21. Wahlperiode

Deutscher Bundestag
Ausschuss für Recht und Verbraucherschutz

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

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN IN PUBLICA COMMODA SEIT 1737

Juristische Fakultät
Institut für Kriminalwissenschaften

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 grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel 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 zehntelsekündlich.").

[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 Anerkennung[8] und dem daraus abgeleiteten Grundsatz der Verfügbarkeit[9] – am 12.7.2023 die e-evidence Verordnung[10] und zeitgleich die Richtlinie zur Benennung von Adressaten (RL-Vertreter)[11] verabschiedet, wobei die RL bis zum 18.2.2026 umzusetzen ist[12] und die VO ab 18.8.2026 gelten wird.[13] Mit Blick auf den vorliegenden Gesetzentwurf [14] (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 zwischen*staatlich* und beruht auf dem Gedanken staatlicher Anerkennung, Private kommen nicht vor (u.a. deshalb ablehnend *Esser*, in: Sosnitza 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, ABl L 191, S. 118. Zur Entstehungsgeschichte 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, ABl 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.bmjv.de/SharedDocs/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. 8[19]) mittels einer „Europäischen Herausgabeanordnung“ („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 Strafverfahren[21] 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 Beweisrechtshilfe[24] – 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*, RDi 2023, 522 (527).

[27] Näher Rl. (EU) 2018/1972, Art. 2 Nr. 4.

[28] Näher Rl. (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 einen[32] im Unionsgebiet ansässigen Adressaten zur Entgegennahme etc. von Herausgabe- und Sicherungsanordnungen benennen (Art. 3 Abs. 1 RL-Vertreter[33]). In der Union niedergelassene Diensteanbieter müssen insoweit eine Niederlassung benennen (Art. 3 Abs. 1(a)); außerhalb der Union oder in einem nicht teilnehmenden Mitgliedstaat[34] 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 Bußgeld[36] 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), persönlichkeitssensible 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 *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 soll die Erlasszuständigkeit – nach dem Ende des RefE quick freeze[46] – 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 Strafverfahren[47] (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 verhältnismäßig[48] 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[49] 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[50] – 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“ erforderlichen[52] – 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 vorgesehen[56] und wurde erst (nicht zuletzt auf Druck Deutschlands, aber vor allem des Europäischen Parlaments[57]) in fortgeschrittenem Verhandlungsstadium als Grundidee eingeführt. Ihre nun vorliegende Form erhielt sie im Rahmen der Trilogverhandlungen.[58] Ob damit ein ausreichend „robustes“ Unterrichtungsverfahren[59] 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-Berichterstatterin), eucrim 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, Notfallanordnung).

[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 geltend[65] 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 richten[66] – 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 Sicherungsanordnungen[67] 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 Jahresgesamtumsatzes 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 Verwendungsverbote[70] 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, ZfIStW 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*, ZfIStw 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 Strafverfahrensrecht[75] 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 Teilprivatisierung[76] 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 Herausgabeanordnung, 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*, 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) 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 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.[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 Unterrichtung[91]), 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*, ZfIStw 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. EJPD/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,* ZfIStw 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 polnischem Staatsbürger in Polen vorgenommene Abtreibung handelt, die dort zwar strafbar, aber hier straflos wäre.[92] Damit wird faktisch der (ohnehin 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 sind[95] 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 genommen 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 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 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 leiten[104] 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-Kenntnis-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 EJPD/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-Formular[114]).[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" Unterrichtungsverfahren[119] 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*, NJECL2024, 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 freeze[130] derzeit an einer Rechtsgrundlage fehlt. Weither 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 Verfahrensverstoßes 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) („somehow 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. Löschungsverpflichtung 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 Sitzstaatprinzip). 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 Marktortprinzip[147] 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, ZfIStW 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*, RDi 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, ZfIStW 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*, RDi 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 sind[149] – 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, ZfIStW 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*, ZfIStw 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 entgegentreten zu können").