E-evidence – direkter Zugriff auf Providerdaten

Von Prof. Dr. Dr. h.c. Kai Ambos, Göttingen/Den Haag*

Ein zentrales Problem grenzüberschreitender Strafverfolgung in der Informationsgesellschaft 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 Menge an Daten („user information")*[6] *heraus.*[7]

Nach kurzer Darstellung der geltenden (nationalen) Rechtslage (I.), wenden wir uns neueren Lösungsansätzen auf völkerrechtlicher und vor allem europäischer Ebene zu (II.). Im Mittelpunkt der Betrachtung steht dabei die auf dem Grundsatz gegenseitiger Anerkennung[8] *und dem daraus ab-*

---

* Der *Verf.* ist ord. Professor an der Georg-August-Universität Göttingen und Richter an den Kosovo Specialist Chambers, Den Haag. Er dankt Frau *Dr. Gabriele Scherer* (BMJ), Frau *Dr. Sonja Heine* (EuStA) sowie Herrn Rechtsanwalt *Dr. Luca Petersen* für wertvolle Hinweise. Frau stud. iur. *Vanessa Rosenberg* dankt der *Verf.* für Hilfe bei der formalen Fertigstellung.

[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, abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118 (3.3.2025).
Zur Europäischen Staatsanwaltschaft insoweit *Frunza-Nicolescu*, eucrim 2023, 210 ff.

[2] Grdl. *Daskal*, The Yale Law Journal 2015, 326 („unterritoriality"); krit. *Burchard*, ZIS 2018, 249; *Hüttemann*, NZWiSt 2024, 82 (93).

[3] Vgl. VO (EU) 2023/1543 (e-evidence-Verordnung [VO]) 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, ABl. EU 2023 Nr. L 191, S. 118, Erwägungsgrund 8; *Burchard*, ZIS 2018, 190 (196); *Tosza*, CLR 2024, 139 (143).

[4] Nach Art. 12 Abs. 3, Abs. 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", sodass Daten oft schon gelöscht seien); *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-VO (Fn. 3), Erwägungsgrund 8; BMJ, Referentenentwurf E-Evidence, Informationspapier, Oktober 2024, abrufbar unter https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Dokumente/Infopapier_E_Evidence.pdf?__blob=publicationFile&v=4 (3.3.2025).

[6] Bei den US-Anbietern geht es um Teilnehmer- und Verkehrsdaten („user information"), keine Inhaltsdaten, siehe die Statistiken bei Google, Meta und Amazon (3.3.2025). Zum hier verwendeten Datenbegriff siehe Fn. 52 mit Haupttext.

[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).

[8] Die VO, (Fn. 3), S. 118 oben, wird auf Art. 82 Abs. 1 AEUV gestützt, dieser gilt aber nur zwischen*staatlich* und beruht auf dem Gedanken staatlicher Anerkennung, Private kommen nicht vor, u.a. deshalb ablehnend *Esser*, in: Sosnitza u.a. (Hrsg.), Digitalisierung im Europäischen Recht, 2022, S. 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.], S. 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, siehe *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").

geleiteten Grundsatz der Verfügbarkeit[9] *beruhende e-evidence-Verordnung der EU,*[10] *die – zeitgleich mit der Richtlinie zur Benennung von Adressaten (RL-Vertreter)*[11] *– am 12.7.2023 verabschiedet wurde, allerdings erst ab 18.8.2026 gelten wird.*[12] *Das BMJ hat Ende Oktober 2024 einen Referentenentwurf („RefE") zur Durchführung der (unmittelbar geltenden) Verordnung*[13] *und zur Umsetzung der Richtlinie vorgelegt.*[14] *Er fiel allerdings der Diskontinuität anheim und kann deshalb erst in der neuen (21.) Legislaturperiode zum Gegenstand des Gesetzgebungsverfahrens werden*.

I. Geltende Rechtslage

Wenn sich im Rahmen eines strafrechtlichen Ermittlungsverfahrens beweisrelevante Daten bei einem Diensteanbieter befinden, so würden deutsche Ermittlungsbehörden zunächst versuchen, diese Daten zu beschlagnahmen (§ 94 Abs. 2 StPO). Der Beschlagnahmebeschluss würde an eine etwaige deutsche Niederlassung des Diensteanbieters zugestellt werden. Sollte sich der Sitz des Diensteanbieters allerdings in einem anderen Land befinden, könnte die Niederlassung auf dieses Land verweisen. Eine Datensicherung in Deutschland könnte in diesem Fall allenfalls durch eine Durchsuchung beim Diensteanbieter samt Zugriff auf die dortigen PCs mit den offen verfügbaren Daten erfolgen (§ 110 Abs. 3 StPO). Das ist ein übliches und gerichtlich sanktioniertes Vorgehen bei offenen Ermittlungen,[15] es ist aber rechtlich umstritten und praktisch nur von begrenzter Wirkung. Aus rechtlicher Sicht kann § 110 Abs. 3 S. 2 StPO den Zugriff auf nicht in Deutschland liegende Daten nicht erlauben, weil in einem grenzüberschreitenden Datenzugriff eine Souveränitätsverletzung des Staates zu sehen ist, in dem sich die Daten befinden.[16] Dieser Staat müsste also rechtshilferechtlich um die Sicherung und Herausgabe der Daten ersucht werden.[17] Handelt es sich dabei um einen EU-Mitgliedstaat könnte immerhin eine EEA erlassen und zur Vollstreckung an diesen Staat übermittelt werden.[18]

Praktisch ist mit großer Wahrscheinlichkeit bei einem nicht zu ermittelnden Speicherort („loss of location")[19] eines ausländischen Diensteanbieters davon auszugehen, dass sich die Daten nicht in Deutschland, sondern auf einem Server im Ausland (ggf. in einer cloud) befinden, der sich zudem nicht im Sitzstaat des Diensteanbieters befindet.[20] Überdies werden die Daten wohl auch durch Authentifizierungen gegen unbefugten Zugriff geschützt sein, sodass schon deshalb der Zugriff von einem in Deutschland befindlichen „Speichermedium" nicht möglich sein wird. Wenn ein Diensteanbieter seine Daten vor ausländischen Strafverfolgungsbehörden schützen will, wird er die Daten (physisch) in einem Staat speichern,

[9] Grdl. *Böse*, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der EU, 2007; jüngst dazu *Brodowski*, ZStW 136 (2024), 659 (670 ff.).

[10] e-evidence-VO (Fn. 3), S. 118. Zur Entstehungsgeschichte ausführlich *Burchard*, ZIS 2018, 190 (193 ff.); auch *Esser* (Fn. 8), S. 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, ABl. EU 2023 Nr. L 191, S. 181. Die RL muss bis 18.2.2026 umgesetzt werden (Art. 7 der RL), eine Evaluierung soll zum 18.8.2029 erfolgen (Art. 8 der RL). Als primärrechtliche Grundlage gibt die RL Art. 53, 62 EUV an, also Regelungen zur Niederlassungsfreiheit. Art. 2 Abs. 2 und Erwägungsgrund 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. 34 Abs. 2 e-evidence-VO. Eine Evaluierung soll es – wie bei der RL – zum 18.8.2029 geben (Art. 33 e-evidence-VO). Die VO gilt nicht für Dänemark wegen dessen opt-out bezüglich Teil III, Titel V AEUV (Raum der Freiheit, der Sicherheit und des Rechts; siehe Erwägungsgrund 101). Irland hat dagegen vom opt-inRecht Gebrauch gemacht, Erwägungsgrund 100.

[13] Art. 288 AEUV.

[14] 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 v. 28.10.2024, abrufbar unter https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_E_Evidence.html (3.3.2025). Nach Auskunft des BMJ (24.3.2025) wird der RefE gerade auf der Grundlage von Rückmeldungen aus Ressorts, Ländern und Verbänden überarbeitet.

[15] LG Koblenz, Beschl. v. 24.8.2021 – 4 Qs 59/21; LG Berlin, Beschl. v. 29.12.2022 – 519 Qs 8/22. So auch *Sonia Heine*, Delegierte Europäische Staatsanwältin, Tagung Arbeitskreis Europäisches Strafrecht, Luzern 19/20.9.2024.

[16] Ebenso *Esser* (Fn. 8), S. 33 f.; *Fiedler*, NStZ 2024, 596 (600 – krit. zu LG Koblenz, Beschl. v. 24.8.2021 – 4 Qs 59/21, und LG Berlin, Beschl. v. 29.12.2022 – 519 Qs 8/22); *Hiéramente/Basar*, jurisPR-StrafR 6/2022, Anm. 1 (ebenfalls krit. zu LG Koblenz [a.a.O.]); *Bechtel*, NZWiSt 2022, 160 (165 f.); *Tsambikakis*, in: Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 3/1, 27. Aufl. 2019, StPO § 110 Rn. 9; *Brodowski*, in: Borges/Hilber (Hrsg.), Beck'scher Online-Kommentar, IT-Recht, Stand: 1.1.2025, StPO § 110 Rn. 12; *Hauschild*, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 1, 2. Aufl. 2023, § 110 Rn. 18; a.A. *Henrichs/Weingast*, in: Barthe/Gerike (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl. 2023, § 110 Rn. 8a; *Wicker*, Cloud Computing und staatlicher Strafanspruch, 2016, S. 356.

[17] Siehe insoweit *Fiedler*, NStZ 2024, 596 (601).

[18] Art. 3 ff., 13 EEA.

[19] Siehe dazu etwa *Burchard*, ZIS 2018, 190 (197).

[20] *Fiedler*, NStZ 2024, 598 f. (601); *Petersen* (Fn. 7), S. 88 f.

der rechtshilferechtlich nur schwer oder überhaupt nicht zugänglich ist. Möglicherweise befindet sich sogar der Unternehmenssitz in einem solchen Staat.

II. Neuere Entwicklungen: Europarat und UNO

Im Rahmen des Europarats, also immerhin für 46 europäische Staaten, wurden zwei zwischenstaatliche Abkommen verabschiedet, die der beschriebenen Situation Rechnung tragen sollen. Nach dem Europäischen Übereinkommen über Computerkriminalität (EuÜbkCompKrim, „Budapest Convention")[21] vom 23. November 2001 sollen die Vertragsparteien die Anordnung der Herausgabe von Daten an Privatpersonen und Diensteanbieter ermöglichen (Art. 18 EuÜbkCompKrim) sowie Diensteanbieter zur Erhebung von Verkehrsdaten sowie Inhaltsdaten in Echtzeit bzw. zur Zusammenarbeit verpflichten (Art. 20 Abs. 1 lit. b, 21 Abs. 1 lit. b EuÜbkCompKrim). Nach dem zweiten Zusatzprotokoll (ZP II)[22] zu diesem Abkommen vom 12. Mai 2022 können zunächst Diensteanbieter um Registrierungsinformation der Domänenamen zur Identifizierung und Kontaktierung der Domäneinhaber ersucht werden (Art. 6 ZP II, Domänenameregistrierungsdaten). Der ersuchende Staat kann eine unmittelbare Anordnung an einen Diensteanbieter („unmittelbar einem Diensteanbieter […] vorzulegende Anordnung") mit Sitz in einem anderem (ersuchten) Vertragsstaat erlassen, „um die Weitergabe bestimmter gespeicherter Bestandsdaten zu erwirken"; der ersuchte Staat muss insoweit entsprechende Ermächtigungsgrundlagen schaffen, damit ein „Diensteanbieter […] zur Erledigung" der Anordnung des ersuchenden Staates „Bestandsdaten weitergeben kann" (Art. 7 Abs. 1, Abs. 2 lit. a ZP II).

Dies ist der entscheidende qualitative Sprung zum direkten Zugriff des ersuchenden Staats auf Daten des Diensteanbieters (der sich im ersuchten Staat befindet).[23] Weigert sich der Diensteanbieter, die Daten innerhalb von 30 Tagen herauszugeben, kann die Anordnung zwischenstaatlich über Art. 8 ZP II oder über sonstige Rechtshilfe (Art. 7 Abs. 7 ZP II) durchgesetzt werden. Insoweit geht es allerdings nicht mehr um eine unmittelbar an den Diensteanbieter gerichtete Anordnung des ersuchenden Staates, sondern um klassische zwischenstaatliche Rechtshilfe, um „Verstärkung der internationalen Zusammenarbeit zwischen Behörden" (Überschrift Abschnitt 3) bezüglich beschleunigter Herausgabe von Bestands- und Verkehrsdaten durch Diensteanbieter (Art. 8 ZP II) sowie um beschleunigte Weitergabe bestimmter „Computerdaten"[24] im Notfall (Art. 9 ZP II).[25] Art. 13 ff. ZP II sehen überdies Bedingungen und Garantien zur Ausgestaltung der Zusammenarbeit vor (insbesondere Datenschutz).

Auf globaler Ebene liegt der Entwurf eines UN-Cybercrime-Übereinkommens vor.[26] Danach sollen Vertragsstaaten eine Herausgabeanordnung („production order") für Daten in Besitz von Privatpersonen und für Bestandsdaten („subscriber information") in Besitz von Diensteanbietern ermöglichen, wobei die Privatperson im Hoheitsgebiet des Anordnungsstaats aufhältig sein muss und die Diensteanbieter dort ihre Dienste anbieten müssen (Art. 27 UN-Cybercrime-Übereinkommen). Die Anknüpfung an die Erbringung von Diensten entspricht dem qualifizierten Marktortprinzip, wie es auch der e-evidence-Verordnung zugrunde liegt (dazu sogleich). Ein Diensteanbieter soll („within its existing technical capability") dazu verpflichtet werden können, Verkehrsdaten in Echtzeit zu sammeln (Art. 29 (1) (b) UN-Cybercrime-Übereinkommen) und Inhaltsdaten abzuhören (Art. 30 (1) (b) UN-Cybercrime-Übereinkommen).

Auf nationaler Ebene verdient insbesondere der US CLOUD („Clarifying Lawful Overseas Use of Data") Act 2018 Erwähnung,[27] denn die USA sind nach wie vor der Sitzstaat der wichtigsten und größten Diensteanbieter. Nach dem CLOUD Act können US-Strafverfolgungsbehörden US-Diensteanbieter auffordern, Daten herauszugeben, unabhängig davon, wo diese belegen sind.[28] Es wird also ein extraterritorialer Datenzugriff ermöglicht, womit der Diensteanbieter in einen Konflikt mit dem Recht des Belegenheitsorts der Daten geraten kann, wenn dieses Recht die Datenherausgabe verbietet.[29] Der Diensteanbieter sieht sich dann zwei konfli-

[21] Siehe https://www.coe.int/en/web/cybercrime/the-budapest-convention (3.3.2025);
deutsche Übersetzung abrufbar unter
https://rm.coe.int/168008157a (3.3.2025).

[22] Siehe https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (3.3.2025); dort auch deutsche Übersetzung.

[23] Siehe dazu auch *Petersen* (Fn. 7), S. 52 ff., 120 f.; knapp *Pfeffer*, eucrim 2023, 170 (172); *Juszcak/Sason*, eucrim 2023, 182 (195).

[24] Vgl. Art. 1 lit. b EuÜbkCompKrim; somit sind neben Bestands- und Verkehrsdaten zumindest begrifflich auch Inhaltsdaten erfasst.

[25] Über das in Art. 35 EuÜbkCompKrim genannte 24/7-Netzwerk.

[26] Siehe Entwurf des „Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" v. 7.8.2024, abrufbar unter
https://documents.un.org/doc/undoc/ltd/v24/055/06/pdf/v2405506.pdf (3.3.2025).
Zum Hintergrund *Pfeffer*, eucrim 2023,170 (172 f.); *Juszcak/Sason*, eucrim 2023, 182 (195 f.).

[27] Eingehend zu den Regelungen und der Funktionsweise des US CLOUD Act siehe *Petersen* (Fn. 7), S. 146 ff. m.w.N.

[28] Vgl. insbesondere 18 U.S.C. § 2713: Verpflichtung für US-Unternehmen, auch auf ausländischen Servern gespeicherte Daten zu übermitteln („[…] to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or *outside* of the United States." [*Hervorhebung* durch den *Verf.*]).

[29] Siehe z.B. Art. 271 schwStGB, wonach strafbar ist, wer Amtshandlungen „auf schweizerischem Gebiet ohne Bewilligung für einen fremden Staat", eine „ausländische Partei"

gierenden Verpflichtungen gegenüber, denen er nicht gleichzeitig entsprechen kann (entweder verletzt er die US-Herausgabeanordnung oder das Recht des Belegenheitsorts).[30] Diese Konfliktlage kann nur durch ein Abkommen zwischen den USA und diesem Staat gelöst werden; die insoweit 2019 initiierten Verhandlungen zwischen den USA und der EU[31] sind derzeit (25.3.2025) aber ausgesetzt.

III. Insbesondere EU-e-evidence Verordnung und Richtlinie

1. Anwendungsbereich, Begrifflichkeiten, Datenarten

Die VO betrifft die Herausgabe und Sicherung (zum Zweck eines späteren Herausgabeersuchens) von elektronischen Beweismitteln (Daten[32], Art. 3 Nr. 8[33]) mittels einer „Europäischen Herausgabeanordnung" („European Production Order Certificate", „EPOC") oder „Europäischen Sicherungsanordnung" („European Preservation Order Certificate-Preservation Request", „EPOC-PR")[34] und zwar „unabhängig davon [!], wo sich die Daten befinden" (Art. 1 Abs. 1). Diese Anordnungen dürfen im Rahmen von Strafverfahren[35] und zur Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Maßregeln (Mindestdauer vier Monate bei Verkehrs- und Inhaltsdaten),[36] die in einem Urteil in Anwesenheit des Betroffenen ergangen sind,[37] 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 Beweisrechtshilfe[38] – immerhin ein ausdrückliches Antragsrecht des Verdächtigen oder Beschuldigten bzw. deren rechtlicher Vertreter vor.[39] 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).[40] Als Diensteanbieter gilt jede natürliche oder juristische Person, die „elektronische Kommunikationsdienste",[41]

---

oder ausländische „Organisation" vornimmt oder solchen „Handlungen Vorschub leistet". Art. 271 soll nach der Rspr. „die Ausübung fremder Staatsgewalt auf dem Gebiet der Schweiz" verhindern und „das staatliche Machtmonopol und die schweizerische Souveränität" schützen (*Husmann*, in: Niggli/Wiprächtiger [Hrsg.], Basler Kommentar, Strafrecht, Bd. 2, 4. Aufl. 2019, Art. 271 Rn. 6 m.w.N. [Hervorhebungen weggelassen]). Erfasst ist damit auch die (amtlich nicht bewilligte) Datenherausgabe an ausländische Strafverfolgungsbehörden, weil diese allein über Rechtshilfe erfolgen darf und damit dem Schweizer Staat obliegt (näher *Husmann* [a.a.O.], Art. 271 Rn. 31 ff.). Allg. zur schweizerischen Rechtslage *Glassey*, eucrim 2023, 204 ff.

[30] Siehe auch *Pfeffer*, eucrim 2023, 170 (171); *Babucke*, wistra 2024, 57.

[31] Siehe Ratsbeschluss von 2019, abrufbar unter https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf (3.3.2025). Die Verhandlungen sind geheim, deshalb gibt es keine offene Quelle. Zum Hintergrund aber *Juszcak/Sason*, eucrim 2023, 182 (194 f.); *Pfeffer*, eucrim 2023, 170 (171 f.).

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

[33] Artikel ohne Bezeichnung beziehen sich auf die e-evidence-VO (Fn. 3)

[34] Bestimmung der Abkürzungen in Erwägungsgrund 50 und Art. 9.

[35] Zur Notwendigkeit einer Regelung für („punitive") Verwaltungsverfahren (insbesondere von OLAF) siehe *Tosza*, eucrim 2023, 216 ff.

[36] Art. 2 Abs. 2 differenziert nicht nach Datenart, aus Erwägungsgrund 40 und Art. 5 Abs. 3 ergibt sich aber, dass die Mindeststrafe nur bei Verkehrs- und Inhaltsdaten, nicht aber bei hier sog. Identifikationsdaten (siehe unten Fn. 52 mit Haupttext) gelten soll; krit. zu dieser unvollständigen Regelung und im Übrigen niedrigen Anwendungsschwelle *Sachoulidou*, NJECL 2024, 256 (269 f.); siehe auch Erwägungsgrund 41 mit Nennung bestimmter Straftaten, bei denen in der Regel nur e-evidence zur Verfügung steht.

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

[38] Das Fehlen eines solchen Antragsrechts in der RL-EEA ist vielfach kritisiert worden, siehe etwa *Karas/Burić/Bonačić/Maršavelski*, in: Ambos/Heinze/Rackow/Šepec (Hrsg.), The European Investigation Order, 2023, S. 29 (45: „[…] does not create a binding European rule which would create a right for the defence to request the issuing of an EIO"); *Scomparin/Ferraris/Cabiale/Peloso/Calavita*, in: Ambos/Heinze/Rackow/Šepec (a.a.O.), S. 69 (83); *Barata/Guimarães/Castilhos*, in: Ambos/Heinze/Rackow/Šepec (a.a.O.), S. 87 (100).

[39] Dieses Antragsrecht wird im RefE (Fn. 14) nicht explizit umgesetzt, sondern nur auf die StPO verwiesen, was sich damit rechtfertigen lässt, dass Art. 1 Abs. 2 VO das Antragsrecht (nur) „im Einklang mit dem nationalen Strafverfahrensrecht" vorsieht. Die StPO sieht – allerdings nicht erzwingbare – Beweisantragsrechte im Ermittlungsverfahren in §§ 136 Abs. 1 S. 5, 163a Abs. 2, 166 vor; insoweit ungenau BRAK, Stellungnahme Nr. 88/2024, Dezember 2024, S. 6, abrufbar unter https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2024/stellungnahme-der-brak-2024-88.pdf (3.3.2025), wonach die StPO ein solches Antragsrecht nicht vorsehe (mit eigenem Regelungsvorschlag, ebd., S. 9); krit. auch *Beukelmann*, NJW-Spezial 2023, 568.

[40] 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*, RDi 2023, 522 (527).

[41] Näher RL (EU) 2018/1972, Art. 2 Nr. 4.

Registrierungsdienste sowie „andere Dienste der Informationsgesellschaft“ (zur Kommunikation, Datenspeicherung)[42] erbringt (Art. 3 Nr. 3).[43] In Deutschland sind ca. 10.000 Diensteanbieter betroffen, davon sind 10 % auslandskontrolliert.[44]

Die Dienste müssen in der Union angeboten werden (siehe schon Art. 2 Abs. 1, Marktortprinzip),[45] 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 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 einen[46] im Unionsgebiet ansässigen Adressaten zur Entgegennahme etc. von Herausgabe- und Sicherungsanordnungen benennen (Art. 3 Abs. 1 RL-Vertreter[47]). In der Union niedergelassene Diensteanbieter müssen insoweit eine Niederlassung benennen (Art. 3 Abs. 1 (a); außerhalb der Union oder in einem nicht teilnehmenden Mitgliedstaat[48] 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.[49] § 3 RefE[50] regelt die unterschiedlichen Konstellationen zur Benennung einer Niederlassung oder eines Vertreters. Kommt der Diensteanbieter dieser Verpflichtung nicht nach, so droht ein Bußgeld[51] aufgrund der entsprechenden Ordnungswidrigkeit (§ 21 Abs. 1 Nr. 1 RefE). Das Bundesamt für Justiz überwacht die Pflichterfüllung des Diensteanbieters (§ 6 RefE).

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“).[52] Im Kern geht es – in telekommunikationsrechtlicher Begrifflichkeit – um Bestandsdaten i.w.S.[53] Verkehrsdaten betreffen die Interaktion (Ursprung und Ziel einer Nachricht, Zeitpunkt und Dauer der Nutzung) sowie sonstige Metadaten (Nr. 11).[54] 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), persönlichkeitssensible Information generiert werden, indem etwa ein Bewegungsprofil erstellt oder ein bestimmtes Nutzerverhalten identifiziert wird.[55]

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 Herausgabe oder Sicherung ersucht wird. Bei den weniger persönlichkeitsrechtssensiblen Identifikationsdaten kann eine Herausgabeanordnung 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 Ermittlungsmaß-

[42] Näher RL (EU) 2015/1535, Art. 1 Abs. 1 lit b.

[43] 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, S. 5 ff., abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/publiservice/publikationen/berichte-gutachten/gutachten/2023-10-24-e-evidence-eu.pdf.download.pdf/2023-10-24-e-evidence-eu-d.pdf (3.3.2025).

[44] RefE (Fn. 14), S. 30 f.

[45] *Esser* (Fn. 8), S. 45; *Brodowski*, ZStW 136 (2024), 659 (675).

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

[47] Siehe oben (Fn. 11).

[48] Das betrifft Dänemark (Fn. 12).

[49] *Petersen*, StraFo 2023, 426 (427); ausführlich dazu *Petersen* (Fn. 7), S. 256 ff.

[50] Siehe oben (Fn. 14).

[51] Gemäß § 21 Abs. 3 Nr. 1 lit. a RefE (Fn. 14) bis zu 500.000 €.

[52] 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.

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

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

[55] Krit. auch *Burchard*, ZIS 2018, 190 (202 Fn. 94); *ders.*, ZRP 2019, 164 (165: in Abgrenzung zu Inhaltsdaten); *Krumwiede*, ZfIStw 3/2024, 202 (211).

nahmen (§§ 94 ff. StPO),[56] insbesondere §§ 100j Abs. 1 S. 1, 100k Abs. 3 StPO. Zuständige Polizeibehörden sind die Ermittlungspersonen der Staatsanwaltschaft i.S.v. § 152 GVG, die allerdings nur im Rahmen der StPO-Zuständigkeiten tätig werden dürfen (§ 7 Abs. 1 RefE),[57] also insbesondere aufgrund § 100j Abs. 1 S. 1 StPO, nicht aber etwa aufgrund § 100k Abs. 3 StPO;[58] jedenfalls sind deren Anordnungen staatsanwaltschaftlich zu validieren (§ 8 Abs. 1 RefE).

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 StPO i.V.m. § 100e Abs. 1 S. 1 StPO), wobei die VO allerdings die staatsanwaltschaftliche Eilkompetenz gem. § 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.[59] 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, § 7 Abs. 2, § 8 Abs. 3 RefE).[60]

Bei der *Sicherung*sanordnung 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 wird die Erlasszuständigkeit grundsätzlich dem Gericht zugewiesen (§ 100e Abs. 1 StPO); es besteht aber eine staatsanwaltschaftliche Eilzuständigkeit gem. §§ 101a Abs. 1a, 100e Abs. 1 S. 2 StPO (§ 9 RefE).

Was die materiellen Voraussetzungen des Erlasses einer *Herausgabe*anordnung angeht, so muss diese, insbesondere mit Blick auf die Beschuldigtenrechte, notwendig und verhältnismäßig[61] 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 Freiheitstrafe[62] 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 verständlich[63] – 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 UAbs. 2).

Eine *Sicherungs*anordnung 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 um-

[56] Grundlegend zur Zuständigkeit nach nationalem Recht siehe EuGH, Urt. v. 16.12.2021 – C-724/19 [ECLI:EU:C:2021:1020] (HP), Rn. 45; EuGH, Urt. v. 8.12.2020 – C-584/19 [ECLI:EU:C:2020:1002] (Staatsanwaltschaft Wien), Rn. 57 ff.

[57] Siehe auch RefE (Fn. 14), S. 43.

[58] Nach § 100j Abs. 3 StPO besteht ein Richtervorbehalt nur bezüglich Abs. 1 S. 2 und S. 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 StPO allein die Staatsanwaltschaft ermächtigt.

[59] Siehe auch RefE (Fn. 14), S. 44.

[60] 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 (siehe auch Erwägungsgrund 36, der alleine auf die objektive Entscheidungsfindung der Staatsanwaltschaft abstellt).

[61] 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“).

[62] Krit. insoweit *Hüttemann*, NZWiSt 2024, 82 (85: „Alltagskriminalität“).

[63] Krit. auch *Hüttemann*, NZWiSt 2024, 82 (86).

stritten.[64] Selbst wenn sie existieren würde, würde es an einer – nach dem „Doppeltürmodell“ erforderlichen[65] – Erlaubnisnorm für Diensteanbieter zur Datenspeicherung fehlen.[66] Deshalb sieht der Referentenentwurf zur Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) in Art. 1 §§ 13a, 24a eine Rechtsgrundlage zur Erfüllung der Pflichten gem. Art. 10 und 11 vor.[67] 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[68] 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 vorgesehen[69] und wurde erst (nicht zuletzt auf Druck Deutschlands, aber vor allem des Europäischen Parlaments[70]) in fortgeschrittenem Verhandlungsstadium als Grundidee eingeführt. Ihre nun vorliegende Form erhielt sie im Rahmen der Trilogverhandlungen.[71] Ob damit ein ausreichend „robustes“ Unterrichtungsverfahren[72] 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“[73] spätestens innerhalb von 8 Stunden (Art. 10 Abs. 4 S. 1).[74] 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

[64] Die insoweit einschlägigen telekommunikationsrechtlichen Regelungen zur Vorratsdatenspeicherung (§§ 175 Abs. 1, 176 TKG) hat das Bundesverwaltungsgericht am 14.8.2023 (BVerwG, Urt. v. 14.8.2023 – 6 C 7.22, Rn. 19 ff.) – infolge der EuGH-Entscheidung zur Vorratsdatenspeicherung vom 20.9.2022 (EuGH, Urt. v. 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 StPO), 100g Abs. 1, 100j Abs. 1 StPO ist ebenfalls umstritten. Vgl. *Rexin*, CR 2024, 64 (67 f.).

[65] 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, Beschl. 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/für den Abruf auf Seiten des Diensteanbieters.

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

[67] BMDV, Entwurf eines ersten Gesetzes zur Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes, Februar 2024, S. 4, 11 („nach dem Bild einer Doppeltür“), abrufbar unter https://cdn.netzpolitik.org/wp-upload/2024/02/2024-02-07_BMDV_RefE_TTDSAendG.pdf (3.3.2025).

[68] In Deutschland soll dies die Staatsanwaltschaft sein, § 10 RefE (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), S. 304.

[69] Krit. *Esser* (Fn. 8), S. 48 ff.

[70] Siehe *Sippel* (EP-Berichterstatterin), eucrim 2023, 109 (guest editorial).

[71] RefE (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.).

[72] RefE (Fn. 14), S. 20.

[73] 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.

[74] Instruktive Unterscheidung der drei Konstellationen bei *Krumwiede,* ZfIStw 3/2024, 202 (206 ff.: Unterrichtung Vollstreckungsbehörde, keine Unterrichtung, Notfallanordnung).

von Ablehnungsgründen zu prüfen (Art. 12 Abs. 1). Als solche kommen (abschließend) in Betracht:[75]

- Schutz der angeforderten Daten durch Immunitäten und Vorrechte (z.B. Beschlagnahmeverbot von Berufsgeheimnisträger gem. § 97 Abs. 1 StPO)[76] 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)[77] 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 geltend[78] 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 allein nach dem (innerstaatlichen) Recht des Vollstreckungsstaats richten[79] – können auch vom Diensteanbieter gegenüber Anordnungs- und Vollstreckungsbehörde vorgebracht werden (Art. 10 Abs. 5 UAbs. 1, Art. 11 Abs. 4 UAbs. 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 UAbs. 2, UAbs. 3, Art. 11 Abs. 4 UAbs. 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, Abs. 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 (§ 18 Abs. 2 RefE); es entscheidet durch unanfechtbaren Beschluss (§ 19 RefE).

Art. 18 gewährt Rechtsschutz gegen die Herausgabeanordnung vor einem Gericht des Anordnungsstaats, das die Rechtmäßigkeit, einschließlich Notwendigkeit und Verhältnismäßigkeit, zu prüfen hat (Abs. 1 und 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. § 14 Abs. 1 RefE erklärt für Rechtsbehelfe gegen Herausgabeanordnungen die §§ 304, 306 bis 310 StPO (bei gerichtlicher Anordnung und Validierung) sowie „in allen anderen Fällen" § 98 Abs. 2 S. 2, S. 3 und S. 5 StPO (insbesondere bei Anordnung und Validierung durch Staatsanwaltschaft) für anwendbar; bei einer Sicherungsanordnung gilt § 101a Abs. 6 S. 2 StPO i.V.m. § 101 Abs. 7 S. 2–4 StPO, sodass der Betroffene die gerichtliche Überprüfung beantragen und gegen diese gerichtliche Entscheidung sofortige Beschwerde einlegen kann (§ 14 Abs. 2 RefE).[80] In der Sache muss das Gericht die (materiellen) Voraussetzungen zum Erlass der jeweiligen Anordnung gem. Art. 4–6 (§ 15 Abs. 1 RefE) und damit auch die Zulässigkeit des Erlasses nach deutschem Recht (Art. 5 Abs. 2 letzter HS, Art. 6 Abs. 3) prüfen; es gilt also ein doppelter (europarechtlicher und nationaler) Maßstab.[81] Liegen die Voraussetzungen nicht vor, ist die Anordnung rechtswidrig und aufzuheben; bereits erlangte Daten sind unverzüglich zu löschen, eventuell darauf beruhende Erkenntnisse dürfen nicht „verwendet" werden (§ 15 Abs. 2 RefE).[82]

Der Adressat einer Herausgabeanordnung kann ferner (nachträglich) amtsgerichtliche Entscheidung wegen der „unterlassene[n] Geltendmachung von Ablehnungsgründen durch die Vollstreckungsbehörde" beantragen (§ 16 Abs. 1–3 RefE). Das Amtsgericht (!) hat dann zu prüfen, ob ein nach Art. 12 Abs. 1 vorliegender Ablehnungsgrund von der Vollstreckungsbehörde ermessensfehlerhaft nicht geltend gemacht wurde, und dabei dieser Gelegenheit zur Stellungnahme zu geben (§ 16 Abs. 5 RefE).[83] Das Gericht hat gegebenenfalls die Rechtswidrigkeit der unterlassenen Geltendma-

[75] Krit. insoweit zum RefE BRAK (Fn. 39), S. 6 („wünschenswert, wenn das […] Prüfprogramm sich auch im Gesetzestext niederschlagen würde").
[76] Siehe auch RefE (Fn. 14), S. 50.
[77] E-evidence-VO (Fn. 3), S. 175 f.
[78] Ggf. auf bestimmte Daten beschränkt und mit Bedingungen versehen, Art. 12 Abs. 4.
[79] Siehe auch *Babucke,* wistra 2024, 57 (60).
[80] Siehe auch RefE (Fn. 14), S. 48 f. Die BRAK (Fn. 39), S. 4, fordert eine ausdrückliche Beschwerdemöglichkeit zum Landgericht.
[81] Siehe auch RefE (Fn. 14), S. 49.
[82] Diese Löschungspflicht und das Verwendungsverbot sind mit Blick auf die in der Regel bereits erfolgte Herausgabe geboten, BRAK (Fn. 39), S. 4.
[83] Damit folgt das BMJ der in der Literatur vertretenen Auffassung, dass es im Falle einer grenzüberschreitenden Ermittlungsmaßnahme – als Ausgleich für die nicht mehr erforderliche ausdrückliche Anerkennung – eines Rechtsbehelfs im Vollstreckungsstaat bedarf, der auf die Geltendmachung der Ablehnungsgründe durch diesen gerichtet ist, vgl. *Petersen* (Fn. 7), S. 324. Für den Betroffenen, der den Schutz der deutschen Gerichtsbarkeit in Anspruch nehmen kann, wird damit der Rechtsschutz im Vergleich zur Verordnung erweitert.

chung festzustellen (§ 17 Abs. 1 RefE), und zwar durch unanfechtbaren Beschluss (§ 17 Abs. 2 RefE). Dieser nachträgliche Rechtsschutz, der nicht in der VO vorgesehen ist, ist zu begrüßen. Die Tatsache, dass er nur eingehende Anordnungen, bei denen Deutschland Vollstreckungsstaat ist (§ 16 Abs. 1 RefE: „Vollstreckungsbehörde" ist), betrifft, liegt in der Logik der VO, die nur eine Unterrichtung der Vollstreckungsbehörde (Art. 8) durch die (ausländische) Anordnungsbehörde bei (deren) eingehenden Anordnungen vorsieht. Wird die Rechtswidrigkeit der unterlassenen Geltendmachung von Ablehnungsgründen festgestellt (§ 17 Abs. 1 RefE), richten sich die Rechtsfolgen dieser Feststellung nach dem Recht der (ausländischen) Anordnungsbehörde.[84] Um den (nachträglichen) Rechtsschutz im Vollstreckungsstaat nicht leerlaufen zu lassen, müsste es also eine Regelung, ggf. abgesichert durch einen Rechtsbehelf, im Anordnungsstaat geben, die Rechtsfolgen an das rechtswidrige Unterlassen der Geltendmachung von Ablehnungsgründen durch die Vollstreckungsbehörde knüpft. Ein solcher Rechtsbehelf hätte in der VO verlangt werden sollen.[85]

Sollte ein Diensteanbieter eine (wirksame) Herausgabe- oder Sicherungsanordnung nicht vollstrecken, kann die Anordnungsbehörde die Vollstreckungsbehörde um Vollstreckung ersuchen (Art. 16 Abs. 1, Abs. 2). Dabei informiert die Vollstreckungsbehörde den Diensteanbieter über die Möglichkeit, Einwände (dazu Art. 16 Abs. 4, Abs. 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 (§ 20 RefE).

Die Mitgliedstaaten müssen wirksame, verhältnismäßige und abschreckende Sanktionen für Fälle der Nichtbefolgung von Herausgabe- oder Sicherungsanordnungen vorsehen (Art. 15 Abs. 1 S. 1 und 2). Sie sollen sich auf maximal 2 % des Jahresgesamtumsatzes des Diensteanbieters belaufen (Art. 15 Abs. 1 S. 3). § 21 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, 4). Bußgeldbehörde ist das Bundesamt für Justiz oder die Staatsanwaltschaft als Vollstreckungsbehörde (Abs. 5).[86]

4. Weitere (spezifische) Kritik

Die VO sieht keine umfassende Regelung zur Zulässigkeit bzw. Verwertung rechtswidrig erlangter Beweise, sondern nur selektive Verwendungsverbote[87] vor.[88] Sie liefert auch keine (sonstige) Harmonisierung relevanter strafprozessualer Aspekte, insbesondere bezüglich Grad des Tatverdachts und beweisrechtlicher Substantiierungsanforderungen (etwa zur Eingrenzung der Datenabfrage).[89] Allerdings ist zu bedenken, dass eine solche Harmonisierung nur durch Richtlinien herbeigeführt werden kann (Art. 82 Abs. 2 AEUV).[90] In der Sache könnte man eine faktische Harmonisierung in der Bestimmung von Mindestbedingungen (Art. 5 Abs. 4 lit. a: Mindesthöchststrafe drei Jahre) und, 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.[91] Der RefE verweist hinsichtlich der Ermittlungsmaßnahmen auf eine „zukünftige Fassung" der StPO mit Blick auf das „Quick-Freeze-Verfahren".[92] 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 Strafverfahrensrecht[93] eine solche Möglichkeit nicht vorsieht? Dafür spricht die unmittelbare An-

[84] Siehe auch RefE (Fn. 14), S. 51: „Welche Rechtsfolgen sich an diese Feststellung im einzelnen Fall anschließen, richtet sich nach dem nationalen Recht der Anordnungsbehörde, die aufgrund der Logik der Verordnung (EU) 2023/1543 stets im Ausland liegt […] (Unterrichtung gemäß Artikel 8 der Verordnung an eine deutsche Staatsanwaltschaft nur bei eingehenden Anordnungen, nicht bei ausgehenden)."

[85] Vgl. auch *Wörner*, in: Ambos/König/Rackow (Hrsg.), Rechtshilferecht in Strafsachen, Kommentar, 2. Aufl. 2020, 4. HT, RL EEA Rn. 417, IRG Vor §§ 91–97 Rn. 511; *Petersen* (Fn. 7), S. 205 ff., 327, 336 f.

[86] Siehe dazu auch RefE (Fn. 14), S. 56 ff.

[87] Vgl. Art 4 Abs. 5, 10 Abs. 4 und 12 Abs. 4 (Löschung von Daten und Verwendungsbeschränkung).

[88] Krit. *Sachoulidou*, NJECL 2024, 256 (272 f.); ungenau *Basar*, jurisPR-StrafR 14/2023, 4; *Krumwiede*, ZfIStw 3/2024, 202 (212: keine Verwendungsverbote). Zum Vorschlag des European Law Institute (ELI) für Mindestanforderungen zur gegenseitigen Zulässigkeit von Beweisen siehe *Bachmaier*, eucrim 2023, 223 ff.

[89] *Burchard*, ZRP 2019, 164 (166); auch *Petersen* (Fn. 7), S. 322.

[90] Zur Rechtsgrundlage der VO siehe schon Fn. 8.

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

[92] RefE (Fn. 14), S. 11 Fn. 3, S. 45 Fn. 4. Zum „quick freeze" siehe BMJ, Entwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung, Oktober 2024, abrufbar unter https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_Einfuehrung_Sicherungsanordnung_Verkehrsdaten.pdf?__blob=publicationFile&v=4 (21.3.2025).
Dieser RefE ist auch der Diskontinuität zum Opfer gefallen und sein Schicksal ist derzeit (25.3.2025) unklar. Krit. zur pauschalen Verweisung auf den achten Abschnitt der StPO im RefE BRAK (Fn. 39), S. 3 f.

[93] Zur dt. Rechtslage siehe schon Fn. 39.

wendbarkeit der VO (Art. 288 UAbs. 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 RefE insinuiert;[94] sie ähnelt insoweit in der Sache einer Richtlinie.

Die VO führt zu einer Teilprivatisierung[95] 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,[96] 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.[97] Wie dem auch sei, die Kooperation Privater dürfte im Bereich elektronischer Beweismittel nachgerade unentbehrlich sein,[98] doch muss 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 (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 (c).

a) Unterrichtungsverfahren

Mit der Einbindung der Vollstreckungsbehörde durch das Unterrichtungsverfahren soll umfassender Rechtsschutz gewährleistet werden,[99] die Unterrichtungspflicht ist aber mehrfach eingeschränkt und wird damit eher zur Ausnahme als zur Regel.[100] Zum einen gilt sie nur bei einer Herausgabeanordnung, zum anderen nur bezüglich Verkehrs- und Inhaltsdaten (Art. 8 Abs. 1). Damit muss weder bei einer auf jegliche Daten gerichteten Sicherungsanordnung, noch bei einer Herausgabeanordnung bezüglich Identifikationsdaten unterrichtet werden.[101] 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 lit. a) und die betroffene Person im Anordnungsstaat ansässig ist (Art. 8 Abs. 2 lit. b).[102] Ob dafür „hinreichende Gründe" bestehen, hat allein die – möglicherweise befangene – Anordnungsbehörde zu entscheiden (Art. 8 Abs. 2).[103] Besonders schutzbedürftige Gruppen, etwa Journalisten, Dissidenten oder Whistleblower, die ein legitimes Interesse haben können, 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)[104] unterrichtet werden müsste (Beispielhaft: die ungarische Regierung kann sich ggf. direkt an den in Deutschland ansässigen Vertretener 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.[105] Systemwidrig ist insoweit die Erweiterung auf zukünftige Taten in Art. 8 Abs. 2 lit. a Alt. 2 und Alt. 3 („wird oder wahrscheinlich begangen werden

[94] Siehe oben Fn. 14: „Umsetzung der Richtlinie […] Durchführung der Verordnung […]."

[95] Entgegen der in der Lit. geäußerten Kritik (*Brodowski*, ZStW 136 [2024], 659 [675]; *Burchard*, ZIS 2018, 249 [265]; *Tosza*, CLR 2024, 141 [141 f., 156]; auch EJPD/BJ [Fn. 43], S. 21) handelt es sich nicht um eine *vollständige* Privatisierung, denn die Herausgabe bzw. Sicherung wird ja von einem (Anordnungs-)Staat verlangt.

[96] *Tosza*, CLR 2024, 139 (156: „paradigm shift", „quantum leap"); ebenso *Sachoulidou*, NJECL 2024, 256 (259, 267).

[97] *Tosza*, CLR 2024, 153.

[98] Sie ist auch im nationalen Recht vorgesehen, siehe 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 UAbs. 2), die der VO und Richtlinie zugrundeliegenden Prinzipien dürfen aber nicht umgangen werden (RL-Vertreter, Erwägungsgrund 9; dazu auch *Weiß/Brinkel*, RDi 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) siehe *Sachoulidou*, NJECL 2024, 256 (259, 266 f.).

[99] RefE (Fn. 14), S. 20 f.

[100] EDRi v. 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/. (3.3.2025); 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.).

[101] Vgl. RefE (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."

[102] Krit. *Krumwiede*, ZfIStw 3/2024, 202 (210 f.); *Basar*, jurisPR-StrafR 14/2023, 4; *Juszcak/Sason*, eucrim 2023, 182 (193).

[103] Krit. auch EDRi (Fn. 100): „considerable interests in avoiding the notification procedure"; zust. EJPD/BJ (Fn. 43), S. 12 („beachtliches Interesse an der Vermeidung der Notifizierung").

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

[105] Vgl. e-evidence-VO, Erwägungsgrund 52.

wird"), denn es geht um e-evidence „im Rahmen eines Strafverfahrens" mit Blick auf „eine konkrete, bereits begangene Straftat",[106] nicht aber um präventiv-polizeiliche Straftatverhütung.[107] Hinsichtlich der „Ansässigkeit" des Tatverdächtigen im Anordnungsstaat (Art. 8 Abs. 2 lit. b) reichen – jenseits einer Registrierung (Meldung) dort – auch bestimmte Bindungen aus;[108] das ist unbestimmt weit.[109]

Praktisch bedeutet die Ausnahme von der Unterrichtung der Vollstreckungsbehörde (bzw. das faktische Unterlassen der Unterrichtung[110]), 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: Deutschland 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 polnischem Staatsbürger in Polen vorgenommene Abtreibung handelt, die dort zwar strafbar, aber hier straflos wäre.[111] Damit wird faktisch der (ohnehin stark eingeschränkte)[112] Grundsatz der beiderseitigen Strafbarkeit ausgehebelt,[113] denn dessen Verletzung kann nur von der Vollstreckungsbehörde geltend gemacht werden (Art. 12 Abs 1 lit. d), die ja aber überhaupt keine Kenntnis von dem Herausgabeverlagen hat. Selbst der oben zustimmend erwähnte Rechtsbehelf von § 16 RefE[114] 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 sind[115] und schon begangene Straftaten überhaupt nicht betreffen.[116]

Die ebenfalls schon o.g. möglichen Ablehnungsgründe muss die Vollstreckungsbehörde nur „gegebenenfalls" („where appropriate", Art 12 Abs. 1) geltend machen.[117] Die Bundesregierung forderte insoweit zu Recht, dass „im Rahmen des Unterrichtungsverfahrens die individualrechtsschützenden Zurückweisungsgründe obligatorisch zu prüfen seien, was in den Erwägungsgründen [und eben auch in Art. 12, Ergänzung durch den *Verf.*] der Verordnung nicht hinreichend klar zum Ausdruck komme."[118] Der hier in Bezug genommene 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,[119] 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.[120] 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 alldem 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

[106] Vgl. Erwägungsgrund 24 und Art. 1 Abs. 1.

[107] Krit. auch *Hüttemann*, NZWiSt 2024, 82 (85: „systemwidrig", „Risiko einer missbräuchlichen Datenerhebung durch den Anordnungsstaat").

[108] Vgl. e-evidence-VO, Erwägungsgrund 53 („bestimmte Bindungen", konkretisiert durch objektive Faktoren wie Dauer, Art und Umstände des Aufenthalts sowie „familiäre und wirtschaftliche Bindungen").

[109] Krit. auch *Hüttemann*, NZWiSt 2024, 82 (86); *Krumwiede*, ZfIStw 3/2024, 202 (211); *Basar*, jurisPR-StrafR 14/2023, 4; EDRi (Fn. 100).

[110] 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 („most participants believed that […] the intercepting authorities have simply not notified them"), abrufbar unter https://www.ejn-crimjust.europa.eu/ejnupload/News/Outcome-Report_Eurojust-meeting-on-EIO-Sept-2018_EN.pdf (3.3.2025).

[111] Bsp. (leicht geändert) nach *Babucke*, wistra 2024, 57 (60 f.).

[112] Siehe zur Ausnahme bei Katalogtaten laut Anhang IV der VO und Mindesthöchststrafe schon oben Fn. 77 mit Haupttext.

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

[114] Siehe oben Fn. 83 mit Haupttext.

[115] Zur Definition schon oben Fn. 73.

[116] Näher *Hüttemann*, NZWiSt 2024, 82 (87).

[117] Krit. *Hüttemann*, NZWiSt 2024, 82 (87).

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

[119] Ganz im Sinne des auch im letzten Satz von Erwägungsgrund 62 betonten Ermessensspielraums der (unabhängigen) Justizbehörden.

[120] In diesem Sinne auch überzeugend RefE (Fn. 14), S. 50, 51; i.E. ebenso BRAK (Fn. 39), S. 5.

nicht in der Lage sein werden, alle Anordnungen (von denen sie Kenntnis haben) gründlich zu prüfen.[121]

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 lit. b, auch Art. 16 Abs. 4 lit. 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.[122]

b) Rechtsschutz

aa) Diensteanbieter

Was die Geltendmachung möglicher Grundrechtsverletzungen durch den privaten Diensteanbieter angeht (Art. 10 Abs. 5 UAbs. 1, Art. 11 Abs. 4 UAbs. 2), so unterliegt die darin liegende Verlagerung des Grundrechtsschutzes auf einen privaten Akteur („Privatisierung") zunächst grundsätzlichen Bedenken,[123] weil sich einerseits private Akteure grundsätzlich nicht von öffentlichen (sondern eben von privaten, geschäftlichen) Interessen leiten lassen[124] und sich andererseits grundrechtliche Schutzpflichten ausschließlich an den Staat richten und sich dieser der daraus erwachsenden Verpflichtung nicht durch Delegation auf Private entziehen kann. 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,[125] 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.[126] 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.[127] Bezüglich der Anordnung hat der Diensteanbieter lediglich eine beschränkte Prüfungsbefugnis mit Blick auf bestimmte (Grund-) Rechte (Immunitäten, Vorrechte, Presse- und Meinungsfreiheit) mit etwaiger In-Kenntnis-Setzung von Anordnungs- und Vollstreckungsbehörde (Art. 10 Abs. 5 UAbs. 1, Art. 11 Abs. 4 UAbs. 2), der in Bezug genommene Anhang III enthält aber einen weitergehenden Prüfungskatalog.[128] Zwar kann er auch auf anderen Gründen beruhende Einwände geltend machen (Art. 10 Abs. 8), doch 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).[129]

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.[130] Überdies setzt er sich datenschutzrechtlichen Haftungsansprüchen aus der Datenschutzgrundverordnung aus,[131] etwa wenn er Daten ohne innerstaatliche Rechtsgrundlage (Art. 6 Abs. 3) speichert.[132] 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 UAbs. 1, Art. 11 Abs. 4 UAbs. 2), 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.[133] 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

[121] 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"]).

[122] Krit. insoweit EDRi (Fn. 100); auch EJPD/BJ (Fn. 43), S. 12; *Tosza*, CLR 2024, 154 f. (insbes. krit. zum einschränkenden Adjektiv „manifest" [„offensichtlich"]).

[123] 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.

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

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

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

[127] Siehe auch *Basar*, jurisPR-StrafR 14/2023, 3; *Rexin*, CR 2024, 64 (72).

[128] Art. 10 Abs. 5 UAbs. 1, Art. 11 Abs. 4 UAbs. 1 verweisen auf das Formular in Anhang III (e-evidence-VO [Fn. 3], S. 172 ff.), das in Abschnitt D eine Liste von Gründen für die Unmöglichkeit der Ausführung enthält. Krit. auch *Tosza*, CLR 2024, 162.

[129] 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.

[130] Ebenso *Hüttemann*, NZWiSt 2024, 82 (92).

[131] Vgl. Art. 15 Abs. 2 VO: „Unbeschadet ihrer Datenschutzpflichten […]". Dazu *Rexin*, CR 2024, 64 (70 f.).

[132] Vgl. schon oben Fn. 64 ff. mit Haupttext.

[133] Vgl. das EPOC-Formular als Anhang I der e-evidence-VO (Fn. 3).

sowie Abschnitt H EPOC-Formular[134]).[135] 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 UAbs. 2, UAbs. 3; ähnlich Art. 11 Abs. 4 UAbs. 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.[136]

Insgesamt kann der private Rechtsschutz durch den Diensteanbieter die Umgehung des Vollstreckungsstaats bei Nicht-Unterrichtung also nicht kompensieren.[137] Deshalb hätte die Unterrichtungspflicht nicht a limine auf Verkehrs- und Inhaltsdaten und Herausgabeanordnungen beschränkt (Art. 8 Abs. 1) werden sollen.[138] Auch ist die Ausnahme von der Unterrichtung gem. Art. 8 Abs. 2 kritisch zu sehen; zumindest hätte man die Entscheidung über die Ausnahmetatbestände nicht allein der Anordnungsbehörde überlassen dürfen. Nur bei umfassender und ausnahmsloser Unterrichtung der Vollstreckungsbehörde kann man tatsächlich von einem „robusten" Unterrichtungsverfahren[139] sprechen. Eine darüberhinausgehende „aktive Prüf- und Validationspflicht des Vollstreckungsstaats"[140] 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

Der Betroffene muss von der Anordnungsbehörde grundsätzlich „unverzüglich" informiert werden (Art. 13 Abs. 1); dem Diensteanbieter ist dies allerdings, wie schon oben gesehen,[141] 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).[142] Im Übrigen muss diese Einschränkung „im Einklang mit dem nationalen Recht" (siehe z.B. § 95a StPO oder § 101 Abs. 4 Nr. 4, Abs. 5–7 StPO) erfolgen.

Wie schon oben erwähnt, beschränkt Art. 18 den Rechtsschutz auf Herausgabeanordnungen;[143] insoweit ist es zu begrüßen, dass der RefE auch Sicherungsanordnungen einbezieht.[144] Immerhin sieht Art. 18 Abs. 1 ausdrücklich einen Rechtsbehelf vor und verweist nicht, wie noch Art. 14 Abs. 1 RL-EEA, nur auf das innerstaatliche Recht. Der Rechtsschutz ist allerdings auf die Anordnung „vor einem Gericht des Anordnungsstaats" (Art. 18 Abs. 2) beschränkt.[145] Das wird kritisch gesehen,[146] 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.[147] Im Ergebnis liegt im fehlenden Rechtsschutz im Vollstreckungsstaat (siehe aber § 16 RefE[148]) eine empfindliche Rechtsschutzverkürzung, weil der Betroffene auf den Rechtsweg im Anordnungsstaat verwiesen wird.[149]

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.[150] 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)[151] die Diensteanbieter dazu verpflichtet,

[134] Laut Abschnitt H EPOC-Formular darf der „Adressat […] die Person, deren Daten angefordert werden, hiervon in keinem Fall in Kenntnis setzen".

[135] Krit. auch *Hüttemann*, NZWiSt 2024, 82 (89); *Krumwiede*, ZfIStw 3/2024, 202 (211).

[136] *Sachoulidou*, NJECL 2024, 256 (268); siehe auch *Tosza*, CLR 2024, 166; *Topalnakos*, eucrim 2023, 200 (201).

[137] Krit. auch *Hüttemann*, NZWiSt 2024, 82 (90: „häufig wirkungslos", „Rechtsschutzlücke").

[138] Für eine Ausweitung und Verallgemeinerung der Unterrichtung auch *Krumwiede*, ZfIStw 3/2024, 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.).

[139] Siehe oben Fn. 72 und Haupttext.

[140] *Krumwiede*, ZfIStw 3/2024, 202 (211).

[141] Vgl. schon oben Fn. 134 mit Haupttext.

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

[143] Krit. *Hüttemann*, NZWiSt 2024, 82 (91: „primärrechtswidrig"); krit. auch *Juszcak/Sason*, eucrim 2023, 182 (188: „somehow unsatisfactory"); *Topalnakos*, eucrim 2023, 200 (202).

[144] Vgl. oben Fn. 80 mit Haupttext.

[145] In der Sache entspricht dies der Rechtsschutzregelung bei der EEA, vgl. Art. 14 Abs. 2 Rl-EEA.

[146] *Hüttemann*, NZWiSt 2024, 82 (91); *Topalnakos*, eucrim 2023, 200 (202 f.); *Sachoulidou*, NJECL2024, 256 (272).

[147] Krit. zu dieser unklaren Formulierung *Sachoulidou*, NJECL 2024, 256 (272).

[148] Siehe oben Fn. 83 mit Haupttext.

[149] Krit. insbesondere zu Mitbetroffenen, die auf einen ggf. „fernen Anordnungsstaat" verwiesen werden, *Brodowski*, ZStW 136 (2024), 659 (676).

[150] Vergleichend auch EJPD/BJ (Fn. 43), S. 20; *Weiß/Brinkel*, RDi 2023, 522 (524: „vergleichbar").

[151] *Petersen* (Fn. 7), S. 255 ff. Zum genuine-link-Erfordernis als allgemeinem strafanwendungsrechtlichen Grundsatz siehe

einen Adressaten zu benennen und alle relevanten Daten herauszugeben oder zu sichern,[152] beruht der US-Ansatz auf der (eigentumsrechtlichen) Verbindung des Diensteanbieters mit den USA (Heimat- oder Sitzstaatprinzip). Jeder so verstandene US-Diensteanbieter ist verpflichtet, alle seine Daten, unabhängig von ihrem Belegenheitsort, zu liefern.[153] Beide Ansätze greifen in die Datenhoheit von Drittstaaten und damit ihre Souveränität ein, das Heimatstaatsprinzip liefert aber einen stärkeren Anknüpfungspunkt als das Marktortprinzip[154] 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, Abs. 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,[155] die sich nur dadurch auflösen lässt, dass der Anordnungsstaat die Anordnung aufhebt oder anpasst – wenig wahrscheinlich, zumal seine eigenen Gerichte zuständig sind[156] – oder der Drittstaat der Datenlieferung zustimmt. Völkerrechtlich setzt dies aber eine Vereinbarung mit der EU (oder den USA) voraus, die eine Ausnahme vom innerstaatlichen Datenlieferungsverbot, ggf. sogar einen speziellen Rechtfertigungsgrund,[157] vorsehen müsste. Auf die entsprechenden (derzeit ausgesetzten) EU-US Verhandlungen wurde schon oben hingewiesen.[158] Fehlt es an einer solchen Vereinbarung, müsste der Anordnungsstaat ein Rechtshilfeersuchen an den Drittstaat stellen.[159]

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“[160] würde nicht nur bedeuten, dass mittel- bis langfristig der Datenschutz unterlaufen würde,[161] sondern auch dass weniger rechtsstaatlich gesinnte Staaten die extraterritoriale Datenbeschaffung als weiteres Instrument politischer Verfolgung missbrauchen könnten.[162]

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.[163] Sie vertraut im Wesentlichen der Selbstkontrolle der Anordnungsbehörde, was man angesichts deren Rolle und dem damit verbundenen Eigeninteresse für wenig begründet halten mag.[164] Inwieweit dies durch eine grundrechtssensible innerstaatliche Umsetzung, wie sie im RefE zum Ausdruck kommt, kompensiert werden kann, wird sich zeigen müssen. Die für 2029 vorgesehene Evaluierung wird deshalb auch und gerade die Frage effektiven Rechtsschutzes einbeziehen müssen.[165]

Aus Verteidigungssicht jedenfalls ist die e-evidence-VO ein weiterer Baustein der traditionell verfolgungslastigen EU-Kriminalpolitik, die es bis heute nicht geschafft hat, transnationale Strafverteidigung 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.[166]

Ambos, Internationales Strafrecht, 5. Aufl. 2018, § 2 Rn. 6 m.w.N.

[152] Ausführlich zu dieser Ausübung von indirect enforcement jurisdiction siehe *Petersen* (Fn. 7), S. 281 ff.

[153] Siehe oben Fn. 28; *Petersen* (Fn. 7), S. 113.

[154] 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; siehe auch *Hüttemann*, NZWiSt 2024, 82 (93).

[155] *Weiß/Brinkel*, RDi 2023, 522 (527 f., zu Rechtsverletzung gezwungen); für die Schweiz siehe EJPD/BJ (Fn. 43), S. 18 f.

[156] Krit. zur Neutralität des Gerichts des Anordnungsstaats *Burchard*, ZRP 2019, 164 (165: „Bock zum Gärtner“); *Hüttemann*, NZWiSt 2024, 82 (86); EJPD/BJ (Fn. 43), S. 16.

[157] Wenn etwa der Drittstaat die Datenherausgabe aus datenschutzrechtlichen oder anderen Gründen sogar kriminalisiert, siehe z.B. Art. 271 schwStGB (Fn. 29).

[158] Siehe oben Fn. 31 und Haupttext.

[159] Siehe 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“).

[160] *Rachut/Maurer*, jurisPR-ITR 23/2023, 4.

[161] *Burchard*, ZIS 2018, 190 (192); *Burchard*, ZRP 2019, 164 (165 f.); krit. auch *Krumwiede*, ZfIStw 3/2024, 202 (214 f.); *Petersen* (Fn. 7), S. 293 f.

[162] Krit. auch *Petersen* (Fn. 7), S. 279.

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

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

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

[166] Krit. *Beukelmann*, NJW-Spezial 2023, 568 (568: „wird es für die Verteidigung noch schwerer, einer internationalen Beweisgewinnung wirksam entgegentreten zu können“).