Deutscher Bundestag **Drucksache 19/8054**

19. Wahlperiode 27.02.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Niema Movassat, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/7639 –

Vereinbarkeit der Initiativen der EU-Kommission und des Europarates zur Herausgabe von im Internet gespeicherten persönlichen Daten

Vorbemerkung der Fragesteller

Am 17. April 2018 hat die Europäische Kommission einen Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vorgelegt (COM (2018) 225 final – 2018/0108 (COD)). Die Justizbehörde eines Mitgliedstaats könnte demnach mit Frist von zehn Tagen Inhaltsdaten und Metadaten anfordern. Im „Notfall" verkürzt sich die Frist auf sechs Stunden. Ähnlich dem deutschen „Quick Freeze" erhalten Internetdienstleister eine „Sicherungsanordnung", damit herausverlangte Daten nicht gelöscht werden. Die Vorschrift beträfe alle Firmen, die in EU-Mitgliedstaaten „interpersonelle Kommunikationsdienste" anbieten, darunter auch „Kleinstprovider". Die Mitgliedsstaaten haben den Vorschlag der Kommission in einigen Punkten sogar verschärft (Ratsdokument 14351/18). Bei Nichterfüllung der Anordnungen können die Firmen etwa mit bis zu zwei Prozent ihres globalen Jahresumsatzes bestraft werden.

Viele der in der Verordnung angesprochenen Firmen haben ihren Sitz in den USA. Die dortige Regierung würde einem direkt an diese gerichteten Herausgabeverlangen auf ihrem Hoheitsgebiet vermutlich nur zustimmen, wenn auch US-Behörden in der Europäischen Union eine solche Maßnahme zugestanden würde. Im vergangenen Jahr hat die US-Regierung einen „CLOUD Act" („Clarifying Lawful Overseas Use of Data – CLOUD – Act") erlassen, der dort niedergelassene Firmen zur Offenlegung von Bestands-, Verkehrs- und Inhaltsdaten zwingt (http://gleft.de/2hK). Er enthält eine Klausel, wonach einzelne EU-Mitgliedstaaten mit der US-Regierung als „Partnerstaaten" ein Durchführungsabkommen schließen können. Die EU-Kommission soll nun ein Rahmenabkommen für die gesamte Europäische Union aushandeln („USA wollen nicht mit EU über Datenzugriff verhandeln", www.golem.de vom 17. Mai 2018).

Zusätzlich zur geplanten Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen verhandelt der Europarat über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität zur Verbesserung der Sicherung elektronischer Beweismittel. Bis Dezember 2019 soll eine Arbeitsgruppe einen

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 26. Februar 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Entwurf mit Bestimmungen für vereinfachte Rechtshilfeverfahren sowie zur garantierten Kooperation der Internetfirmen ausarbeiten (Bundestagsdrucksache 18/11578, Antwort zu Frage 1). Die USA ist Unterzeichnerin des Abkommens, das Protokoll würde also auch für US-Firmen gelten. Ein EU-Durchführungsabkommen für den „CLOUD Act“, so es denn zustande kommt, könnte sich wie die neue EU-Gesetzgebung auf das Zusatzprotokoll berufen. Aus Sicht der Fragestellerinnen und Fragesteller ist aber unklar, ob und wie sich die Initiativen der EU-Kommission und des Europarates voneinander unterscheiden oder doppeln.

1. Wie definiert die Bundesregierung die Begriffe „Bestandsdaten“, „Zugangsdaten“ und „Verkehrsdaten“, und wie hat sie sich im Rat hierzu positioniert (Bundestagsdrucksache 19/3392, Antwort zu Frage 7)?

Die Begriffe der „Bestandsdaten“ und „Verkehrsdaten“ sind im Telekommunikationsgesetz (TKG) definiert. Der Begriff der „Zugangsdaten“ wird in den Legislativvorschlägen zu E-Evidence definiert und erläutert, siehe Artikel 2 Absatz 8 der E-Evidence-Verordnung (EPOC-VO) in der Fassung der Allgemeinen Ausrichtung vom Dezember 2018. Als Zugangsdaten werden solche Daten bezeichnet, die die konkreten Umstände der Nutzung bestimmter Dienste betreffen und die zwecks Identifikation eines Nutzers erhoben werden sollen. Aus Sicht der Bundesregierung sind die in der EPOC-VO verwendeten Datenkategorien nachvollziehbar, obgleich sie nicht mit den Datenkategorien im deutschen Recht identisch sind.

2. Inwiefern hält es die Bundesregierung für sachgerecht, dass die Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen auch für Kleinstprovider gelten soll, und welche Ausnahmen befürwortet sie hierzu (Bundestagsdrucksache 19/3392, Antwort zu Frage 5)?

Die Bundesregierung hält die grundsätzliche Einbeziehung auch von Klein- und Kleinstunternehmen in den Anwendungsbereich der EPOC-VO für sachgerecht, da andernfalls „sichere Datenhäfen“ entstehen könnten. Die Bundesregierung hat sich in den Verhandlungen zum Vorschlag der EPOC-VO allerdings dafür eingesetzt, übermäßige Belastungen für kleinere Unternehmen zu vermeiden, indem hier beispielsweise die in der Vorbemerkung der Fragesteller angesprochenen Reaktionsfristen verlängert werden. Der Vorschlag, den Verordnungstext anzupassen, fand unter den Mitgliedstaaten der Europäischen Union zwar keine Mehrheit, dafür wurde aber Erwägungsgrund 45a zur EPOC-VO in der Textfassung der Allgemeinen Ausrichtung vom Dezember 2018 angepasst. Dieser Erwägungsgrund sieht nunmehr vor, dass die Schwierigkeiten, die Kleinstunternehmen mit der Einhaltung der Herausgabefristen haben könnten, im Rahmen des Sanktionsmechanismus besonders zu berücksichtigen sind.

3. Wie soll aus Sicht der Bundesregierung der Schutz von Berufsgeheimnisträgern in der Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen umgesetzt werden, und wie soll festgestellt werden, in welchen Fällen Herausgabeanordnungen den Kernbereich der privaten Lebensführung oder Berufsgeheimnisse betreffen (Bundestagsdrucksache 19/5207, Antwort zu Frage 2)?

Die Bundesregierung hat sich – gemeinsam mit anderen Mitgliedstaaten der Europäischen Union – während der gesamten Verhandlungen zur EPOC-VO intensiv für den Schutz von Berufsgeheimnisträgern und den Schutz des Kernbereichs

der privaten Lebensgestaltung eingesetzt. Die Anpassungen, die die EPOC-VO in der Textfassung der Allgemeinen Ausrichtung vom Dezember 2018 gegenüber der von der Europäischen Kommission vorgelegten Textfassung erfahren hat, setzen das Anliegen der Bunderegierung bereits teilweise um. So ist bei einer Herausgabeanordnung, die auf die Erlangung von Inhaltsdaten gerichtet ist, zwingend ein Notifizierungsverfahren vorgesehen (Artikel 7a VO-E). Danach muss der Anordnungsstaat zugleich mit dem Erlass der Herausgabeanordnung an den Provider auch den Vollstreckungsstaat unterrichten, also den Mitgliedstaat der Europäischen Union, in dem der Provider seinen gesetzlichen Vertreter benannt hat. Der notifizierte Mitgliedstaat kann in diesem Verfahren Bedenken erheben, wenn der Herausgabeanordnung im Einzelfall Immunitäten und Vorrechte des Datennutzers, worunter auch Berufsgeheimnisse fallen, entgegenstehen. Ist die Anordnung auf die Herausgabe von Transaktionsdaten gerichtet, hat der Anordnungsstaat in ein Konsultationsverfahren mit dem Vollstreckungsstaat einzutreten, sofern Anlass besteht, dass Immunitäten oder Vorrechte berührt sein können (Artikel 5 Absatz 7 VO-E). Beide Normen werden flankiert durch eine neu aufgenommene Regelung in Artikel 12a VO-E, wonach der Schutz von Immunitäten und Vorrechten auch dann geltend gemacht werden kann, wenn der Diensteanbieter die Daten bereits an den Anordnungsstaat übermittelt hat.

Die Bundesregierung sieht diese Anpassungen als wichtige Verbesserungen der EPOC-VO an, wünscht sich mit Blick auf den erforderlichen Grundrechtsschutz jedoch noch weitere Nachjustierungen im Zuge des anstehenden Trilogs. Die Bundesregierung wünscht sich unter anderem, dass die Notifizierungslösung auch auf die Transaktionsdaten erstreckt wird. Zudem ist aus Sicht der Bundesregierung wichtig, dass dem notifizierten Mitgliedstaat ausdrücklich das Recht zugestanden wird, die Herausgabeanordnung im begründeten Einzelfall zurückzuweisen, wenn deren Vollzug gegen die europäischen Grundrechte verstoßen würde. Die Bundesregierung sieht dieses Recht für den Vollstreckungsstaat mit Blick auf die Rechtsprechung des EuGH (insbesondere zum Europäischen Haftbefehl und zur Vorratsdatenspeicherung) deshalb als erforderlich an, weil der Vollstreckungsstaat andernfalls nicht in der Lage wäre, der allgemeinen Grundrechtsklausel aus Artikel 1 Absatz 2 VO-E Rechnung zu tragen. In diesem Zusammenhang setzt sich die Bundesregierung insbesondere auch für den absolut zu gewährleistenden Schutz des Kernbereichs privater Lebensgestaltung ein.

4. Wie hat sich die Bundesregierung im Rat zur Frage positioniert, ob die Herausgabe der Telekommunikationsdaten einem abgestuften Verfahren folgen soll und etwa Anordnungen zur Herausgabe von Teilnehmer- und Zugangsdaten für alle Straftaten erlassen werden dürfen, Anordnungen zur Herausgabe von Transaktions- und Inhaltsdaten jedoch nur für Straftaten mit einer zu erwartenden bestimmten Höchststrafe?

Die Bundesregierung begrüßt den von der Europäischen Kommission vorgeschlagenen Ansatz, je nach Sensibilität der betroffenen Datenkategorien abgestufte Regelungen zu schaffen. Insbesondere teilt die Bundesregierung den Ansatz, dass für Transaktions- und Inhaltsdaten als besonders sensible Datenkategorien strengere Anordnungsvoraussetzungen gelten sollen. Diese Anordnungen sollen, sofern es sich nicht um Straftaten handelt, die in bestimmten EU-Richtlinien benannt werden (Artikel 5 Absatz 4 Buchstabe b und c VO-E), nur zur Ermittlung von Straftaten erlassen werden können, die mit einer Mindesthöchststrafe von drei Jahren bedroht sind (Artikel 5 Absatz 4 Buchstabe a VO-E). Die Bundesregierung hatte sich in den Verhandlungen für eine höhere Mindesthöchststrafe für Herausgabeanordnungen, nämlich für fünf Jahre, ausgesprochen. Die Mehrheit

der Mitgliedstaaten hat sich jedoch dem Textvorschlag der Kommission angeschlossen.

Insgesamt wünscht sich die Bundesregierung, dass der differenzierende Ansatz der Kommission im Text der EPOC-VO noch konsequenter durchgehalten wird. Mit Blick darauf, dass der Europäische Gerichtshof sowohl die Transaktionsdaten als auch die Inhaltsdaten als sensible Datenkategorie einstuft, hält es die Bundesregierung für erforderlich, auch bei Herausgabeanordnungen, die auf die Erlangung von Transaktionsdaten gerichtet sind, ein Notifikationsverfahren vorzusehen, siehe bereits die Antwort zu Frage 3.

5. Inwiefern sollte aus Sicht der Bundesregierung bei bestimmten Straftaten (etwa mit einer Mindestfreiheitsstrafe von drei Jahren) auch möglich sein, eine mehrmonatige Vorratsdatenspeicherung der begehrten Daten zu erwirken, die womöglich sogar verlängert werden könnte?

Die Europäische Sicherungsanordnung ist eine ausschließlich anlassbezogene Datensicherung im Zuge von konkreten strafrechtlichen Ermittlungen im Anordnungsstaat und deshalb nicht als Vorratsdatenspeicherung einzustufen. Der mit einer Europäischen Sicherungsanordnung verbundene Eingriff in die Grundrechte der Dateninhaber ist geringer, als dies bei einer Europäischen Herausgabeanordnung der Fall ist. Die Bundesregierung hält deshalb den von der Europäischen Kommission in Artikel 6 VO-E gewählten Ansatz, den Erlass einer Europäischen Sicherungsanordnung nicht von einer bestimmten Mindesthöchststrafe des den Ermittlungen im Anordnungsstaat zugrunde liegenden Delikts abhängig zu machen, sondern stattdessen allgemein die Verhältnismäßigkeit des Eingriffs zu verlangen, für vertretbar.

6. Wie sollen deutsche Firmen aus Sicht der Bundesregierung prüfen, ob Tatbestände, nach denen „Bestandsdaten“, „Zugangsdaten“ und „Verkehrsdaten“ ohne eine Notifizierung deutscher Behörden und damit ohne juristische Prüfung herausgegeben werden sollen, hierzulande überhaupt strafbar sind, wie beispielsweise der Straftatbestand „Rebellion“, der in Spanien existiert, aber nicht in Deutschland?

Die Prüfung, ob eine Straftat vorliegt, erfolgt durch den Anordnungsstaat. Der von der Europäischen Kommission vorgelegte Vorschlag der EPOC-VO verzichtet auf das Erfordernis der beiderseitigen Strafbarkeit, so dass eine Europäische Herausgabeanordnung grundsätzlich auch dann erlassen werden kann, wenn die Tat im Vollstreckungsstaat nicht strafbar ist. Stattdessen soll durch das Erfordernis der Mindesthöchststrafe von drei Jahren bei auf Transaktions- und Inhaltsdaten gerichteten Herausgabeanordnungen gewährleistet werden, dass Anordnungen nur für Straftaten, denen ein besonderes Gewicht zukommt, erlassen werden, siehe bereits Antwort zu Frage 4. Der Provider kann zwar im Vollstreckungsverfahren einwenden, dass keine Straftat mit einer Mindesthöchststrafe von drei Jahren vorliegt (Artikel 14 Absatz 4 Buchstabe b VO-E), eine abschließende Prüfung durch den Provider ist dafür jedoch letztlich nicht erforderlich. Dies ist nach Artikel 14 Absatz 6 VO-E vielmehr Aufgabe der zuständigen Behörden des Vollstreckungsstaates.

7. Wie hat sich die Bundesregierung mit dem Vorschlag zur Aufnahme weiterer Eingriffsvoraussetzungen („safeguards“) sowie eines Tandem-Verfahrens in den Verordnungsentwurf durchsetzen können (Bundestagsdrucksache 19/5207, Antwort zu Frage 3), und wie soll sich dies auf herausverlangte „Bestandsdaten“, „Zugangsdaten“ und „Verkehrsdaten“ sowie auf „Inhaltsdaten“ unterschiedlich auswirken?

Auf die Antworten zu den Fragen 3 und 4 wird zunächst verwiesen. Die Bundesregierung hat sich intensiv in die Verhandlungen zur EPOC-VO eingebracht und konnte so zahlreiche Impulse für Nachbesserungen am Textvorschlag der Kommission setzen. Wichtige Anliegen der Bundesregierung haben bereits Eingang in den Verordnungsentwurf gefunden. So wurde mit Blick auf die „safeguards“ Erwägungsgrund 12a in den Text der EPOC-VO in der Fassung der Allgemeinen Ausrichtung vom Dezember 2018 aufgenommen, der das „ne bis in idem“-Prinzip verankert. In Erwägungsgrund 29 der EPOC-VO wurde das Erfordernis des Grundrechtsschutzes stärker hervorgehoben. Für Fälle, in denen die Herausgabeanordnung auf die Erlangung verschiedener Datenkategorien gerichtet ist („Mischfälle“), wird in Erwägungsgrund 33a VO-E auf Betreiben der Bundesregierung nun klargestellt, dass die jeweils für die Datenkategorien geltenden Standards einzuhalten sind, also keine „Vereinheitlichung auf niedrigem Standard“ erfolgen darf. Daneben schließt der neu aufgenommene Artikel 3 Absatz 1a VO-E aus, dass eine Europäische Herausgabe- oder Sicherungsanordnung auf Veranlassung eines anderen Mitgliedstaates oder eines Drittstaates erlassen wird. Der neue Artikel 12b VO-E enthält ergänzend dazu eine ausdrückliche Vorschrift zur Spezialitätsbindung. Die Unterrichtungspflichten gegenüber betroffenen Personen in Artikel 11 VO-E sowie auch die Rechtsbehelfsregelungen in Artikel 17 VO-E wurden in wichtigen Punkten verbessert.

Mit Blick auf das Bestreben der Bundesregierung, ein Tandem-Verfahren in der EPOC-VO zu verankern, konnten ebenfalls wichtige Fortschritte erzielt werden. Das Verfahren zum Erlass von Herausgabeanordnungen, die auf die Erlangung von Transaktionsdaten gerichtet sind, wurde verbessert (Artikel 5 Absatz 7 VO-E), und für Herausgabeanordnungen, die auf die Erlangung von Inhaltsdaten gerichtet sind, wurde ein Notifikationsverfahren aufgenommen (Artikel 7a VO-E). Der zusätzlich aufgenommene Artikel 12a VO-E ergänzt diese Verbesserungen für Daten, die bereits an den Anordnungsstaat übermittelt wurden.

Die Artikel 5 Absatz 7, 7a und 12a VO-E lassen Einwände gegen die grenzüberschreitende Datengewinnung oder die Datennutzung aufgrund von im Einzelfall bestehenden Immunitäten und Vorrechten, mit Blick auf die Meinungs- und Pressefreiheit sowie mit Blick auf Interessen der nationalen Sicherheit und Verteidigung zu.

Trotz der bereits erzielten Verhandlungserfolge hat die Bundesregierung – gemeinsam mit sechs anderen Mitgliedstaaten – die allgemeine Ausrichtung auf dem JI-Rat im Dezember 2018 nicht mitgetragen. Die Bundesregierung setzt darauf, dass im Trilog mit der EPOC-VO Lösungen gefunden werden, die der Überprüfung durch den Europäischen Gerichtshof und durch die nationalen Verfassungsgerichte Stand halten. Die Bundesregierung setzt sich daher weiterhin dafür ein, dass beispielsweise in Artikel 5 VO-E eine deutlichere Grundrechtsbindung erfolgt, dass die Notifikationslösung in Artikel 7a VO-E auch auf Herausgabeanordnungen erstreckt wird, die auf die Erlangung von Transaktionsdaten gerichtet sind, dass der notifizierte Mitgliedstaat eine echte Widerspruchmöglichkeit im Notifikationsverfahren erhält, und dass insgesamt ein drohender Grundrechteverstoß als berechtigter Einwand im Notifikationsverfahren festgeschrieben wird.

Die Bundesregierung hält zudem auch weitere Nachbesserungen für wünschenswert, beispielsweise eine weitere Überarbeitung von Artikel 17 VO-E in dem Sinne, dass auch gegen die Europäische Sicherungsanordnung Rechtsbehelfe möglich sein müssen.

8. Sollen aus Sicht der Bundesregierung im Rahmen der Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (etwa im „Tandem-Verfahren“ oder einer „Notifikationslösung“; vgl. Ratsdokument 15020/18 sowie Bundestagsdrucksache 19/3392, Antwort zu Frage 21) nur die Regierung bzw. dort zuständigen Behörden informiert werden, auf deren Hoheitsgebiet sich ein betreffender Server befindet, für den eine Firma eine Herausgabeanordnung erhält (in vielen Fällen vermutlich Irland), oder auch die Regierung bzw. dort zuständigen Behörden des Landes, deren Staatsangehörigkeit die von der Maßnahme betroffene Person besitzt (vgl. http://gleft.de/2D8)?

Die EPOC-VO in der Fassung der Allgemeinen Ausrichtung vom Dezember 2018 sieht für Herausgabeanordnungen, die auf die Erlangung von Inhaltsdaten gerichtet sind, eine Notifikation des Vollstreckungsstaats vor. Der Vollstreckungsstaat ist der Mitgliedstaat, in dem der Provider seinen Vertreter benannt hat. Die Benennung des Vertreters richtet sich nach der Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, die die Kommission zusammen mit der EPOC-VO vorgeschlagen hat. Hat der Provider keinen Vertreter benannt, ist die Niederlassung des Providers entscheidend, an die die Anordnung übermittelt wurde (Artikel 7 Absatz 2 VO-E). Auf den Speicherort der Daten bzw. den Ort, an dem der Server steht, kommt es nicht an. Auch dem Staat der Staatsangehörigkeit der betroffenen Person kommt keine Rolle im Verfahren zu.

Die Bundesregierung trägt den im Kompromisswege erarbeiteten Ansatz, auf den Vollstreckungsstaat abzustellen, grundsätzlich mit. Zwar ist aus Sicht der Bundesregierung der Mitgliedstaat des dauernden Aufenthalts der von der Datenabfrage betroffenen Person der „grundrechtsnähere“ Staat. Allerdings wirft dieser Ansatz Probleme auf, wenn der Aufenthaltsstaat den Ermittlungsbehörden im Anordnungsstaat nicht bekannt ist, oder wenn mehrere Personen mit verschiedenen Aufenthaltsstaaten betroffen sind. Auch nach den Vorstellungen der Bundesregierung hätte es vor allem für erstgenannte Fälle einer Auffanglösung bedurft. Auch die Bundesregierung hatte für diese Auffanglösung die Einbindung des Vollstreckungsstaates vorgeschlagen, denn diesem Mitgliedstaat kommt ohnehin eine wichtige Rolle im Verfahren nach der EPOC-VO zu.

Ergänzend weist die Bundesregierung darauf hin, dass sie sich für eine Konkretisierung der Kriterien für die Benennung der gesetzlichen Vertreter der Diensteanbieter einsetzt und dadurch mittelbar einen weitgehenden Gleichlauf des Vollstreckungsstaats und des Aufenthaltsstaats des Datennutzers erreichen möchte. Nach diesem Vorschlag soll der gesetzliche Vertreter insbesondere in dem Mitgliedstaat benannt werden, auf den der Dienstanbieter seine Tätigkeit ausgerichtet hat und in dem ein Schwerpunkt seines Nutzeraufkommens liegt.

9. Nach welchem Verfahren und in welchen Fällen sollen die staatlichen Behörden des von einem Herausgabeverlangen im Rahmen der Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen mitbetroffenen Mitgliedstaats aus Sicht der Bundesregierung „frühzeitig eingebunden werden und so ein arbeitsteiliges Zusammenwirken der zuständigen Behörden erreicht wird“ (Bundestagsdrucksache 19/3392, Antwort zu Frage 1)?

Die Bundesregierung spricht sich für ein Notifikationsverfahren mit einer echten Widerspruchsmöglichkeit des Vollstreckungsstaats mindestens bei Transaktions- und Inhaltsdaten aus, siehe bereits die Antworten zu vorstehenden Fragen.

a) Nach welcher Maßgabe soll aus Sicht der Bundesregierung ein betroffener Staat über ein an eine Firma gerichtetes Herausgabeverlangen informiert werden, und welche Kanäle (etwa Brief, Fax oder E-Mail) könnten hierfür genutzt werden („Elektronische Beweismittel: Zugriff auf Nutzerdaten ohne Kontrolle“, https://futurezone.at vom 16. Januar 2019)?

Zu den Maßgaben der Notifikation wird auf vorstehende Ausführungen Bezug genommen. Sichere Übertragungswege und hohe technische Anforderungen zur Gewährleistung der Authentizität der Anordnungsbehörde sind aus Sicht der Bundesregierung unerlässlich. Auf Betreiben der Bundesregierung wurde auch insoweit der Vorschlag der Europäischen Kommission noch weiter verbessert, siehe Artikel 8 Absatz 2 und Artikel 9 Absatz 1 VO-E in der Fassung der Allgemeinen Ausrichtung vom Dezember 2018 mit den ergänzenden Erwägungsgründen 39 und 40. Die konkrete Umsetzung dieser Anforderungen wird Teil der Durchführungsarbeiten zur EPOC-VO auf Ebene der Europäischen Union sowie auch in den Mitgliedstaaten sein.

b) Wie soll aus Sicht der Bundesregierung in Bezug auf ein Herausgabeverlangen mit Daten umgegangen werden, deren Speicherort oder Hoster unbekannt ist, bzw. auf welche Weise ließe sich diese Fallgestaltung lösen (Bundestagsdrucksache 19/3392, Antwort zu Frage 11)?

Auf die Antwort der Bundesregierung zu Frage 11 der Kleinen Anfrage auf Bundestagsdrucksache 19/3392 wird verwiesen. Da eine Herausgabe- oder Sicherungsanordnung grundsätzlich an den Vertreter des Providers zu richten ist, sind Speicherort und Hoster nicht entscheidend.

10. Welche Haltung vertritt die Bundesregierung zur Frage, ob Behörden der Mitgliedstaaten direkt auf Daten bei Internetdienstleistern zugreifen können sollen, und wie hat sie sich in der Diskussion um diese Frage im Rat positioniert (Ratsdokument 9418/18)?

Die Bundesregierung hatte sich im Zuge der von der Europäischen Kommission geleiteten Vorarbeiten zu den E-Evidence-Legislativvorschlägen dafür ausgesprochen, europaweit einheitliche Lösungen für die Frage des „direct access“ zu entwickeln, also für Datenzugriffe, die ohne Hilfeleistung durch die Provider im Rahmen von zulässigen Ermittlungsmaßnahmen möglich sind. Dies wurde jedoch im Legislativvorschlag nicht aufgegriffen.

a) Was ist der Bundesregierung über Bemühungen der Europäischen Kommission bekannt, über „Maßnahmen zum direkten Zugang“ weiter zu reflektieren (COM (2018) 225 final – 2018/0108 (COD))?

Der Bundesregierung liegen dazu keine Erkenntnisse vor.

b) Welche „Möglichkeiten des Zugangs“ setzen Bundesbehörden im Rahmen ihrer Befugnisnormen und anwendbaren völkerrechtlichen Verträge ein (Bundestagsdrucksache 19/3392, Antwort zu Frage 11; bitte für einige denkbare Einzelfälle darstellen)?

Die Ermittlungsmöglichkeiten für die Strafverfolgungsbehörden in der Bundesrepublik Deutschland richten sich nach § 110 Absatz 3 der Strafprozessordnung.

11. Welche Haltung vertrat die Bundesregierung in den Diskussionen zum Verordnungsentwurf zur Frage, ob der von der Europäischen Kommission vorgeschlagene Rechtsakt auch für in Echtzeit abgehörte Telefonate („real-time interception of data“) gelten soll (Ratsdokument 9418/18, Bundestagsdrucksache 19/3392, Antwort zu Frage 2)?

Die grenzüberschreitende Gewinnung von elektronischen Beweismitteln in Echtzeit ist gegenwärtig nicht Gegenstand der EPOC-VO. Die Bundesregierung hält dies für sachgerecht.

a) Mit welchen Argumenten hatten sich nach Kenntnis der Bundesregierung „Minister aus Belgien, Portugal, Zypern, Frankreich, Griechenland, Italien und Estland“ für das Abhören von Kommunikationsdaten in Echtzeit ausgesprochen („Zugriff auf Daten: EU-Justizminister uneins über Polizei-Befugnisse“, www.euractiv.de vom 5. Juni 2018)?

Für eine Einbeziehung von Echtzeitmaßnahmen steht das Argument einer effizienteren Strafverfolgung durch erweiterte Möglichkeiten der grenzüberschreitenden Beweisgewinnung im Raum. Zudem wird zum Teil darauf verwiesen, dass auch der US-amerikanische CLOUD Act eine Abfrage von Echtzeitmaßnahmen zulasse.

b) Inwiefern sind aus Sicht der Bundesregierung gemäß dem Verordnungsentwurf bzw. der vom Rat verabschiedeten Position auch online gesicherte Geräte-Backups von einem Herausgabeverlangen umfasst?

Nach Ansicht der Bundesregierung können auch online gesicherte Geräte-Backups von einem Herausgabeverlangen umfasst sein.

12. Wann will die EU-Kommission nach Kenntnis der Bundesregierung mit den Verhandlungen mit der US-Regierung hinsichtlich eines für alle Mitgliedstaaten geltenden Durchführungsabkommen für den „Clarifying Lawful Overseas Use of Data (CLOUD) Act“ zur verpflichtenden Offenlegung von Bestands-, Verkehrs- und Inhaltsdaten beginnen, und welche Haltung der US-Regierung ist der Bundesregierung hierzu bekannt?

Nach Vorlage eines Entwurfs für ein Verhandlungsmandat zum Abschluss eines Verwaltungsabkommens mit den USA zur Erhebung elektronischer Beweismittel am 5. Februar 2019 beabsichtigt die Kommission, die Verhandlungen im Juni 2019 zu beginnen. Zuvor hat jedoch der Rat über das Mandat zu beraten und einen Beschluss zu fassen. Zur Haltung der US-Regierung zum Beginn der Verhandlungen liegen der Bundesregierung keine Erkenntnisse vor.

a) Was ist der Bundesregierung darüber bekannt, inwiefern die US-Regierung mit einzelnen EU-Mitgliedstaaten (etwa mit Großbritannien) selbst entsprechende Gespräche oder Verhandlungen führt?

Der Bundesregierung ist bekannt, dass die US-Regierung seit längerem mit Großbritannien über ein bilaterales Abkommen verhandelt. Darüber, ob die US-Regierung auch mit anderen Mitgliedstaaten der Europäischen Union Gespräche führt, liegen der Bundesregierung keine Erkenntnisse vor. Im Hinblick auf die jüngst erfolgte Vorlage eines Entwurfs für ein Verhandlungsmandat durch die Europäische Kommission geht die Bundesregierung davon aus, dass es zu Verhandlungen der Europäischen Union mit den USA kommen wird.

b) Mit welcher Fragestellung stand das Thema der Herausgabe elektronischer Beweismittel in Strafsachen nach Kenntnis der Bundesregierung auf der Agenda der jüngsten EU-US-Ministertreffen?

Das Thema des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln wurde im Rahmen der beiden EU-US Ministertreffen für den Justiz- und Innenbereich im Jahr 2018, die am 22./23. Mai und am 8./9. November 2018 stattfanden, erörtert. Die Mitgliedstaaten nehmen an diesen Treffen nicht selbst teil, die EU wird jeweils durch die amtierende und nächste Präsidentschaft sowie die Kommission vertreten. Die Mitgliedstaaten werden dann in der jeweils nächsten Ratssitzung über das Ergebnis informiert.

- EU-US Ministertreffen am 22./23. Mai 2018

Nach den der Bundesregierung hierzu vorliegenden Informationen haben beide Seiten einander über die jeweiligen aktuellen Gesetzgebungsvorhaben zur Regelung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln informiert, d. h. den US-CLOUD Act und die Kommissionsvorschläge zur Verordnung über Europäische Herausgabe- und Sicherungsanordnungen sowie zur Richtlinie zur Benennung der gesetzlichen Vertreter der Diensteanbieter. Beide Seiten hätten ihren Willen bekräftigt, Kompatibilität der jeweiligen Vorhaben sicherzustellen. Allerdings gebe es unterschiedliche Interpretationen zu den angemessenen Verfahren und Instrumenten, und deshalb bedürfe es weiterer Klarstellung und Diskussion.

- EU-US Ministertreffen am 8./9. November 2018

Nach Kenntnis der Bundesregierung hat die Kommission über die laufenden Beratungen zu den Gesetzgebungsvorschlägen zu E-Evidence informiert. Die USA hätten sich interessiert daran gezeigt, mit der EU ein (Rahmen-)Abkommen zum Zugang zu elektronischen Beweismitteln auszuhandeln.

13. Was ist der Bundesregierung über den Stand der Arbeiten an einem Zweiten Zusatzprotokoll des Budapester Übereinkommens über Computerkriminalität („Cybercrime-Konvention“) bekannt?

Das derzeit verhandelte Zweite Zusatzprotokoll soll die Budapest Konvention ergänzen und hat die grenzüberschreitende Beweiserhebung durch Strafverfolgungsbehörden zum Gegenstand. Die Budapest Konvention stammt aus dem Jahr 2001 und wurde ausgehandelt, um dem grenzüberschreitenden Charakter der Kriminalität im Internet Rechnung zu tragen. Das Übereinkommen enthält Vorgaben sowohl für konkrete Straftatbestände (unter anderem Verletzungen des Urheberrechts, Betrugstatbestände, Kinderpornographie, Angriffe auf die Netzsicherheit) als auch zum Verfahrensrecht (Erstreckung von Durchsuchungen auf externe

Speicher, Möglichkeit der schnellen Datensicherung). Ein weiterer Komplex befasst sich mit Fragen der internationalen Zusammenarbeit.

Ziel dieses Zusatzprotokolls ist eine stärkere Zusammenarbeit zwischen den Parteien bei der Sicherung elektronischer Beweismittel und der Verfolgung von Computerkriminalität.

Der Text des Zweiten Zusatzprotokolls soll zunächst durch von den Parteien entsandte Experten erarbeitet werden. Für die Bundesregierung nimmt eine Expertin aus dem Bundesministerium der Justiz und für Verbraucherschutz an diesen Arbeiten teil. Die letzte Sitzung fand am 12. und 13. Februar 2019 statt und hat sich mit den Themen „Beschleunigung der Verfahren zum Austausch von Bestands- und Verkehrsdaten zwischen den beteiligten Staaten“ und „freiwillige Herausgabe von Bestands- und Verkehrsdaten durch Provider“ befasst. Am Ende dieses Prozesses soll ein vom zuständigen Ausschuss gebilligter Vertragstext stehen, der danach von den Parteien der Budapest Konvention gezeichnet und ratifiziert werden kann. Weder die Zeichnung noch die Ratifizierung sind hierbei für die teilnehmenden Parteien verpflichtend. Der Abschluss der Arbeiten der Expertengruppe ist für Dezember 2019 geplant.

14. Welche Mitgliedstaaten des Europarates oder sonstigen Teilnehmer beteiligen sich nach Kenntnis der Bundesregierung aktiv an den Verhandlungen für das geplante Zweite Zusatzprotokoll des Budapester Übereinkommens über Computerkriminalität bzw. der damit beauftragten Arbeitsgruppe zu Cloud-Beweismitteln des Europarates („Cloud Evidence Group“)?

Die folgenden Staaten entsenden regelmäßig Experten zu der Expertengruppe („Protocol Drafting Group“): Albanien, Australien, Chile, Deutschland, Dänemark, Estland, Finnland, Frankreich, Großbritannien, Italien, Japan, Kanada, Mauritius, Niederlande, Norwegen, Polen, Rumänien, Schweiz, Senegal, Slowakei, Spanien, Sri Lanka, Tschechische Republik, Türkei, Ukraine, Vereinigte Staaten von Amerika.

15. In welchen Abschnitten enthält das geplante Zweite Zusatzprotokoll des Budapester Übereinkommens über Computerkriminalität nach Kenntnis der Bundesregierung ähnliche Inhalte wie die geplante Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen?

16. In welchen wesentlichen Punkten unterscheidet sich das geplante Zweite Zusatzprotokoll des Budapester Übereinkommens über Computerkriminalität aus Sicht der Bundesregierung von der geplanten Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen?

Die Fragen 15 und 16 werden gemeinsam beantwortet.

Wie in der Antwort zu Frage 13 ausgeführt, wird der Text des Zweiten Zusatzprotokolls derzeit von einer Expertengruppe erarbeitet. Diese Arbeiten sind noch nicht so weit fortgeschritten, dass es bereits einen fertigen Vertragsentwurf gäbe. Die „Terms of Reference“ des Zusatzprotokolls sehen vor, dass ein mögliches Element des Zusatzprotokolls die direkte Kooperation mit Diensteanbietern in den Bereichen Abfrage von Bestandsdaten, Sicherung von Daten und Anfragen in Notfällen ist. Anders als bei der EPOC-VO ist eine Einbeziehung von Verkehrs- oder Inhaltsdaten in die direkte Kooperation mit Diensteanbietern jedoch nicht beabsichtigt.

17. Wie soll aus Sicht der Bundesregierung mit Herausgabeverlangen im Rahmen des geplanten Zweiten Zusatzprotokolls des Budapester Übereinkommens über Computerkriminalität umgegangen werden, wenn sich die betroffenen Firmen außerhalb des Hoheitsgebiets einer Vertragspartei des Europarates befinden?

Als völkerrechtlicher Vertrag bindet das Zusatzprotokoll nur die Vertragsparteien. Daher sind nur die Staaten, die den Vertragstext zeichnen und ratifizieren, verpflichtet, diesen innerhalb ihres Territoriums umzusetzen. Die Bestimmungen des Zweiten Zusatzprotokolls werden daher auf dem Territorium eines Staates, der dieses nicht gezeichnet oder ratifiziert hat, keine Anwendung finden.

18. Wie sollte die EU-Kommission aus Sicht der Bundesregierung ihr Verhandlungsmandat hinsichtlich des CLOUD Act inhaltlich gestalten, damit sich die Arbeiten an der Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und dem geplanten Zweiten Zusatzprotokoll des Budapester Übereinkommens über Computerkriminalität nicht doppeln bzw. keine Friktionen zwischen beiden Rechtsakten geschaffen werden?

Aus Sicht der Bundesregierung besteht in der Herstellung der Kompatibilität beider Regelungen, der EPOC-VO einerseits und des CLOUD Acts andererseits, eine der größten Herausforderungen der Verhandlungsführung. Dies betrifft insbesondere die Frage, wie die Einbeziehung eines weiteren Staates neben dem Anordnungsstaat geregelt werden kann. Während der CLOUD Act eine solche Einbeziehung nicht vorsieht, geht die EPOC-VO in der Fassung der Allgemeinen Ausrichtung vom Dezember 2018 bei Herausgabeanordnungen, die auf die Erlangung von Inhaltsdaten gerichtet sind, von der Einbindung des Vollstreckungsstaates durch den Anordnungsstaat aus. Vor diesem Hintergrund begrüßt die Bundesregierung, dass im Verhandlungsmandat eine enge Einbindung des Rates vorgesehen ist.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333