pflichtenkollision, Drittstaat, Reziprozität

Sowohl die e-evidence VO als auch der US CLOUD Act sehen einen grenzüberschreitenden Zugriff auf extraterritoriale Daten vor und können damit in Konflikt mit dem Recht des Belegenheitsorts der Daten geraten.¹⁴³ Während in Ergänzung der e-evidence VO die RL-Vertreter (im Sinne des schon genannten qualifizierten Marktortprinzips) auf Dienste innerhalb der EU abstellt und aufgrund dieses Anknüpfungspunkts (*genuine link*)¹⁴⁴ die Diensteanbieter dazu verpflichtet, einen Adressaten zu benennen und alle relevanten Daten herauszugeben oder zu sichern,¹⁴⁵ beruht der US-Ansatz auf der (eigentumsrechtlichen) Verbindung des Diensteanbieters mit den USA (Heimat- oder Sitzstaatsprinzip). Jeder so verstandene US-Diensteanbieter ist verpflichtet, alle seine Daten, unabhängig von ihrem Belegenheitsort, zu liefern.¹⁴⁶ Beide Ansätze greifen in die Datenhoheit von Drittstaaten und damit ihre Souveränität ein, das Heimatstaatsprinzip liefert aber einen stärkeren Anknüpfungspunkt als das Marktortprinzip¹⁴⁷ und wirkt auch restriktiver: Während die US-Behörden im Falle eines ausländischen Diensteanbieters auf zwischenstaatliche Rechtshilfe angewiesen sind, erlaubt die e-evidence VO auch dann einen Durchgriff, wenn der (ausländische) Diensteanbieter seine Dienste (auch) in der EU anbietet.

Die Geltendmachung widersprechender Verpflichtungen aus dem Recht eines Drittstaats obliegt dem Diensteanbieter (Art. 17 Abs. 1, 2), die Überprüfung der Anordnungsbehörde und ggf. einem Gericht des Anordnungsstaats (Art. 17 Abs. 3-8). Auch hier findet also eine Verantwortungsverlagerung auf den privaten Diensteanbieter statt, der damit in eine Pflichtenkollision gerät,¹⁴⁸ die sich

¹³⁸ Vgl. Wörner, in: Ambos et al., Rechtshilferecht in Strafsachen, Kommentar, 2. Aufl. 2020, 4. HT, RL EEA Rn. 417, Vor §§ 91-97 IRG, Rn. 511; Petersen (Fn. 7), S. 205 ff., 327, 336 f.; Ambos, ZfStW 2025, 212.

¹³⁹ Krit. auch BRAK, Stellungnahme 29/2025, Juli 2025, 5 f.; DAV, Stellungnahme 42/2025, Juli 2025, 7 f.; Bundesapothekenkammer, Stellungnahme, 29.7.2025, 1 f.; für diese Streichung (und die anderer Rechtsbehelfe) aber DRiB (Fn. 45), 3 f.

¹⁴⁰ Darauf weist BRAK (Fn. 139), 6 hin.

¹⁴¹ Ähnlich BRAK (Fn. 139), 6.

¹⁴² S. auch BRAK (Fn. 139), 7.

¹⁴³ Vergleichend auch EJPD/BJ (Fn. 29), 20; Weiß/Brinkel, RD 2023, 522 (524) („vergleichbar“).

¹⁴⁴ Petersen (Fn. 7), S. 255 ff. Zum genuine-link-Erfordernis als allgemeinem strafanwendungsrechtlichen Grundsatz s. Ambos, Internationales Strafrecht, 5. Aufl. 2018, § 2 Rn. 6 m.w.N.

¹⁴⁵ Ausführlich zu dieser Ausübung von *indirect enforcement jurisdiction* s. Petersen (Fn. 7), S. 281 ff.

¹⁴⁶ Petersen (Fn. 7), S. 113; Ambos, ZfStW 2025, 206 f.

¹⁴⁷ Ähnlich Rachut/Maurer, jurisPR-ITR 23/2023, 3; zu den Souveränitätsbedenken auch Hüttemann, NZWiSt 2024, 82 (88); Babucke, wistra 2024, 57 (59); Petersen, StraFo 2023, 426 (427, 431 f.). Der Souveränitätseinwand greift natürlich nicht innerhalb der EU, denn die Mitgliedstaaten haben ja durch die Vereinbarung der e-evidence VO insoweit auf ihre Datenhoheitsrechte verzichtet; s. auch Hüttemann, NZWiSt 2024, 82 (93).

¹⁴⁸ Weiß/Brinkel, RD 2023, 522 (527 f.) (zu Rechtsverletzung gezwungen); für die Schweiz s. EJPD/BJ (Fn. 29), 18 f.

nur dadurch auflösen lässt, dass der Anordnungsstaat die Anordnung aufhebt oder anpasst – wenig wahrscheinlich, zumal seine eigenen Gerichte zuständig sind¹⁴⁹ – oder der Drittstaat der Datenlieferung zustimmt. Völkerrechtlich setzt dies aber eine Vereinbarung mit der EU (oder den USA) voraus,¹⁵⁰ die eine Ausnahme vom innerstaatlichen Datenlieferungsverbot, ggf. sogar einen speziellen Rechtfertigungsgrund,¹⁵¹ vorsehen müsste. Die entsprechenden EU-US Verhandlungen liegen derzeit auf Eis. Fehlt es an einer solchen Vereinbarung, müsste der Anordnungsstaat ein Rechtshilfeersuchen an den Drittstaat stellen.¹⁵²

Aus dem völkerrechtlichen Grundsatz der Gegenseitigkeit (Reziprozität) kann in unserem Zusammenhang folgen, dass andere Staaten ebenso expansiv extraterritorial wie die EU (und in geringerem Maße die USA) Daten herausverlangen und sich dabei auf den Präzedenzfall des EU-Rechts berufen. Dieser „Nachahmungseffekt“¹⁵³ würde nicht nur bedeuten, dass mittel- bis langfristig der Datenschutz unterlaufen würde,¹⁵⁴ sondern auch dass weniger rechtsstaatlich gesinnte Staaten die extraterritoriale Datenbeschaffung als weiteres Instrument politischer Verfolgung missbrauchen könnten.¹⁵⁵

IV. Fazit

So notwendig der transnationale Datenzugriff zur Beweisbeschaffung, gerade in transnationalen Kriminalitätsbereichen, auch ist, so viel effizienter er sich gegenüber traditioneller Rechtshilfe auch erweisen mag, so darf doch das Missbrauchspotential nicht unterschätzt werden. Deshalb bedarf es wirksamer rechtsstaatlicher Sicherungen, die, wie wir gesehen haben, von der e-evidence VO nur unzureichend bereitgestellt werden.¹⁵⁶ Sie vertraut im Wesentlichen der Selbstkontrolle der Anordnungsbehörde, was man angesichts deren Rolle und dem damit verbundenen Eigeninteresse für wenig begründet halten mag.¹⁵⁷ Insoweit kommt einer grundrechtssensiblen innerstaatliche Umsetzung große Bedeutung zu. Leider stellt der GesE 2025 insoweit gegenüber dem RefE 2024 einen Rückschritt dar. Die für 2029 vorgesehene Evaluierung wird deshalb auch und gerade die Frage effektiven Rechtsschutzes einbeziehen müssen.¹⁵⁸

Aus Verteidigungssicht jedenfalls ist die e-evidence VO ein weiterer Baustein der traditionell verfolgungslastigen EU-Kriminalpolitik, die es bis heute nicht geschafft hat, transnationale Strafverteidi-

¹⁴⁹ Krit. zur Neutralität des Gerichts des Anordnungsstaats *Burchard*, ZRP 2019, 164 (165) („Bock zum Gärtner“); *Hüttemann*, NZWiSt 2024, 82 (86); *EJPD/BJ* (Fn. 29), 16.

¹⁵⁰ Dafür auch *GdP*, Stellungnahme, 1.8.2025, 5 („zwingend erforderlich“).

¹⁵¹ Wenn etwa der Drittstaat die Datenherausgabe aus datenschutzrechtlichen o.a. Gründen sogar kriminalisiert, s. z.B. Art. 271 schwStGB, dazu *Ambos*, ZfStW 2025, 206 f. mit Fn. 29.

¹⁵² S. auch *Hüttemann*, NZWiSt 2024, 82 (93); *Petersen* (Fn. 7), S. 339 („[...] internationale Lösung in Form von Rechtshilfeverträgen (oder vertragsloser Rechtshilfe) zwischen der Union und Drittstaaten erforderlich“).

¹⁵³ *Rachut/Maurer*, jurisPR-ITR 23/2023, 4.

¹⁵⁴ *Burchard*, ZIS 2018, 190 (192); *Burchard*, ZRP 2019, 164 (165 f.); krit. auch *Krumwiede*, ZfStw 2024, 202 (214 f.); *Petersen* (Fn. 7), S. 293 f.

¹⁵⁵ Krit. auch *Petersen* (Fn. 7), S. 279.

¹⁵⁶ Krit. auch *Basar*, jurisPR-StrafR 14/2023, 5 („Zuwachs an Ermittlungskompetenzen steht kein gleichlaufender Zuwachs an Rechtsschutz gegenüber“).

¹⁵⁷ S. auch *Basar*, jurisPR-StrafR 14/2023, 4 („... fehlen wirksame Kontrollmechanismen und die Rechtmäßigkeitsprüfung obliegt überwiegend der Anordnungsbehörde im Wege der Selbstkontrolle“).

¹⁵⁸ Für „constant scrutiny“ und „monitoring“ auch *Juszcak/Sason*, eucrim 2023, 182 (197).

gung zu institutionalisieren. Transnationale Beweisgewinnung im Sinne der e-evidence VO verstärkt diese Asymmetrie noch weiter und es ist fraglich, ob ihr mit rein privat organisierter Verteidigung wirksam entgegengetreten werden kann.¹⁵⁹

¹⁵⁹ Krit. *Beukelmann*, NJW-Spezial 2023, 568 („wird es für die Verteidigung noch schwerer, einer internationalen Beweisgewinnung wirksam entgegenzutreten zu können“).