BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 28/2018
September 2018
Registernummer: 25412265365-88

Zum Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM[2018] 225 final vom 17. April 2018)

Mitglieder des Ausschusses Europa

Rechtsanwalt und Notar a.D. Kay-Thomas Pohl, Vorsitzender
Rechtsanwalt Dr. Martin Abend, LL.M.
Rechtsanwalt Dr. Hans-Joachim Fritz
Rechtsanwältin Dr. Margarete Gräfin von Galen
Rechtsanwalt Andreas Max Haak
Rechtsanwalt Dr. Frank J. Hospach
Rechtsanwalt Guido Imfeld
Rechtsanwalt Dr. Georg Jaeger
Rechtsanwalt Dr. Stefan Kirsch
Rechtsanwalt Dr. Christian Lemke
Rechtsanwalt Andreas von Máriássy
Rechtsanwältin Dr. Kerstin Niethammer-Jürgens
Rechtsanwalt Dr. Hans-Michael Pott
Rechtsanwalt Jan K. Schäfer
Rechtsanwältin Stefanie Schott (Berichterstatterin)
Rechtsanwalt Dr. Thomas Westphal

Rechtsanwältin Dr. Heike Lörcher, Bundesrechtsanwaltskammer
Rechtsanwältin Hanna Petersen, LL.M., Bundesrechtsanwaltskammer
Rechtsanwältin Doreen Barca-Cysique, LL.M., Bundesrechtsanwaltskammer

Die Bundesrechtsanwaltskammer (BRAK) ist die Dachorganisation der anwaltlichen Selbstverwaltung in Deutschland. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit etwa 164.500 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Die Kommission hat am 17. April 2018 einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM[2018] 225 final vom 17. April 2018) sowie einen flankierenden 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

(COM[2018] 226 final vom 17. April 2018) vorgelegt. Die Vorschläge sehen vor, dass Strafverfolgungsbehörden eines Mitgliedstaats Unternehmen, die elektronische Kommunikationsleistungen in anderen Mitgliedstaaten anbieten (Diensteanbieter), unabhängig vom Sitz des Unternehmens und vom Ort der Speicherung der Daten (sog. Marktortprinzip) sanktionsbewehrt dazu verpflichten können, elektronische Beweismittel für laufende Strafverfahren zu sichern (Europäische Sicherungsanordnung) und an die Strafverfolgungsbehörden im Anordnungsstaat herauszugeben (Europäische Herausgabeanordnung). Das soll grundsätzlich auch dann gelten, wenn die Daten in Drittstaaten gespeichert sind.

Der Zugriff auf elektronische Beweismittel dürfte inzwischen eine der wichtigsten Erkenntnisquellen im Rahmen strafrechtlicher Ermittlungsverfahren sein. Insoweit erkennt die Bundesrechtsanwaltskammer grundsätzlich das Bedürfnis an, den grenzüberschreitenden Zugriff auf die bei Diensteanbietern gespeicherten Daten zu erleichtern und die Verfahren zu beschleunigen. Der Verordnungsentwurf geht über dieses Ziel jedoch weit hinaus und ist in seinen Regelungen teilweise unverhältnismäßig.

Das Vorgehen der Kommission wirkt überhastet. Der Umstand, dass die USA die Kommission im März 2018 mit dem Erlass des „Cloud Act“ überrascht haben, der den Zugriff auf im Ausland gespeicherte Daten erlaubt, rechtfertigt es nicht, um den Preis der Aufgabe europäischer Grundrechte und Datenschutzrechte schnellstmöglich „zurückzuschießen“. Mehrere europäische Vorschriften, auf die der Entwurf verweist, sind ihrerseits noch nicht verabschiedet worden. Aus Sicht der Bundesrechtsanwaltskammer wäre es sinnvoll, zumindest zunächst die praktischen Auswirkungen der Richtlinie zur Europäischen Ermittlungsanordnung, deren Umsetzungsfrist erst am 22. Mai 2017 abgelaufen ist (Art. 35 Abs. 1 RL 2014/41/EU) abzuwarten, um sich daraus möglicherweise ergebende Schwächen im Rahmen einer gesonderten Regelung für Herausgabe- und Sicherungsanordnungen zu vermeiden. Demgegenüber geht die Kommission mit der Verordnung für elektronisch gespeicherte Daten über die weitreichenden Neuerungen der Richtlinie zur Europäischen Ermittlungsanordnung nochmals weit hinaus, indem die Kontrollmöglichkeiten im Vollstreckungsstaat so weitgehend beschränkt werden, dass faktisch keine materiell-rechtliche Prüfung im Vollstreckungsstaat – etwa der Notwendigkeit und Verhältnismäßigkeit oder der Missbräuchlichkeit der Maßnahme – erfolgen kann.

Die Bundesrechtsanwaltskammer lehnt es ab, dass die in der Praxis angeblich bestehenden, in ihren genauen Ursachen nicht identifizierten Schwierigkeiten der grenzüberschreitenden Zusammenarbeit im Bereich elektronischer Beweismittel dadurch überwunden werden sollen, dass die von Eingriffen betroffenen Personen (Diensteanbieter, Beschuldigte und drittbetroffene Dateninhaber) in diesem grundrechtsrelevanten Bereich im Vollstreckungsstaat schutzlos gestellt werden.

Dies wird dem besonderen Schutzbedürfnis, das personenbezogenen Daten sowohl auf europäischer[1], als auch auf deutscher nationaler Ebene[2] zugebilligt wird, nicht gerecht.

Das Datenschutzniveau in Europa ist nach wie vor sehr uneinheitlich. Die europäische Datenschutz-Grundverordnung (DSGVO)[3] enthält lediglich von allen Staaten zu beachtende Mindeststandards hinsichtlich der Verarbeitung personenbezogener Daten, wobei der Zugriff auf solche Daten durch Behörden im Rahmen von Strafverfahren explizit vom Anwendungsbereich ausgenommen ist (Art. 2 Abs. 2 d) DSGVO).

---

[1] Grundrechtschutz gemäß Art. 6 Abs. 1 EUV i.V.m. Art. 7 und Art. 8 EUGrdRCh.

[2] Grundgesetzlich gewährter Schutz nach Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 2 GG als Recht auf „informationelle Selbstbestimmung“, vgl. z.B. BVerfG, Urteil v. 02.03.2006 – 2 BvR 2099/04, BVerfGE 115, 166.

[3] 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 (Datenschutz-Grundverordnung).

Darüber hinaus ist wegen der fehlenden Kontrolle im Vollstreckungsstaat nicht auszuschließen, dass die Instrumente rechtsmissbräuchlich genutzt werden. Da das Prinzip der beiderseitigen Straffbarkeit keine Anwendung findet, können Anordnungen auch zur Verfolgung von Straftaten erlassen werden, die im Vollstreckungsstaat keinen Straftatbestand erfüllen. Als Straftatbestand zum Erlass einer Anordnung käme daher beispielsweise auch die politisch motivierte Verfolgung wegen zu diesem Zweck geschaffenen Delikten in Betracht. Diese Gefahr erachtet die Bundesrechtsanwaltskammer gerade vor dem Hintergrund der aktuellen politischen Entwicklungen in mehreren Ländern der Europäischen Union als nicht hinnehmbar.

Im Einzelnen hat die Bundesrechtsanwaltskammer insbesondere Bedenken hinsichtlich folgender vorgesehener Änderungen:

1. Fehlende Vorschaltung einer gerichtlichen oder zumindest behördlichen Überprüfung im Vollstreckungsstaat

Der Entwurf sieht erstmals einen direkten Zugriff ausländischer Ermittlungsbehörden auf Diensteanbieter[4] vor, die ihre Dienstleistungen in einem Mitgliedsstaat der EU anbieten, somit unmittelbar auf (private) natürliche und juristische Personen. Diese können nach dem Entwurf durch Ermittlungsbehörden anderer Mitgliedstaaten verpflichtet werden, sämtliche Daten ihrer Nutzer herauszugeben, ohne dass die Rechtmäßigkeit der Anordnung vorab nach dem Recht des Vollstreckungsstaates überprüft wird. Nach Ansicht der Bundesrechtsanwaltskammer geht das über das Prinzip der gegenseitigen Anerkennung im Sinne des Art. 82 Abs. 1 AEUV hinaus. Weder zielen die Regeln (nur) auf die Anerkennung ausländischer gerichtlicher Entscheidungen im Sinne des Art. 82 Abs. 1 Unterabsatz 2 Buchstabe a AEUV, noch geht es um die Zusammenarbeit von Behörden im Sinne des Art. 82 Abs. 1 Unterabsatz 2 Buchstabe d AEUV. Vielmehr sehen die Regelungen des Verordnungsentwurfes den unmittelbaren einseitigen Vollzug sowohl behördlicher als auch gerichtlicher Anordnungen in einem anderen Mitgliedstaat vor.[5]Rechtsbehelfe der Diensteanbieter gegen die Herausgabe- und Sicherungsanordnung sind ebenfalls nur in sehr beschränktem Umfang vorgesehen, wobei eine materiell-rechtliche Prüfung nach eigenem Recht vollständig ausgeschlossen wird (siehe dazu unter 2.).

Die Bundesrechtsanwaltskammer erachtet einen derart weitreichenden Eingriff in die Souveränität der Mitgliedstaaten und in die Rechte der von der Maßnahme Betroffenen als unverhältnismäßig. Er ist weder erforderlich noch angemessen.

Erforderlich ist ein schnelles Handeln, das die (vorläufige) Beschneidung von Rechten rechtfertigen könnte nur für die Sicherung von Daten. Die Zwischenschaltung eines inländischen Verfahrens vor Umsetzung der Sicherung kann in diesem Bereich zum Verlust der Daten führen. Sind die Daten jedoch einmal gesichert, wäre es möglich und angemessen, vor Herausgabe der Daten eine gerichtliche oder zumindest eine behördliche Überprüfung durchzuführen. Der Verordnungsentwurf unterscheidet bereits nach der Art der Anordnung, einerseits zur Sicherung und andererseits zur Herausgabe von Daten, behandelt diese aber weitgehend gleich, so dass sich die Frage stellt, warum sich eine Behörde je auf die Sicherung von Daten beschränken sollte. Die Erfahrungen – etwa mit dem Europäischen Haftbefehl – zeigen, dass eine (Rest-)Kontrolle auch im Vollstreckungsstaat dringend geboten ist, da mitnichten

---

[4] Nach Art. 2 Ziff. 3 lit b) handelt es sich dabei u.a. um natürliche oder juristische Personen, die bestimmte Kommunikationsdienste bzw. Dienste der Informationsgesellschaft anbieten und bei denen die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist. Rechtsanwälte, Architekten usw. fallen daher mit ihrer eigentlichen, auf elektronischem Weg erbrachten Tätigkeit nicht in den Anwendungsbereich.

[5] Siehe dazu auch Beschluss des Bunderats v. 6. Juli 2018, Drucksache 215/1/18.

gewährleistet ist, dass ein hinreichendes Maß an Rechtsstaatlichkeit und angemessenem Grundrechtsschutz (einschließlich des in der Menschenwürde gründenden Schutzes des Kernbereichs privater Lebensgestaltung) in allen Mitgliedstaaten der Europäischen Union umfassend gewährleistet wird.[6]

Das Erfordernis einer Überprüfung gilt in besonderem Maße für Inhaltsdaten sowie für Transaktionsdaten.[7] Zumindest in Bezug auf diese Daten wäre die Einführung einer gerichtlichen Überprüfung im Vollstreckungsstaat wünschenswert. Zur Gewährleistung ausreichenden Grundrechtsschutzes könnte auf die Gründe des Art. 11 Abs. 1 RL 2014/41/EU zur Versagung der Anerkennung der Anordnung zurückgegriffen werden. Verbieten es die Ermittlungen, den Betroffenen vor Herausgabe der Daten zu informieren, muss das Gericht zumindest die tatsächliche und rechtliche Entscheidungsgrundlage zur Anordnung so vollständig zur Verfügung gestellt bekommen, dass es die Rechtmäßigkeit der Maßnahme nach eigenen Maßstäben prüfen kann. Grundsätzlich denkbar wäre auch, stattdessen eine gerichtliche Instanz auf europäischer Ebene zu schaffen. Dies wäre aber mit weitreichenden Reformen verbunden und einer Beschleunigung des Verfahrens zumindest gegenwärtig nicht zuträglich.

Kommt die Einführung einer gerichtlichen Kontrolle im Vollstreckungsstaat oder auf europäischer Ebene nicht in Betracht, so ist zu fordern, dass zumindest eine Notifikationslösung ähnlich Art. 31 RL 2014/41/EU eingeführt wird. Die zuständige Behörde des Vollstreckungsstaats wäre vor Erlass der Anordnung zu unterrichten und könnte der Sicherstellung bzw. insbesondere der Herausgabe der Daten innerhalb einer bestimmten Frist widersprechen, wenn die Maßnahme in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde. Auch insoweit könnte auf den Prüfungsmaßstab des Art. 11 Abs. 1 RL 2014/41/EU zurückgegriffen werden.

2. Keine effektiven Prüfungs- und Rechtsbehelfsmöglichkeiten

Die mit der fehlenden gerichtlichen Überprüfung eingehender Anordnungen im Vollstreckungsstaat verbundene Gefahr der Verletzung von Grundrechten wird zusätzlich dadurch verschärft, dass der Verordnungsentwurf nur sehr beschränkte Möglichkeiten der von der Maßnahme Betroffenen vorsieht, die Durchführung der Anordnung zu verweigern bzw. zu verhindern.

2.1 Keine grundrechtsrelevante Überprüfung durch den Diensteanbieter

Die Möglichkeiten der Diensteanbieter, gegen eine Europäische Herausgabe- oder Sicherungsanordnung vorzugehen, sind extrem begrenzt. Einen Ablehnungsgrund sieht Art. 14 Abs. 4 bzw. Abs. 5 VO-E nur vor, wenn die Sicherungs-/ Herausgabeanordnung nicht von der zuständigen Behörde erlassen oder validiert wurde, wenn der Anwendungsbereich der Verordnung aus verschiedenen genannten Gründen nicht eröffnet ist, wenn sich die Maßnahme nicht an den richtigen Adressaten richtet oder wenn sie faktisch nicht erfüllt werden kann.

Als einzigen Ablehnungsgrund gegen die Ausführung der Sicherungs- und Herausgabeanordnung, der eine grundrechtsrelevante Prüfung erlauben würde, nennt Art. 14 Abs. 4 lit f) bzw. Abs. 5 lit. e) VO-E, dass „ausschließlich aus den in dem EPOC[-PR] genannten Gründen hervor geht, dass es offenkundig gegen die Grundrechte-Charta verstößt oder offensichtlich missbräuchlich ist.“ Dieser Ablehnungsrund läuft aber nach der Systematik der Verordnung ins Leere, da entsprechende Informationen sich aus

[6] Vgl. hierzu – pars pro toto – nur EuGH, laufende Rs. C-216/18 PPU.

[7] Transaktionsdaten sind Daten, die unter anderem Rückschlüsse auf den Standort zulassen (Art. 2 Ziffer 8 VO-E). Die Bundesrechtsanwaltskammer begrüßt die Einführung dieser Differenzierung, da auch diese Kategorie besonders sensible Daten umfasst, die in höherem Maße schutzbedürftig sind, als reine Teilnehmer- oder Zugangsdaten. Inwieweit eine genaue Trennung dieser Daten technisch möglich ist, vermag die Bundesrechtsanwaltskammer nicht zu beurteilen.

dem Zertifikat nicht ergeben, bzw. sich nicht einmal daraus ergeben dürfen. Es sind keinerlei Angaben zum Sachverhalt oder zu rechtlichen Erwägungen im EPOC(-PR) vorgesehen. Die einzige sachlich-rechtliche Voraussetzung für den Erlass einer Herausgabeanordnung ist nach Art. 5 Abs. 5 lit. i) VO-E die Nennung von Gründen für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme. Diese Angaben dürfen aber in das Zertifikat gemäß Art. 8 Abs. 3 S. 2 und Abs. 4 S. 2 VO-E nicht übernommen werden.

Auch wenn der Diensteanbieter erkennt, dass die angeforderten Daten durch Immunitäten und Vorrechte im Sinne des Art. 5 Abs. 7 VO-E besonders geschützt sind, hat er nach dem Entwurf keine Möglichkeit die Herausgabe an die Anordnungsbehörde zu verweigern.

Dieser vollständige Ausschluss grundrechtsrelevanter Einwendungen ist nach Ansicht der Bundesrechtsanwaltskammer inakzeptabel.

Art. 11 Abs. 1 lit a) bis h) RL 2014/41/EU sieht für die von ihrem Regelungsgegenstand vergleichbare, da ebenfalls auf die Herausgabe von Beweismitteln im Strafverfahren gerichtete Europäische Ermittlungsanordnung Gründe für die Versagung der Anerkennung der Vollstreckung vor, die dazu geeignet sind, zu verhindern, dass eine als grob rechtswidrig erachtete Maßnahme durchgeführt werden muss. Zumindest diese Ablehnungsgründe sind dem Diensteanbieter jedenfalls gegen die Sicherungsanordnung und gegen die Herausgabeanordnung zu gewähren.[8]

Als Mindestangaben im EPOC und EPOC-PR sind die in Art. 5 Abs. 1 der Richtlinie 2014/41/EU aufgeführten Informationen zu verlangen.

2.2 Beschränkte Rechtsbehelfsmöglichkeiten des Betroffenen

Der von der Datenherausgabe betroffene Nutzer der Dienste hat unabhängig davon, ob er selbst Beschuldigter ist oder nicht, ebenfalls keine Möglichkeit, Rechtsbehelfe im Staat des Diensteanbieters, d.h. im Vollstreckungsstaat einzulegen.

Im Anordnungsstaat ist eine gerichtliche Überprüfung nur für den Fall der Anforderung von Transaktions- und Inhaltsdaten zwingend vorgesehen. Diese Prüfung ist, da der Betroffene über die verdeckte Maßnahme nicht informiert wird, nicht kontradiktorisch ausgestaltet, in dem Sinne, dass er die Möglichkeit hat, das Vorbringen der Anordnungsbehörde zu ergänzen oder den der Anordnung zugrunde gelegten Annahmen zu widersprechen.

Die von der Dateneinholung betroffenen Personen sollen nach Art. 17 VO-E „wirksame Rechtsbehelfe“ im Anordnungsstaat geltend machen können. Da der Diensteanbieter aber auf Aufforderung der Anordnungsbehörde die Person, deren Daten angefordert worden sind, nicht von der erfolgten Datenherausgabe in Kenntnis setzen darf (Art. 11 Abs. 1 VO-E), wird der Betroffene in der Praxis auch nachdem die Anordnungsbehörde die Daten erlangt hat, (zunächst) keine Möglichkeit haben, Einwendungen zu erheben und eine rechtliche Prüfung zu erzwingen. Er wird die Auswertung der Daten dann auch nach dem Recht des Anordnungsstaates nicht verhindern können.

[8] Wobei Art. 11 Abs. 1 lit h) EEA ausgenommen werden kann, da der Entwurf, anders als die EEA, die danach erlaubten Ermittlungsmaßnahmen abschließend benennt.

3. Kein ausreichender Schutz von privilegierten Daten

Der Zugriff auf Immunitäten und Vorrechte wird nach dem Entwurf nur dadurch verhindert, dass die Anordnungsbehörde, sofern sie „Grund zu der Annahme hat, dass angeforderte Transaktions- oder Inhaltsdaten durch Immunitäten und Vorrechte geschützt sind“, vor Erlass der Herausgabeanordnung die zuständigen Behörden im Vollstreckungsstaat kontaktiert, um den Sachverhalt zu klären (Art. 5 Abs. 7 S. 1 VO-E). Nur wenn die Anordnungsbehörde danach 'feststellt', dass Immunitäten und Vorrechte bestehen, erlässt sie die Anordnung nicht (Art. 5 Abs. 7 S. 2 VO-E). Ausgehend von dieser Formulierung, kommt es selbst für den Fall, dass tatsächlich ein Konsultationsverfahren mit den Behörden im Vollstreckungsstaat aufgenommen wird, letztlich allein auf die Qualifizierung der Daten durch die Behörde im Anordnungsstaat an. Eine einvernehmliche Lösung mit den Stellen des Vollstreckungsstaates ist ebenso wenig vorgesehen, wie eine Klärung von Zweifelsfällen auf europäischer Ebene.

Auch für den Fall, dass der Diensteanbieter feststellt, dass besonders geschützte Daten angefordert werden, ist keine Rechtsschutzmöglichkeit vorgesehen.

Für Transaktions- und Inhaltsdaten muss im Anordnungsstaat eine gerichtliche Überprüfung gem. Art. 4 Abs. 2 lit. b) 18 VO-E erfolgen, ein Hinweis darauf, um welche Art von Daten es sich bei den angeforderten handelt, ist aber weder als Voraussetzung der Anordnung vorgesehen, noch als Inhalt des EPOC oder des EPOC-PR. Dass das Gericht des Anordnungsstaates die besondere Schutzbedürftigkeit der angeforderten Daten erkennt, ist daher nicht gewährleistet. Soweit es sich bei den durch Immunitäten und Vorrechte geschützten Daten um Teilnehmer- oder Zugangsdaten handelt, findet überhaupt keine gerichtliche Kontrolle statt, obwohl auch diese Daten von dem besonderen Schutzbedürfnis umfasst sind.

Der Schutz besonders sensibler Daten hängt damit allein von einer sorgsamen Prüfung und der richtigen Einordnung der Daten durch die anordnende Behörde ab. Die Bundesrechtsanwaltskammer ist der Auffassung, dass dies zum Schutz dieser Daten nicht genügt. Auch insoweit ist eine Prüfung durch ein Gericht oder eine Behörde im Vollstreckungsstaat zwingend erforderlich, wobei das Gericht bzw. die Behörde auf eine möglichst genaue Bezeichnung der angeforderten bzw. der gesicherten Daten angewiesen ist.

4. Zu weit gefasster sachlicher und räumlicher Anwendungsbereich

4.1 Keine Beschränkung der Anwendbarkeit des Entwurfs auf schwere Straftaten

Eine weitere Verschärfung zu Lasten der Betroffenen tritt dadurch ein, dass der Verordnungsentwurf lediglich als Voraussetzung für eine Herausgabeanordnung und nur für Transaktions- und Inhaltsdaten überhaupt eine Beschränkung auf bestimmte Delikte vorsieht. Folglich kann die Sicherung von Daten sowie die Herausgabe von Teilnehmer- und Zugangsdaten für jede im Anordnungsstaat unter Strafe stehende Tat verlangt werden.

Die für die Herausgabe von Transaktions- und Inhaltsdaten in Art. 5 Abs. 4 VO-E vorgesehene Beschränkung ist nicht geeignet, die Verhältnismäßigkeit des Zugriffs zu wahren: Für andere als die in Art. 5 Abs. 4 Lit b) VO-E i.V.m. Art. 3, 4 und 5 des Rahmenbeschlusses 2001/413/JI des Rates[9] konkret

[9] Rahmenbeschlusses 2001/413/JI des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln.

aufgeführten, mittels eines Informationssystems begangenen Straftaten, wird lediglich ein Höchststrafmaß im Anordnungsstaat von mindestens drei Jahren verlangt (Art. 5 Abs. 4 lit a) VO-E). Strafbarkeit und Strafmaß im Vollstreckungsstaat finden nach dem Verordnungsentwurf keine Berücksichtigung. Die angeforderten Daten müssen auch dann herausgegeben werden, wenn die der Anordnung zugrundeliegende Tat im Vollstreckungsstaat überhaupt keinen Straftatbestand erfüllt. Dies eröffnet nach Ansicht der Bundesrechtsanwaltskammer Missbrauchsmöglichkeiten und erhöht die Gefahr unverhältnismäßiger Zugriffe auf Daten.

Die Ausweitung des Anwendungsbereichs auf alle Tatbestände mit einem Höchst-Strafmaß von mindestens drei Jahren wird der Schwere des Eingriffs nicht gerecht. Davon dürften in vielen Mitgliedstaaten auch Taten geringer Kriminalität erfasst werden.[10] Zu fordern ist die Aufnahme eines Katalogs von konkret benannten Straftaten, der auf schwere Kriminalität zu beschränken ist.

4.2 Zu weiter räumlicher Anwendungsbereich

Der Verordnungsentwurf beansprucht Beachtung von allen Diensteanbietern, die ihre Dienstleistungen in der EU anbieten und die ihren Sitz oder eine Vertretung in einem anderen als dem Anordnungsstaat haben. Der Entwurf enthält keine Sicherung dafür, dass Sachverhalte, die ausschließlich oder vorrangig einen einzigen Mitgliedstaat betreffen, auch (nur) von diesem zu regeln sind: So ist es nach dem Verordnungsentwurf denkbar, dass ein anderer EU-Mitgliedstaat eine Europäische Herausgabeanordnung gegen einen Diensteanbieter mit Sitz und Speicherort in Deutschland wegen eines Strafverfahrens erlässt, das wegen einer Tat mit (auch) maßgeblichem Bezug zu Deutschland gegen einen deutschen Staatsangehörigen mit Wohnsitz in Deutschland geführt wird. Dieses Legislativverfahren hätte dem Europäischen Gesetzgeber Anlass gegeben, allgemeine und wirksame Vorkehrungen gegen eine mehrfache, parallele Strafverfolgung zu treffen.[11] Jedenfalls aber sind Ablehnungsgründe zu ergänzen, die einen Minimalschutz vor überbordender bzw. doppelter Strafverfolgung gewährleisten, und die auch in bestehenden Rechtsakten zur gegenseitigen Anerkennung strafjustizieller Entscheidungen enthalten sind: „ne bis in idem“ sowie das Bestehen eines vorrangigen Bezugs zu einem anderen Mitgliedstaat (vgl. Art. 11 Abs. 1 lit. d, lit. e RL 2014/41/EU).

5. Keine Vorgaben zur Eingrenzung der angeforderten Daten

Für problematisch hält die Bundesrechtsanwaltskammer darüber hinaus, dass Angaben zur näheren Bestimmung der angeforderten Daten nicht vorgesehen sind. Die Zeitspanne für die die Herausgabe angefordert wird, muss nur „gegebenenfalls“ in der Anordnung enthalten sein (Art. Artikel 5 Abs. 5 lit. e, bzw. Art. 6 Abs. 3 lit. e VO-E). Vorgaben dazu, in welchen Fällen eine zeitliche Begrenzung vorzunehmen ist und wann nicht, enthält der Entwurf nicht. Zu fordern ist eine möglichst präzise Benennung der konkret verlangten Daten eines bestimmten Zeitraums.

---

[10] So gelten etwa im deutschen Recht hohe Anforderungen zur Sicherstellung der Verhältnismäßigkeit des Zugriffs auf elektronische Beweismittel. § 100 g Abs. 2 StPO verlangt für den Zugriff auf gespeicherte Verkehrsdaten das Vorliegen bestimmter (zu benennender) Tatsachen, die den Verdacht auf das Vorliegen einer der in einem Katalog aufgeführten besonders schweren Straftaten begründet, die auch im Einzelfall besonders schwer wiegen muss. Darüber hinaus enthält § 101 StPO detaillierte Verfahrensvorschriften, insbesondere zur Information der von der Maßnahme Betroffenen.

[11] Siehe hierzu das Eckpunktepapier der Bundesrechtsanwaltskammer: Für eine klare, verlässliche und verbindliche Regelung zur Vermeidung paralleler Strafverfolgung in der Europäischen Union, Stellungnahme Nr. 33/2016.

6. Missachtung des Rechts von Drittstaaten

Sind die Daten in einem Drittstaat gespeichert, dessen Recht es dem Diensteanbieter verbietet, sie an die Anordnungsbehörde heraus zu geben, so soll ein Gericht des Anordnungsstaates darüber entscheiden, ob die Rechtsvorschriften des Drittstaates zu beachten sind (vgl. Art. 15 Abs. Abs. 4 VO-E). Nach Ansicht der Bundesrechtsanwaltskammer kann es nicht dem Anordnungsstaat zustehen, das Recht eines Drittstaates zu bewerten und darüber zu entscheiden, ob dieses in einem konkreten Fall zu berücksichtigen ist oder nicht. Das gilt auch nachdem die USA dem widersprechende Regelungen erlassen haben fort. Die dramatischen Folgewirkungen, die ein Verdikt auf völkerrechtlicher Ebene haben wird, liegen auf der Hand. Daher ist Art. 15 Abs. 4 VO-E zu streichen und auch im „Überprüfungsverfahren bei einander widersprechenden Verpflichtungen aus anderen Gründen“ (Art. 16 VO-E) die Entscheidungsprärogative des Drittstaats anzuerkennen.

7. Fazit

Die Bundesrechtsanwaltskammer lehnt den Vorschlag insgesamt ab, da er in seiner Konzeption unverhältnismäßig ist und die von den Maßnahmen Betroffenen weitgehend rechtlos stellt. Ein dringendes Bedürfnis für den Erlass dieser Rechtsakte vermag die Bundesrechtsanwaltskammer (derzeit) nicht zu erkennen.

Hält der Europäische Gesetzgeber trotz der erheblichen Bedenken an diesem Vorschlag fest, so sind wenigstens folgende Korrekturen dringend vorzunehmen:

1.
a) Jedenfalls vor Herausgabe von Transaktions- und Inhaltsdaten ist ein gerichtliches Verfahren im Vollstreckungsstaat durchzuführen, in dem die Rechtmäßigkeit der Anordnung nach eigenem Recht überprüft wird. Der Katalog der zu prüfenden Punkte könnte Art. 11 Abs. 1 RL 2014/41/EU entnommen werden.

Zumindest muss die zuständige Behörde des Vollstreckungsstaates vorab über die Anordnung informiert werden, damit sie die Möglichkeit hat, die Einhaltung wesentlicher Rechtsstandards – ebenfalls entsprechend dem Katalog des Art. 11 Abs. 1 RL 2014/412/EU – zu überprüfen und der Herausgabe der Daten erforderlichenfalls innerhalb einer bestimmten Frist zu widersprechen.

b) Das Gericht bzw. die Behörde des Vollstreckungsstaates ist durch eine ausreichende Informationsgrundlage in die Lage zu versetzen, tatsächlich eine effektive (Vorab-)Kontrolle der Europäischen Sicherungs- und Herausgabeanordnungen vorzunehmen. Als Mindestangaben sind die in Art. 5 Abs. 1 EEA aufgeführten Informationen zu verlangen.

2.
a) Dem Diensteanbieter sind Ablehnungsgründe sowohl gegen die Sicherung als auch gegen die Herausgabe von Daten zuzugestehen, die denen des Art. 11 Abs. 1 lit. a) bis g) EEA entsprechen.

b) Notwendige Voraussetzung für die Geltendmachung dieser Gründe ist, dass EPOC und EPOC-PR inhaltliche Angaben zum Gegenstand und zum Hintergrund der Anordnung sowie zur Notwendigkeit und Verhältnismäßigkeit enthalten. Als Mindestangaben sind die in Art. 5 Abs. 1 EEA aufgeführten Informationen zu verlangen. Darüber hinaus müssen die angeforderten Daten inhaltlich und zeitlich konkretisiert werden.

3.
Der sachliche Anwendungsbereich des Verordnungsvorschlags ist durch einen Katalog von (besonders schweren) Anlasstaten einzugrenzen und muss das Prinzip der beiderseitigen Strafbarkeit beachten.

4.
Verletzungen des Kernbereichs privater Lebensgestaltung und Verletzungen von Berufsgeheimnissen müssen zwingend zu einem Beweisverwendungsverbot führen und mit einer Löschungsverpflichtung flankiert werden.

5.
Art. 15 Abs. 4 VO-E ist zu streichen und auch im „Überprüfungsverfahren bei einander widersprechenden Verpflichtungen aus anderen Gründen“ (Art. 16 VO-E) die Entscheidungsprärogative des Drittstaats anzuerkennen.

***