KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Maria Lesina

Europäische Herausgabe- und Sicherungsanordnung

Ludwig-Maximilians-Universität München
Betreuer: Prof. Dr. Mark Zöller
Abgabedatum: 26.10.2020

Inhaltsverzeichnis

I. Einleitung

Die fortschreitende Digitalisierung hat weitreichende Auswirkungen auf unseren Alltag. Heutzutage entstehen digitale Daten in nahezu jedem gesellschaftlichen Kontext.[1] Sie entstehen zum Beispiel durch die Nutzung von Social Media und Messenger-Diensten, bei der IP-Telefonie, beim bargeldlosen Bezahlen und bei der Verwendung von Smart Watches sowie Smart Home Systemen.[2] Wir leben in „den Zeiten des gläsernen Menschen“[3]. Noch nie zuvor lagen so viele Daten über uns vor. In der Zusammenschau haben diese Datenmengen eine große Aussagekraft.[4] Auch im Bereich der Kriminalität stellen E-Mail-, Messenger- und Social Media-Dienste wichtige Kommunikationsmittel dar.[5] Demgemäß haben Strafverfolgungsbehörden ein großes Interesse an den gespeicherten Daten.[6] Elektronische Beweismittel werden immer bedeutender für die Strafverfolgung.[7] Doch die zunehmende Digitalisierung bietet Strafverfolgungsbehörden nicht nur noch nie dagewesene Möglichkeiten bei der Aufklärung von Straftaten, sondern stellt diese auch vor neue Herausforderungen.[8] Die Behörden stehen bei der Erlangung und Sicherung dieser elektronischen Beweise vor zahlreichen rechtlichen und praktischen Hindernissen.[9] Digitale Daten sind nicht an einen bestimmten Ort gebunden und werden häufig auf Servern im Ausland gespeichert, sodass Ermittlungen zum Großteil grenzüberschreitend erfolgen müssen. Deshalb kommt es verstärkt auf eine internationale Zusammenarbeit an.[10] Doch die derzeit zur Verfügung stehenden Rechtsinstrumente der internationalen Zusammenarbeit sind nicht an die Flüchtigkeit von elektronischen Beweismitteln angepasst.[11] Der herkömmliche Rechtshilfeweg hat sich als zu umständlich und langwierig herausgestellt.[12] Deswegen ist in den letzten Jahren das Bedürfnis nach einem neuen Kooperationsinstrument entstanden.[13] So sieht z.B. *Burchard* in der Regelung des grenzüberschreitenden Zugriffs auf in der Cloud gespeicherte Daten „eine der drängendsten Aufgaben der Internetära“.[14]

Die Europäische Kommission hat im April 2018 einen Vorschlag für ein neues Kooperationsinstrument zum grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen unterbreitet.[15] Es handelt sich dabei um die „Europäische Herausgabe- und Sicherungsanordnung“. Die vorliegende Arbeit befasst sich umfassend mit den aktuellen „E-Evidence“-Gesetzgebungsvorschlägen der Europäischen Kommission. Der erste Teil dieser Arbeit beleuchtet zunächst einige strafprozessual relevante Besonderheiten elektronischer Beweismittel und die Unzulänglichkeiten der derzeit zur Verfügung stehenden Rechtsinstrumente für die internationale Zusammenarbeit in Strafsachen. Anschließend werden die grundlegenden Regelungen des Gesetzgebungsvorschlages dargestellt. Der zweite Teil der Arbeit setzt sich kritisch mit den Vorschlägen auseinander und erörtert eine Reihe rechtsstaatlicher Bedenken.

1 *Fährmann*, MMR 2020, 228.
2 *Fährmann*, MMR 2020, 228.
3 *Burchard*, Das Ende der Souveränität (und anderer Fundamentalprinzipien der Rechtshilfe)?, S. 1.
4 *Blechschmitt*, MMR 2018, 361.
5 *Gössling/Nagel*, ITRB 2019, 41.
6 *Fährmann*, MMR 2020, 228.
7 *Warken*, NZWiSt 2017, 289.
8 *Fährmann*, MMR 2020, 228.
9 *Gössling/Nagel*, ITRB 2019, 41.
10 *Gössling/Nagel*, ITRB 2019, 41.
11 *Hamel*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren, 2020, S. 107.
12 *Burchard* (Fn. 3), S. 1.
13 *Böse*, KriPoZ 2019, 140.
14 *Burchard* (Fn. 3), S. 1.
15 COM (2018) 225 final; COM (2018) 226 final.

II. Europäische Herausgabe- und Sicherungsanordnung

1. „E-Evidence“

a) Problemaufriss

Elektronische Beweismittel weisen eine Reihe von Besonderheiten auf, die ihre Erlangung und Sicherung erschweren. Ein wesentliches Kennzeichen elektronischer Daten ist ihre fehlende Körperlichkeit.[16] Herkömmliche Beweismittel befinden sich tatsächlich physisch auf dem Territorium eines Landes.[17] Daten hingegen sind nicht starr an einen Ort gebunden, vielmehr bestimmen vom Service-Provider generierte Algorithmen ihren Weg.[18] In der Regel bieten Service-Provider ihre Dienste weltweit an. Dabei haben sie meist eine Hauptniederlassung in einem Staat und einige weitere Niederlassungen in anderen Staaten. Die Datenspeicherorte sind jedoch unabhängig von diesen Niederlassungen verteilt.[19] Zudem findet die Speicherung elektronischer Daten nicht mehr zwingend als Gesamtheit an einem Ort statt, sondern erfolgt oftmals aus sicherheitsrelevanten und/oder unternehmerischen Gesichtspunkten in vielen Einzelteilen auf einer Vielzahl von Rechnern. Diese können dann weltweit verstreut sein, weshalb sich rechtliche und praktische Hürden für das Strafverfahren ergeben.[20] Möchten Strafverfolgungsbehörden auf Daten zugreifen, die im Ausland gespeichert sind, so stellen sich rechtliche Fragen hinsichtlich der Beachtung des Territorialitätsprinzips und der Beeinträchtigung der Souveränität des betroffenen ausländischen Staates.[21] Der herkömmliche Weg bei grenzüberschreitenden Ermittlungen in Strafsachen ist das Rechtshilfeverfahren. Befinden sich Beweismittel im Ausland, so können Strafverfolgungsbehörden ein traditionelles Rechtshilfeersuchen stellen, um mit Hilfe der Behörden des ausländischen Staates an diese Beweismittel zu gelangen.[22] Vor allem in Betracht der Flüchtigkeit von Daten hat sich jedoch das System der Rechtshilfe für den grenzüberschreitenden Zugriff auf elektronische Beweismittel als zu langsam und bürokratisch herausgestellt.[23] Elektronische Beweismittel sind durch ihre Volatilität gekennzeichnet und oft nur eine begrenzte Zeit verfügbar.[24] Oftmals ist Service-Providern die Löschung gespeicherter Daten aus Datenschutzgründen vorgeschrieben. Nur unter engen gesetzlichen Voraussetzungen kann eine längerfristige Sicherung der Daten erfolgen.[25] Zudem lassen sich elektronische Daten leicht und vor allem schnell verschieben. Zum Teil wird die permanente Ortsänderung der Daten automatisiert vom Service-Provider durchgeführt.[26] Diese Aspekte machen einen zügigen Zugriff auf die elektronischen Beweismittel erforderlich. Das Rechtshilfeverfahren kann jedoch durchschnittlich mehrere Monate andauern und ist damit nicht an die Besonderheiten der digitalen Welt angepasst.[27]

b) Europäische Ermittlungsanordnung

Wichtige Neuerungen für die grenzüberschreitende Sicherung von Beweisen im Rahmen von Strafermittlungen

16 *Warken*, NZWiSt 2017, 289 (290).
17 *Hamel*, in: Hoven/Kudlich, S. 105.
18 *Hamel*, in: Hoven/Kudlich, S. 105.
19 *Hamel*, in: Hoven/Kudlich, S. 105.
20 *Warken*, NZWiSt 2017, 289 (290).
21 *Warken*, NZWiSt 2017, 289 (295).
22 *Gössling/Nagel*, ITRB 2019, 41.
23 *Mosna*, ZStW 2019, 808 (811).
24 *Hamel*, in: Hoven/Kudlich, S. 104.
25 *Warken*, NZWiSt 2017, 289 (297).
26 *Warken*, NZWiSt 2017, 289 (297).
27 *Warken*, NZWiSt 2017, 289 (297).

brachte die im April 2014 verabschiedete Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen.[28] In Deutschland wurde diese Richtlinie vornehmlich durch Änderungen im Gesetz über die internationale Rechtshilfe in Strafsachen im Jahr 2017 umgesetzt.[29] Die Europäische Ermittlungsanordnung ersetzt innerhalb der Europäischen Union das klassische Rechtshilfeabkommen in Strafsachen und ermöglicht den Strafverfolgungsbehörden der Mitgliedstaaten, die Sammlung und Weitergabe von Beweismitteln aller Art in einem anderen Mitgliedstaat zu verlangen. Zur Gewährleistung einer raschen und effektiven Zusammenarbeit zwischen den Mitgliedstaaten wurden verbindliche Fristen und Formblätter eingeführt.[30] Innerhalb von 30 Tagen nach Eingang einer Ermittlungsanordnung muss der Mitgliedstaat entscheiden, ob er der Anordnung Folge leistet. Die Vollstreckung einer Ermittlungsanordnung kann unter bestimmten Voraussetzungen verweigert werden,[31] beispielsweise wenn die Anordnung wesentlichen Rechtsgrundsätzen des Landes zuwiderläuft oder nationalen Sicherheitsinteressen schadet.[32] Entscheidet sich die Vollstreckungsbehörde, die Ermittlungsmaßnahme anzuerkennen, muss die Ermittlungsmaßnahme spätestens 90 Tage nach Erlass durchgeführt werden.[33] Diese Fristen sind jedoch, wenn man die Flüchtigkeit von Daten bedenkt, immer noch zu lang für den grenzüberschreitenden Zugriff auf elektronische Beweismittel.

c) „E-Evidence" – Vorschläge der Europäischen Kommission

Am 17. April 2018 hat die Europäische Kommission ihre Gesetzgebungsvorschläge zum grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen präsentiert. Diese bestehen aus der Verordnung für Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (im Folgenden Verordnungsvorschlag) und der Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.[34] Das Gesetzesvorhaben soll einen Rechtsrahmen für die direkte Zusammenarbeit von Ermittlungsbehörden und Service-Providern schaffen.[35] Die Erhebung und Sicherung von elektronischen Beweismitteln in der EU soll dadurch erleichtert und effizienter gestaltet werden.[36] Der Unterschied gegenüber der bisherigen internationalen Zusammenarbeit in Strafsachen besteht darin, dass die Behörde eine Anordnung unmittelbar an den in einem anderen Mitgliedstaat operierenden Service-Provider, besser gesagt an dessen Vertreter, richten kann, ohne die jeweilige nationale Behörde einzuschalten.[37] Der Service-Provider ist daraufhin zur Übermittlung bzw. vorläufigen Sicherung der Daten verpflichtet, ohne dass es einer vorherigen Entscheidung der jeweiligen nationalen Behörde bedarf.[38] So wird der umständliche und bürokratische Behördenweg der Rechtshilfe umgangen.[39]

aa) Der Vorschlag für eine Verordnung über Europäische Herausgabeordnungen und Sicherungsanordnungen

Kompetenzrechtlich ist der Verordnungsvorschlag gestützt auf Art. 82 AEUV, der die justizielle Zusammenarbeit

28 Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen.
29 *Thomae*, in: Hoven/Kudlich, S. 139.
30 Art. 12 Abs. 3 und 4 RL 2014/41/EU.
31 *Thomae*, in: Hoven/Kudlich, S. 139.
32 Art. 12 Abs. 3 und 4 RL 2014/41/EU.
33 *Thomae*, in: Hoven/Kudlich, S. 139.
34 COM (2018) 225 final; COM (2018) 226 final.
35 *Gössling/Nagel*, ITRB 2019, 41 (44).
36 *Gössling/Nagel*, ITRB 2019, 41.
37 *Gössling/Nagel*, ITRB 2019, 41 (44).
38 *Böse*, KriPoZ 2019, 140 (143).
39 *Böse*, KriPoZ 2019, 140 (141).

basierend auf dem Grundsatz der gegenseitigen Anerkennung regelt.[40] Zuständige Justizbehörden sollen direkt von einem Service-Provider, der in der Union elektronische Dienstleistungen anbietet, verlangen können, elektronische Beweismittel im Hinblick auf ein späteres Herausgabeersuchen zu sichern (Sicherungsanordnung) oder herauszugeben (Herausgabeanordnung), ungeachtet, wo die Daten gespeichert sind oder wo der Dienst sitzt.[41] Die vom Anordnungsstaat erlassene Herausgabe- oder Sicherungsanordnung entfaltet eine transnationale Bindungswirkung, ohne dass es einer vorherigen Anerkennung durch eine Justizbehörde des Vollstreckungsstaates bedarf.[42] Der Verordnungsvorschlag stellt klar, dass der Zweck der Europäischen Herausgabe- und Sicherungsanordnung nicht die Verhütung von Straftaten ist, sondern die effektive Strafverfolgung.[43] Die Verordnung würde die Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen nicht ersetzen, sondern nur ergänzen. Mit der Europäischen Herausgabe- und Sicherungsanordnung soll den Strafverfolgungsbehörden ein zusätzliches Rechtsinstrument zur Verfügung stehen, dass die Besonderheiten der digitalen Welt berücksichtigt.[44]

(1) Anwendungsbereich

Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen umfassen die Herausgabe und Sicherung gespeicherter Daten von einem Service-Provider und dürfen nur für Strafverfahren während des Ermittlungs- und des Gerichtsverfahrens erlassen werden.[45] Der Verordnungsvorschlag erstreckt sich auf alle Service-Provider, die ihre Dienste in der EU anbieten. Der Begriff „Service-Provider" wird in Art. 2 Nr. 3 des Verordnungsvorschlages definiert. Danach ist „Service-Provider" jede natürliche oder juristische Person, die „elektronische Kommunikationsdienste im Sinne des Artikels 2 Absatz 4 der Richtlinie über den europäischen Kodex für die elektronische Kommunikation, Dienste der Informationsgesellschaft im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates, bei denen die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist, einschließlich sozialer Netzwerke, Online-Marktplätze, die Transaktionen zwischen ihren Nutzern erleichtern, und anderen Anbietern von Hosting-Diensten, Internetdomänennamen- und IP-Adressendienste wie IP-Adressenanbieter, Domänennamen-Register, Domänennamen-Registrierungsstellen und damit verbundene Datenschutz- und Proxy-Dienste anbietet." Von der Verordnung sind ausdrücklich auch Service-Provider erfasst, die nicht in der EU niedergelassen sind.[46] Vorausgesetzt ist lediglich das Anbieten von Dienstleistungen in EU. Durch das Anbieten von Diensten in der Union ergeben sich für die Service-Provider zahlreiche Vorteile. Das rechtfertigt laut Kommissionsvorschlag die Tatsache, dass alle Service-Provider, die davon profitieren, gleichermaßen der Verordnung unterliegen. Durch die Ausweitung des Anwendungsbereiches sollen nicht nur gleiche Ausgangsbedingungen für die Teilnehmer derselben Märkte gelten, sondern auch eine Strafbarkeitslücke vermieden werden.[47]

(2) Voraussetzungen für den Erlass einer Herausgabe- und Sicherungsanordnung

Es gibt eine Reihe von Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung. Diese sind in Art. 5 des Verordnungsvorschlages festgelegt. Die Anordnung darf nur erlassen werden, wenn dies im Einzelfall notwendig und verhältnismäßig ist. Darüber hinaus kann sie nur erlassen werden, wenn im Anordnungsstaat in einer vergleichbaren innerstaatlichen Situation eine ähnliche Maßnahme zur Verfügung stünde. Dass sie auch im

40 *Hamel*, in: Hoven/Kudlich, S. 111.
41 *Basar,* jurisPR-StrafR 5/2019, Anm. 1.
42 *Böse*, KriPoZ 2019, 140 (141).
43 COM (2018) 225 final, S. 8.
44 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
45 Art. 3 Abs. 2 Verordnungsvorschlag, COM (2018) 225 final.
46 Art. 3 Verordnungsvorschlag, COM (2018) 225 final.
47 *Tosza*, NJECL 2020, 161 (172).

Vollstreckungsstaat rechtmäßig wäre, ist allerdings nicht erforderlich.

Der Vorschlag unterscheidet zwischen verschiedenen Datenkategorien. Je nach Datenkategorie gelten unterschiedliche Anforderungsmaßstäbe für den Erlass einer Herausgabeanordnung. Es können Teilnehmerdaten, Zugangsdaten, Transaktionsdaten und Inhaltsdaten von den zuständigen Behörden mit einer Europäischen Herausgabeanordnung eingeholt werden.[48] Diese werden in Art. 2 Nr. 7, 8, 9 und 10 des Verordnungsvorschlages legaldefiniert.

Als Teilnehmerdaten werden Daten kategorisiert, die Informationen über die Identität einer Person offenbaren. Dazu zählen beispielsweise der Name, das Geburtsdatum, die Postanschrift, Rechnungs- und Zahlungsdaten, die Telefonnummer und die IP-Adresse des Kunden. Auch die Art der Dienstleistung und ihre Dauer sind von dieser Datenkategorie umfasst.[49] Zugangsdaten umfassen Daten, die sich auf den Beginn und die Beendigung einer Zugangssitzung für einen Dienst beziehen, ausschließlich zu dem Zweck, den Benutzer des Dienstes zu identifizieren. Dazu gehören beispielsweise das Datum und die Uhrzeit der Nutzung oder Anmeldung und Abmeldung vom Dienst in Verbindung mit der IP-Adresse des Nutzers.

Bei Transaktionsdaten handelt es sich um Daten über die Erbringung einer von einem Service-Provider angebotenen Dienstleistung, die Kontext- oder Zusatzinformationen über eine solche Dienstleistung liefern und von einem Informationssystem des Service-Providers generiert oder verarbeitet werden. Das können z.B. Sende- und Empfangsdaten einer Nachricht sein oder auch Daten zum Standort des Geräts.

Inhaltsdaten sind alle in einem digitalen Format gespeicherten Daten wie Text, Sprache, Videos, Bilder und Tonaufzeichnungen, ausgenommen von Teilnehmer-, Zugangs- oder Transaktionsdaten.[50] Alle diese Datentypen enthalten personenbezogene Daten und fallen somit unter die Garantien im Rahmen der Datenschutzvorschriften der EU.[51]

Eine Herausgabeanordnung für Teilnehmer- und Zugangsdaten kann für jede Straftat erlassen werden. Bei Transaktions- und Inhaltsdaten liegen die Anforderungen etwas höher. Herausgabeanordnungen für Transaktions- und Inhaltsdaten können nur für Straftaten erlassen werden, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden oder die mittels eines Informationssystems begangen wurde.[52] Bei dem Erlass einer Europäischen Herausgabe- oder Sicherungsanordnung muss stets eine justizielle Behörde entweder als anordnende oder als validierende Behörde tätig werden. Für Anordnungen zur Herausgabe von Transaktions- oder Inhaltsdaten ist ein Richter oder ein Gericht erforderlich. Handelt es sich bei den betreffenden Daten um Teilnehmer- oder Zugangsdaten, so kann die Validierung auch von einem Staatsanwalt übernommen werden.[53]

Die Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung ähneln den Voraussetzungen für die Europäische Herausgabeanordnung. Eine Europäische Sicherungsanordnung kann jedoch unabhängig vom abgefragten Datentyp für jede Straftat erlassen werden und es genügt, wenn ein Staatsanwalt diese Anordnung validiert.

(3) Ausführung und Fristen

Die Herausgabe- und Sicherungsanordnungen werden unter Verwendung spezieller Formblätter (EPOC und

48 Art. 5 Abs. 3 Verordnungsvorschlag, COM (2018) 225 final.
49 Art. 2 Nr. 7 Verordnungsvorschlag, COM (2018) 225 final.
50 Art. 2 Nr. 10 Verordnungsvorschlag COM (2018) 225 final.
51 Art. 2 Verordnungsvorschlag COM (2018) 225 final.
52 *Von Galen*, in: Hoven/Kudlich, S. 127.
53 Art. 4 Verordnungsvorschlag, COM (2018) 225 final.

EPOC-PR) direkt an den Service-Provider übermittelt.[54] Diese Zertifikate enthalten Informationen zu den angewendeten Strafvorschriften, zu den konkret angeforderten Daten und zur Anordnungsbehörde und werden unmittelbar an den vom Vertreter des Service-Providers entsandt.

Für die Ausführung einer Herausgabeanordnung ist eine verbindliche Frist von zehn Tagen vorgesehen. In Eilfällen kann diese Frist gem. Art. 9 Abs. 2 des Verordnungsvorschlages auf sechs Stunden verkürzt werden.[55] Im Falle einer Sicherungsanordnung ist der Service-Provider dazu verpflichtet die betreffenden Daten vorerst für 60 Tage zu sichern.[56]

(4) Vertraulichkeit und Nutzerinformationen

Bei der Ausführung der jeweiligen Anordnung ist der Service-Provider gemäß Art. 11 des Verordnungsvorschlages verpflichtet, die Vertraulichkeit der gesicherten bzw. herausgegebenen Daten zu garantieren. Die Notifizierung der Person, deren Daten angefordert wurden, kann durch die Anordnungsbehörde untersagt werden. In diesem Fall ist die Anordnungsbehörde nach Art. 11 Abs. 2 des Verordnungsvorschlages verpflichtet die betroffene Person selbst zu informieren, wenn es sich bei der betreffenden Anordnung um eine Herausgabeanordnung handelt. Um eine Behinderung des Verfahrens zu vermeiden, ist es der Anordnungsbehörde jedoch gestattet, diese Unterrichtung aufzuschieben. Handelt es sich bei der Maßnahme um eine Sicherungsanordnung, so hat eine Information der betroffenen Personen nicht zu erfolgen.[57]

(5) Ablehnungsgründe

Der Service-Provider kann die Anordnung unter bestimmten Voraussetzungen ablehnen. Die Ablehnungsgründe sind für die Herausgabeanordnung in Art. 9 des Verordnungsvorschlages und für die Sicherungsanordnung in Art. 10 des Verordnungsvorschlages aufgezählt. Der Service-Provider kann der Anordnung entgegentreten, wenn er nicht in den persönlichen Anwendungsbereich der Verordnung fällt, ihm die Ausführung aus tatsächlichen Gründen unmöglich ist oder das Formular unvollständig oder fehlerhaft ausgefüllt ist. In diesem Fall wird der Service-Provider gleichwohl verpflichtet, die Anordnungsbehörde darüber in Kenntnis zu setzen und zunächst um „Klarstellung“ zu bitten. Wendet der Service-Provider ein, dass eine Herausgabeanordnung offenkundig gegen die Charta der Grundrechte der Europäischen Union (GRC) verstößt oder offensichtlich missbräuchlich ist, so hat er die Behörde des Vollstreckungsstaates zu kontaktieren. Diese kann dann nach Art. 9 Abs. 5 des Verordnungsvorschlages die Anordnungsbehörde um Klarstellung ersuchen. Entscheidet sich die Vollstreckungsbehörde davon abzusehen, so ist die Anordnungsbehörde dem Service-Provider gegenüber nicht verpflichtet, sich mit dessen Bedenken auseinanderzusetzen.[58] Darüber hinaus kann der Service-Provider die Anordnung ablehnen, wenn die Befolgung einer Europäischen Herausgabeanordnung im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats steht.[59] Die Geltendmachung dieses Ablehnungsgrunds erfordert einen begründeten Einwand durch den Service-Provider und führt, sofern die Anordnungsbehörde die Anordnung aufrechterhält, zu einer Prüfung durch ein Gericht des Anordnungsstaats. Nur in dem Fall, dass die Rechtsvorschrift des Drittstaats den Grundrechtsschutz betrifft, sind dessen Behörden zu informieren, und deren etwaiger Widerspruch gegen eine Herausgabeanordnung zu beachten.[60]

54 Art. 8 Verordnungsvorschlag, COM (2018) 225 final.
55 *Gössling/Nagel*, ITRB 2019, 41 (45).
56 Art. 10 Verordnungsvorschlag, COM (2018) 225 final.
57 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
58 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
59 Art. 15 Verordnungsvorschlag, COM (2018) 225 final.
60 *Brodowski*, ZIS 2018, 493 (503).

(6) Vollstreckungsverfahren und Sanktionen

Verweigert der Service-Provider die Anordnung, so kommt dem Staat, in dem der betroffene Service-Provider niedergelassen ist, die Rolle zu, eine Sanktion zu verhängen und die Anordnung zu vollstrecken.[61] Dem Service-Provider drohen in diesem Fall Strafen von bis zu 2 % seines globalen Jahresumsatzes. [62]

(7) Rechtsschutz

Gem. Artikel 17 des Verordnungsvorschlages haben Verdächtige und Beschuldigte, deren Daten im Wege einer Europäischen Herausgabeanordnung eingeholt wurden, unbeschadet der nach der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 verfügbaren Rechtsbehelfe das Recht, während des Strafverfahrens, für das die Anordnung erlassen wurde, wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen. Personen, deren Daten angefordert wurden, bei denen es sich aber nicht um Verdächtige oder Beschuldigte in einem Strafverfahren handelt, haben ebenfalls ein Recht auf einen Rechtsbehelf. Der Rechtsbehelf kann nur vor einem Gericht im Anordnungsstaat eingelegt werden. Betroffenen einer Sicherungsanordnung stehen keine spezifischen Rechtsbehelfe zur Verfügung.

bb) Der Vorschlag für eine Richtlinie zur Bestellung von Vertretern

Ergänzend zum Verordnungsvorschlag hat die Europäische Kommission einen Vorschlag für eine Richtlinie zur Bestellung von Vertretern unterbreitet.[63] Der Vorschlag stützt sich auf Art. 53 und 62 AEUV, die „den Erlass von Maßnahmen zur Koordinierung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung und Erbringung von Dienstleistungen vorsehen".[64] Ziel dieser Richtlinie ist es, zu bestimmen, an wen die Behörden der Mitgliedstaaten Anordnungen zur Erlangung von Beweismitteln, die sich im Besitz von Service-Providern befinden, richten können.[65] Die Zustellung gerichtlicher Anordnungen an Service-Provider soll über einen Vertreter erfolgen. Jeder Service-Provider, der seine Dienste in mehreren Mitgliedstaaten der EU anbietet, soll mindestens einen Vertreter in einem dieser Mitgliedstaaten benennen, an den die gerichtlichen Anordnungen adressiert werden können. Diese Vertreter sind dann im Namen der Service-Provider rechtlich dafür verantwortlich, dass den gerichtlichen Anordnungen und Beschlüssen nachgekommen wird. Das soll für mehr Rechtssicherheit sorgen und etwaige Hindernisse, bei der Zustellung von Anordnungen an Service-Provider verhindern.[66]

2. Kritische Auseinandersetzung mit den E-Evidence-Gesetzgebungsvorschlägen

Trotz des anzuerkennenden Bedarfs an einem schnellen grenzüberschreitenden Zugang zu elektronischen Beweismitteln bestehen erhebliche rechtstaatliche Bedenken gegen die geplanten Regelungen.[67] Für die Erlangung und Verwertung elektronischer Beweismittel gelten „die allgemeinen Verfahrensgrundrechte und -prinzipien, wie sie sich aus dem Rechtsstaatsprinzip oder ausdrücklich aus dem Grundgesetz, der GRC und der Konvention zum Schutz der Menschenrechte und der Grundfreiheiten (EMRK) ergeben".[68]

61 *Niekrenz*, Juridikum 2020, 160 (164).
62 *Thomae*, in: Hoven/Kudlich, S. 142.
63 COM (2018) 226 final.
64 COM (2018) 226 final, S. 5.
65 COM (2018) 226 final, S. 3.
66 COM (2018) 226 final, S. 3 f.
67 DAV, Stellungnahme Nr. 42/2018, S. 7.
68 *Warken*, NZWiSt 2017, 289 (292).

Die E-Evidence Gesetzgebungsvorschläge könnten eine unverhältnismäßige Beeinträchtigung der in der GRC garantierten Rechte darstellen.
Im Folgenden werden einige rechtstaatliche Bedenken gegenüber dem Verordnungsvorschlag geschildert und das Ausmaß der Grundrechts- und Interessenbeeinträchtigung dargestellt.

a) Verlust der innerstaatlichen justiziellen Überprüfungsinstanz

Die direkten Adressaten von Herausgabe- (bzw. Sicherungs-)Anordnungen sind die privaten Service-Provider bzw. deren Vertreter. Sie haben nach Art. 9 des Verordnungsvorschlages eine (oberflächliche) Rechtskontrolle durchzuführen.[69] Eine staatliche Überprüfungsmöglichkeit durch den Vollstreckungsstaat ist jedoch nicht vorgesehen. So werden hoheitliche Aufgaben privaten Unternehmen auferlegt, was kritisch zu sehen ist.[70] Denn die fehlende Einbeziehung von Justizbehörden führt zu einer mangelnden Kontrolle des Grundrechtschutzes. Die Service Provider müssen die Anordnung unter der Androhung von Strafzahlungen binnen knapp bemessener Fristen ausführen.[71] Fraglich ist, ob es unter solchen Bedingungen überhaupt zu einer umfassenden rechtlichen Prüfung der Anordnungen durch den Service-Provider kommen kann.[72] Die Prüfungsmöglichkeiten der Service-Provider sind zudem stark beschränkt. Denn ein etwaiger Grundrechtsverstoß kann nur auf der Grundlage der im zugesendeten Zertifikat enthaltenen Informationen überprüft werden.[73] Diese sind für eine rechtliche Prüfung wohl kaum aussagekräftig. So sind gemäß Art. 8 des Verordnungsvorschlages die komplette Begründung in Bezug auf die Notwendigkeit und Verhältnismäßigkeit oder weitere Einzelheiten zu dem Fall gerade nicht Bestandteil des Zertifikats. Unter diesen Umständen erscheint eine umfassende Grundrechtsprüfung schwierig.
Private Unternehmen handeln zudem meist aus wirtschaftlichen Überlegungen. Da dem Service-Provider durch die Verordnung bei Nichtbefolgung der Anordnungen Strafzahlungen drohen, wird dieser kaum gewillt sein, der Anordnungsbehörde zu widersprechen und sich dem Haftungsrisiko auszusetzen. [74]

b) Fehlende Benachrichtigungspflichten und Fehlen effektiver Rechtsmittel

Das neue Kooperationsinstrument weist zudem gravierende Defizite im gerichtlichen Rechtschutz auf.[75] Das betrifft sowohl die betroffenen Nutzer als auch die Service-Provider.

aa) Rechtsbehelfe der Betroffenen
Nach dem Verordnungsvorschlag sind die Betroffenen von Sicherungsanordnungen nicht über die Maßnahme in Kenntnis zu setzen, wenn der Sicherungsanordnung keine Herausgabeanordnung folgt.[76]
Die fehlende Benachrichtigungspflicht wird in dem Vorschlag mit dem Fehlen eines entsprechenden Rechtsbehelfes gegen Sicherungsanordnungen begründet.[77] Das ist wenig überzeugend. Eine Sicherungsanordnung stellt zwar insgesamt einen geringfügigeren Eingriff als die Herausgabeanordnung dar, doch die Tatsache, dass es sich dabei

69 *Burchard*, ZIS 2018, 249 (265).
70 DAV, Stellungnahme Nr. 42/2018, S. 7.
71 *Thomae*, in: Hoven/Kudlich, S. 142.
72 *Brodowski*, ZIS, 2018, 493 (503).
73 *Burchard*, ZIS 2018, 249 (265).
74 DAV, Stellungnahme Nr. 42/2018, S. 7.
75 *Böse*, KriPoZ 2019, 140 (143).
76 DAV, Stellungnahme Nr. 42/2018, S. 9.
77 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.

um eine faktisch heimliche Maßnahme handelt, spricht für eine hohe Eingriffsintensität.[78] Die Sicherung personenbezogener Daten ohne Kenntnis des Betroffenen ist eine Beeinträchtigung der in Art. 7 und Art. 8 GRC garantierten Grundrechte auf die Achtung des Privatlebens und den Schutz personenbezogener Daten. Dem Betroffenen einer Sicherungsanordnung müsste folglich das Recht auf einen wirksamen Rechtsbehelf gem. Art. 47 Abs. 1 GRC zustehen.

Betroffene einer Herausgabeanordnung müssen zwar über die Maßnahme in Kenntnis gesetzt werden, die Notifizierung kann jedoch aufgeschoben werden, wenn der Anordnungsstaat das für erforderlich hält, um das Verfahren nicht zu gefährden. Die fehlende Kenntnis des Betroffenen führt dazu, dass er rechtlich gar nicht gegen die Maßnahme vorgehen kann, auch wenn ihm Rechtsbehelf zustehen würde.[79] Das stellt eine unverhältnismäßige Beeinträchtigung von Art. 47 Abs. 1 GRC dar.

Zu kritisieren ist weiterhin, dass der betroffene Nutzer den gerichtlichen Rechtsschutz gegen die Übermittlung seiner Daten allein im Anordnungsstaat erlangen kann.[80] Das kann diesen vor einige Hindernisse stellen und ist eine unverhältnismäßige Belastung des Betroffenen.

bb) Rechtsbehelfe des Service-Providers

Der Service-Provider als der direkte Adressat einer Herausgabe- oder Sicherungsanordnung hat nach Art. 47 Abs.1 GRC auch einen Anspruch auf gerichtlichen Rechtsschutz. Denn gemäß Art. 47 Abs.1 GRC hat jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, einen wirksamen Rechtsbehelf einzulegen. Auch juristische Personen sind davon umfasst, soweit ihnen ein Recht zusteht.[81]

Service-Provider werden in ihrem Recht auf unternehmerische Freiheit (Art. 16 GRC) verletzt, indem sie Daten ihrer Nutzer herausgeben müssen. Darüber hinaus stellt die Sanktionierung bei Nichtbefolgung der Anordnung einen Eingriff in das Eigentumsrecht (Art. 17 GRC) dar. Nach dem Verordnungsvorschlag hat der Service-Provider jedoch kein Recht, die Rechtmäßigkeit einer gegen ihn ergangenen Europäischen Herausgabeanordnung im Ausstellungsstaat gerichtlich überprüfen zu lassen.[82] Er kann lediglich die Rechtmäßigkeit der Sanktion rechtlich prüfen lassen.

c) Unzureichender Schutz besonderer Vertrauensverhältnisse

Zu kritisieren ist weiterhin, dass besondere Vertrauensverhältnisse durch den Kommissionsentwurf nicht ausreichend geschützt werden. Sie können nicht als Versagungsgrund geltend gemacht werden.[83] So gefährdet die Verordnung unter anderem den Schutz der Anwalt-Mandanten-Kommunikation, aber auch Journalisten, Politiker, Oppositionelle und Ärzte sind dadurch beeinträchtigt.[84] Denn genau diese Personengruppen sind auf den Schutz ihrer Daten angewiesen und wählen ihren Datenspeicherort mit Bedacht. Bestimmte Cloudmodelle beruhen gerade darauf, dass Daten ihrer Nutzer an Orten sicher gespeichert werden, wo die Datenschutzstandards hoch sind.[85] Der Verordnungsvorschlag verkennt die Bedeutung solcher „Datenschutzhäfen“[86] und bietet diesen schützenswerten Personengruppen keinen ausreichenden Schutz.

78 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.
79 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.
80 *Böse*, KriPoZ 2019, 140 (143).
81 Art. 47 GRC
82 *Böse*, KriPoZ 2019, 140 (143).
83 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
84 DAV, Stellungnahme Nr. 42/2018, S. 12 f.
85 *Burchard*, ZRP 2019, 164 (165).
86 *Burchard*, ZRP 2019, 164 (165).

Das „digitale Asyl“ [87] wird Betroffenen genommen, indem für diese nur die Immunitäten und Vorrechte des Strafverfolgungsstaats gelten sollen, also nicht die Datenschutzrechte am Speicherort.[88]

d) Doppelbestrafung des Adressaten, der die Vollstreckung verweigert

Von Galen kritisiert die Tatsache, dass es zu einer Doppelbestrafung des Service-Providers kommen kann, wenn dieser die Vollstreckung einer Herausgabeanordnung hartnäckig verweigert.[89]
Wird die Herausgabeanordnung durch den Service-Provider nicht oder nicht korrekt ausgeführt oder verstößt er gegen die Pflicht, die Durchführung der Herausgabeanordnung gegenüber den Betroffenen vertraulich zu halten, so wird dieses Verhalten gem. Art. 13 des Verordnungsvorschlages sanktioniert.[90] Befolgt der Service-Provider die Herausgabeanordnung nicht, soll die Vollstreckung der Anordnung nach Art. 14 des Verordnungsvorschlages durch eine nationale Vollstreckungsbehörde erfolgen. Sollte der Adressat seiner Pflicht, die Anweisung der Vollstreckungsbehörde zu befolgen, nicht nachgehen, so kann er ein weiteres Mal von der Vollstreckungsbehörde sanktioniert werden.[91] Der Adressat, der also beharrlich die Ausführung der Herausgabeanordnung ablehnt – zunächst gegenüber der Anordnungsbehörde und dann gegenüber der Vollstreckungsbehörde – kann wegen derselben Verweigerungshaltung zweimal bestraft werden.[92]
Von Galen sieht darin einen Verstoß gegen den internationalen anerkannten Grundsatz ne bis in idem.[93] Dieser Grundsatz ist in Art. 50 GRC festgelegt. Gemäß Art. 50 GRC darf niemand wegen einer Straftat, derentwegen er bereits in der Union nach dem Gesetz rechtskräftig verurteilt oder freigesprochen worden ist, in einem Strafverfahren erneut verfolgt oder bestraft werden. Die hartnäckige Weigerung der Anordnung Folge zu leisten, kann durchaus als eine einheitliche Tat angesehen werden.[94] Folglich kann den Bedenken von *von Galen* zugestimmt werden.

e) Verzicht auf beidseitige Strafbarkeit

Zu kritisieren ist weiterhin, dass in dem Verordnungsvorschlag das Erfordernis beidseitiger Strafbarkeit im Gegenteil zur Europäischen Ermittlungsanordnung nicht als Erlassvoraussetzung für europäische Herausgabe- und Sicherungsanordnungen vorgesehen ist.[95] Die nationalen Strafrechtssysteme der Mitgliedsstaaten der EU sind in weiten Teilen unterschiedlich ausgestaltet.[96] So kann es dazu kommen, dass beispielsweise maltesische Behörden von einem deutschen Service-Provider die Herausgabe von Daten für ein Strafverfahren anordnen, das einen Schwangerschaftsabbruch betrifft, der in Deutschland allerdings legal wäre.[97] Es würde sinnvoller erscheinen, der europäische Gesetzgeber würde in einem Katalog die Straftaten festlegen, für welche die Verordnung gilt.[98]

87 *Niekrenz*, Juridikum 2020, 160 (167).
88 *Burchard,* ZRP 2019, 164 (165).
89 *Von Galen*, in: Hoven/Kudlich, S. 133.
90 *Von Galen*, in: Hoven/Kudlich, S. 133.
91 *Von Galen*, in: Hoven/Kudlich, S. 133.
92 *Von Galen*, in: Hoven/Kudlich, S. 133.
93 *Von Galen*, in: Hoven/Kudlich, S. 133.
94 *Von Galen*, in: Hoven/Kudlich, S. 133.
95 *Niekrenz*, Juridikum 2020, 160 (165).
96 *Hecker*, Europäisches Strafrecht, 5. Aufl. (2015), Rn. 5.
97 *Niekrenz*, Juridikum 2020, 160 (165).
98 *Thomae*, in: Hoven/Kudlich, S 142.

f) Zu weitreichender Anwendungsbereich

Wie bereits oben dargelegt, muss die Straftat, zu deren Verfolgung eine Herausgabeanordnung auf den Zugriff von Transaktions- und Inhaltsdaten ergeht, nach dem Recht des Ausstellungsstaates mit einem Höchstmaß von mindestens drei Jahren Freiheitsstrafe geahndet werden können.[99] Fraglich ist, ob diese Voraussetzung zur Verhältnismäßigkeit der Grundrechtseingriffe beiträgt. Denn eine Mindesthöchststrafe von drei Jahren ist bei einer Vielzahl von Straftaten vorgesehen, die keinesfalls nur den Bereich der schweren Kriminalität umfassen.[100] So würde zum Beispiel in Deutschland der Tatbestand des einfachen Diebstahls (§ 242 StGB) oder der Körperverletzung (§223 StGB) darunterfallen. Ob für diese Straftaten eine grenzüberschreitende Anordnung zur Herausgabe sensiblerer Daten verhältnismäßig wäre, ist allerdings zweifelhaft. Bloße Bagatelldelikte müssten von dem Anwendungsbereich ausgenommen werden.[101]

g) Folgen der Entterritorialisierung der Cloud

Herkömmlich werden Zugriffsmöglichkeiten auf Daten vom Datenspeicherort abhängig gemacht (Territorialitätsprinzip). Der Verordnungsvorschlag beruht jedoch auf der Annahme einer umfassenden Entterritorialisierung der Cloud.[102] Nach dem Kommissionsvorschlag wird die Zugriffsmöglichkeit auf Daten davon abhängig gemacht, ob der Service-Provider im Inland seine Dienste anbietet (Marktortprinzip). [103] Der Datenspeicherort spielt dabei keine Rolle.
Dies wird unter anderem mit dem Argument begründet, dass es Nutzern „egal“ wäre, wo ihre Daten abgespeichert werden. Diese Annahme trifft jedoch, wie bereits oben dargestellt, nicht zu. Zudem verletzen unilaterale Beibringungsanordnungen die Territorialhoheit des Staates des Serverstandortes, was zu Vertrauenskonflikten führen kann.[104]
Die EU sollte darüber hinaus berücksichtigen, dass wenn europäische Strafverfolger von Service-Providern aus Drittländern, die in der EU aktiv sind, die Herausgabe sämtlicher Daten verlangen dürfen, diese das gem. dem Reziprozitätsprinzip in Zukunft ähnlich handhaben könnten und von europäischen Service-Providern die Herausgabe von auf europäischen Servern gespeicherten und/oder europäische Bürger betreffenden Daten verlangen.[105] Fraglich ist, ob das wünschenswert ist.

III. Ausblick

Mit dem Vorschlag der Kommission soll ein harmonisierter Rahmen für die direkte Zusammenarbeit zwischen Strafverfolgungsbehörden und Service-Providern geschaffen werden.[106] Der grenzüberschreitende Zugriff auf elektronische Beweismitteln in der EU soll dadurch effektiv gestaltet werden.[107] Der Verordnungsvorschlag ver-

99 *Böse*, KriPoZ 2019, 140 (143).
100 *Böse*, KriPoZ 2019, 140 (143).
101 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.
102 *Burchard*, ZRP 2019, 164 (175).
103 *Burchard*, ZIS 2018, 249 (254).
104 *Burchard* (Fn. 3), S. 7.
105 *Burchard*, ZRP 2019, 164 (166).
106 *Böse*, An assessment of the Commission's proposals on electronic evidence, 2018, S. 48.
107 *Gössling/Nagel*, ITRB 2019, 41.

folgt damit zwar einen legitimen Zweck, entspricht jedoch nicht den unionsverfassungsrechtlichen Mindeststandards.[108] Der Grundrechtsschutz der Betroffenen kommt deutlich zu kurz, wenn die Wahrung der Grundrechte nicht von den Mitgliedstaaten, in deren Hoheitsgebiet der Auftrag ausgeführt werden soll, überprüft wird, sondern von dem Service-Provider und/oder der Anordnungsbehörde. [109] Diese sind faktisch nicht in der Lage einen angemessenen Schutz zu gewährleisten.[110] Die fehlenden Benachrichtigungspflichten der Betroffenen stellen einen intensiven und unverhältnismäßigen Grundrechtseingriff dar. Auch das Fehlen effektiver Rechtsmittel ist untragbar. Mit dem Verordnungsvorschlag der Kommission werden eine Reihe von Kooperationshindernissen beseitigt. Dies beschleunigt zwar das Verfahren, doch fällt zu Lasten des Grundrechtsschutzes. So wird der Einzelne des Schutzes beraubt, den ihm der traditionelle Rahmen der internationalen Rechtshilfe bietet.[111] Die Schutzinteressen der betroffenen Personen und die Interessen der Service-Provider sowie die Souveränitätsinteressen jener Staaten, in deren Territorium die angefragten Daten gespeichert sind, werden nicht hinreichend gewichtet.[112] Das Strafverfolgungsinteresse kann die weitreichenden rechtsstaatlichen Defizite nicht rechtfertigen. Die Beeinträchtigung der Grundrechte der Betroffenen und der Service-Provider ist unverhältnismäßig und der Vorschlag sollte umfassenden Änderungen unterzogen werden. Vollstreckungsbehörden müssten mehr in das Verfahren einbezogen werden, um den Grundrechtsschutz der Betroffenen zu gewährleisten. Die Voraussetzungen für den Erlass einer Herausgabe- oder Sicherungsanordnung müssten zudem präziser gestaltet werden. Der Rechtsschutz müsste ausgebaut werden. Daten schutzbedürftiger Personen und Berufsgruppen sollten nur unter bestimmten Bedingungen abgefragt werden dürfen.[113] Darüber hinaus erscheint es aus Gründen der Verhältnismäßigkeit sinnvoll, der Sicherungsanordnung den Vorrang zu lassen und die Herausgabeanordnung ohne vorheriges Sicherungsverfahren lediglich Fälle zu beschränken, in denen ansonsten der Verlust der elektronischen Beweiskette zu befürchten ist.[114] In seiner jetzigen Form kann dem Kommissionsvorschlag nicht zugestimmt werden.

[108] *Burchard*, ZRP 2019, 164 (166).
[109] *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
[110] *Böse* (Fn. 107), S. 48.
[111] *Böse* (Fn. 107), S. 48.
[112] *Burchard*, ZRP 2019, 164 (164).
[113] *Burchard*, ZRP 2019, 164 (167).
[114] *Basar*, jurisPR-StrafR 5/2019, Anm. 1.