

Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel – Rückzug des Staates aus der Rechtshilfe?

von Prof. Dr. Martin Böse*

Abstract

Um den grenzüberschreitenden Zugriff auf elektronische Beweismittel zu erleichtern, hat die Kommission im April 2018 ein neues Kooperationsinstrument vorgeschlagen, mit dem ein Service-Provider grenzüberschreitend ohne Mitwirkung des betroffenen Gebietsstaates zur Herausgabe bzw. Sicherung von ihm gespeicherter Nutzerdaten aufgefordert werden kann. Der folgende Beitrag legt dar, dass die Verdrängung des ersuchten Mitgliedstaats (bzw. der Vollstreckungsstaats) aus der strafrechtlichen Zusammenarbeit nicht nur aus kompetenzrechtlichen Erwägungen, sondern auch und vor allem mit Blick auf die grundrechtliche Schutzfunktion des Rechtshilfeverfahrens schwerwiegenden Einwänden ausgesetzt ist und der Vorschlag darüber hinaus mit einem weitreichenden Abbau individualschützender Rechtshilfehindernisse und gravierenden Lücken im gerichtlichen Rechtsschutz einhergeht.

I. Einführung

Mit den neuen Möglichkeiten moderner Kommunikations- und Informationstechnologien (e-mail, social media, cloud computing etc.) haben elektronische Daten als Ermittlungsansatz und Beweismittel für die Verfolgung von Straftaten zunehmende Bedeutung erlangt.¹ Die Flüchtigkeit dieser Daten stellt die Ermittlungsbehörden allerdings bei der Erhebung vor besondere Herausforderungen, insbesondere wenn die (möglicherweise) für die Untersuchung relevanten Daten in einem anderen Land gespeichert und verarbeitet werden als dem, in dem das betreffende Ermittlungsverfahren geführt wird. Um eine schnelle grenzüberschreitende Erhebung der zur Strafverfolgung benötigten elektronischen Beweismittel zu ermöglichen bzw. zu erleichtern, hat die Kommission im April 2018 die Einführung eines neuen Kooperationsinstruments vorgeschlagen, nämlich die Europäische Herausgabe- und Sicherungsanordnung.² Mit dem folgenden Beitrag soll dieses neue Instrument kritisch gewürdigt und aufgezeigt werden, dass sich aus dem mit ihm einhergehenden Wandel von bilateralen Kooperationsmodellen zur unilateralen transnationalen Beweiserhebung schwer-

wiegende Konsequenzen für den Grundrechtsschutz ergeben.³

Der Beitrag beginnt mit einem Überblick über Hintergrund und Gegenstand des Kommissionsvorschlags und den Stand des bisherigen Gesetzgebungsverfahrens auf Unionsebene (II.). Nach einem kritischen Blick auf die vertragliche Ermächtigung, auf die der Vorschlag gestützt wird (III.), folgt eine grundsätzliche Kritik an dem neuen Kooperationsmechanismus und der darin enthaltenen (weitgehenden) Abschaffung des Rechtshilfeverfahrens bzw. seiner Ersetzung durch einen Notifikationsmechanismus (IV.). Sodann wird untersucht, wie sich der Abbau bislang bestehender Rechtshilfehindernisse auf den Grundrechtsschutz auswirkt (V.) und welche Folgen die neue Aufgabenteilung zwischen ersuchendem und ersuchtem Staat für den gerichtlichen Rechtsschutz hat (VI.).

II. Die Europäische Herausgabe- und Sicherungsanordnung

1. Hintergrund

Das Bedürfnis für ein neues Kooperationsinstrument wird vor allem mit den Unzulänglichkeiten der bislang bestehenden Möglichkeiten der Strafverfolgungsbehörden begründet, grenzüberschreitend auf elektronische Beweismittel zuzugreifen. Dies gilt vor allem für die traditionelle zwischenstaatliche Rechtshilfe, wonach der Staat, in dem das Ermittlungsverfahren geführt wird, den anderen Staat um die Erhebung und anschließende Übermittlung der Daten ersucht, der ersuchte Staat über die Bewilligung des Ersuchens entscheidet und anschließend die zur Leistung von Rechtshilfe erforderlichen innerstaatlichen Maßnahmen ergreift (vgl. § 59 ff. IRG). Obwohl das Europarats-Übereinkommen gegen Computerkriminalität (Budapester Übereinkommen) eine Reihe von Bestimmungen zur

* Der Verfasser ist Professor für Strafrecht und Strafprozessrecht sowie Internationales und Europäisches Strafrecht an der Rheinischen Friedrich-Wilhelms-Universität Bonn. Der Beitrag beruht auf einem Gutachten, das der Verfasser für das Europäische Parlament im Auftrag des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE Committee) im September 2018 verfasst hat, und auf einem Vortrag, den er am 7.3.2019 auf der Konferenz „Europäisches Strafrecht nach der österreichischen Ratspräsidentschaft“ an der Wirtschaftsuniversität Wien gehalten hat. Das Gutachten mit dem Titel „An assessment of the Commission’s proposals on electronic evidence“, abrufbar unter: [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU\(2018\)604989_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf) (zuletzt abgerufen am 30.4.2019).

¹ Eingehend *Warzen*, NZWiSt 2017, 289 ff.

² Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, KOM (2018) 225 endg.; s. auch den begleitenden 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.

³ Der Kommissionsvorschlag wirft darüber hinaus eine Reihe weiterer Fragen auf, die an dieser Stelle nicht behandelt werden können; insoweit sei daher auf das Gutachten (*Fn.) und auf die Arbeitspapiere des Europäischen Parlaments (Fn. 24) verwiesen.

Erleichterung und Beschleunigung des Rechtshilfeverkehrs vorsieht⁴, hat sich das Rechtshilfeverfahren in der Praxis mitunter als sehr aufwändig und langwierig erwiesen; nach einem Bericht des auf der Grundlage des Budapester Übereinkommens eingesetzten Ausschusses (Cybercrime Convention Committee, T-CY) aus dem Jahr 2014 vergehen bis zur einer Entscheidung über eingehende Ersuchen in der Regel zwischen sechs und 24 Monaten.⁵ Das unionsrechtliche Instrument der Europäischen Ermittlungsanordnung (vgl. §§ 91a ff. IRG)⁶ schafft insoweit nach Ansicht der Kommission auch keine Abhilfe, da es im Grundsatz weiterhin an einer Beteiligung des ersuchten Staates (Vollstreckungsstaates) und damit an einem im Vergleich zu einer direkten Übermittlung (s. dazu sogleich) aufwändigen und langwierigen Verfahren festhält.⁷

Als Alternative zum Rechtshilfeverfahren hat sich in der Praxis die direkte grenzüberschreitende Zusammenarbeit mit Service-Providern auf freiwilliger Grundlage entwickelt; allein im Jahr 2016 richteten die Strafverfolgungsbehörden der Mitgliedstaaten mehr als 120.000 Auskunftersuchen an die fünf großen US-amerikanischen Provider (Apple, Facebook, Google, Microsoft, Twitter); allerdings wurden die angefragten Daten in weniger als der Hälfte der Fälle übermittelt.⁸ In dieser Quote zeigen sich damit bereits die Nachteile einer freiwilligen Zusammenarbeit, denn diese steht und fällt mit der Kooperationsbereitschaft des jeweiligen Providers, die je nach Unternehmenspolitik erheblich variieren kann; darüber hinaus ist es für die zuständigen Behörden mitunter schwierig, die innerhalb des Unternehmens zuständige Stelle zu ermitteln und zu kontaktieren.⁹

Um diese Nachteile einer freiwilligen Zusammenarbeit zu überwinden, haben einige Mitgliedstaaten die nach innerstaatlichem Recht bestehenden Befugnisse zum Erlass von Herausgabeanordnungen dahingehend erweitert, dass

Service-Provider auch dann zur Übermittlung von Nutzerdaten verpflichtet werden können, wenn die Daten auf einem im Ausland befindlichen Server gespeichert werden. Im Fall „Yahoo“ hat der belgische Kassationsgerichtshof die völkerrechtliche Zulässigkeit eines solchen Vorgehens mit der Begründung bejaht, dass die Kooperationspflicht sich auf eine Mitwirkung im Inland (Beschaffung der Daten) beziehe und daher nicht die Gebietshoheit des Staates verletze, in dem die Daten gespeichert seien.¹⁰ Diese Sichtweise, der auch das Cybercrime Convention Committee für die Auslegung der entsprechenden Bestimmung des Budapester Übereinkommens (Art. 18)¹¹ und der US-amerikanische Gesetzgeber mit dem Cloud-Act¹² gefolgt sind, ist allerdings nicht unumstritten, da mit dem grenzüberschreitenden Zugriff die Gefahr besteht, dass die Regeln und Grenzen der strafrechtlichen Zusammenarbeit unterlaufen werden.¹³ Aus der Perspektive der Kommission führen die unterschiedlichen Regelungen in den Mitgliedstaaten aber vor allem zu Rechtsunsicherheit bei Service-Providern und Nutzern, so dass ein einheitlicher unionsrechtlicher Rahmen für den grenzüberschreitenden Zugriff auf Providerdaten geschaffen werden sollte.¹⁴

2. Der Kommissionsvorschlag

Um die Defizite der bestehenden Kooperationsmechanismen zu beheben, hat die Kommission im April 2018 mit der Europäischen Herausgabe- und Sicherungsanordnung ein neues Instrument zur grenzüberschreitenden Erhebung elektronischer Beweismittel vorgeschlagen.¹⁵ Da die relevanten Daten vorwiegend von den Anbietern elektronischer Kommunikations- und Informationsdienste verarbeitet und gespeichert werden, wird der Begriff „elektronische Beweismittel“ dabei auf von entsprechenden Dienstleistern (Service-Providern) gespeicherte Daten beschränkt.¹⁶ Im Unterschied zur traditionellen Rechtshilfe und zur Europäischen Ermittlungsanordnung sieht der Verordnungsentwurf vor, dass die Strafverfolgungsbehör-

⁴ Art. 25 ff. Übereinkommen des Europarats über Computerkriminalität v. 23.11.2001, BGBl. II 2008, S. 1242. Zur Zeit wird ein zweites Zusatzprotokoll zu dem Übereinkommen vorbereitet, das die internationale Zusammenarbeit weiter erleichtern und beschleunigen soll, s. dazu die Informationen unter <https://www.coe.int/en/web/cybercrime/t-cy-drafting-group> (zuletzt abgerufen am 30.4.2019).

⁵ 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/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c> (zuletzt abgerufen am 25.4.2019; zur Umsetzung der daraufhin erlassenen Empfehlungen s. ferner Cybercrime Convention Committee (T-CY), Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers, adopted by T-CY 18 (27–28 November 2017), abrufbar unter <https://rm.coe.int/t-cy-2017-2-mla-follow-up-rep/168076d55f> (zuletzt abgerufen am 30.4.2019).

⁶ Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. EU L 130/1.

⁷ 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. 12.

⁸ Commission 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 final, S. 15.

⁹ Kommission, Non-paper (Fn. 7), S. 7 f.; zu den unterschiedlichen Übermittlungsquoten S. 10.

¹⁰ Cour de Cassation, Urt. v. 1.12.2015, P.13.2082.N – Yahoo.

¹¹ Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), adopted by the T-CY following the 16th plenary by written procedure on 1 March 2017, T-CY(2015)16, para. 3.5, abrufbar unter <https://rm.coe.int/16806f943e> (zuletzt abgerufen am 30.4.2019).

¹² § 103(a)(1) Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 23 March 2018; s. zu den Hintergründen eingehend *Burchard*, ZIS 2018, 190 (198 ff.).

¹³ S. dazu *Burchard*, ZIS 2018, 249 (253 ff.); s. auch die eingehende völkerrechtliche Analyse bei *Currie*, Canadian Yearbook of International Law, vol. 54 (2016), 63 ff.; kritisch zur weiten Auslegung von Art. 18 des Europarats-Übereinkommens: *de Hert/Parlar/Siefert*, Computer Law & Security Review, Vol. 34 (2018), 327 ff.

¹⁴ Kommission, Non-paper (Fn. 7), S. 13.

¹⁵ S. den Vorschlag einer entsprechenden Verordnung (Fn. 2).

¹⁶ Art. 2 Abs. 6 des Verordnungsentwurfs (Fn. 2).

den der Mitgliedstaaten eine solche Anordnung unmittelbar an den in einem anderen Mitgliedstaat operierenden Service-Provider richten können und dieser daraufhin zur Übermittlung (Herausgabeanordnung) bzw. vorläufigen Sicherung (Sicherungsanordnung) der bezeichneten Daten verpflichtet ist, ohne dass es einer vorherigen Entscheidung des letztgenannten Mitgliedstaates bedarf.¹⁷ Dessen Mitwirkung als Vollstreckungsstaat ist vielmehr auf die – voraussichtlich seltenen – Fälle beschränkt, in denen der Service-Provider der Anordnung nicht nachkommt und daher weitere Maßnahmen zu deren Durchsetzung bzw. zur Verhängung von Sanktionen erforderlich sind.¹⁸ Die vom Ausstellungsstaat erlassene Herausgabeanordnung und Sicherungsanordnung entfaltet daher aus sich heraus eine transnationale Bindungswirkung, ohne dass es einer vorherigen Anerkennung durch den Vollstreckungsstaat bedarf.

Um die Funktionsfähigkeit des neuen Instruments zu gewährleisten, sieht ein begleitender Richtlinienentwurf vor, dass jeder Service-Provider, der seine Dienste in mehreren Mitgliedstaaten der Union anbietet, mindestens einen Vertreter in einem dieser Mitgliedstaaten benennen muss, an den Europäische Herausgabe- und Sicherungsanordnungen gerichtet werden können; der Vertreter muss mit den Befugnissen und Ressourcen ausgestattet sein, die erforderlich sind, um den Anordnungen nachzukommen.¹⁹ Die Pflicht zur Bestellung eines solchen Vertreters soll auch für Service-Provider bestehen, die nicht in einem Mitgliedstaat der Union, sondern in einem Drittstaat (z.B. den USA) niedergelassen sind.²⁰ Maßgeblich ist allein, dass die betreffenden Dienstleistungen in der Union angeboten werden (Marktortprinzip); auf den Ort, an dem die Daten gespeichert werden, kommt es hingegen nicht an.²¹ Der Kommissionsvorschlag weist damit implizit die Bedenken zurück, wonach der unilaterale Zugriff auf die in einem Drittstaat gespeicherten Daten dessen territoriale Souveränität bzw. Gebietshoheit verletzt, und schließt sich den auf nationaler und internationaler Ebene bestehenden Tendenzen an, wonach ein solches Vorgehen aufgrund anderer territorialer Anknüpfungspunkte (Sitz des

Service-Providers bzw. Marktortprinzip, s. oben) völkerrechtlich zulässig ist (s. oben 1.).

Nach intensiven Beratungen hat der Rat unter der österreichischen Präsidentschaft im Dezember 2018 eine allgemeine Ausrichtung angenommen, welche den Inhalt des Kommissionsvorschlags in weiten Teilen übernimmt²², allerdings für bestimmte Fälle vorsieht, dass dem Vollstreckungsstaat eine Kopie der erlassenen Herausgabeanordnung übermittelt wird, damit dieser gegebenenfalls Einwände gegen die Übermittlung der angeforderten Daten erheben kann (Notifikationsmechanismus; s. dazu näher unten IV.3.).²³ Im Unterschied zum Rat hat sich das Europäische Parlament noch nicht auf eine Position verständigt, sondern sieht vielmehr in einer Reihe von Fragen noch Klärungs- und Diskussionsbedarf.²⁴ Das neue Kooperationsinstrument konnte daher nicht mehr vor den Wahlen verabschiedet werden. Es ist jedoch damit zu rechnen, dass die rechtspolitische Diskussion anschließend wieder aufgenommen wird, weshalb die grundsätzlichen Einwände gegen den neuen Mechanismus im Folgenden dargelegt werden sollen.

III. Art. 82 Abs. 1 AEUV als vertragliche Ermächtigungsgrundlage?

Bedenken begegnet bereits die für die Einführung des neuen Kooperationsinstruments herangezogene vertragliche Ermächtigung (Art. 82 Abs. 1 AEUV). Nach der Vorstellung der Kommission wird mit der Europäischen Herausgabe- bzw. Sicherungsanordnung das Prinzip der gegenseitigen Anerkennung umgesetzt (Art. 82 Abs. 1 lit. a AEUV).²⁵ Dabei wird indes verkannt, dass diese Bestimmung die Union ermächtigt, „Regeln und Verfahren“ für eine Anerkennung gerichtlicher bzw. justizieller Entscheidungen festzulegen, und damit – anders als im Rahmen der zivilrechtlichen Zusammenarbeit (Art. 81 Abs. 2 lit. a AEUV) – keine „automatische“ Anerkennung von Entscheidungen ohne Beteiligung des Vollstreckungsstaates umfasst (vgl. auch Art. 82 Abs. 1 lit. d AEUV: „Zusammenarbeit zwischen den Justizbehörden“).²⁶ Dass eine solche Mitwirkung bei der Vollstreckung Europäischer

¹⁷ Art. 9, 10 des Verordnungsentwurfs (Fn. 2).

¹⁸ Art. 13, 14 des Verordnungsentwurfs (Fn. 2).

¹⁹ Art. 3 Abs. 1, 7 des Richtlinienentwurfs (Fn. 2).

²⁰ Art. 3 Abs. 2 des Richtlinienentwurfs (Fn. 2).

²¹ Art. 1 Abs. 1, Art. 3 Abs. 1 des Verordnungsentwurfs (Fn. 2); s. auch

Art. 1 Abs. 4 S. 1, Art. 3 Abs. 1, 2 des Richtlinienentwurfs (Fn. 2).

²² Rats-Dok. 15292/18.

²³ Art. 7a des geänderten Verordnungsvorschlags, Rats-Dok. 15292/18, S. 34.

²⁴ S. die folgenden Arbeitspapiere des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE Committee) zu dem Verordnungsvorschlag der Kommission: Arbeitsdokument, 7.12.2018 (PE 631.925v02-00); 2. Arbeitsdokument (A), 6.2.2019 (PE 634.729v01-00); 2. Arbeitsdokument (B), 6.2.2019 (PE 634.730v01-00); 3. Arbeitsdokument (A), 13.2.2019 (PE634.849v01-00); 3. Arbeitsdokument (B), 13.2.2019 (PE634.850v01-00); 4. Arbeitsdokument (A), 11.3.2019 (PE636.343v01-00); 4. Arbeitsdokument (B), 11.3.2019 (PE636.344v01-00); 4. Arbeitsdokument (C), 11.3.2019 (PE636.345v01-00); 5. Arbeitsdokument (A), 8.3.2019 (PE636.335v01-00); 5. Arbeitsdokument (B), 8.3.2019 (PE636.336v01-00); 5. Arbeitsdokument (C), 8.3.2019 (PE636.337v01-00); 6th Working Document (A), 1.4.2019 (PE637.466v01-00); 6th Working Document (B), 1.4.2019 (PE637.468v01-00); 6th Working Document (C), 1.4.2019 (PE637.469v01-00); 7th Working Document, 1.4.2019 (PE637.465v01-00).

²⁵ Kommissionsvorschlag für eine Verordnung (Fn. 2), S. 5.

²⁶ S. auch die Stellungnahme Nr. 28/2018 der Bundesrechtsanwaltskammer (September 2018), S. 3, abrufbar unter <https://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2018/september/stellungnahme-der-brak-2018-28.pdf> (zuletzt abgerufen am 30.4.2019).

Herausgabe- und Sicherungsanordnungen vorgesehen ist, ändert nichts daran, dass diese Anordnungen für den Adressaten unmittelbar verbindlich sind, also im Einzelfall keiner Anerkennung durch den Vollstreckungsstaat mehr bedürfen.²⁷ In diesem Punkt weicht der Kommissionsvorschlag von der bisherigen Gesetzgebungspraxis bei der Umsetzung des Prinzips der gegenseitigen Anerkennung ab, wonach der Vollstreckungsstaat im Einzelfall über die Anerkennung und Vollstreckung der vom Ausstellungsstaat erlassenen Anordnung (z.B. einer Europäischen Ermittlungsanordnung) entscheidet.²⁸

Gegen die von der Kommission vertretene weite Auslegung des Art. 82 Abs. 1 AEUV spricht auch, dass der Vertrag für extraterritoriale Ermittlungsmaßnahmen (z.B. die grenzüberschreitende Observation oder Nachteile, vgl. Art. 40, 41 Schengener Durchführungsübereinkommen) eine eigenständige vertragliche Ermächtigung vorsieht, die den Erlass eines entsprechenden Rechtsaktes an bestimmte Bedingungen knüpft, um dem mit derartigen Maßnahmen verbundenen Eingriffen in die Gebietshoheit des betroffenen Mitgliedstaates Rechnung zu tragen (Art. 89 AEUV). Inhaltlich wird die Zulässigkeit derartiger Maßnahmen davon abhängig gemacht, dass sie in Verbindung und in Absprache mit dem Gebietsstaat durchgeführt werden (Art. 89 S. 1 AEUV). Zudem ist im Gesetzgebungsverfahren eine einstimmige Beschlussfassung im Rat vorgesehen (Art. 89 S. 2 AEUV), d.h. jeder Mitgliedstaat kann durch sein Veto den Erlass eines entsprechenden Rechtsaktes verhindern.²⁹ Da eine Europäische Herausgabeordnung aufgrund ihrer transnationalen Bindungswirkung ebenso in die Gebietshoheit des Vollstreckungsstaates eingreift wie z.B. eine grenzüberschreitende Observation (Art. 40 SDÜ), führt eine Heranziehung des Art. 82 Abs. 1 AEUV als Ermächtigungsgrundlage im Ergebnis dazu, dass die in Art. 89 AEUV vorgesehenen Sicherungen zum Schutz der territorialen Souveränität der Mitgliedstaaten unterlaufen werden.

IV. Territoriale Souveränität und Grundrechtsschutz

1. Die Verantwortung des Gebiets- bzw. Vollstreckungsstaates

Der Schutz der territorialen Souveränität, der in der Begrenzung der vertraglichen Ermächtigungsgrundlagen zum Ausdruck kommt, liegt nicht allein im Interesse der Mitgliedstaaten, sondern dient auch und vor allem dem Schutz der Grundrechte ihrer Bürger, denn die Gebietsho-

heit ist untrennbar mit der Verpflichtung des Staates verbunden, bei der Ausübung von Hoheitsgewalt die Grundrechte der auf seinem Gebiet befindlichen Personen zu achten und zu schützen und auch im Rahmen der grenzüberschreitenden Zusammenarbeit in Strafsachen dafür Sorge zu tragen, dass menschenrechtliche und rechtsstaatliche Mindeststandards gewahrt werden.³⁰ Diese Anforderungen sind auch bei der grenzüberschreitenden Übermittlung von Daten zu beachten.³¹ In seinem Beschluss zum Übereinkommen gegen Computerkriminalität und dem dort vorgesehenen Zugriff anderer Vertragsstaaten auf Inlandsdaten (Art. 32) hat das BVerfG diese Verantwortung des Gebietsstaates bestätigt und die Verfassungsbeschwerde nur deshalb zurückgewiesen, weil die Beschwerdeführer die Möglichkeit einer Grundrechtsverletzung bei einem grenzüberschreitenden Zugriff auf öffentlich zugängliche Daten (Art. 32 lit. a des Übereinkommens) bzw. bei einem Zugriff mit Zustimmung der betroffenen Person (Art. 32 lit. b des Übereinkommens) nicht hinreichend substantiiert dargelegt hatten.³² Demgegenüber liegt bereits in der Anerkennung der rechtlichen Bindungswirkung einer Europäischen Herausgabeordnung ein Eingriff in die Grundrechte des Service-Providers vor, für den der Gebietsstaat (mit-)verantwortlich ist; da es sich um nicht öffentlich zugängliche Daten handelt und eine datenschutzrechtliche Einwilligung nicht vorliegt³³, ist aus den gleichen Gründen auch ein Eingriff in die Grundrechte des betroffenen Nutzers anzunehmen. Infolge der „automatischen“ Anerkennung einer Herausgabe- oder Sicherungsanordnung kann der Gebiets- bzw. Vollstreckungsstaat seiner Verantwortung für den Grundrechtsschutz nicht mehr gerecht werden; auf diese Bedenken haben sowohl der Deutsche Bundesrat³⁴ als auch das Europäische Parlament³⁵ hingewiesen.

2. Grundrechtsschutz durch Ausstellungsstaat oder Service-Provider?

Im Rechtshilfeverfahren nimmt der ersuchte Staat bzw. Vollstreckungsstaat seine Schutzfunktion über die jeweils anwendbaren Rechtshilfevoraussetzungen und -hindernisse (u.a. beiderseitige Strafbarkeit, ordre-public-Vorbehalt) und eine entsprechende Anwendung besonderer Eingriffs- bzw. Übermittlungsschwellen (vgl. z.B. § 100g StPO) wahr (s. auch unten V.1.). Fällt die Prüfung dieser Schutzvorschriften weg, stellt sich die Frage, ob dieses Defizit durch anderweitige Schutzmechanismen kompensiert werden kann. Dies setzt indes voraus, dass die entsprechende Schutzfunktion von einer anderen Stelle wahrgenommen wird; insoweit kommen allein der Service-

²⁷ Burchard, ZIS 2018, 249 (267).

²⁸ S. zur Europäischen Ermittlungsanordnung Art. 9 Richtlinie 2014/41/EU (Fn. 6).

²⁹ Böse, in: Schwarze, EU-Kommentar, 4. Aufl. (2019), Art. 89 AEUV Rn. 1, 2; Spaeth, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Bd. 2, 7. Aufl. (2015), Art. 89 AEUV Rn. 2.

³⁰ S. allgemein zum ordre-public-Vorbehalt: BVerfGE 59, 280 (282 f.); 108, 129 (136 f.); 113, 154 (162 f.); 140, 317 (347); s. auch zur EMRK: EGMR, Urt. v. 7.7.1989 (Soering v. Vereinigtes Königreich), NJW 1990, 2183, 2185 (Rn. 91), 2188 (Rn. 113); zur Zusammenarbeit zwischen den EU-Mitgliedstaaten: EGMR, Urt. v. 17.4.2018 – 21055/11 (Pirozzi v. Belgien), Rn. 59 ff.

³¹ BVerfGE 141, 220 (342); s. auch Böse, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, 2007, S. 137 ff.; zum vorliegenden Zusammenhang Burchard, ZIS 2018, 249 (251).

³² BVerfGE 142, 234 (254 ff.); s. dagegen die abweichende Meinung des Richters Huber, a.a.O., 257 ff. Zum Teil wird die Übertragung von Hoheitsrechten auf ausländische Staaten als verfassungswidrig angesehen, weil eine entsprechende Ermächtigung in der Verfassung (vgl. Art. 23, 24 GG) fehlt, s. dazu näher Sauer, in: Kahl/Waldhoff/Walter, Bonner Kommentar zum Grundgesetz (198. Aktualisierung, Mai 2019), Art. 24 Rn. 98 ff., 108.

³³ S. insoweit Burchard, ZIS 2018, 249 (252).

³⁴ BR-Drs. 215/18, S. 6.

³⁵ 3rd Working Document (A) (Fußn. 24), S. 5.

Provider oder der Ausstellungsstaat in Betracht.

In dem Kommissionsvorschlag findet sich dieser Gedanke insofern wieder, als die zuständige Behörde des Ausstellungsstaates bei entsprechenden Anhaltspunkten zu klären hat, ob die angeforderten Transaktions- oder Inhaltsdaten nach dem Recht des Vollstreckungsstaates durch Immunitäten und Vorrechte geschützt sind, und daraufhin gegebenenfalls von der Anforderung dieser Daten absieht.³⁶ Dieser Schutzmechanismus greift jedoch nur, wenn die Ausstellungsbehörde über entsprechende Anhaltspunkte verfügt, was wiederum Kenntnisse des Rechts des Vollstreckungsstaates voraussetzt. Darüber hinaus ist damit zu rechnen, dass die Prüfung der nach dem Recht des Vollstreckungsstaates geltenden Schutzstandards durch das Strafverfolgungsinteresse des Ausstellungsstaates überlagert wird und diesem daher die notwendige Distanz fehlt, um über die Einhaltung der nach dem Recht des Vollstreckungsstaates geltenden Standards zu wachen.³⁷ So wäre es kaum vorstellbar, dass eine Behörde des Ausstellungsstaates von dem Erlass einer Herausgabeanordnung absieht, weil die Strafverfolgung (im Ausstellungsstaat!) gegen rechtsstaatliche oder menschenrechtliche Mindeststandards verstößt (ordre-public-Vorbehalt, s. dazu sogleich). Der Ausstellungsstaat kann daher die Schutzfunktion des Vollstreckungsstaates nicht in einer Weise wahrnehmen, die einen effektiven Grundrechtsschutz sicherstellt.

Der Service-Provider vermag diese Aufgabe noch viel weniger zu übernehmen. Soweit er selbst als Adressat der Herausgabeanordnung in seinen Grundrechten betroffen ist, liegt dies auf der Hand. Aber auch mit Blick auf die Grundrechte seiner Kunden, d.h. der betroffenen Nutzer, bestehen erhebliche Bedenken gegen die Zuweisung einer solchen Schutzfunktion, da er nicht nur Adressat einer verbindlichen Herausgabeanordnung, sondern überdies bei einem Verstoß gegen die Übermittlungspflicht Vollstreckungsmaßnahmen bzw. Sanktionen ausgesetzt ist; der Service-Provider ist damit bereits im Ausgangspunkt in einer sehr viel schwächeren Position als der Vollstreckungsstaat, wenn es darum geht, einer Herausgabeanordnung im Interesse eines wirksamen Grundrechtsschutzes entgegenzutreten.³⁸ Diese Skepsis findet weitere Nahrung in dem Umstand, dass für eine Prüfung von Übermittlungshindernissen wenig Zeit (in dringenden Fällen sechs Stunden)³⁹, lediglich rudimentäre Informationen (nämlich der Inhalt der Anordnung⁴⁰) und in der Regel nur begrenzte Ressourcen zur Verfügung stehen.⁴¹ Dass der Service-Provider unter diesen Umständen kaum imstande sein wird, einen ordre-public-Verstoß zu prüfen bzw. festzustellen, hat der Rat implizit anerkannt, indem er ein ent-

sprechendes, noch im Kommissionsvorschlag vorgesehene Weigerungsrecht⁴² in der allgemeinen Ausrichtung gestrichen hat.⁴³

3. Grundrechtsschutz durch Notifikation des Vollstreckungsstaates?

Um der Schutzverantwortung des Vollstreckungsstaates gerecht zu werden, hat der Rat den Kommissionsvorschlag durch ein Notifikationsmodell ergänzt, das den Vollstreckungsstaat in das neue Kooperationsinstrument einbindet, indem es den Ausstellungsstaat unter bestimmten Voraussetzungen verpflichtet, den Vollstreckungsstaat von dem Erlass einer Herausgabeanordnung zu unterrichten und diesem Gelegenheit zur Stellungnahme zu geben.⁴⁴

Dieses Notifikationsmodell ist jedoch nicht geeignet sicherzustellen, dass der Vollstreckungsstaat die ihm zukommende Schutzfunktion wirksam wahrnehmen kann. Dies liegt zunächst daran, dass der Anwendungsbereich auf Inhaltsdaten beschränkt ist, mithin Transaktionsdaten (vgl. insoweit § 100g StPO) ausnimmt, und sich die Gelegenheit der Stellungnahme allein auf Immunitäten und Vorrechte (insbesondere Berufsgeheimnisse, vgl. § 160a StPO), aber nicht auf andere Übermittlungshindernisse bezieht. Ein umfassender Grundrechtsschutz, insbesondere mit Blick auf mögliche Folgen einer Übermittlung (ordre-public-Verstoß), kann das Modell bereits aus diesem Grund nicht gewährleisten.⁴⁵ Darüber hinaus ermöglicht es der Notifikationsmechanismus dem Vollstreckungsstaat nicht, die nach seinem Recht geltenden Schutzstandards durchzusetzen, sondern es bleibt dem Ausstellungsstaat überlassen, die vom Vollstreckungsstaat erhobenen Einwände durch eine Anpassung oder Rücknahme der Herausgabeanordnung umzusetzen.⁴⁶ In diesem Punkt unterscheidet sich der Vorschlag von der grenzüberschreitenden Nacheile, die einzustellen ist, wenn der Gebietsstaat widerspricht oder nicht innerhalb einer bestimmten Frist zustimmt (Art. 40 Abs. 2 SDÜ; vgl. oben III.). Da die Unterrichtung keine aufschiebende Wirkung hat, versagt der Mechanismus überdies immer dann, wenn der Service-Provider die angeforderten Daten bereits vor einer Stellungnahme des Vollstreckungsstaates übermittelt hat.⁴⁷

V. Defizite im materiellen Grundrechtsschutz

Mit der Verdrängung des Vollstreckungsstaates aus der ihm obliegenden Schutzfunktion geht ein Abbau bislang bestehender Rechtshilfeshindernisse einher, der zu weiteren Defiziten im Grundrechtsschutz führt (1.) und nicht

³⁶ Art. 5 Abs. 7 des Verordnungsentwurfs. Nach der allgemeinen Ausrichtung des Rates (Fn. 22) gilt dies nicht, sofern der betroffene Nutzer sich im Ausstellungsstaat aufhält.

³⁷ Burchard, ZIS 2018, 249 (266).

³⁸ S. auch die Stellungnahme Nr. 42/18 des Deutschen Anwaltvereins durch den Ausschuss Strafrecht (September 2018), S. 8.

³⁹ Art. 9 Abs. 1, Abs. 2 des Verordnungsentwurfs (Fn. 2).

⁴⁰ S. insoweit Art. 5 Abs. 5 des Verordnungsentwurfs (Fn. 2).

⁴¹ Brodowski, ZIS 2018, 493 (504); Burchard, ZIS 2018, 249 (260, 266).

⁴² Art. 9 Abs. 5 S. 2 des Verordnungsentwurfs (Fn. 2).

⁴³ Rats-Dok. 15292/18, S. 37.

⁴⁴ Art. 7a des Verordnungsentwurfs, Rats-Dok. 15292/18, S. 34.

⁴⁵ Darüber hinaus werden im Ausstellungsstaat ansässige Nutzer vom Anwendungsbereich ausgenommen, obwohl nach dem Recht des Vollstreckungsstaates auch insoweit ein entsprechender Schutz besteht.

⁴⁶ Art. 7a Abs. 2 S. 2 des Verordnungsentwurfs, Rats-Dok. 15292/18, S. 34.

⁴⁷ Vgl. Art. 7a Abs. 2 S. 2, Abs. 4 des Verordnungsentwurfs, Rats-Dok. 15292/18, S. 34.

durch die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung kompensiert wird (2.).

1. Abbau von Rechtshilfe- bzw. Vollstreckungshindernissen

Nach dem bislang geltenden unionsrechtlichen Rahmen steht für die grenzüberschreitende Herausgabe von Providerdaten als Kooperationsinstrument die Europäische Ermittlungsanordnung⁴⁸ zur Verfügung. Ein Blick auf die Gründe, aus denen die Vollstreckung einer Europäischen Ermittlungsanordnung abgelehnt werden kann, führt zu der ernüchternden Feststellung, dass der durch diese Ablehnungsgründe gewährleistete Schutz des Betroffenen weitgehend entfällt. Dies gilt zunächst für die Vollstreckungshindernisse, die in dem Kommissionsvorschlag nicht aufgegriffen und damit vollständig gestrichen werden, nämlich das Erfordernis der beiderseitigen Strafbarkeit, der Ablehnungsgrund für Taten, die im Vollstreckungsstaat begangen worden und dort straflos sind, und die entsprechende Anwendung von Eingriffsvoraussetzungen für besonders schwerwiegende Ermittlungsmaßnahmen.⁴⁹ Zwar wird das Erfordernis der beiderseitigen Strafbarkeit dadurch eingeschränkt, dass bei 32 Deliktsbereichen und bei weniger schwerwiegenden Ermittlungsmaßnahmen (z.B. der Identifizierung des Inhabers einer bestimmten IP-Adresse) auf dessen Prüfung verzichtet wird.⁵⁰ Im Übrigen hält das Unionsrecht mit der Europäischen Ermittlungsanordnung jedoch an diesen traditionellen Rechtshilfeshindernissen fest. Dies gilt insbesondere für den beim grenzüberschreitenden Zugriff auf Transaktions- und Inhaltsdaten, die von Service-Providern gespeichert werden, bedeutsamen Grundsatz, dass gravierende Ermittlungseingriffe für ein ausländisches Strafverfahren nur unter den gleichen Bedingungen zulässig sind wie für ein inländisches Strafverfahren (vgl. § 100g StPO).⁵¹

Soweit solche Daten dem besonderen Schutz durch Vorrechte und Befreiungen (insbesondere einem besonders geschützten Berufsgeheimnis) unterliegen, wird dies auch mit dem Kommissionsvorschlag anerkannt, die Prüfung des entsprechenden Übermittlungshindernisses aber dem Ausstellungsstaat überantwortet; auf diese Weise kann ein effektiver Schutz jedoch nicht gewährleistet werden (s. oben IV. 2. und 3.).⁵² Diese Bedenken gelten entsprechend, soweit die Ausstellungsbehörde gewährleisten soll, dass das von ihr selbst (!) geführte Strafverfahren nicht gegen den Grundsatz „ne bis in idem“ (Art. 50 GRC, Art. 54 SDÜ) verstößt⁵³, und die Prüfung des ordpublic-Vorbehalts auf den Service-Provider übertragen

(Kommission) oder ersatzlos gestrichen (Rat) wird (s. oben IV.2.).

2. Grundrechtsschutz durch hohe Anordnungsvoraussetzungen?

Die vorstehenden Bedenken ließen sich allerdings ausräumen, soweit die nach dem Recht des Vollstreckungsstaats vorgesehenen Eingriffsvoraussetzungen für die Erhebung besonders sensibler Daten dadurch ersetzt werden, dass bereits die Ausstellung einer Europäischen Herausgabeanordnung besonders hohen Anforderungen unterworfen wird, die ein vergleichbares Schutzniveau gewährleisten. Soweit mit der Herausgabeanordnung Transaktions- oder Inhaltsdaten angefordert werden sollen, setzt deren Erlass in materieller Hinsicht im Wesentlichen zweierlei voraus: Erstens müssen die Anordnungsvoraussetzungen nach dem Recht des Ausstellungsstaates beachtet werden, und die Anordnung muss notwendig und verhältnismäßig sein.⁵⁴ Zweitens muss die Straftat, zu deren Verfolgung die Anordnung ergeht, nach dem Recht des Ausstellungsstaates mit einem Höchstmaß von mindestens drei Jahren Freiheitsstrafe geahndet werden können oder von einem Rechtsakt zur Strafrechtsharmonisierung (u.a. Terrorismus, Betrug und Fälschung im unbaren Zahlungsverkehr, sexuelle Ausbeutung von Kindern, Angriffe auf Informationssysteme) erfasst werden.⁵⁵ Die erste Bedingung verweist im Wesentlichen auf das Recht des Ausstellungsstaates; ein eigenständiger unionsrechtlicher Mindeststandard kann somit allein über die zweite Voraussetzung begründet werden. Diese stellt nach Ansicht der Kommission sicher, dass Transaktions- oder Inhaltsdaten nicht zur Verfolgung von Bagatelldaten angefordert werden.⁵⁶

Gegenüber dieser Einschätzung sind jedoch erhebliche Zweifel anzumelden, denn eine Mindesthöchststrafe von drei Jahren ist bei einer Vielzahl von Tatbeständen vorgesehen, die keineswegs nur den Bereich der schweren (oder auch nur der mittleren) Kriminalität umfassen (z.B. Diebstahl, Körperverletzung).⁵⁷ Über die Verweisung auf die sekundärrechtliche Harmonisierung werden sogar Straftaten einbezogen, die nach Unionsrecht mit einer Höchststrafe von nur einem Jahr Freiheitsstrafe zu ahnden sind.⁵⁸ Mit der Mindesthöchststrafe von drei Jahren und der Zuordnung zu einem harmonisierten Deliktsbereich werden zwei Kriterien kombiniert, über die bislang der Verzicht auf die Prüfung der beiderseitigen Strafbarkeit begründet wurde.⁵⁹ Mit der alternativen Verknüpfung werden die Anforderungen, anders als bei den bestehenden Rechtsakten zur Einschränkung der beiderseitigen Strafbarkeit,

⁴⁸ Richtlinie 2014/41/EU (Fn. 6).

⁴⁹ Art. 11 Abs. 1 lit. e, g, h Richtlinie 2014/41/EU (Fn. 6).

⁵⁰ Art. 11 Abs. 1 lit. g i.V.m. Anhang D, Art. 11 Abs. 2 i.V.m. Art. 10 Abs. 2 lit. e Richtlinie 2014/41/EU (Fn. 6); in dem letztgenannten Fall sind auch besondere Eingriffsschwellen nach dem Recht des Vollstreckungsstaates nicht entsprechend anwendbar.

⁵¹ Vgl. auch die besonderen materiellen Eingriffsvoraussetzungen nach Art. 126ng, Art. 67 Abs. 1 der niederländischen StPO (Wetboek van Strafvordering) oder § 135 Abs. 2 Nr. 3 der österreichischen StPO; s. insoweit Böse, Assessment (*Fn.), S. 39 f.

⁵² S. auch die weiteren Bedenken in der Stellungnahme des Deutschen Anwaltvereins (Fn. 38), S. 12 f., und der Bundesrechtsanwaltskammer (Fn. 26), S. 9 (u.a. zum Fehlen eines ausdrücklich geregelten Verwertungsverbot).

⁵³ Vgl. Erwägungsgrund 12a des Verordnungsentwurfs, Rats-Dok. 15292/18, S. 4.

⁵⁴ Art. 5 Abs. 2 des Verordnungsentwurfs (Fn. 2).

⁵⁵ Art. 5 Abs. 4 des Verordnungsentwurfs (Fn. 2).

⁵⁶ Vgl. die Begründung des Kommissionsvorschlags für eine Verordnung (Fußn. 2), S. 16.

⁵⁷ S. dazu näher Böse, Assessment (*Fn.), S. 40.

⁵⁸ S. nur Art. 5 Abs. 2 und 3 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates: Mindesthöchststrafe von ein, zwei oder drei Jahren Freiheitsstrafe, ABl. EU L 335/1.

⁵⁹ Art. 11 Abs. 1 lit. g Richtlinie 2014/41/EU (Fn. 6).

noch weiter abgesenkt und damit nicht nur das Ziel verfehlt, hohe Anforderungen an einen Ermittlungseingriff zu formulieren, sondern noch einmal deutlich sichtbar, dass mit dem neuen Kooperationsinstrument nicht einmal grundlegende rechtshilferechtliche Sicherungen (beiderseitige Strafbarkeit) gewahrt werden.

VI. Defizite im gerichtlichen Rechtsschutz

Das neue Kooperationsinstrument hat schließlich auch gravierende Konsequenzen für den gerichtlichen Rechtsschutz; dies gilt sowohl für den betroffenen Nutzer (1.) als auch für den Adressaten der Herausgabeordnung (2.).

1. Rechtsbehelfe des betroffenen Nutzers

Der gerichtliche Rechtsschutz richtet sich im Ausgangspunkt nach dem Gegenstand der gerichtlichen Überprüfung, d.h. der hoheitlichen Maßnahme, die (möglicherweise) die Rechte des Betroffenen verletzt (Art. 47 Abs. 1 GRC). Da im Vollstreckungsstaat die Europäische Herausgabeordnung nicht durch eine eigene Entscheidung anerkannt wird, sondern diese unmittelbar rechtlich verbindlich ist, fehlt es im Vollstreckungsstaat bereits an einer Entscheidung (z.B. über die Bewilligung), die der betroffene Nutzer anfechten könnte. Aus der Sicht des Kommissionsvorschlages ist es daher folgerichtig, dass der betroffene Nutzer gerichtlichen Rechtsschutz gegen die Übermittlung „seiner“ Daten allein im Ausstellungsstaat erlangen kann.⁶⁰ Der Rechtsschutz erstreckt sich dabei auch auf die Frage, ob die Daten unter Verstoß gegen das Recht des Vollstreckungsstaates erlangt worden sind, soweit dieses von der Ausstellungsbehörde zu beachten ist (s. oben III., IV.2. zu Vorrechten und Immunitäten).⁶¹ In dieser Rechtsschutzkonzentration setzen sich damit allerdings auch die Nachteile fort, die durch die fehlende Beteiligung des Vollstreckungsstaates entstanden sind, nämlich die begrenzte Prüfungskompetenz (Vorrechte und Befreiungen; nicht: besondere Eingriffsschwellen) und die praktischen Schwierigkeiten einer Anwendung ausländischen Rechts.⁶² Anders als nach der ähnlichen Regelung bei der Europäischen Ermittlungsanordnung kann das Gericht im Ausstellungsstaat nämlich nicht an eine gerichtliche Entscheidung im Vollstreckungsstaat anknüpfen, mit der die Rechtswidrigkeit der dort erfolgten Beweiserhebung festgestellt wird.⁶³

2. Rechtsbehelfe des Service-Providers

Als Adressat einer Herausgabeordnung hat auch der Service-Provider Anspruch auf gerichtlichen Rechtsschutz (Art. 47 Abs. 1 GRC). Dies gilt zunächst für die

Entscheidung, mit der im Vollstreckungsstaat zur Durchsetzung der Herausgabeordnung eine Sanktion verhängt worden ist.⁶⁴ Das Gericht des Vollstreckungsstaates prüft allerdings nur die Rechtmäßigkeit der Vollstreckung bzw. der Sanktion. Die Rechtmäßigkeit der Europäischen Herausgabeordnung unterliegt nicht der gerichtlichen Kontrolle im Vollstreckungsstaat, da diese auch nicht von der Vollstreckungsbehörde geprüft wird.⁶⁵ Der gerichtliche Rechtsschutz ist auch insoweit akzessorisch und bezieht sich deshalb allein auf die Rechtmäßigkeit der Vollstreckung, nicht aber auf die Rechtmäßigkeit der Herausgabeordnung nach dem Recht des Ausstellungsstaates.⁶⁶

Der gerichtliche Rechtsschutz im Ausstellungsstaat ist allerdings nur insoweit geregelt, als der Kommissionsvorschlag bei einem drohenden Konflikt mit dem Recht eines Drittstaates, das die Übermittlung der angeforderten Daten untersagt, einen Überprüfungsmechanismus vorsieht.⁶⁷ Die allgemeine Bestimmung über gerichtliche Rechtsbehelfe soll hingegen nur auf Personen Anwendung finden, deren Daten angefordert werden.⁶⁸ Der Service-Provider hätte damit ausweislich des Vorschlags kein Recht, die Rechtmäßigkeit einer gegen ihn ergangenen Europäischen Herausgabeordnung (z.B. die Beachtung besonderer Eingriffsvoraussetzungen) im Ausstellungsstaat gerichtlich überprüfen zu lassen. Dieses Ergebnis ist mit dem Anspruch auf gerichtlichen Rechtsschutz (Art. 47 Abs. 1 GRC) schlechthin unvereinbar.⁶⁹

VII. Fazit

Mit der Europäischen Herausgabeordnung wird der ersuchte Mitgliedstaat (bzw. der Vollstreckungsstaat) weitgehend aus der strafrechtlichen Zusammenarbeit verdrängt. Dies ist nicht nur aus kompetenzrechtlichen Erwägungen (s. oben III.), sondern auch und vor allem mit Blick auf die grundlegende Schutzfunktion des Rechtshilfverfahrens schwerwiegenden Einwänden ausgesetzt, denn dieser Rückzug des Vollstreckungsstaates aus der Rechtshilfe und die dadurch ausgelösten Defizite im Grundrechtsschutz können weder durch eine Übernahme dieser Schutzfunktion durch den Ausstellungsstaat oder den privaten Service-Provider (s. oben IV. 2.) noch durch das vom Rat favorisierte Notifikationsmodell (s. oben IV.3) kompensiert werden. Diese Defizite setzen sich in einem Abbau individualschützender Rechtshilfemindernde (V.) und Lücken im gerichtlichen Rechtsschutz (VI.) fort.

Mit dieser Kritik soll die praktische Notwendigkeit, den grenzüberschreitenden Zugriff auf elektronische Beweismittel zu erleichtern und zu beschleunigen, keineswegs in

⁶⁰ Art. 17 des Verordnungsentwurfs (Fn. 2).

⁶¹ Art. 18 des Verordnungsentwurfs (Fn. 2); Art. 12a des Verordnungsentwurfs, Rats-Dok. 15292/18, S. 40.

⁶² Zu weiteren Kritikpunkten (u.a. Ineffektivität des Rechtsschutzes aufgrund nachträglicher Unterrichtung): Stellungnahme des Deutschen Anwaltvereins (Fn. 38), S. 10 f., und der Bundesrechtsanwaltskammer (Fn. 26), S. 5.

⁶³ Vgl. Art. 14 Abs. 7 Richtlinie 2014/41/EU (Fn. 6); s. dazu Böse, ZIS 2014, 152 (161).

⁶⁴ Art. 14 Abs. 10 S. 2 des Verordnungsentwurfs (Fn. 2).

⁶⁵ Vgl. die abschließende Liste der Gründe, aus denen eine Vollstreckung der Europäischen Herausgabeordnung abgelehnt werden kann, in Art. 14 Abs. 4 des Verordnungsentwurfs (Fn. 2).

⁶⁶ Vgl. insoweit Art. 5 Abs. 2, Abs. 4 des Verordnungsentwurfs (Fn. 2).

⁶⁷ Art. 15, 16 des Verordnungsentwurfs (Fn. 2); Art. 16 des Verordnungsentwurfs, Rats-Dok. 15292/18, S. 46 ff.

⁶⁸ Art. 17 Abs. 1 und 2 des Verordnungsentwurfs (Fn. 2); Art. 17 Abs. 1 des Verordnungsentwurfs, Rats-Dok. 15292/18, S. 48.

⁶⁹ Böse, Assessment (*Fn.), S. 42 f.

Abrede gestellt werden. Der dafür nach dem Kommissionsvorschlag zu entrichtende Preis, nämlich der Verzicht auf den durch den Vollstreckungsstaat gewährleisteten Grundrechtsschutz, erscheint dafür indes zu hoch. Ein solcher Schritt wäre allenfalls unter der Voraussetzung denkbar, dass für die materiellen Eingriffsvoraussetzungen ein unionsrechtlich harmonisierter Mindeststandard festgelegt wird, der einen effektiven Grundrechtsschutz gewährleistet (vgl. Art. 82 Abs. 2 lit. d AEUV).⁷⁰ Solange ein solcher Standard fehlt, ist die Einbindung des Vollstreckungsstaates ein unverzichtbares Element des Grundrechtsschutzes im Rahmen der grenzüberschreitenden Zusammenarbeit. Dabei sollte man sich auch vor Augen hal-

ten, dass der Ruf nach einer Beschleunigung und Erleichterung der grenzüberschreitenden Zusammenarbeit den Vollstreckungsstaat auch im Zusammenhang mit anderen Ermittlungsmaßnahmen (z.B. Einfrieren von Vermögensgegenständen⁷¹, heimliche grenzüberschreitende Datenerhebung⁷²) aus seiner Schutzfunktion verdrängen könnte. Diese Sorge sollte Grund genug sein, zunächst die bestehenden Kooperationsinstrumente, insbesondere die erst kürzlich von den Mitgliedstaaten umgesetzte Europäische Ermittlungsanordnung, daraufhin zu prüfen, ob und inwieweit die Möglichkeit besteht, die praktische Zusammenarbeit zu erleichtern und zu verbessern.⁷³

⁷⁰ Da der Vorschlag die Anordnungsvoraussetzungen nach dem jeweils anwendbaren nationalen Recht unberührt lässt, wird auch das mit dem Kommissionsvorschlag verfolgte Ziel, durch eine unionsweite Regelung Rechtssicherheit für Service-Provider und Nutzer zu gewährleisten, nicht erreicht, s. dazu Böse, Assessment (*Fn.), S. 43 ff.

⁷¹ Vgl. insoweit die Verordnung (EU) 2018/1805 des Europäischen Parlaments und des Rates vom 14.11.2018 über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen, ABl. EU L 303/1.

⁷² S. die entsprechenden Überlegungen im Rat, Rats-Dok. 9418/18, S. 2 f.

⁷³ Böse, Assessment (*Fn.), S. 47; s. auch die bereits vom Cybercrime Convention Committee erarbeiteten Empfehlungen und deren Umsetzung in den Vertragsstaaten (Fn. 5).