Das neue E-Evidence-Gesetzespaket – Eine kritische Analyse

Von Wiss. Mitarbeiter **Laurin Krumwiede**, Mannheim*

Im August 2023 ist das EU-Gesetzespaket zur sog. E-Evidence, bestehend aus der Verordnung (EU) 2023/1543 und der flankierenden Richtlinie (EU) 2023/1544 in Kraft getreten. Erleichtert werden soll damit der grenzüberschreitende Zugang zu elektronischen Beweismitteln, die zur Ermittlung und Verfolgung von Straftaten verwendet werden. Einer mitgliedstaatlichen Justizbehörde wird zukünftig möglich sein, gegenüber einer benannten Niederlassung oder einem Vertreter eines Diensteanbieters in einem anderen Mitgliedstaat direkt die Herausgabe oder Sicherstellung von elektronischen Beweismitteln anzuordnen. Der Speicherort der Daten spielt keine Rolle. Damit ist ein Wandel von einem bilateralen Datenzugangsmodell zu einer „unilateral-transnationalen" Beweiserhebung verbunden. Dies gibt Anlass dazu, die bisherige Zugriffspraxis in Erinnerung zu rufen, das neue Gesetzespaket zu analysieren und einer kritischen Würdigung im Hinblick auf den Grundrechts- und Rechtsschutz zuzuführen. Abschließend wird das neue Gesetzespaket in seiner internationalen Dimension beleuchtet.

I. Hintergrund

Elektronische Beweismittel sind in Strafverfahren von hoher Relevanz. Täter hinterlassen bei fast allen Arten von Straftaten und insbesondere im Bereich der Cyberkriminalität[1] digitale Spuren, die bei der Identifizierung bzw. Überführung helfen können.[2] Aus einer im Jahr 2017 vonseiten der Europäischen Kommission durchgeführten Umfrage unter den Mitgliedstaaten ging dementsprechend hervor, dass elektronische Beweismittel in etwa 85 % der Strafverfahren von Bedeutung sind.[3] Häufig befinden sich die Beweisdaten jedoch nicht innerhalb des jeweils ermittelnden EU-Mitgliedstaates, da die Datenspeicherung heutzutage global und grenzenlos erfolgt.[4] So befinden sich in schätzungsweise 65 % der Fälle die Diensteanbieter, an die die Ersuchen gerichtet werden, in einem anderen Land.[5]

Mit dem Zugriff auf Daten, die sich auf einem Server im Ausland befinden, ist ein Eingriff in die territorialen Souveränitätsrechte des anderen Staates verbunden.[6] Für den transnationalen Datenzugriff ist deshalb grundsätzlich ein Rechtshilfeverfahren anzustrengen, sofern es sich nicht um offen zugängliche Daten im Ausland i.S.v. Art. 32 lit. a der Cybercrime-Konvention[7] handelt und der Betroffene auch keine Zustimmung nach Art. 32 lit. b der Konvention erteilt hat.[8] Das traditionelle zwischenstaatliche Rechtshilfeersuchen nach §§ 59 ff. IRG sieht für den Fall der Bewilligung die Möglichkeit vor, dass der ersuchte Staat die gewünschte Eingriffsmaßnahme ausführt. In Art. 25 ff. der Cybercrime-Konvention sind darüber hinaus Bestimmungen zur Erleichterung und Beschleunigung des Rechtshilfeverkehrs enthalten. Die Datenbeschaffung über diesen förmlichen Weg gestaltete sich allerdings als zeitaufwendig und umständlich.[9] Bis über das Rechtshilfeersuchen entschieden wurde, vergingen regelmäßig sechs bis 24 Monate.[10] Sowohl das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der EU[11] als auch die Europäische Ermittlungsanordnung[12] (vgl. §§ 91a ff. IRG) vermochten nach Bewertung der Kommission der Verfahrensverzögerung nur wenig entgegenzusetzen.[13]

Die Mitgliedstaaten bzw. Strafjustizbehörden suchten daher nach alternativen Wegen für den grenzüberschreitenden

* Der *Verf.* ist Doktorand und Wiss. Mitarbeiter am Lehrstuhl für Deutsches, Europäisches und Internationales Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht der Universität Mannheim bei Prof. *Dr. Laura Neumann*.

[1] Zu den verschiedenen Definitionsansätzen von Cyberkriminalität Cyberkriminalität *Sieber/Tropina/von zur Mühlen/Boran/Wright/Broadhurst/Krüger*, Comprehensive Study on Cybercrime, 2013 abrufbar unter https://cli.re/XeD5rj (17.5.2024).

[2] *Rojszczak*, Modern Law Review 85 (2022), 997 (998).

[3] Europäische Kommission, Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD (2018) 119 endg., S. 14.

[4] *Siry*, New Journal of European Criminal Law 10 (2019), 227 (228 f.).

[5] Europäische Kommission (Fn. 3), S. 14, 258.

[6] *Sankol*, K&R 2008, 279 (281).

[7] Übereinkommen des Europarats über Computerkriminalität v. 23.11.2001, BGBl. II 2008, S. 1242.

[8] *Gössling/Nagel*, IT-Rechtsberater 2019, 41.

[9] Vgl. Europäische Kommission, FAQ: New EU rules to obtain electronic evidence, abrufbar unter http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm (17.5.2024).

[10] Cybercrime Convention Committee, T-CY assessment report, The mutual legal assistance provisions of the Budapest Convention on Cybercrime, adopted by the T-CY at its 12th Plenary (2–3 December 2014), S. 123, abrufbar unter https://rm.coe.int/16802e726c (17.5.2024).

[11] Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. EU 2000 Nr. C 197, S. 3.

[12] Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. EU 2014 Nr. L 130/1.

[13] Europäische Kommission (Fn. 3), S. 22 f.; Europäische Kommission, Non-paper, Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, Rats-Dok. 15072/16, S. 10–12; kritisch hierzu *Böse*, An assessment of the Commission's proposals on electronic evidence, European Parliament 2018; *Maymir*, Internet Policy Review 9 (2020), 1, abrufbar unter policyreview-2020-3-1495.pdf (17.5.2024).

Zugang zu digitalen Beweismitteln. Zum einen wurden die im innerstaatlichen Recht normierten Befugnisse ausgeweitet.[14] Im „Yahoo"-Fall befand das Kassationsgericht Belgiens beispielsweise, dass die Herausgabeanordnung aufgrund der Pflicht zur Beschaffung der angeforderten Daten inländischen Charakter hat, da die Mitwirkung des adressierten Diensteanbieters im Inland stattfindet.[15] In Deutschland wurde für die Eingriffsmaßnahme der Onlinesichtung nach § 110 Abs. 3 StPO von der Beteiligung des anderen Staates im Rechtshilfeverfahren abgesehen, solange wenigstens auch möglich erschien, dass die Daten im Inland ihren Speicherort haben.[16] Nach dem Urteil des LG Koblenz aus dem Jahr 2021 sollte für den Verzicht sogar schon ausreichen, dass Unkenntnis darüber besteht, in welchem konkreten ausländischen Staat sich der Datenspeicherort befindet.[17] Zum anderen war die Datenzugangspraxis zu einem beträchtlichen Teil (etwa 58 % aller Datenanfragen) von einer direkten grenzüberschreitenden Zusammenarbeit mit den Diensteanbietern auf freiwilliger Basis geprägt.[18] Verglichen mit förmlichen Rechtshilfeersuchen erwies sich diese Vorgehensweise im Erfolgsfall häufig als schneller und effizienter.[19]

Die nationalen Vorstöße waren inhaltlich jedoch wenig aufeinander abgestimmt.[20] Aufgrund der divergierenden Handhabung herrschte eine Rechtsfragmentierung und damit Rechtsunsicherheit für die beteiligten Akteure.[21] In den Fällen des freiwilligkeitsbasierten Datenzugangs hingen die Ermittlungen ferner von der Kooperationsbereitschaft der Diensteanbieter ab. Viele Diensteanbieter stellten ihre eigenen Regeln und Anforderungen für eine Datenübermittlung auf und einige verweigerten die freiwillige Herausgabe grundsätzlich bzw. sahen sich hierzu nicht in der Lage, weil sie sich widersprechenden Vorschriften des ausländischen Staates, in dem sich ihr Sitz oder der Datenspeicherort befindet, verpflichtet sahen.[22] Somit lag die durchschnittliche Erfolgsquote für die direkten Datenanfragen der mitliedstaatlichen Justizbehörden bei den großen Diensteanbietern wie bspw. Facebook (Meta Platforms), Google, Apple oder Microsoft nach dem SIRIUS-Bericht[23] von Europol aus dem Jahre 2019 bei lediglich 66 %. Nach Schätzung der Europäischen Kommission wurden die angefragten Daten sogar lediglich in weniger als der Hälfte der Fälle übermittelt.[24] Zu Recht wurden rechtsstaatliche Bedenken geäußert.[25] Denn der Souveränitätsgrundsatz, die Bestimmungen zur strafrechtlichen Zusammenarbeit und auch die Beschuldigtenrechte wurden ausgehebelt.[26]

Angesichts dessen hoben sowohl die Europäische Kommission im Jahre 2015 in der Europäischen Sicherungsagenda[27] und der Europäische Rat in seinen Schlussfolgerungen[28] im Jahr 2016 das Bedürfnis nach einem EU-weit einheitlichen Rechtsrahmen zur grenzüberschreitenden Sicherung und Übertragung von elektronischen Beweismitteln hervor. Im Anschluss an die Non-paper der Kommissionsdienste[29] und einem Technical Document[30] brachte die Europäische Kommission 2018 den Gesetzesvorschlag bestehend aus einer Verordnung[31] und einer Richtlinie[32] hervor, der reichlich

[14] *Böse*, KriPoZ 2019, 140 (141).
[15] Cour de Cassation, Urt. v. 1.12.2015 – P.13.2082.N (Yahoo).
[16] Beschluss des Bundesrates vom 6.7.2018, BR-Drs. 215/18 (B), S. 13; *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, Kommentar, 67. Aufl. 2024, § 110 Rn. 7b.
[17] LG Koblenz, Beschl. v. 24.8.2021 – 4 Qs 59/21; Bezugnahme auf *Hegmann*, in: Graf (Hrsg.), Beck'scher Online Kommentar StPO, Stand: 1.4.2024, § 110 Rn. 16.
[18] Europol, SIRIUS EU, Electronic Evidence Situation Report 2023, S. 24, abrufbar unter https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS%20EUEESR%202023.pdf (17.5.2024).
[19] Europol, SIRIUS EU Digital Evidence Situation Report 2019, S. 11–13, abrufbar unter https://www.europol.europa.eu/publications-documents/sirius-eu-digital-evidence-situation-report-2019 (17.5.2024).
[20] *Bell*, Strafverfolgung und die Cloud – Strafprozessuale Ermächtigungsgrundlagen und deren völkerrechtliche Grenzen, 2019, S. 173; *Gössling/Nagel*, IT-Rechtsberater 2019, 41 (42).
[21] Europäische Kommission (Fn. 13 – Non-paper), S. 13.
[22] Europol (Fn. 18), S. 24.
[23] Europol (Fn. 19), S. 13.
[24] Europäische Kommission (Fn. 3), S. 15.
[25] Vgl. *Burchard*, ZRP 2019, 164.
[26] *Currie*, Canadian Yearbook of International Law, 54 (2016), 63.
[27] Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und Den Ausschuss der Regionen, Die Europäische Sicherheitsagenda, KOM (2015) 185 endg., S. 24 f.
[28] Europäischer Rat, Schlussfolgerungen vom 9. Juni 2016, Ratsdok. 10007/16.
[29] Europäische Kommission (Fn. 13 – Non-paper); Europäische Kommission, Non paper from the Commission Services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward v. 8.6.2017, abrufbar unter https://home-affairs.ec.europa.eu/system/files/2017-05/20170522_non-paper_electronic_evidence_en.pdf (17.5.2024).
[30] Technical Document from the Commission Services: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace v. 22.5.2017, abrufbar unter https://home-affairs.ec.europa.eu/system/files/2020-09/20170522_technical_document_electronic_evidence_en.pdf (17.5.2024).
[31] Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, KOM (2018) 225 endg.

kritisiert wurde.[33] Im Gegensatz zum Rat, der bereits im Dezember 2018 eine allgemeine Ausrichtung annahm,[34] ließ das Europäische Parlament mit seiner Verständigung auf eine Verhandlungsposition bis Ende 2020 auf sich warten.[35] Die anschließenden Trilog-Verhandlungen mündeten schließlich in dem Kompromisstext vom 20.1.2023.[36] Der europäische Gesetzgeber verabschiedete das E-Evidence-Gesetzespaket am 12.7.2023 und am 28.7.2023 wurde es im Amtsblatt der EU veröffentlicht.[37]

II. Das neue E-Evidence-Gesetzespaket

Das Gesetzespaket besteht aus der unmittelbar anwendbaren[38] Verordnung (EU) 2023/1543[39] und der Richtlinie (EU) 2023/1544[40]. Die in Kraft getretene Verordnung, in welcher die maßgeblichen Eingriffsbefugnisse geregelt sind, ist in ihrer Anwendbarkeit nach Art. 34 Abs. 2 der Verordnung (VO) zeitlich aufgeschoben, sodass sie erst ab dem 18. August 2026 gilt.[41] Gestützt wird sie „insbesondere" auf die Rechtsgrundlage des Art. 82 Abs. 1 AEUV.[42] Danach können im Rahmen der justiziellen Zusammenarbeit in Strafsachen Maßnahmen zur gegenseitigen Anerkennung von Urteilen und gerichtlichen Entscheidungen in der Europäischen Union erlassen werden. Die in der Verordnung enthaltenen Eingriffsbefugnisse stehen dementsprechend nur für Strafverfahren und die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung mit einer Mindestdauer von vier Monaten, deren Anordnung aufgrund eines Strafverfahrens durch ein Urteil erfolgte, zur Verfügung (Art. 2 Abs. 2 VO). Sie dienen rein repressiven Zwecken.[43] Demgegenüber findet die Richtlinie ihre primärvertragliche Stütze in Art. 53 i.V.m. 62 AEUV und ist nicht auf die justizielle Zusammenarbeit beschränkt. Existierende Regelungen und Verfahren, wie insbesondere die Europäische Ermittlungsanordnung oder die Rechtshilfe, werden durch das E-Evidence-Gesetzgesetzespaket nicht ersetzt, sondern ergänzt.[44] Bevor näher auf die in der Verordnung enthaltenen Instrumente (2.), die Vollstreckung und Sanktionen (3.) und den Rechtsschutz (4.) eingegangen wird, soll zunächst die Zielsetzung und der Anwendungsbereich des neuen Gesetzespaketes umrissen werden (1.).

1. Ziel und Anwendungsbereich des E-Evidence-Gesetzespaketes

Die grenzüberschreitende Sicherung oder Herausgabe elektronischer Beweismittel soll künftig durch den EU-weit harmonisierten E-Evidence-Rechtsrahmen ermöglicht und beschleunigt werden. Wo sich der Datenspeicher- bzw. Serverstandort befindet, ist dabei irrelevant (Art. 1 Abs. 1 VO). Die Verordnung steht somit in einer Linie mit den national sowie international sich abzeichnenden Tendenzen, die ein vom Speicherort unabhängiges unilateral-transnationales Datenzugangsmodell präferieren.[45] Gemäß Art. 2 Abs. 1 VO kommt es allein darauf an, dass der Diensteanbieter innerhalb der Union Dienstleistungen anbietet (sog. Marktortprinzip).[46] Dann hat er nämlich innerhalb der EU-Mitgliedstaaten eine Niederlassung oder für den Fall, dass die Niederlassung in einem Drittstaat liegt, einen gesetzlichen Vertreter zu benennen. An diesen sog. Adressaten kann die Justizbehörde eines Mitgliedstaates grenzüberschreitend direkt eine Anordnung zur Sicherung oder Herausgabe elektronischer Beweismittel richten.

---

[32] Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, KOM (2018) 226 endg.

[33] Vgl. *Deutscher Richterbund*, Stellungnahme Nr. 16/19, abrufbar unter https://www.drb.de/positionen/stellungnahmen/stellungnahme/news/16-19 (19.5.2024);
BRAK, Stellungnahme 28/2018, abrufbar unter https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2018/september/stellungnahme-der-brak-2018-28.pdf (19.5.2024);
DAV, Stellungnahme 42/2018, abrufbar unter file:///C:/Users/irina/Downloads/dav-sn_42-2018_e-evidence.pdf (19.5.2024);
EDRi, Recommendations on cross-border access to data. Position Paper v. 25.4.2018; *EuroISPA*, E-Evidence Position Paper 1806 v. 6.2018.

[34] Ratsdok. 15292/18 v. 12.12.2018.

[35] EP-LIBE, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, A9-0256/2020, PE642.987v02-00 v. 11.12.2020 (Bericht *Sippel*).

[36] Rat der Europäischen Union, Pressemitteilung v. 25.1.2023, abrufbar unter https://www.consilium.europa.eu/de/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/ (18.5.2024).

[37] ABl. EU 2023 Nr. L 191, S. 118–180, 181–190.

[38] *Weiß/Brinkel*, RDi 2023, 522 (524 f.), zum Verhältnis zum nationalen Recht.

[39] Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, ABl. EU 2023 Nr. L 191, S. 118–180.

[40] Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 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. 181–190.

[41] Vgl. *Kibler/Sandhu*, NVwZ 2018, 528 (530), zur Terminologie der Anwendbarkeit.

[42] Kritisch hierzu *Esser*, StraFo 2019, 403 (406).

[43] 24. Erwägungsgrund der VO.

[44] Vgl. Europäische Kommission (Fn. 31), S. 2.

[45] *Burchard*, ZIS 2018, 190 (202).

[46] *Nadeborn*, StraFo 2022, 144 (146).

Elektronische Beweismittel im Sinne der Verordnung sind dabei solche Daten, die von oder im Namen eines Diensteanbieters in elektronischer Form gespeichert werden und die zur Ermittlung und Verfolgung von Straftaten verwendet werden.[47] Anders als noch im Kommissionsentwurf[48] existieren nunmehr die Datenkategorien der Teilnehmerdaten (Art. 3 Nr. 9 VO), der Daten zur Identifizierung von Nutzern (Art. 3 Nr.10 VO), der nicht ausschließlich der Identifizierung dienenden Verkehrsdaten (Art. 3 Nr. 11 VO) sowie der Inhaltsdaten (Art. 3 Nr. 12 VO).[49] Zur Vereinfachung wird nachfolgend zweigliedrig unterschieden zwischen den sog. Teilnehmer- und Identifizierungsdaten und den sog. Verkehrs- und Inhaltsdaten. Zum Zeitpunkt der Anordnung müssen die Daten in elektronischer Form von dem Diensteanbieter oder in seinem Auftrag gespeichert worden sein. Überwachungsmaßnahmen sind damit nicht von der Verordnung gedeckt.[50] Hierin liegt ein wesentlicher Unterschied zur Europäischen Ermittlungsanordnung, da diese auch Ermittlungsmaßnahmen einschließlich des Einsatzes von Überwachungsmaßnahmen zulässt.

Die Verordnung zielt wohlgemerkt nicht darauf ab, die Übermittlung aller Arten von Daten zu erleichtern. Sie beschränkt sich in materieller Hinsicht auf Informationen im Besitz von Anbietern bestimmter digitaler Dienste nach Art. 3 Nr. 3 VO. Erstens sind Anbieter elektronischer Kommunikationsdienste gem. Art. 3 Nr. 3 lit. a VO erfasst. Elektronische Kommunikationsdienste sind in Art. 2 Nr. 4 der Richtlinie (EU) 2018/1972 bzw. in § 3 Nr. 61 TKG legaldefiniert.[51] Es handelt sich um meist entgeltlich über elektronische Kommunikationsnetze erbrachte Dienste, die in der Übertragung von Signalen über Telekommunikationsnetze bzw. Rundfunknetze bestehen.[52] Anstelle einer technischen Ausrichtung wird ein funktionaler Ansatz verfolgt, bei dem darauf abgestellt wird, ob die Kommunikation ermöglicht wird.[53] Schließlich sollen nicht nur die herkömmlichen Sprachtelefon-, Textmitteilungs- und E-Mail-Dienste, sondern ebenso die mittlerweile äquivalent genutzten Online-Dienste wie Internet-Telefonie (Voive-over-IP), Messengerdienste oder Web-gestützte E-Mail-Dienste umfasst sein.[54] Nicht unter Art. 3 Nr. 3 lit. a VO fallen der lineare Rundfunk, die Videoabrufdienste, Websites, Streamingdienste, Blogs und die Kommunikation mit Sprachassistenten oder Chatbots.[55] Zweitens befinden sich Anbieter von Diensten der Informationsgesellschaft nach Art. 3 Nr. 3 lit. c VO im Anwendungsbereich der Verordnung. Diese werden in Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 legaldefiniert. Vereinfacht gesagt sind solche Anbieter erfasst, die es den Nutzern im Fernabsatz und auf individuellen Abruf eines Empfängers ermöglichen, miteinander zu kommunizieren, oder ihnen Dienste anbieten, die für die Speicherung oder anderweitige Verarbeitung von Daten in ihrem Namen genutzt werden können.[56] Gemeint sind Online-Marktplätze oder auch andere Hosting-Dienste, einschließlich Cloud-Computing-Diensten, sowie Plattformen für Online-Spiele und Online-Glücksspiele.[57] Drittens werden Anbieter von Infrastrukturdiensten, sowie mit Domänennamen verbundene Datenschutz- und Proxy-Dienste in Art. 3 Nr. 3 lit. b VO genannt. Andere Kategorien von Diensteanbietern, etwa aus dem Gesundheitssektor oder der Datenverarbeitung, sind nicht erfasst.[58] Ausgenommen sind ebenso Anbieter der Finanzdienstleistungen i.S.d. Art. 2 Abs. 2 lit. b der Richtlinie 2006/123/EG.

Die Mitgliedstaaten haben nach Art. 3 Abs. 1 der Richtlinie (RL) sicherzustellen, dass die Diensteanbieter für die Entgegennahme, Einhaltung und Vollstreckung von Entscheidungen und Anordnungen sog. Adressaten festlegen. Die Diensteanbieter mit Rechtspersönlichkeit müssen in den Mitgliedstaaten eine niedergelassene Einrichtung schriftlich benennen (Art. 3 Abs. 1 lit. a RL i.V.m. Art. 2 Nr. 5 RL). Gibt es eine solche Niederlassung nicht, so stellen die Mitgliedstaaten sicher, dass ein rechtlicher Vertreter bestimmt wird (Art. 3 Abs. 1 lit. b RL i.V.m. Art. 2 Nr. 6 RL). Die schriftliche Kommunikation zwischen den Behörden und den Adressaten erfolgt über ein dezentrales IT-System, dessen Host die Europäische Kommission ist.[59] Die Mitgliedstaaten haben ferner den gesetzlichen Rahmen dafür zu schaffen, dass die Diensteanbieter ihre Adressaten mit den notwendigen Befugnissen und Ressourcen ausstatten, um den mitgliedstaatlichen Entscheidungen und Anordnungen nachzu-

[47] Zusammenfassung Dokument EUR-Lex 32023R1543, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R1543 (18.5.2024).
[48] Art. 2 Nr. 6 VO-E (Fn. 31).
[49] EP-LIEBE (Fn. 35), S. 27–28, Vorschlag zu Art. 2 Nr. 6–10 VO-E.
[50] EP-LIEBE (Fn. 35), S. 10.
[51] *Basar*, jurisPR-StrafR 14 (2023), Anm. 1.
[52] *Weber*, Rechtswörterbuch, Telekommunikationsdienste.
[53] 15. Erwägungsgrund der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation; *Schütz*, in: Geppert/Schütz (Hrsg.), Beck'scher Kommentar zum TKG, 5. Aufl. 2023, § 3 Rn. 142.
[54] Referentenentwurf des Bundesministeriums für Wirtschaft und Energie und des Bundesministeriums für Verkehr und digitale Infrastruktur Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts, § 3 Nr. 61, S. 276.
[55] *Tinnefeld/Buchner*, in: Wolff/Brink/Ungern-Sternberg (Hrsg.), Beck'scher Online-Kommentar zum Datenschutzrecht, Stand: 1.2.2024, Syst. I. Rn. 109; *Körber* in: Säcker/Körber (Hrsg.), TKG, TTDSG, Kommentar, 4. Aufl. 2023, TKG § 3 Rn. 33.
[56] 27. Erwägungsgrund der VO.
[57] 27. Erwägungsgrund der VO.
[58] 28. Erwägungsgrund der VO.
[59] *Bertuzzi*, Euractiv v. 30.11.2022, abrufbar unter https://www.euractiv.com/section/data-protection/news/eu-settles-rules-for-accessing-electronic-evidence-across-borders/ (19.5.2024).

kommen.[60] Die Richtlinie reagiert damit auf die mangelhafte Infrastruktur und Personallage der Diensteanbieter.[61] Wurde ein Adressat nicht benannt oder bestellt, dann kann auch eine andere Niederlassung oder ein anderer Vertreter des Diensteanbieters in der Union adressiert werden.[62] Art. 3 Abs. 5 RL sieht vor, dass die Adressaten und der Diensteanbieter gesamtschuldnerisch haftbar gemacht werden können, wenn sie ihrem Pflichtenprogramm nicht entsprechen.

2. Das Instrumentarium

Wie bereits im Verordnungsentwurf[63] der Kommission bilden die Herausgabeanordnung (sog. European Production Order – im Folgenden EPO) und die Sicherungsanordnung (sog. European Preservation Order – im Folgenden EPO-PR) zusammen das funktionelle Kernstück der Ermittlungsbefugnisse.[64] Dadurch können sich die zuständigen Justizbehörden und ausnahmsweise auch andere Strafverfolgungsbehörden in der EU grenzüberschreitend unmittelbar an die Adressaten wenden und diese mittels eines Zertifikats (EPOC/EPOC-PR) zur Herausgabe oder zur vorübergehenden Sicherung der elektronischen Beweismittel verpflichten. Während die EPO-PR ausschließlich der Datensicherung dient, um etwa einer Modifikation oder einem Verlust hinsichtlich späterer Maßnahmen vorzubeugen, umfasst die EPO nach gesetzgeberischer Intention die Pflicht des Adressaten zur Sicherung und Herausgabe der Daten.

Die grenzüberschreitende Sicherung und Übermittlung von Daten besteht prinzipiell aus zwei Hauptphasen, nämlich der Anordnungsphase durch die Anordnungsbehörde im sog. Anordnungsstaat und der Ausführungsphase im sog. Vollstreckungsstaat, in dem sich der verpflichtete Adressat befindet.[65] In Bezug auf die zweite Phase sieht die Verordnung grundsätzlich allein die direkte Verpflichtung des Adressaten vor. In bestimmten Fällen ist die Behörde des Vollstreckungsstaates, die sog. Vollstreckungsbehörde, durch die Anordnungsbehörde im Wege der Unterrichtung einzubeziehen. Die Einbindung erfolgt dergestalt, dass das EPOC zur selben Zeit dem Adressaten und der Vollstreckungsbehörde übermittelt wird. Zur Veranschaulichung soll im Folgenden in drei Anordnungskonstellationen unterschieden werden. Die erste Konstellation betrifft die Anordnungen, für die keine Unterrichtung der Vollstreckungsbehörde vorgesehen ist (a). In der zweiten Konstellation erfolgt im Regelfall eine Beteiligung der Vollstreckungsbehörde durch die Anordnungsbehörde im Wege der Unterrichtung (b). Schließlich wird die Konstellation der Anordnung in Notfällen aufgegriffen (c).

a) Konstellationen ohne Unterrichtung der Vollstreckungsbehörde

Für die EPO betreffend Teilnehmer- und Identifizierungsdaten und die EPO-PR bezüglich sämtlicher Datenkategorien trifft die Anordnungsbehörde gem. Art. 8 Abs. 1 VO keine Pflicht zur Unterrichtung der Vollstreckungsbehörde. Nach hiesiger Ansicht *darf* die Vollstreckungsbehörde aber durchaus unterrichtet werden. Dies ist mit dem Wortsinn von Art. 8 Abs. 1 VO vereinbar und lässt sich in gesetzessystematischer Hinsicht damit begründen, dass es der Vollstreckungsbehörde nach Maßgabe von Art. 10 Abs. 1 VO freigestellt ist, schlicht untätig zu bleiben.

aa) Anordnungsphase

Im Hinblick auf die EPO betreffend Teilnehmer- und Identifizierungsdaten ist die zuständige Anordnungsbehörde der Richter, das Gericht, der Ermittlungsrichter oder der Staatsanwalt, Art. 4 Abs. 1 lit. a VO.[66] Nach Art. 4 Abs. 1 lit. b, Abs. 4 VO kann auch eine andere im Anordnungsstaat zuständige Ermittlungsbehörde die Anordnung erlassen. Hierfür bedarf es aber einer ex-ante-Validierung durch eine der genannten Justizbehörden. Die Anordnungsbehörde hat für den Erlass die Anordnungsvoraussetzungen des Art. 5 VO zu beachten. Die Anordnung muss nach Art. 5 Abs. 2 VO notwendig und verhältnismäßig sein. Den Rechten des Betroffenen ist Rechnung zu tragen und in einem vergleichbaren innerstaatlichen Fall muss eine ähnliche Anordnungsmaßnahme unter denselben Voraussetzungen zur Verfügung stehen. Gemäß Art. 5 Abs. 3 VO kann die EPO für alle Straftaten und zur Vollstreckung von in Strafverfahren ergangenen mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung erlassen werden. Nach dem 46. Erwägungsgrund ist die Vollstreckungsbehörde zu konsultieren, wenn „Grund zur Annahme“ eines möglicherweise parallelen Strafverfahrens besteht.[67]

Mit Blick auf Art. 9 Abs. 2 UAbs. 1 VO hat das EPOC in formeller Hinsicht zwingend die in Abs. 5 lit. a–h VO genannten Angaben zu enthalten. Zu adressieren sind gem. Art. 7 Abs. 1 VO die benannte Niederlassung oder der bestellte Vertreter des betroffenen Diensteanbieters. Nach Art. 5 Abs. 6 S. 1 VO muss es sich dabei grundsätzlich um einen i.S.d. Art. 4 Nr. 7 der Datenschutz-Grundverordnung[68] ver-

[60] Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses 2018/C 367/17, ABl. EU 2018 Nr. C 367, S. 88–92, zur bisherigen Rechtsfragmentierung.
[61] *Basar*, jurisPR-StrafR 5 (2019), Anm. 1.
[62] 50. Erwägungsgrund der VO.
[63] Art. 2 Nr. 1 und Nr. 2, Art. 5 f. VO-E (Fn. 31).
[64] *Basar*, jurisPR-StrafR 5 (2019), Anm. 1.
[65] *Rojszczak*, Modern Law Review 85 (2022), 997 (1003).
[66] Zur Problematik der Unabhängigkeit deutscher Staatsanwaltschaften im Zusammenhang mit der E-Evidence-Verordnung *Wallenta*, Deutsche Staatsanwaltschaften zwischen Verfassungsrecht und europäischem Leitbild, 2021, S. 31, 33 f.
[67] Rahmenbeschluss 2009/948/JI des Rates v. 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren, ABl. EU 2009 Nr. L 328, S. 42.
[68] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

antwortlich zeichnenden Diensteanbieter handeln.[69] Das sind diejenigen, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Die EPO ist also nicht an den Auftragsverarbeiter, beispielsweise Anbieter von Infrastruktur oder bestimmten Cloud-Computing-Diensten (IaaS- und PaaS-Anbieter)[70], zu richten.[71] Das hat den Grund, dass diese mangels Kenntnis der inhaltlichen Bedeutung der von ihnen verarbeiteten Daten oder der Identität der betroffenen Person keine ernsthafte Prüfung der Anordnung durchführen könnten. Art. 5 Abs. 6 S. 2 VO sieht hierzu dennoch praxisrelevante Ausnahmen vor.[72]

Die Erlassvoraussetzungen der EPO-PR betreffend sämtlicher Datenkategorien entsprechen den vorstehenden inhaltlichen und formellen Anforderungen weitgehend. Die zuständigen Anordnungsbehörden folgen aus Art. 4 Abs. 3 lit. a, lit. b, Abs. 4 VO und die Erlassvoraussetzungen aus Art. 6 VO sind größtenteils deckungsgleich.

bb) Ausführungsphase

Im Falle der EPO zur Erlangung von Teilnehmer- und Identifizierungsdaten verlangt die Anordnungsbehörde die Daten direkt von dem Adressaten heraus, ohne die Vollstreckungsbehörde zu beteiligen. Nach Erhalt der EPOC wird der Adressat gem. Art. 10 Abs. 1 VO umgehend zur Sicherung der angeforderten Daten tätig und hat diese nach Art. 10 Abs. 3 VO innerhalb von zehn Tagen nach EPOC-Erhalt unmittelbar der Anordnungsbehörde oder der im EPOC angegebenen Strafverfolgungsbehörde zu übermitteln.

Der Adressat kann die Ausführung gegenüber der Anordnungsbehörde ablehnen, wenn die Anordnungsvoraussetzungen nicht erfüllt sind und die EPO dennoch erlassen wurde (arg. e contr. Art. 16 Abs. 4 VO). In Art. 10 Abs. 5–8 VO sind des Weiteren Prüf- und Informationspflichten der Adressaten statuiert. Nimmt er aufgrund der im EPOC enthaltenen Informationen einen Verstoß gegen geschützte Immunitäten und Vorrechte von Personengruppen oder besonders geschützte Beziehungen oder gegen die Presse- oder Medienfreiheit im Vollstreckungsstaat an, so hat er die Anordnungs- und Vollstreckungsbehörde in Kenntnis zu setzen, Art. 10 Abs. 5 UAbs. 1 VO. Die Anordnungsbehörde entscheidet dann von sich aus oder auf Ersuchen der Vollstreckungsbehörde über die Rücknahme, Anpassung oder Aufrechterhaltung der EPO, Art. 10 Abs. 5 UAbs. 2 VO. Geschützt sind zum Beispiel Diplomaten, Berufsgeheimnisträger oder Journalisten in Bezug auf Quellenschutz.[73] Im Unionsrecht gibt es keine einheitliche Definition dessen, was eine Immunität oder ein Vorrecht ist.[74] Die genaue Bestimmung bleibt dem nationalen Recht vorbehalten. In anderen Instrumenten zur gegenseitigen Anerkennung, wie der Europäischen Ermittlungsanordnung, wird hierauf eingegangen.[75] Der Adressat hat die Anordnungsbehörde ferner unverzüglich in Kenntnis zu setzten, wenn er die Anordnung wegen formaler Probleme nicht ausführen kann, weil die EPOC unvollständig bzw. offensichtlich fehlerhaft ist oder unzureichende Informationen enthält (Art. 10 Abs. 6 VO), die Ausführung faktisch unmöglich ist (Art. 10 Abs. 7 VO) oder die Daten aus anderen Gründen nicht bereitgestellt werden können (Art. 10 Abs. 8 VO).[76]

Nach Erhalt der EPOC-PR betreffend sämtlicher Datenkategorien hat der Adressat die angeforderten Daten unverzüglich zu sichern. In Art. 11 Abs. 4–7 VO sind wiederum Prüf- und Informationspflichten des Adressaten statuiert. Die gesicherten Daten können Gegenstand weiterer Maßnahmen, wie einer EPO oder auch einer Europäischen Ermittlungsanordnung oder anderer Ersuche nach Rechtshilfeabkommen sein. Gemäß Art. 11 Abs. 1 S. 1 VO endet die Sicherungspflicht jedoch nach 60 Tagen, sofern nicht ein Herausgabeersuch gestellt wurde. Wurde zwischenzeitlich ein Ersuchen um Herausgabe gestellt, so ist eine verlängerte Sicherung um weitere 30 Tage nach Art. 11 Abs. 1 S. 2 VO möglich. Bestätigt die Anordnungsbehörde während des Sicherungszeitraums, dass ein Ersuchen um Herausgabe der Daten gestellt wurde, so sichert der Adressat so lang wie erforderlich und ggf. bis zur Herausgabe. Die Anordnungsbehörde hat den Adressaten unverzüglich in Kenntnis zu setzen, sobald eine Sicherung nicht mehr erforderlich ist, Art. 11 Abs. 3 VO.

b) Konstellation mit Unterrichtung der Vollstreckungsbehörde

Für die EPO zur Erlangung von Verkehrs- und Inhaltsdaten ist im Regelfall eine Unterrichtung der Vollstreckungsbehörde durch die Anordnungsbehörde gem. Art. 8 Abs. 1 VO erforderlich, da diese in ihrer Eingriffsintensität qualifiziert ist.[77] Bereits an dieser Stelle sei darauf hingewiesen, dass zu der Unterrichtungspflicht eine gewichtige Ausnahmeregelung in Art. 8 Abs. 2 VO geschaffen wurde.

aa) Anordnungsphase

Als Anordnungsbehörde kommen bei der EPO bezüglich Verkehrs- und Inhaltsdaten gem. Art. 4 Abs. 2 lit. a VO nur noch ein Richter, ein Gericht oder ein Ermittlungsrichter in Betracht, nicht jedoch ein Staatsanwalt. Art. 4 Abs. 2 lit. b, Abs. 4 VO sehen allerdings vor, dass die im Anordnungsstaat

[69] Für Kritik an Art. 2 Abs. 3 VO-E siehe *European Data Protection Board*, Stellungnahme 23/2018 zu den Vorschlägen der Kommission über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (Artikel 70 Absatz 1 Buchstabe b), S. 10 f., abrufbar unter https://www.edpb.europa.eu/sites/default/files/files/file1/edpb-2018-09-26-eevidence_de.pdf (19.5.2024).

[70] Sog. Infrastructure as a Service und Platform as a Service.

[71] 42. Erwägungsgrund der VO zur Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter.

[72] Der Verantwortliche ist trotz angemessener Bemühungen der Anordnungsbehörde nicht zu ermitteln (lit. a) oder die Ermittlungen könnten gefährdet werden, wenn die Anordnung an den Verantwortlichen gerichtet würde (lit. b); kritisch hierzu *Weiß/Brinkel*, RDi 2023, 522 (527).

[73] *Basar*, jurisPR-StrafR 14 (2023), Anm. 1.

[74] Hierzu 47. Erwägungsgrund der VO.

[75] Art. 11 Abs. 1 lit. a und 20. Erwägungsgrund der Richtlinie 2014/41/EU.

[76] Hierzu 58. und 59. Erwägungsgrund der VO.

[77] Hierzu 51. Erwägungsgrund der VO.

zuständige Ermittlungsbehörde die Herausgabeanordnung unter der Bedingung einer ex-ante-Validierung erlassen kann. Neben den Herausgabevoraussetzungen aus Art. 5 Abs. 1 und 2 VO ist nach Art. 5 Abs. 4 VO erforderlich, dass die fragliche Tat mit mindestens drei Jahren Freiheitsstrafe im Höchstmaß bedroht wird oder es sich um eine harmonisierte Straftat i.S.v. Art. 5 Abs. 4 lit. b–d VO handelt. Damit sind geringfügige Straftaten wie beispielsweise die Beleidigung, Verleumdung oder die Veröffentlichung von die Privatsphäre verletzenden Inhalten in vielen Mitgliedstaaten nicht umfasst.[78] Das EPOC muss gem. Art. 9 Abs. 2 UAbs. 2 VO sämtliche in Art 5 Abs. 5 VO aufgeführten Angaben enthalten. Eine EPO zur Erlangung von Verkehrs- und Inhaltsdaten, die das Berufsgeheimnis betreffen und im Rahmen einer für die Geschäftstätigkeit bereitgestellten Infrastruktur gespeichert sind bzw. verarbeitet werden, ist außerdem nur zulässig, sofern der Berufsgeheimnisträger im Anordnungsstaat wohnhaft ist oder die Ermittlungen andernfalls gefährdet würden oder das Berufsgeheimnis im Einklang mit dem anwendbaren Recht aufgehoben wurde, Art. 5 Abs. 9 lit. a–c VO. Wenn „Grund zur Annahme" besteht, dass die Daten nach dem Recht des Vollstreckungsstaates durch Immunitäten, Vorrechte oder die Presse- und Meinungsfreiheit geschützt sind,[79] kann die Anordnungsbehörde nach Art. 5 Abs. 10 UAbs. 1 VO vor dem Erlass der EPO den Sachverhalt vor allem durch Konsultation der Vollstreckungsbehörden klären.[80] Liegt einer der Fälle vor, so untersagt Art. 5 Abs. 10 UAbs. 2 VO die Anordnung. Gleiches gilt, wenn die Anordnung dem ne bis in idem-Grundsatz zuwiderliefe.

bb) Ausführungsphase

Nach Erhalt eines EPOC hat der Adressat auch in hiesiger Konstellation umgehend die Sicherung der Daten vorzunehmen. Ist die Vollstreckungsbehörde aber zugleich gem. Art. 8 Abs. 1 VO zu unterrichten, so gilt abweichend zur ersten Konstellation nun Art. 10 Abs. 2 VO. Nur wenn die Vollstreckungsbehörde nicht innerhalb von zehn Tagen nach EPOC-Erhalt einen der in Art. 12 VO genannten Ablehnungsgründe geltend macht oder wenn sie bereits vor Ablauf der zehntägigen Frist der Anordnungsbehörde und dem Adressaten bestätigt, keinen Ablehnungsgrund geltend zu machen, muss der Adressat die angeforderten Daten nach Ablauf der zehntägigen Frist bzw. sobald wie möglich nach der Bestätigung unmittelbar der Anordnungsbehörde oder den im EPOC angegebenen Strafverfolgungsbehörden übermitteln. Die Unterrichtung der Vollstreckungsbehörde entfaltet insoweit aufschiebende Wirkung für die Herausgabepflicht des Adressaten (Art. 8 Abs. 4 VO).[81] Ist die Vollstreckungsbehörde gem. Art. 8 Abs. 2 VO nicht zu unterrichten, dann bleibt es bei den oben unter B. II. 1. b) dargelegten Ausführungspflichten.

Dem Adressaten werden die o.g. Prüf- und Informationspflichten nach Art. 10 Abs. 5–8 VO ebenso für die EPO betreffend Verkehrs- und Inhaltsdaten anheimgestellt. Der zusätzliche Unterrichtungsmechanismus in Art. 8 VO, zurückgehend auf einen Vorschlag des Rats,[82] soll der Wahrung der territorialen Souveränität des Vollstreckungsstaates dienen.[83] Damit verbunden ist der Schutz von Individualgrundrechten.[84] Auf Drängen einzelner Ratsmitglieder beinhaltet Art. 8 Abs. 2 VO mit seinem Wohnsitzkriterium jedoch eine weitreichende Ausnahme von der Unterrichtungspflicht.[85] Hat die Anordnungsbehörde zum Zeitpunkt des Erlasses der Anordnung hinreichende Gründe zu der Annahme, dass die Straftat im Anordnungsstaat begangen wurde, begangen wird oder wahrscheinlich begangen werden wird *und* die Person, deren Daten angefordert werden, im Anordnungsstaat ansässig ist, dann bedarf es keiner Unterrichtung der Vollstreckungsbehörde. In den verbleibenden Fällen, die eine Notifikation gebieten, geschieht die Unterrichtung der Vollstreckungsbehörde, indem die Anordnungsbehörde ihr gem. Art. 9 Abs. 1 und Abs. 2 VO das EPOC zur gleichen Zeit wie dem Adressaten übermittelt. Auf dieser Grundlage wird die notifizierte Vollstreckungsbehörde in die Lage versetzt, zu prüfen, ob und inwieweit sie die enumerativen Ablehnungsgründe des Art. 12 Abs. 1 lit. a–d VO geltend macht. Ablehnungsgründe sind der Schutz der angeforderten Daten durch Immunitäten oder Vorrechte bzw. die Presse- und Meinungsfreiheit, der Ausnahmefall einer offensichtlichen Verletzung eines in Art. 6 EUV und in der Charta verankerten Grundrechts, der Verstoß gegen den ne bis in idem-Grundsatz und das Prinzip der beiderseitigen Strafbarkeit.[86] Für den Fall, dass die notifizierte Behörde einen Ablehnungsgrund annimmt, hat sie sich nach Art. 12 Abs. 3 S. 1 VO in geeigneter Weise mit der Anordnungsbehörde in Verbindung zu setzen. Dann kann die Anordnungsbehörde die EPO anpassen oder zurückziehen. Andernfalls beschließt die Vollstreckungsbehörde, einen Versagungsgrund geltend zu machen, und setzt den Adressaten und die Anordnungsbehörde hiervon in Kenntnis, Art. 12 Abs. 3 S. 2. Gemäß 12 Abs. 2 VO hat der Adressat infolge der Geltendmachung die Ausführung der EPO zu beenden und darf die Daten nicht übermitteln. Die Anordnungsbehörde hat die Anordnung zu widerrufen.

c) Konstellationen der Notfallanordnungen

Gemäß Art. 4 Abs. 5 S. 1 VO dürfen in Notfällen i.S.v. Art. 3 Nr. 18 VO ausnahmsweise die Ermittlungsbehörden (Art. 4 Abs. 1 lit. b, Abs. 3 lit. b VO) ohne eine vorausgehende Validierung durch eine Justizbehörde eine EPO betreffend Teilnehmer- und Identifizierungsdaten oder eine EPO-PR erlassen, vorausgesetzt eine Validierung kann nicht rechtzeitig

[78] *Rojszczak*, Modern Law Review 85 (2022), 997 (1009).
[79] Vgl. oben B. II. 1. b); 47. Erwägungsgrund der VO.
[80] Vgl. Europäische Kommission (Fn. 31), S. 11, zum ausreichenden Schutz durch die Erlassjustizbehörde.
[81] Anders der Vorschlag des Rates, Ratsdok. 11314/21 v. 26.8.2021, S. 2.
[82] Ratsdok. 15020/18 v. 30.11.2018, S. 37 (Art. 7a).
[83] *Esser*, in: Sosnitza/Pache/Hilgendorf/Reinbacher/Schenke/Schuster/Schwarz/Suerbaum/Teichmann (Hrsg.), Digitalisierung im EU-Recht, 2022, S. 31 (57).
[84] *Böse*, KriPoZ 2019, 140 (144).
[85] Ratsdok. 10881/22 v. 30.06.2022, S. 127 f.
[86] EP-LIEBE (Fn. 35), S. 42–43 zur Erweiterung der Ablehnungsgründe.

eingeholt werden und sie dürften dies im vergleichbaren nationalen Fall auch.[87] Gemäß Art. 4 Abs. 5 S. 2 VO bedarf es einer Ex-post-Validierung. Art. 4 Abs. 5 S. 3 VO statuiert bei Nichtgewährung der nachträglichen Validierung die Pflicht zur Zurückziehung der Anordnung oder Löschung bzw. Verwendungsbeschränkung der mittlerweile erlangten Daten.

In Notfällen hat der Adressat gem. Art. 10 Abs. 4 VO die angeforderten Daten spätestens in der Zeit von acht Stunden herauszugeben.[88] Falls die benannte Niederlassung oder der Vertreter eines Diensteanbieters nicht innerhalb der Fristen auf ein EPOC oder ein EPOC-PR reagiert, so kann nach Art 7 Abs. 2 VO ein EPOC oder ein EPOC-PR ausnahmsweise an jede andere Niederlassung oder jeden anderen Vertreter des Diensteanbieters in der Union gerichtet werden. Wenn eine Unterrichtung gem. Art. 8 Abs. 1 VO erforderlich ist, so hat diese nach Art. 8 Abs. 4 VO in Notfällen ausnahmsweise keine aufschiebende Wirkung. Macht die Vollstreckungsbehörde innerhalb von 96 Stunden Ablehnungsgründe gegen die Verwendung der Daten geltend, hat die Anordnungsbehörde die Daten zu löschen oder deren Verwendung anderweitig zu beschränken bzw. die von der Vollstreckungsbehörde aufgestellten Voraussetzungen für die Verwendung zu erfüllen, Art. 10 Abs. 4 VO.

3. Vollstreckung und Sanktionen

Leistet der Adressat der Anordnung ohne Angabe von Gründen seiner Ausführungspflicht aus Art. 10 und Art. 11 VO nicht Folge, so ist eine Vollstreckung durch die Vollstreckungsbehörde möglich, Art. 16 Abs. 1 und Abs. 9 VO. Zunächst muss die Vollstreckungsbehörde die EPO oder EPO-PR unverzüglich und spätestens innerhalb von fünf Werktagen nach Erhalt anerkennen, es sei denn, sie nimmt einen Ablehnungsgrund gem. Art. 16 Abs. 4 und Abs. 5 VO an. In der anschließenden förmlichen Aufforderung ist der Adressat gem. Art. 16 Abs. 3 VO auf die ihm zustehenden Ablehnungsgründe nach Abs. 4 lit. a–f und Abs. 5 lit. a–e, den Fristlauf und die drohenden finanziellen Sanktionen für den Fall der Nichtbefolgung hinzuweisen. War auch die Aufforderung vergebens, verhängt die Vollstreckungsbehörde durch Beschluss finanzielle Sanktionen, Art. 16 Abs. 10 VO. Den Mitgliedstaaten obliegt es nach Art. 15 Abs. 1 VO Vorschriften zu den finanziellen Sanktionen zu erlassen. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein und können gem. Art. 15 Abs. 1 S. 3 VO bis zu 2 % des vom Diensteanbieter im vorangegangenen Geschäftsjahr weltweit erzielten Jahresumsatzes betragen. Diensteanbieter, die gutgläubig die Anordnung befolgen, sind nach Art. 15 Abs. 2 VO von der Haftung gegenüber den Nutzern oder Dritten ausgeschlossen.

4. Rechtsschutz

Der Verordnungsgeber hat anders als im Kommissionsvorschlag[89] in Art. 13 Abs. 1 VO die Pflicht für die Anordnungsbehörde statuiert, dass die Person, deren Daten angefordert werden, grundsätzlich unverzüglich über die Herausgabe der Daten zu informieren ist.[90] Nach Art. 13 Abs. 3 VO ist dabei auch auf die nach Art. 18 VO verfügbaren Rechtsbehelfe hinzuweisen. Die Anordnungsbehörde darf jedoch zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht behindert werden, oder zum Schutze der öffentlichen Sicherheit, der öffentlichen Ordnung und der Rechte und Freiheiten anderer die Erteilung der Informationen aufschieben oder unterlassen und gewährte Informationen einschränken, Art. 13 Abs. 2 VO.[91] Des Weiteren sollen die betroffenen Personen[92] nach Art. 18 Abs. 1 VO das Recht haben, wirksame Rechtsbehelfe gegen eine EPO[93] vor einem Gericht des Anordnungsstaates einzulegen, wobei Verdächtigen und Beschuldigten dies während des Strafverfahrens möglich sein muss. Wie schon im Verordnungsentwurf wird auf das nationale Recht bezüglich der weiteren inhaltlichen und formalen Ausgestaltung des Rechtsbehelfs verwiesen.[94] Gemäß Art. 18 Abs. 2 VO umfasst das Recht auf Einlegung eines Rechtsbehelfs die Möglichkeit, die Rechtmäßigkeit der Maßnahme, einschließlich ihrer Notwendigkeit und Verhältnismäßigkeit, anzufechten, wobei die Grundrechtsgarantien im Vollstreckungsstaat hiervon unberührt bleiben. Es gibt mithin keine Bestimmung, dass das Gericht des Anordnungsstaats die Grundrechtsgarantien des Vollstreckungsstaats in seiner Entscheidung als Prüfungsmaßstab zugrunde zu legen hat. Allerdings bleiben dem Betroffenen mögliche Rechtsbehelfe nach dem nationalen Recht, der Datenschutz-Grundverordnung und der JI-Richtlinie offen. Gemäß Art. 1 Abs 2 VO kann der Erlass einer EPO oder einer EPO-PR außerdem von einem Verdächtigen, Beschuldigten oder ihrem Verteidiger im Rahmen der Verteidigungsrechte nach dem nationalen Strafverfahrensrecht beantragt werden.

[87] Hierzu 37. Erwägungsgrund der VO.
[88] Vgl. Art. 9 Abs. 2 VO-E (Fn. 31).
[89] Art. 11 VO-E (Fn. 31); Kritisch hierzu EP-LIBE, *Sippel/Franz*, 6. Arbeitsdokument (A) v. 1.4.2019, S. 2 f., abrufbar unter www.europarl.europa.eu/doceo/document/LIBE-DT-637466_DE.pdf (19.5.2024).
[90] EP-LIEBE (Fn. 35), S. 44–45.
[91] Siehe Art. 13 Abs. 3 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie).
[92] Für Diensteanbieter ist kein ausdrücklicher Rechtsbehelf gegen eine Anordnung vorgesehen.
[93] Gegen Sicherungsanordnungen (EPO-PR) ist kein Rechtsbehelf vorgesehen.
[94] Art. 17 VO-E (Fn. 31).

Diensteanbietern räumt die Verordnung lediglich gegen die Sanktionsbeschlüsse Rechtsbehelfe ein, Art. 16 Abs. 10 S. 2 VO. Da sich der Speicherort der Daten in einem Drittstaat befinden kann, sind Diensteanbieter womöglich einander widersprechenden Rechtsverpflichtungen ausgesetzt. Konfligiert aus Sicht des Diensteanbieters die Befolgung einer Herausgabeanordnung mit dem Gesetz eines Drittstaates, sind die Anordnungs- und Vollstreckungsbehörde nach Art. 17 Abs. 1 VO zu informieren, wobei der Einwand gem. Art. 17 Abs. 2 VO begründet werden muss. Beabsichtigt die Anordnungsbehörde dennoch die EPO aufrechtzuerhalten, so hat sie eine gerichtliche Prüfung im Anordnungsstaat zu beantragen, Art. 17 Abs. 3 VO. Das Gericht hat nicht nur nach Art. 17 Abs. 4 und Abs. 5 VO festzustellen, ob eine Kollision mit anwendbarem Recht eines Drittstaates vorliegt, sondern auch anhand einer umfangreichen Abwägung nach Maßgabe der Kriterien in Art. 17 Abs. 6 VO über die Aufrechterhaltung zu entscheiden. Für die EPO-PR gilt dies nicht.

III. Defizite im Grundrechtsrechtsschutz

Das Prinzip der territorialen Souveränität dient über die mitgliedstaatlichen Belange hinaus vor allem der Wahrung und Sicherung grund- und datenschutzrechtlicher Standards der Bürger.[95] Der Staat ist nicht nur bei der eigenen Ausübung von Hoheitsgewalt dazu verpflichtet, die Grund- und Datenschutzrechte der Personen in seinem territorialen Gebiet zu achten und zu wahren, sondern hat insbesondere auch im Feld der transnationalen Zusammenarbeit in Strafsachen den Schutz der menschenrechtlichen und rechtsstaatlichen Mindeststandards sicherzustellen.[96] Das gebotene Mindestniveau des Grundrechtsschutzes muss dort, wo eine Beteiligung des Vollstreckungsstaates gar nicht stattfindet, kompensatorisch durch strenge Anordnungsvoraussetzungen für den Anordnungsstaat verbürgt sein.[97]

1. Konstellationen ohne Unterrichtung der Vollstreckungsbehörde

Für eine Vielzahl von Anordnungskonstellationen findet keine Beteiligung der Vollstreckungsbehörde durch eine Unterrichtung statt. Der Unterrichtungsmechanismus weist erhebliche Lücken auf und kompensierende Anordnungshürden sind zulasten des Grundrechtsschutzes nicht geschaffen worden.

Die vom Rat[98] eingebrachte Idee einer Beteiligung der Vollstreckungsbehörde, welche der Kommissionsvorschlag überhaupt nicht vorsah,[99] ist prinzipiell zu begrüßen. Allerdings schlug das Europäische Parlament im Rahmen der Trilog-Verhandlungen[100] mit guten Gründen vor, dass unabhängig von der Datenkategorie in allen Fällen einer EPO oder EPO-PR gleichzeitig eine Unterrichtung der Vollstreckungsbehörde erfolgen sollte.[101] Der nunmehr in Kraft getretene Art. 8 VO bleibt hinter dem Vorschlag des Parlaments zurück. Um effektiv dem drohenden Verlust von elektronischen Beweismitteln entgegenwirken zu können, mag die Nichtunterrichtung der Vollstreckungsbehörde im Falle einer EPO-PR noch gerechtfertigt erscheinen, um das gesetzgeberische Ziel eine unverzügliche Datensicherung zu verwirklichen.[102] Nach der Sicherungsanordnung besteht jedenfalls die Gefahr des Datenverlustes vorerst nicht mehr. Für eine Unterrichtung der Vollstreckungsbehörde wäre dann ausreichend Zeit. Angemessen erschiene deshalb ein Notifizierungsverfahren für die EPO hinsichtlich aller Datenkategorien. Schließlich bedürfen personenbezogene Daten, wozu auch Daten zur Identifizierung wie IP-Adressen gehören,[103] sowohl auf europäischer Ebene nach Art. 6 Abs. 1 EUV i.V.m. Art. 7 GRCh und Art. 8 GRCh, als auch national nach Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 2 GG eines besonderen Schutzes.[104] Zumindest eine Verwendungseinschränkung für Teilnehmer- und Identifizierungsdaten bei erhöhter Grundrechtsrelevanz, wie beispielsweise im Falle eines sich ergebenden Bewegungsprofils, wäre geboten.[105] Die Pflicht zur Unterrichtung des Mitgliedstaates, in dem der durch die Maßnahme Betroffene seinen Wohnsitz hat (sog. „Betroffenenstaat“)[106], fehlt gänzlich.

Diese Lücken im Unterrichtungsmechanismus werden nicht durch strenge Anordnungsvoraussetzungen ausgeglichen. So erscheint bereits problematisch, dass die Verordnung kein Rangverhältnis für die Herausgabe- und Sicherungsanordnung vorsieht. Den Anordnungsbehörden wird damit Raum gelassen, die Herausgabe womöglich vorschnell der Sicherstellungsanordnung vorzuziehen.[107] Denn die EPO betreffend Teilnehmer- und Identifizierungsdaten hat gegenüber der EPO-PR keine qualifizierten Anordnungsvoraussetzungen zu erfüllen, obwohl sie in ihrer Eingriffsqualität intensiver ist.[108] Der Eingriff des Staates in die Persönlichkeitsrechte muss jedoch auf das absolut Notwendige beschränkt sein.[109] Zudem lässt die Formulierung in Art. 5 Abs. 5 lit. e VO, wonach „erforderlichenfalls“ eine Zeitspanne für die Herausgabe der Daten anzugeben ist, eine ausreichende Bestimmung des Eingriffsumfangs missen. Für die EPO betreffend Teilnehmer- und Identifizierungsdaten ist nicht einmal

[95] *Burchard*, ZIS 2018, 249 (251).
[96] *Böse*, KriPoZ 2019, 140 (143).
[97] *Böse*, KriPoZ 2019, 140 (143).
[98] Ratsdok. 15020/18 v. 30.11.2018, S. 37 (Art. 7a).
[99] Art. 9 Abs. 5 UAbs. 2, Art. 13, 14 VO-E (Fn. 31).
[100] Vgl. hierzu Ratsdok. 11314/21 v. 26.8.2021, S. 3.
[101] EP-LIEBE (Fn. 35), S. 35; Der Unterrichtung sollte nur in den Fällen der EPO betreffend Verkehrs- und Inhaltsdaten aufschiebende Wirkung zukommen.
[102] Vgl. *BRAK* (Fn. 33), S. 3.
[103] EuGH (2. Kammer), Urt. v. 19.10.2016 – C-582/14 (Breyer/Deutschland).
[104] Siehe hierzu BVerfG, Urt. v. 2.3.2006 – 2 BvR 2099/04 = BVerfGE 115, 166.
[105] *Burchard*, ZRP 2019, 164 (166).
[106] *Berthélémy*, EDRi v. 7.2.2023, abrufbar unter https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/ (19.5.2024).
[107] *v. Galen*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, 2020, S. 127, 128 ff.
[108] *Basar*, jurisPR-StrafR 14 (2023), Anm. 1.
[109] *Rojszczak*, Modern Law Review 85 (2022), 997 (1001).

ein Richtervorbehalt in Art. 4 VO normiert, wenngleich es sich um eine heimliche Eingriffsmaßnahme handelt.[110]

Des Weiteren wäre eine unabhängig von der Datenkategorie festgeschriebene Prüfpflicht der Anordnungsbehörde hinsichtlich möglicherweise betroffener Immunitäten und Sonderrechte bzw. der Presse- und Meinungsfreiheit angebracht. Art. 5 Abs. 10 VO schreibt indes nur die Prüfung für die EPO bezüglich Verkehrs- und Inhaltsdaten vor. Diese Verkürzung des Grundrechtsschutzes lässt sich nicht damit rechtfertigen, dass die EPO betreffend Teilnehmer- und Identifizierungsdaten eine geringere Eingriffsintensität aufweise. Auch solche Daten sind nämlich dazu geeignet, Aufschluss über ein bestimmtes Nutzerverhalten und Gewohnheiten des Betroffenen zu geben.[111] Überhaupt besteht die Gefahr, dass das Instrumentarium der Verordnung gezielt zur Identifizierung beispielsweise von unliebsamen politischen Gegnern, Journalisten und ihren Quellen oder Whistleblowern missbräuchlich genutzt wird.[112] Immerhin geht aus dem EU-Untersuchungsbericht zur Spähsoftware „Pegasus" hervor, dass Mitgliedstaaten systematischen Missbrauch staatlicher Überwachungsbefugnisse in der Vergangenheit betrieben.[113]

In der Ausführungsphase vermögen die Prüf- und Informationspflichten des Adressaten nach Art. 10 Abs. 5–8 VO bzw. Art. 11 Abs. 4–7 VO die vorgenannten Defizite nicht auszugleichen. Denn die Adressaten bzw. die privaten Diensteanbieter erweisen sich strukturell als unzuverlässige Verteidiger der Grundrechte.[114] Unklar ist zum einen, nach welchen Kriterien der Adressat die Prüfung durchzuführen hat. Weder kennt der Adressat bzw. Diensteanbieter die materielle Bedeutung der Daten noch ist stets der Beruf des Betroffenen bekannt.[115] Art. 5 Abs. 5 VO i.V.m. Art. 9 Abs. 2 UAbs. 1 VO sehen noch dazu vor, dass die Angaben in der EPOC auf lit. a–h beschränkt werden. Auch droht den Diensteanbietern unter Umständen die Vollstreckung bzw. Sanktionierung im Falle der Nichtumsetzung der Anordnung, womit ihnen für die Wahrnehmung einer strengen Anordnungsüberprüfung wenig Anreize gesetzt werden.[116] Dies gilt zumal, weil die privaten Diensteanbieter nur über begrenzte Ressourcen für die Wahrnehmung der Anordnungsüberprüfung verfügen.

2. Konstellationen mit Unterrichtung der Vollstreckungsbehörde

Auch für Konstellationen, in denen grundsätzlich eine Beteiligung der Vollstreckungsbehörde nach Art. 8 Abs. 1 VO vorgesehen ist, zeichnet sich ein defizitärer Grundrechtsschutz ab. Das vom Rat durchgesetzte Wohnsitzkriterium[117] in Art. 8 Abs. 2 VO stellt eine weitreichende Ausnahme von dem Unterrichtungsgrundsatz dar und das Merkmal der Ansässigkeit im Anordnungsstaat in Art. 8 Abs. 2 lit. b VO lässt die notwendige tatbestandliche Schärfe missen. Der 53. Erwägungsgrund gibt zwar für die Beurteilung durch die Anordnungsbehörde verschiedene objektive Umstände an die Hand. Und in dieser Hinsicht ist das Merkmal der Registrierung im Anordnungsstaat auch ein geeigneter Anhaltspunkt für die Beurteilung der Ansässigkeit. Doch erscheinen vor allem solche Umstände problematisch, die anstelle der Registrierung ebenso auf den Wohnsitz hinweisen sollen. Exemplarisch zu nennen ist an dieser Stelle etwa die Absichtsbekundung „sich in diesem Mitgliedstaat niederzulassen" oder die „bestimmte Bindung" zu einem Staat bzw. „familiäre oder wirtschaftliche Bindungen". Ein Kurzurlaub bzw. ein Urlaubsaufenthalt ohne weitere Verbindung soll hingegen nicht ausreichen. Denkbar viele Fallgestaltungen lassen sich erwägen, in denen in Ermangelung eines hinreichenden Differenzierungsmaßstabs geradezu willkürlich sowohl für als auch gegen die Ansässigkeit argumentiert werden kann.

Problematisch ist weiterhin, dass zulasten des Grundrechtsschutzes keine aktive Prüf- und Validationspflicht des Vollstreckungsstaates besteht. Zwar sollen die Vollstreckungsbehörden das Recht haben, die Informationen in der Anordnung „auf der Grundlage einer obligatorischen und pflichtgemäßen Prüfung" zu bewerten und diese gegebenenfalls abzulehnen.[118] Im unmittelbar verbindlichen Gesetzestext fehlt in Art. 8 Abs. 1 VO und Art. 12 Abs. 1 VO indes eine aktive Pflicht der Vollstreckungsbehörde zur Prüfung oder Validation. Damit bleibt zulasten des Grundrechtsschutzes ungewiss, ob die Anordnung tatsächlich innerhalb der Ablehnungsfrist durch den Vollstreckungsstaat überprüft wird.[119] Die Zweifel werden dadurch verstärkt, dass immerhin neun Mitgliedstaaten aufgrund der verfahrensbedingten Mehrbelastung ihre Vorbehalte gegen das Notifizierungsverfahren zum Ausdruck gebracht haben.[120] Darunter befand sich auch Irland, in dem einige große US-Diensteanbieter wie Google, Meta Platforms oder X (Twitter) ihren Firmensitz haben.[121]

Zwar ist zu begrüßen, dass Art. 12 Abs. 1 lit. a VO als Ablehnungsgrund Immunitäten und Vorrechte sowie die

[110] *DAV* (Fn. 33), S. 9.
[111] *Basar*, in: Sosnitza/Pache/Hilgendorf/Reinbacher/Schenke/Schuster/Schwarz/Suerbaum/Teichmann (Fn. 83), S. 20.
[112] *Berthélémy* (Fn. 106).
[113] EP-LIBE, Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)), A9-0189/2023, PE738.492 v04-00 v. 22.5.2023 (Bericht *in 't Veld*).
[114] *Tosza*, New Journal of European Criminal Law 11 (2020), 161 (182).
[115] *Rojszczak*, Modern Law Review 85 (2022), 997 (1010).
[116] *DAV* (Fn. 33), S. 8.
[117] Näher hierzu oben II. 2. b) bb).
[118] 62. Erwägungsgrund der VO.
[119] *Niekrenz*, Datenschutz und Datensicherheit 2020, 535 (536).
[120] Ratsdok. 15020/18 v. 30.11.2018, S. 37 Fn. 34.
[121] Haufe v. 2.6.2020, abrufbar unter https://www.haufe.de/compliance/recht-politik/wird-irische-datenschutzbehoerde-gegen-facebook-co-aktiv_230132_517448.html (19.5.2024).

Freiheit der Presse und das Recht auf freie Meinungsäußerung aufgreift, was im Wesentlichen auf die Bemühungen des Europäischen Parlaments zurückgeht.[122] Mit Skepsis wird demgegenüber die in Art. 12 Abs. 1 lit. b VO restriktive Formulierung für die Ablehnungsgründe betrachtet. Die Verordnung spricht hier von „Ausnahmefällen", in denen eine „offensichtliche Verletzung eines einschlägigen in Artikel 6 EUV und der Charta verankerten Grundrechts" angenommen werden muss, was eine besonders zurückhaltende Prüfung aufseiten des Vollstreckungsstaates bedingen kann. Das in Art. 12 Abs. 1 lit. d VO verankerte Prinzip der beiderseitigen Strafbarkeit erfährt zudem im Katalog der Anlage IV eine umfassende Einschränkung. Ohne das Erfordernis einer Strafbarkeit im Vollstreckungsstaat ist jedoch zu befürchten, dass Anordnungen mit politischer Färbung Erfolg haben könnten.[123]

Die aufgezeigten Schwächen im Unterrichtungsmechanismus werden auch insoweit nicht durch strenge Anforderungen auf der Anordnungsebene ausgeglichen. Insbesondere stellt sich hinsichtlich Art. 5 Abs. 10 VO die Frage, wie die Anordnungsbehörde überhaupt Kenntnis von betroffenen Immunitäten, Vorrechten oder Presse- und Meinungsfreiheiten nach dem Recht des Vollstreckungsstaates erlangen soll. Eine präventive Pflicht zur Ermittlung entsprechender Umstände wurde nicht statuiert. Zudem nimmt Art. 5 Abs. 10 VO unmissverständlich keinen Bezug auf Betroffenenstaaten, in dem die Betroffenen ihren Wohnsitz haben bzw. aus denen sie ihre Immunitäten oder Sonderrechte herleiten können.[124]

3. Weitere Grundrechtsschutzdefizite für alle Anordnungskonstellationen

Freilich stellt die Verordnung mit der EPO und EPO-PR Eingriffsinstrumente bereit, die durch die unmittelbare Bindungswirkung gegenüber den Diensteanbietern geeignet sind, das Ermittlungsverfahren zeitlich zu konzentrieren und dem Ziel einer effektiven Strafverfolgung Rechnung zu tragen.[125] Kritisch zu sehen ist gleichwohl, dass der Grundrechtsschutz nicht in gleichem Maße gestärkt wurde. Besonders problematisch erscheint, dass die Verordnung keine Beweisverwertungsverbote vorsieht. Doch ohne strikte Beweisverwertungsverbote, wie vom Europäischen Parlament gefordert,[126] bieten die Beschränkungen in der Verordnung keinen ausreichenden grundrechtlichen Schutz.[127] Insbesondere für bestehende Aussage- und Zeugnisverweigerungsrechte und Daten schutzbedürftiger Personengruppen wird kein effektiver Grundrechtsschutz gewährleistet.[128] Das Fehlen von Beweisverwertungsverboten für das gerichtliche Verfahren im Hinblick auf rechtswidrig übermittelte Daten konfligiert zudem mit dem Schutzprinzip des europäischen Datenschutzrechts nach Art. 5 Abs. 1 lit. a, Art. 17 Abs. 1 lit. d DSGVO und Art. 4 Abs. 1 lit. a RL (EU) 2016/680.[129] Ohne Beweisverwertungsverbote lässt die Verordnung ein Schlupfloch für die missbräuchliche Anwendung offen. Aufzugreifen ist beispielsweise Art. 168a im polnischen Änderungsgesetz zur Strafprozessordnung, den die PiS-Partei am 11.2.2016 einführte.[130] Rechtswidrig erlangte Beweismittel können danach vor Gericht eingebracht werden. Urteile des Obersten Gerichtshofs Polens, wonach Art. 168a sogar in Teilen als unvereinbar mit der polnischen Verfassung eingestuft wurde, vermochten nicht zur Änderung oder Aufhebung dieses Artikels verhelfen.[131]

Auch Regelungen zur weiteren Verwendung, Zweckbindung oder Weitergabe der Daten durch die Anordnungsbehörde existieren trotz der Vorschläge vonseiten des Rats und des Europäischen Parlaments nicht.[132] Obwohl die Zweckbindung der Verarbeitung ein wichtiger Grundsatz des EU-Datenschutzrechts ist, der sich unmittelbar aus Art. 5 Abs. 1 lit. b DSGVO ergibt,[133] bleibt es damit bei den Bestimmungen der Richtlinie (EU) 2016/680, die in Bezug auf die Bedingungen, die für die Übermittlung zwischen den Mitgliedstaaten festgelegt werden können, recht begrenzt sind.

Der ursprüngliche Entwurf sah kein Anordnungsverbot im Zusammenhang mit dem ne bis in idem-Grundsatz (Art. 50 GRCh und Art. 54 SDÜ) vor, was eine Nachbesserung erforderlich machte.[134] Zumindest im 46. Erwägungsgrund wird das Doppelbestrafungsverbot nunmehr aufgegriffen, wobei sich indes die Frage stellt, wie die Anordnungsbehörde von den entscheidenden Umständen erfahren soll. Denn der Anordnungsbehörde wird keine grundsätzlich vorgeschaltete Pflicht zur Ermittlung entsprechender Umstände anheimgestellt.[135] Hat die Strafverfolgungsbehörde im Zuge der Ermittlungen Scheuklappen auf, so könnte sie tatsächlich ermittelbare Annahmegründe im Sinne des 46. Erwägungsgrundes versehentlich ausblenden.

[122] EP-LIEBE (Fn. 35), S. 42 f.
[123] *Basar*, jurisPR-StrafR 14 (2023), Anm. 1.
[124] *Berthélémy* (Fn. 106).
[125] *Nemeth/Müller/Feiler*, derstandard v. 5.6.2023, abrufbar unter https://www.derstandard.de/story/3000000172389/missbrauchspotenzial-in-neuer-eu-verordnung-zu-digitalen-beweismitteln (19.5.2024).
[126] EP-LIBE (Fn. 35), S. 45 f.
[127] *Esser* (Fn. 83), S. 53.
[128] *Thomae*, in: Hoven/Kudlich (Fn. 107), S. 139 (143).
[129] *Basar*, jurisPR-StrafR 14 (2023), Anm. 1.
[130] Abrufbar unter https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000437/T/D20160437L.pdf (19.5.2024).
[131] Oberster Gerichtshof Polen, Urt. v. 26.6.2019 – IV KK 328/18, abrufbar unter http://www.sn.pl/orzecznictwo/SitePages/Baza_orzeczen.aspx?ItemSID=43030-57a0abe2-a73c-441d-9691-b79a0c36be5c&ListName=Orzeczenia3 (19.5.2024).
[132] Ratsdok. 10206/19 v. 11.6.2019, S. 40 f.; EP-LIBE (Fn. 35), S. 45 f.
[133] Vgl. EuGH, Gutachten 1/15 v. 26.7.2017, PNR-Abkommen EU-Kanada, 205.
[134] Vgl. Ratsdok. 10206/19 v. 11.6.2019, Erwägungsgrund 12a VO-E; *Esser* (Fn. 83), S. 53.
[135] *Esser*, StraFo 2019, 403 (411).

IV. Defizite im Rechtsschutzsystem

Zu begrüßen sind die Anstrengungen des Europäischen Parlaments[136] hinsichtlich der grundsätzlich unverzüglichen Information von Betroffenen, deren Daten auf der Grundlage einer EPO nach Art. 13 Abs. 1 VO angefordert werden.[137] Gleichwohl kann die Ausnahme in Art. 13 Abs. 2 VO („aufschieben, einschränken oder unterlassen") in Extremfällen zur Folge haben, dass sich der Betroffene nicht gerichtlich gegen die Anordnung zur Wehr setzen kann oder überhaupt von der Eingriffsmaßnahme erfährt. Das mag insbesondere dann der Fall sein, wenn im Rahmen des Ermittlungsverfahrens die Daten auf die EPO hin herausgegeben werden, es letztlich aber nicht zu einer Anklage kommt. Besonders kritisch wird es schließlich, wenn nicht einmal eine Beteiligung des Vollstreckungsstaates stattfand. Besser wäre gewesen, wenn sich der parlamentarische Vorschlag, dass die Ausnahmeanordnung auf Grundlage einer gerichtlichen Anordnung ergehen muss, durchgesetzt hätte.[138]

Da die Grundrechtsgarantien des Vollstreckungsstaates nicht Prüfungsmaßstab für den Rechtsbehelf vor dem Gericht des Anordnungsstaates sind (vgl. Art. 18 Abs. 2 Hs. 1 VO), bleibt im Hinblick auf die Rechtschutzmöglichkeiten des Betroffenen fraglich, ob oder wie sie ansonsten konkret Einzug finden.[139] Verglichen mit den Rechtsschutzmöglichkeiten gegen die Europäische Ermittlungsanordnung im Vollstreckungsstaat bzw. dem dortigen gerichtlichen Prüfungsmaßstab (vgl. § 91i IRG), könnte hierin eine strukturelle Absenkung des Rechtsschutzniveaus liegen. Zudem sind mit dem Rechtsschutz im Anordnungsstaat für Rechtsschutzsuchende aus anderen Mitgliedstaaten ggf. eine Sprachbarriere und eine finanzielle Belastung aufgrund der potentiell weiten Entfernung verbunden, was eine wirksame Verteidigung erschwert.[140] Außerdem sind die Vorgaben in Art. 18 Abs. 2–5 VO vage. Das Antragsrecht in Art. 1 Abs 2 VO nach Maßgabe des nationalen Strafverfahrensrechts erweist sich hierzulande nicht als ein „scharfes Schwert der Verteidigung", da es in der deutschen Strafprozessordnung kein starkes Antragsrecht gibt.[141] Für „Mitbetroffene"[142], deren Daten beiläufig mitübermittelt wurden, werden keine Rechtsbehelfe zur Verfügung gestellt.[143]

Ausweislich des Rechtsstaatlichkeitsberichts weisen eine Reihe von Mitgliedstaaten Rechtsstaatlichkeitsdefizite auf.[144] Exemplarisch befand der EGMR, dass bestimmte Urteile des polnischen Verfassungstribunals aufgrund von Mängeln im Verfahren zur Besetzung freier Richterstellen nicht als Ergebnis eines unabhängigen Gerichts angesehen werden können.[145] In die Verordnung schaffte es entgegen dem parlamentarischen Vorschlag[146] dennoch nur ein Verweis im 64. Erwägungsgrund auf Art. 7 EUV. Dieser wird zusätzlich dadurch entschärft, dass der Vollstreckungsstaat genau feststellen muss, ob „unter Berücksichtigung der persönlichen Situation der betreffenden Person, der Art der Straftat, die Gegenstand des Strafverfahrens ist, und des Sachverhalts, der der Anordnung zugrunde liegt, und angesichts der von der Anordnungsbehörde übermittelten Informationen wesentliche Gründe für die Annahme vorliegen, dass die Gefahr einer Verletzung des Rechts einer Person auf ein faires Verfahren besteht". Hinzu kommt, dass der 64. Erwägungsgrund nur auf die EPO bzgl. der Verkehrs- und Inhaltsdaten Bezug nimmt.

V. Internationale Dimension und Ausblick

Moderne Cloud-basierte Dienste nutzen weltweit parallele Datenspeicherorte. Zum Beispiel unterhält Google mehrere Datenzentren in den USA, der EU, Chile, Singapur, Taiwan und Japan.[147] Im Kommissionsentwurf zur Verordnung heißt es dementsprechend, das Internet kenne keine Grenzen und elektronische Beweismittel seien volatil.[148] Damit entschied sich der europäische Verordnungsgeber gegen das Konzept der Datenlokalisierung, bei dem die Daten im Staatsgebiet des Staates, in dem die Dienste angeboten werden, zu speichern sind. Einen solchen Lösungsweg verfolgen beispielsweise die Staaten China, Russland, Indien, Indonesien oder Vietnam.[149] Stattdessen wurde mit dem E-Evidence-Gesetzespaket ein unilaterales Datenzugangsmodell unabhängig vom tatsächlichen Speicherort, der häufig in Drittstaaten wie den USA liegt, gewählt.[150] Nach dem Verständnis des Verordnungsgebers wird die territoriale Souveränität bzw. Gebietshoheit der Drittstaaten, aus denen die Daten durch den Diensteanbieter beigebracht werden, aufgrund des territorialen Anknüpfungspunktes des Marktortprinzips nicht verletzt.

Einen ganz ähnlichen Ansatz verfolgen die USA mit ihrem bereits 2018 verabschiedeten Clarifying Lawful Overse-

[136] EP-LIEBE (Fn. 35), S. 44 f.
[137] Näher hierzu oben II. 4.
[138] EP-LIBE (Fn. 35), S. 45.
[139] *Berthélémy* (Fn. 106).
[140] *Beukelmann*, NJW-Spezial 2023, 568.
[141] *Beukelmann*, NJW-Spezial 2023, 568.
[142] *Esser*, StraFo 2019, 403 (409).
[143] Kritisch hierzu *Burchard*, ZRP 2019, 164 (166).
[144] Europäische Kommission, Rule Of Law Report 2023 Country Chapter Abstracts And Recommendations 2023, abrufbar unter https://commission.europa.eu/document/c74b48f1-3ce0-4909-a51f-7f41f5ca4ad1_en (19.5.2024).
[145] EGMR, Urt. v. 7.5.2021 – 4907/18 (Xero Flor/Polen).
[146] EP-LIEBE (Fn. 35), S. 39.
[147] Vgl. https://www.google.com/intl/de/about/datacenters/locations/ (19.5.2024).
[148] Europäische Kommission (Fn. 31), S. 1 f.
[149] *Marcén*, The push for the international regulation of cross-border access to electronic evidence and human rights, 2023, abrufbar unter https://www.researchgate.net/publication/369289242_The_push_for_the_international_regulation_of_cross-border_access_to_electronic_evidence_and_human_rights (19.5.2024).
[150] *Burwell/Propp*, Atlantic Council 2020, abrufbar unter https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf (19.5.2024).

as Use of Data (CLOUD) Act[151], der den bisherigen Stored Communications Act ergänzt. In dem Zusatz zu Titel 18 des United States Code wird geregelt, dass die Anbieter von elektronischen Kommunikationsdiensten oder Ferndienstleistungen zur Erhaltung, Sicherung oder Offenlegung des Inhalts einer drahtgebundenen oder elektronischen Nachricht sowie aller Aufzeichnungen oder anderer Informationen eines Kunden oder Abonnenten, die im Besitz oder unter Kontrolle des Anbieters sind, verpflichtet sind. Dadurch können US-Behörden die Internetanbieter zu einer Datenherausgabe verpflichten, auch wenn die Daten im Ausland gespeichert sind. Zudem lässt der CLOUD-Act die Möglichkeit bilateraler Abkommen mit anderen Staaten zu. Aktuell befinden sich die EU und die USA noch in den Verhandlungen,[152] wobei aus den Verhandlungsrichtlinien im Anhang zu der Empfehlung für einen Beschluss des Rates hervor geht, dass ein unilateral-transnationales Datenzugangsmodell entwickelt werden soll.[153] Das Ziel ist die direkte, transatlantische Zusammenarbeit zwischen den europäischen oder amerikanischen Justizbehörden mit den Diensteanbietern.[154]

Vorteilhaft an dem Abkommen wäre, dass widersprüchliche Verpflichtungen der Diensteanbieter, insbesondere in Bezug auf den Datenschutz und die Sicherheit informatorischer Systeme, vermieden werden können.[155] Derzeit ist nämlich für den Diensteanbieter mit der Herausgabe von in den USA gespeicherten Daten das Risiko verbunden, gegen die Kollisionsnormen des Stored Communications Acts zu verstoßen, wonach die Herausgabe von in den USA gespeicherten Daten an ausländische Behörden grundsätzlich untersagt ist.[156] Dabei ist noch immer der Großteil der Daten westlicher Staaten in den USA gespeichert.[157] Die Regelung des Art. 17 VO kann derartige Pflichtenkollisionen aufgrund von Kollisionsnormen in Drittstaaten nicht langfristig lösen.[158] Art. 17 Abs. 1 VO ermöglicht den Diensteanbietern ein vorläufiges Recht zur Verweigerung der Datenherausgabe für derartige Fälle. Beantragt die Anordnungsbehörde daraufhin gem. Art. 17 Abs. 3 S. 2 VO eine Überprüfung durch das zuständige Gericht des Anordnungsstaates, so wird die Ausführung der EPO bis zum Abschluss des gerichtlichen Überprüfungsverfahrens ausgesetzt. Das Gericht prüft gem. Art. 17 Abs. 4–6 VO insbesondere, ob das Recht des Drittstaates überhaupt im konkreten Fall Anwendung findet (Art. 17 Abs. 4 lit. a VO) und eine Rechtskollision gegeben ist (Art. 17 Abs. 4 lit. b VO). Ist dies der Fall, so entscheidet es nach Maßgabe der Abwägungskriterien aus Art. 17 Abs. 6 VO, ob die EPO aufgehoben oder trotzdem aufrechterhalten werden soll. Letzteres verdeutlicht die Brisanz der E-Evidence-Verordnung im Verhältnis zu Drittstaaten und verlagert wiederum die Sanktionsgefahren auf den Diensteanbieter.[159] Ferner ist anzumerken, dass Diensteanbieter anderer Drittstaaten, wie insbesondere China, zunehmend an Relevanz gewinnen.[160] Mithin sind auch insoweit widersprüchliche Verpflichtungen der Diensteanbieter in Aussicht.

Nachteilhaft an dem entstehenden Abkommen mit den USA könnte andererseits sein, dass sich bereits jetzt erste Parallelen zwischen dem E-Evidence-Gesetzespaket und dem entstehenden Abkommen in den Defiziten im Grund-, Daten- und Rechtsschutz abzeichnen. In seiner Stellungnahme empfahl der Europäische Datenschutzbeauftragte zwar zurecht die Aufnahme zusätzlicher Garantien sowie die frühzeitige Einbindung von Justizbehörden des anderen Staates, aus dem die Daten stammen, damit diesen die grundrechtliche Überprüfung der Anordnung bzw. Geltendmachung von Ablehnungsgründen möglich ist.[161] Doch ob die Verhandlungen sich von dieser Empfehlung leiten lassen, wird mit Skepsis gesehen. Schließlich beinhaltet auch das mittlerweile abgeschlossene Abkommen zwischen den USA und dem Vereinigten Königreich keine systematische Unterrichtung der Justizbehörden des Staates, aus denen die Diensteanbieter ihre Daten beibringen. Da dieses Abkommen das erste mit den USA war, wird es als Blaupause für weitere Abkommen gesehen.[162] Auch das zweite Zusatzprotokoll zu dem von den meisten EU-Mitgliedstaaten ratifizierten Übereinkommen des

[151] Text abrufbar unter https://web.archive.org/web/20230627092155/http://www.justice.gov/criminal-oia/page/file/1152896/download (19.5.2024).

[152] HomelandSecurity v. 21.6.2023, abrufbar unter https://www.dhs.gov/news/2023/06/21/eu-us-joint-statement-following-eu-us-ministerial-justice-and-home-affairs (19.5.2024).

[153] Beschluss (EU) 2019/1172 des Rates vom 6. Juni 2019, ABl. EU 2019 Nr. L 184/1.

[154] Europäische Kommission, Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen (KOM [2019] 70 endg.).

[155] *Abraha*, International Journal of Law and Information Technology 29 (2/2021), 118 (151).

[156] 18 U.S. Code § 2701 „Unlawful access to stored communications".

[157] *Burwell/Propp* (Fn. 150).

[158] *Meißner*, Verfassungsblog v. 28.6.2023, abrufbar unter https://verfassungsblog.de/digitale-beweise-im-eu-us-datenschutzkonflikt/ (19.5.2024).

[159] *Weiß/Brinkel*, RDi 2023, 522 (529)

[160] *Erie/Streinz*, New York University Journal of International Law and Politics 54 (1/2021), 4.

[161] Stellungnahme 2/2019 Stellungnahme des EDSB zu dem Mandat für die Verhandlung eines Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln, S. 21, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_eu_us_agreement_e-evidence_en_de.pdf (19.5.2024).

[162] *Christakis*, European Law Blog v. 17.10.2019, abrufbar unter https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/ (19.5.2024).

Europarats über Computerkriminalität sieht nur vor, dass die gleichzeitige Notifizierung für die Vertragsparteien freiwillig ist.

Schließlich könnte der unilaterale Ansatz auch Vorbild für weitere Drittstaaten sein. Immerhin wird das E-Evidence-Gesetzespaket selbst als eine Reaktion auf den amerikanischen CLOUD-Act gesehen.[163] Mit der weiteren Verbreitung des unilateralen Datenzugangsmodells wären jedoch Risiken verbunden. Angenommen werden Nachteile für die Kooperationsbereitschaft und das Vertrauen zwischen den Staaten im Rahmen der internationalen Strafverfolgung, weil die Staaten zunehmend auf den einseitigen Zugang anstelle des arbeitsteiligen Vorgehens setzen.[164] Vor allem steht aber die Errungenschaft des hohen Grundrechts- und Datenschutzniveaus in der EU auf dem Spiel.[165] Denn die hiesigen datenschutz- und grundrechtlichen Bestimmungen blieben bei der unilateralen Anordnung von drittstaatlichen Behörden gegenüber den Diensteanbietern, die in der EU Daten speichern, unberücksichtigt. Der proklamierte „Brüsseler Effekt“[166] im Grund- und Datenschutz erfährt dann eine Feuertaufe. Als letzte Instanz zur Wahrung europäischer Grund- und Datenschutzrechte wären einmal mehr die Diensteanbieter auf den Plan gerufen, welche dieser Rolle schlechthin nicht gerecht werden können und sich wiedersprechenden Verpflichtungen ausgesetzt sähen.

[163] *Esser* (Fn. 83), S. 43.
[164] *Burchard*, ZIS 2018, 190 (193); *Burchard*, ZIS 2018, 249 (264).
[165] *Mantelero*, Computer Law & Security Review 40 (2021), Article 105500.
[166] *Bradford*, The Brussels Effect, How the European Union rules the world, 2019.