Bundesrat **Drucksache 215/18 (Beschluss)**

06.07.18

Beschluss
des Bundesrates

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

COM(2018) 225 final

Der Bundesrat hat in seiner 969. Sitzung am 6. Juli 2018 gemäß §§ 3 und 5 EUZBLG die folgende Stellungnahme beschlossen:

1. Der Bundesrat begrüßt grundsätzlich die Zielrichtung des Verordnungsvorschlags, den Strafverfolgungsbehörden geeignete Instrumente für den Umgang mit den zeitgemäßen Kommunikationsmethoden von Straftätern zur Verfügung zu stellen.

2. Er begrüßt daher den Entschluss der Kommission, für die Herausgabe und Sicherung von elektronischen Beweismitteln, die bei Internet-Diensteanbietern gespeichert sind, einen EU-weiten Rechtsrahmen festzulegen. Die Notwendigkeit einer Regelung auf der Ebene der EU liegt angesichts der zunehmenden Bedeutung elektronischer Beweismittel zur Bekämpfung sowohl der Internet- als auch aller sonstiger Formen der Kriminalität auf der Hand. Erforderlich ist daher ein Rechtsinstrument, das effektiv, praktikabel und zeitnah die Gewinnung von elektronischen Beweismitteln bei Internet-Diensteanbietern ermöglicht, jedoch zugleich in angemessener Weise dem Grundrechtsschutz gerecht wird und die bewährten Prinzipien internationaler strafrechtlicher Zusammenarbeit fortentwickelt.

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 0720-2946

3. Der Bundesrat geht davon aus, dass die vorgeschlagenen Maßnahmen einen höheren Verwaltungsaufwand für die Informations- und Kommunikationstechnologie-Branche bedeuten. Denn trotz der vorgesehenen Vereinheitlichung der Ersuchen ist davon auszugehen, dass die sogenannten Diensteanbieter mit einer größeren Zahl von Anfragen konfrontiert werden. Er bittet die Bundesregierung daher, sich bei den weiteren Verhandlungen auf europäischer Ebene für eine möglichst geringe Bürokratiebelastung und – soweit diese unvermeidbar ist – für Entlastungen der betroffenen Unternehmen an anderer Stelle einzusetzen.

4. Der Bundesrat ist sich der über die EU hinaus strahlenden Wirkung eines solchen Regelungsvorschlags bewusst. Mit dem Verordnungsvorschlag sowie dem parallel vorgelegten Richtlinienvorschlag zur Festlegung einheitlicher Regelungen für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren (BR-Drucksache 218/18) soll ein Rechtsregime geschaffen werden, das Internet-Diensteanbieter zur Sicherung und Herausgabe von Beweismitteln verpflichtet, unbeschadet des Umstands, ob ihr Sitz innerhalb der EU liegt oder die von ihnen verarbeiteten Daten auf Servern innerhalb der EU oder in einem Drittstaat gespeichert werden. Dies stellt ein Novum in der internationalen strafrechtlichen Zusammenarbeit dar, die bisher für die Vornahme strafprozessualer Handlungen an den Ort der Vornahme und die bestehende Verfügungsberechtigung des Adressaten über die geforderten Beweismittel anknüpft.

5. Der Bundesrat begrüßt das Bestreben der Kommission, in der vorgeschlagenen Verordnung das sogenannte Marktortprinzip zu verankern. Mit dem Marktortprinzip wird der Umstand in den Mittelpunkt gerückt, ob ein Internet-Diensteanbieter seine Dienste auf dem Gebiet der EU anbietet. Die damit verbundene Abkehr vom Territorialitätsprinzip bedeutet zwar einen Verzicht auf das Kriterium des Speicherorts der Daten. Dieses weist angesichts der Natur der Daten mit ihrer großen Mobilität und Volatilität aber ohnehin einen hohen Grad an Beliebigkeit auf. Durch das Marktortprinzip werden auch Internet-Diensteanbieter erfasst, die ihre Dienste auf dem Gebiet der Union anbieten, aber ihren Geschäftssitz außerhalb der Union haben. Hierzu zählen zahlreiche marktbeherrschende Unternehmen, bei denen den Strafverfolgungsbehörden nach dem derzeitigen Recht ein schneller und leichter Zugang zu den Daten, insbesondere zu Transaktions- und Inhaltsdaten, im Regelfall nicht möglich ist.

Darüber hinaus kann mit dem Kriterium des Marktorts den erheblichen Schwierigkeiten bei der Bestimmung des Speicherorts begegnet werden. Das Kriterium des Marktorts wird den tatsächlichen Gegebenheiten auch besser gerecht als das Kriterium des Geschäftssitzes des Internet-Diensteanbieters. Denn letzterer ist im Regelfall nicht deckungsgleich mit seinem (beabsichtigten) Wirkungskreis.

6. Der Bundesrat weist jedoch darauf hin, dass die Regelungen des von der Kommission gemäß Artikel 82 Absatz 1 AEUV gewählten Rechtsinstruments einer unmittelbar anwendbaren Verordnung für die staatsanwaltschaftliche und gerichtliche Praxis schwer handhabbar sein dürfte. Denn die Rechtsanwender müssten neben dem bestehenden nationalen Recht die unmittelbar anwendbaren Regelungen des Verordnungsvorschlags beachten und sämtliche Rechtsgrundlagen in aufeinander abgestimmter Weise anwenden. Ein derartiges Regime parallel anzuwendender unterschiedlicher Regelungsschichten ist kompliziert und wird die Akzeptanz und die Geeignetheit des Instruments im Hinblick auf die an sich erstrebte Erleichterung der Gewinnung elektronischer Beweismittel erheblich reduzieren. Das gilt umso mehr, als die Verordnung gemäß Artikel 23 des Verordnungsvorschlags neben der Richtlinie 2014/41/EU vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen bestehen bleiben soll und die Ermittlungsbehörden neben einer Herausgabeanordnung parallel Europäische Ermittlungsanordnungen nutzen können sollen. Dasselbe Ziel, die Erlangung elektronischer Daten, könnte sodann entweder über unmittelbar anwendbares europäisches Recht oder über nationales Recht in Umsetzung europäischen Rechts erreicht werden. Eine unmittelbar anwendbare Verordnung stellt zudem im Strafrechtsbereich nach wie vor einen Fremdkörper dar. Die Verordnung über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen ist noch nicht verabschiedet. Selbst im Falle einer Verabschiedung dieses Gesetzgebungsvorschlags in Form einer Verordnung würde es sich bei diesem Gesetzgebungsakt um eine sehr eng begrenzte Ausnahme im Strafrechtsbereich handeln. Insbesondere im Zusammenhang mit der Erhebung von Beweismitteln ist ein vergleichbares Regelungsinstrument nach wie vor unbekannt. Ferner enthält der Verordnungsvorschlag bereits zum jetzigen Zeitpunkt Regelungen wie Artikel 13, Artikel 17 Absatz 2 oder Artikel 17 Absatz 6, die gegebenenfalls einer Umsetzung in nationales Recht bedürfen. Der Bundesrat bittet daher, zu prüfen, ob nicht das Rechtsinstrument einer Richtlinie gegenüber der Verordnung vorzuziehen ist. Bei der Umsetzung der Regelungen einer Richtlinie in nationales Recht kann eine Einpassung in vor-

handene und bewährte Strukturen und Verfahren erfolgen. Die Rechtsanwender müssten nicht parallel Regelungen verschiedener Rechtsebenen anwenden, sondern könnten sich in ihnen bekannten Strukturen und Verfahren bewegen.

7. Der Bundesrat fordert die Bundesregierung auf, sich weiterhin für eine stärkere Einbindung des Vollstreckungsstaats und für eine stärkere Wahrung der Hoheitsrechte der Mitgliedstaaten einzusetzen.

   a) Er macht darauf aufmerksam, dass Bedenken hinsichtlich der Rechtsgrundlage bestehen, auf die die Kommission den Verordnungsvorschlag stützt (Artikel 82 Absatz 1 AEUV), soweit der Verordnungsvor-schlag in den Artikeln 7 bis 10 eine unmittelbare Zusammenarbeit zwischen dem Internet-Diensteanbieter und der Anordnungsbehörde ohne Einbindung einer justiziellen Stelle in dem Mitgliedstaat, in dem die Daten herausgegeben werden sollen, erlaubt. Eine solche direkte Zusammenarbeit lässt sich nicht ohne weiteres unter den Begriff der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen in Artikel 82 Absatz 1 Unterabsatz 2 Buchstabe a AEUV subsumieren. Denn in erster Linie zielt der Vorschlag der Kommission auf eine unmittelbare Beweisaufnahme in einem anderen Mitgliedstaat und nur zweitrangig auf die Anerkennung einer Entscheidung des Anordnungsstaats durch eine Behörde des Vollstreckungsstaats. Die justiziellen Behörden des anderen betroffenen Mitgliedstaats sollen nach dem Verordnungsvorschlag im Regelfall nicht eingebunden werden; ob dies noch als eine Zusammenarbeit zwischen Behörden der Mitgliedstaaten (Artikel 82 Absatz 1 Unterabsatz 2 Buchstabe d AEUV) angesehen werden kann, erscheint ebenso fraglich. Soweit die Kommission in Bezug auf die Rechtsgrundlage einen Vergleich mit der justiziellen Zusammenarbeit in Zivilsachen vornimmt, ist darauf hinzuweisen, dass zwischen der justiziellen Zusammenarbeit in Zivil- und Strafsachen wesentliche strukturelle Unterschiede bestehen, die zu einer mangelnden Vergleichbarkeit beider Rechtsgebiete führen. Soweit im Bereich der justiziellen Zusammenarbeit in Zivilsachen eine gesonderte Anerkennung von Entscheidungen durch den Anerkennungsstaat entfällt, entspricht dies der Logik des Integrationsprozesses. Sie spiegelt den inzwischen erreichten Harmonisierungsstand wieder, in dem die Zivilgerichte der Mitgliedstaaten grenzüberschreitende Streitigkeiten zunehmend auf der Basis angeglichenen Rechts entscheiden und das Gemeinschaftsrecht dezentral vollziehen. Eine vergleichbare Harmonisierung der Strafrechtssysteme hat bislang nicht stattgefunden und stößt auch

an enge kompetenzielle Grenzen im Strafrecht. Das Strafrecht zählt traditionell zum Kernbereich der nationalen Selbstbestimmung. Durch die stärkere Einbindung der Behörden des Vollstreckungsmitgliedstaats und deren justizielle Entscheidungen über die Zulässigkeit der Maßnahmen könnten diese Bedenken zu der Rechtsgrundlage des Artikels 82 Absatz 1 AEUV ausgeräumt werden.

b) Der Bundesrat gibt zu bedenken, dass die von der Kommission vorgeschlagene Lösung, dass sich die Anordnungsstelle unmittelbar und ohne Beteiligung des Vollstreckungsmitgliedstaats mit den Herausgabe- und Sicherungsanordnungen an den betroffenen Internet-Diensteanbieter wenden darf, mit den bisherigen Prinzipien der justiziellen Zusammenarbeit in Strafsachen bricht. Eine derartige Regelung würde tiefe Einschnitte im Hinblick auf die Souveränität der Mitgliedstaaten bedeuten. Zwar erlaubt Artikel 23 Absatz 1 Satz 2 des Grundgesetzes die Übertragung von Hoheitsrechten auf die EU. Das schließt nicht aus, dass sodann einzelne Behörden eines anderen Mitgliedstaats mit der Wahrnehmung von Hoheitsrechten bestimmter Aufgaben mit Wirkung gegenüber Deutschland betraut werden. Nicht zulässig ist hingegen die Übertragung von Hoheitsrechten an einzelne oder mehrere andere Mitgliedstaaten. Im Hinblick auf den besonders grundrechtssensiblen Bereich des Strafrechts und der Strafverfolgung bedarf eine umfassende Übertragung von Hoheitsrechten an die Union jedenfalls einer besonders genauen Prüfung.

c) Der Bundesrat weist darauf hin, dass die im Verordnungsvorschlag vorgesehenen Regelungen zur Vermeidung der Verletzung von Immunitäten, Zeugnisverweigerungsrechten und anderen Vorrechten im Vollstreckungsstaat sowie von Grundrechten durch den Anordnungsstaat und den Internet-Diensteanbieter als nicht ausreichend erscheinen. Soweit der Verordnungsvorschlag vorsieht, dass der Internet-Diensteanbieter den Vollstreckungsstaat zu unterrichten hat, wenn er der Ansicht ist, dass die Anordnung offensichtlich gegen Grundrechte verstößt oder offensichtlich missbräuchlich ist (Artikel 9 Absatz 5 Unterabsatz 2 des Verordnungsvorschlags), vermag diese Vorschrift über die Defizite der derzeitigen Regelung nicht hinwegzuhelfen. Denn mit dieser Regelung wird einer privaten Rechtsperson, dem Internet-Diensteanbieter, eine Prüfungspflicht in Bezug auf die Rechtmäßigkeit strafprozessualer Maßnahmen auferlegt. Die Bewilligung von Rechtshilfeersuchen und die damit einhergehende Prüfung von grundrechtlichen Garantien sind jedoch staatliche Aufgaben. Mit der vorgeschlagenen

Regelung würde es daher im Bereich der Rechtshilfe zu einer Privatisierung staatlicher Aufgaben kommen. Darüber hinaus ist dem Internet-Diensteanbieter eine vollständige und verlässliche Überprüfung der Grundrechte des Betroffenen ohnehin nicht möglich, da das zu übermittelnde Zertifikat die für die Überprüfung notwendigen Informationen nicht bereithält. Insbesondere dürfen gemäß Artikel 8 Absatz 3 des Verordnungsvorschlags die Aspekte der Notwendigkeit und der Verhältnismäßigkeit der Anordnung oder nähere Angaben zu den Ermittlungen nicht übermittelt werden. Auch die Schilderung des Tatverdachts ist nicht vorgesehen.

d) Der Bundesrat verweist in diesem Zusammenhang auf die Rechtsprechung des Bundesverfassungsgerichts, das aus Anlass der Prüfung der Verfassungsgemäßheit der Anwendbarkeit der Regelung des Europaratsübereinkommens über Computerkriminalität einen Prüfmaßstab für die Datenübermittlung an ausländische Strafverfolgungsbehörden formuliert hat: Danach hat der deutsche Gesetzgeber im Falle der Übermittlung von personenbezogenen Daten an ausländische Behörden dafür Sorge zu tragen, dass die grundgesetzlichen Grenzen der Datenerhebung und -verarbeitung nicht in ihrer Substanz unterlaufen und dass insbesondere elementare rechtstaatliche Grundsätze nicht verletzt werden (BVerfG, Beschluss vom 21. Juni 2019, 2 BvR 637/09, Randnummer 34).

e) Er macht darüber hinaus darauf aufmerksam, dass die Gefahr besteht, dass durch eine unmittelbare Zusammenarbeit zwischen dem Anordnungsstaat und dem Internet-Diensteanbieter Immunitätsvorschriften, Zeugnisverweigerungsrechte oder andere Schutzrechte auch dadurch unterlaufen werden könnten, dass deren Prüfung ausschließlich dem Anordnungsstaat auferlegt wird. Zugleich besteht die Gefahr, dass nationale Interessen des Vollstreckungsstaats faktisch außen vor bleiben. Artikel 5 Absatz 7 des Verordnungsvorschlags, der vorsieht, dass die Anordnungs-behörde bei der Anforderung von Transaktions- und Inhaltsdaten eine Abklärungspflicht trifft, wenn sie die Verletzung von solchen Rechten oder von grundlegenden Interessen des Vollstreckungsstaats befürchtet, und Artikel 18 des Verordnungsvorschlags, der festlegt, dass etwaige Immunitätsvorschriften und andere Vorrechte nach dem Recht des Mitgliedstaats des Adressaten beziehungsweise grundlegende Interessen des Mitgliedstaats des Adressaten auch noch im Rahmen des Strafverfahrens des Anordnungs-staats Berücksichtigung finden können, stellen keinen Ausgleich für die fehlende Beteiligung des Vollstreckungsstaats dar. Denn diese Mechanismen setzen voraus,

dass die Möglichkeit der Verletzung von Vorrechten oder nationalen Interessen in dem Vollstreckungsstaat, also fremden Rechts oder fremder nationaler Interessen, von der Anordnungsbehörde oder dem späteren Gericht überhaupt erkannt wird. Zugleich wird dem Anordnungsstaat die Prüfung und Auslegung fremden Rechts auferlegt. Soweit grundlegende Interessen des Vollstreckungsstaats betroffen sind, setzt eine angemessene Berücksichtigung dieser Interessen voraus, dass der Anordnungsstaat von den nationalen Interessen des Vollstreckungsstaats Kenntnis hat oder erlangt, selbst wenn diese im Einzelfall als vertraulich eingestuft sind.

f) Der Bundesrat sieht damit die Gefahr, dass bei der Gewinnung elektronischer Beweismittel die Strafverfolgungsbehörden des Vollstreckungsstaats in einem vergleichbaren innerstaatlichen Fall unterschiedlichen strafprozessualen Anforderungen unterliegen. Dies kann im Ergebnis dazu führen, dass die Behörden des Anordnungsstaats auf dem Territorium des Vollstreckungsstaats über weitreichendere Befugnisse verfügen als dessen Behörden – eine Konsequenz, die bislang im Rechtshilferecht ausdrücklich ausgeschlossen worden ist (vergleiche § 59 Absatz 3 IRG).

Aus diesen Gründen hält der Bundesrat eine stärkere Einbindung des Vollstreckungsstaats in das Herausgabeverfahren – zumindest soweit die Herausgabe von besonders grundrechtssensiblen Transaktions- und Inhaltsdaten betroffen ist – unbedingt für erforderlich. Um den Besonderheiten der Beweisgewinnung in elektronischen Speichern gerecht zu werden, könnte dies etwa durch die sogenannte Notifikationslösung in Anlehnung an Artikel 31 der Richtlinie 2014/41/EU und mit damit einhergehenden Zurückweisungsgründen erfolgen. Durch die Verankerung einer solchen Regelung, bei der zeitgleich mit dem Herantreten der Anordnungsbehörde an den Internet-Diensteanbieter eine Unterrichtung des Vollstreckungsstaats zu erfolgen hat und letzterer innerhalb eines bestimmten Zeitfensters der Herausgabe der Daten widersprechen kann, wird der betroffene Vollstreckungsstaat in einem Mindestmaß an der Herausgabe der Daten beteiligt. Durch die Möglichkeit, der Herausgabe in bestimmten Fällen widersprechen zu können, kann sichergestellt werden, dass dem in der Bundesrepublik Deutschland geltenden Grundrechts- und Datenschutz ausreichend Rechnung getragen wird. Insbesondere im Hinblick auf die besonders sensiblen Transaktions- und Inhaltsdaten, die entweder einzeln oder in ihrer Gesamtheit sehr genaue Rückschlüsse auf das Privatleben der betroffenen Personen zulassen, ist eine Beteiligung des Vollstreckungsstaats sicherzustellen.

8. Der Bundesrat spricht sich dafür aus, dass zur Gewährleistung eines ausreichenden Grundrechtsschutzes in der Verordnung eine Vorschrift vergleichbar mit Artikel 11 Absatz 1 Buchstabe h der Richtlinie 2014/41/EU verankert wird, die dem Vollstreckungsstaat in Bezug auf Transaktions- und Inhaltsdaten eine Ablehnung der Anerkennung oder Vollstreckung der Anordnung ermöglicht, wenn eine solche Ermittlungsmaßnahme nach nationalem Recht des Vollstreckungsstaats auf eine Liste oder Kategorie von Straftaten oder auf Straftaten, die mit einem bestimmten Mindeststrafmaß bedroht sind, beschränkt ist und die der Anordnung zugrundeliegende Straftat keine dieser Straftaten ist. Ohne einen derartigen Zurückweisungsgrund wäre es möglich, dass der Anordnungsstaat Daten erlangt, die im Vollstreckungsstaat bei einem rein nationalen Sachverhalt für dieselbe Straftat nicht zur Verfügung stehen würden. Zum einen würden dadurch nationale Grundrechtsstandards des jeweils betroffenen Mitgliedstaats unterlaufen. Zum anderen ist zu befürchten, dass das Fehlen eines solchen Zurückweisungsgrunds in der Konsequenz dazu führt, dass bestimmte Standards von den Mitgliedstaaten auch für rein nationale Fälle abgesenkt werden.

9. Er gibt zu bedenken, dass das Prinzip der gegenseitigen Strafbarkeit bei der Herausgabe von grundrechtssensiblen Daten nicht vollständig in den Hintergrund treten darf. Soweit Artikel 5 Absatz 4 des Verordnungsvorschlags die Herausgabe von Transaktions- und Inhaltsdaten ermöglicht, wenn Straftaten verwirklicht worden sind, die im Rahmenbeschluss 2001/413/JI vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln oder in der Richtlinie 2011/93/EU vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie, der Richtlinie 2013/40/EU vom 12. August 2013 über Angriffe auf Informationssysteme oder der Richtlinie (EU) 2017/541 vom 15. März 2017 zur Terrorismusbekämpfung genannt sind, erscheint eine gesonderte Normierung des Prinzips der gegenseitigen Strafbarkeit als nicht zwingend. Der genannte Rahmenbeschluss oder die genannten Richtlinien regeln, dass die Mitgliedstaaten hinsichtlich der dort genannten Straftaten Strafbestimmungen einführen. Damit ist sichergestellt, dass hinsichtlich der dort genannten Straftaten ein gewisses Maß an gegenseitiger Strafbarkeit gewährleistet ist. Soweit Artikel 5 Absatz 4 des Verordnungsvorschlags die Herausgabe von Transaktions- und Inhaltsdaten jedoch auch dann ermöglicht, wenn eine Straftat vorliegt, die im Anordnungsstaat im Höchstmaß

mit einer Freiheitsstrafe von drei Jahren bewehrt ist, ist weder eine gegenseitige Strafbarkeit als Voraussetzung normiert noch ein bestimmter Straftatenkatalog analog der Richtlinie 2014/41/EU vorgesehen. Damit besteht für einen anderen Mitgliedstaat die Möglichkeit, Transaktions- und Inhaltsdaten für Taten zu erlangen, die in dem Mitgliedstaat, in dem die Daten herausgegeben werden sollen, keiner Strafnorm unterworfen sind. Der Bundesrat hält es daher für geboten, für die Herausgabe von Transaktions- und Inhaltsdaten für die grundsätzliche Einhaltung des Prinzips der gegenseitigen Strafbarkeit und die Einführung eines Straftatenkatalogs parallel zu Artikel 11 Absatz 1 Buchstabe h in Verbindung mit Anhang D der Richtlinie 2014/41/EU Sorge zu tragen.

10. Klarstellend weist der Bundesrat darauf hin, dass, soweit lediglich die Herausgabe von Teilnehmer- oder Zugangsdaten begehrt wird, die Einhaltung des Prinzips der gegenseitigen Strafbarkeit und die Normierung von Zurückweisungsgründen für Fälle, in denen bei rein nationalen Sachverhalten die Daten nicht erlangt werden können, hingegen nicht als zwingend angesehen werden. Diese Beweiserhebungen sollen lediglich der Identifizierung eines Beschuldigten dienen und sind daher mit einem wesentlich geringeren Grundrechtseingriff verbunden als die Herausgabe von Transaktions- und Inhaltsdaten. Zudem würde ein Gleichlauf mit der Richtlinie 2014/41/EU hergestellt werden. Soweit die Richtlinie 2014/41/EU Versagungsgründe auf Grundlage des Prinzips der gegenseitigen Strafbarkeit oder des Fehlens von Katalogtaten normiert, besteht bei diesen Versagungsgründen eine Ausnahme für weniger eingriffsintensive Ermittlungsmaßnahmen wie der Identifizierung des Inhabers eines bestimmten Telefonanschlusses oder einer bestimmten IP-Adresse (Artikel 10 Absatz 2, Artikel 11 Absatz 1 Buchstabe g und h, Absatz 2 der Richtlinie 2014/41/EU). Aufgrund des geringeren Eingriffscharakters bei einer bloßen Sicherung der Daten – die Daten werden auf der Grundlage der Sicherungsanordnung nicht herausgegeben – und des Eilcharakters dieser Maßnahme werden auch in Bezug auf Sicherungsanordnungen die Zulässigkeit der Maßnahme nach dem nationalen Recht des Vollstreckungsstaats und das Prinzip der gegenseitigen Strafbarkeit ebenfalls als nicht zwingend angesehen.

11. Der Bundesrat gibt zu bedenken, dass die vorgeschlagene Verordnung einer Erleichterung der Erlangung elektronischer Beweismittel dienen soll. Dazu im Widerspruch steht, dass nach Artikel 4 Absatz 1 und Absatz 3 des Verordnungsvorschlags auch Herausgabe- und Sicherungsanordnungen betreffend Be-

standsdaten mindestens durch einen Staatsanwalt zu erlassen und zu validieren sind. Im gegenwärtigen System werden Auskunftsbegehren in Bezug auf Bestandsdaten vielfältig von den polizeilichen Ermittlungsbeamtinnen und -beamten ohne Einbindung der Staatsanwaltschaft getätigt. Ein Großteil der Ersuchen um Bestandsdaten wird auch weiterhin Diensteanbieter betreffen, deren europäischer Sitz in einem Mitgliedstaat liegt, der es erlaubt, dass ausländische Strafverfolgungsbehörden unmittelbar an die dort ansässigen Diensteanbieter herantreten, welche entsprechende Ersuchen auf freiwilliger Basis beantworten können. Die nunmehr vorgesehene zwingende Beteiligung der Staatsanwaltschaften würde in Bezug auf die Bestandsdaten eine Verschlechterung des Status quo bedeuten. Im Laufe der weiteren Verhandlungen sollte dafür Sorge getragen werden, dass Anordnungen in Bezug auf Bestandsdaten auch von polizeilichen Ermittlungsbeamtinnen und -beamten erlassen werden dürfen oder das bestehende Regime freiwilliger Auskunftserteilung von dem Regelwerk unberührt bleibt.

12. Ebenfalls ist der Bundesrat der Auffassung, dass staatsanwaltliche Anordnungen zur Herausgabe von Transaktions- und Inhaltsdaten entgegen Artikel 4 Absatz 2 des Verordnungsvorschlags nicht eine Validierung durch ein Gericht oder einen Ermittlungsrichter benötigen. Nach Artikel 5 Absatz 2 des Verordnungsvorschlags darf eine Europäische Herausgabeanordnung nur erlassen werden, wenn in einem vergleichbaren innerstaatlichen Fall eine ähnliche Maßnahme zur Verfügung stünde, mithin also die Vereinbarkeit nach innerstaatlichem Recht gewährleistet ist. Demzufolge muss die das Verfahren führende Staatsanwaltschaft daher ohnehin eine gerichtliche Entscheidung einholen, wenn dies nach innerstaatlichem Recht erforderlich ist. Im Übrigen obliegt aber die Prüfung der für die internationale Zusammenarbeit erforderlichen Anforderungen in den meisten Mitgliedstaaten der Staatsanwaltschaft. Daher sehen auch die anderen Rechtsakte zur gegenseitigen Anerkennung (beispielsweise Europäischer Haftbefehl oder Europäische Ermittlungsanordnung) die Staatsanwaltschaften als zuständige Anordnungsbehörde vor. Warum im vorliegenden Fall von diesem bislang bewährten System abgewichen werden soll, ist nicht ersichtlich.

13. Der Bundesrat ist ferner der Auffassung, dass die vorgesehenen Legislativakte zur Gewinnung elektronischer Beweismittel nicht zu einer Erosion der bisherigen und bewährten Prinzipien der Rechtshilfe und des international arbeitsteili-

gen Strafverfahrens führen dürfen. Wegen ihrer über die EU hinausgehenden Wirkung werden sie maßgeblich für die Herausbildung internationaler Standards sein, die für die Beweisgewinnung durch Strafverfolgungsbehörden von Drittstaaten im Wege der Reziprozität ebenso bindend sein sollten.

14. Dies gilt namentlich für den US-amerikanischen „Clarifying Lawful Overseas Use of Data Act“ (CLOUD-Act), dessen Auswirkungen der Bundesrat mit großer Sorge betrachtet. Danach sind Diensteanbieter verpflichtet, jegliche Inhalts- und andere Daten, einschließlich der Übermittlungen von fortlaufenden Kommunikationsvorgängen (sogenannte Echtzeit-Überwachung), die einen bestimmten Nutzer betreffen und sich in seinem Besitz, seiner Verwahrung oder unter seiner Kontrolle befinden, unabhängig von ihrem Speicherort auf ein entsprechendes Verlangen einer zuständigen US-Behörde herauszugeben. Hiergegen kann lediglich eingewandt werden, dass es sich um eine Person handelt, die nicht US-Staatsangehöriger ist, dort nicht ihren Aufenthalt hat, und die Herausgabeverpflichtung nicht in Einklang mit den Gesetzen eines Drittstaats steht. Diese Umstände können, müssen aber nicht zu einer Änderung oder Aufhebung der Herausgabeverpflichtung führen. Umgekehrt sieht der CLOUD-Act vor, dass ein IT-Diensteanbieter sich nach US-Recht nicht rechtswidrig verhält, wenn er den Inhalt oder die Überwachung einer elektronischen Kommunikation auf Anordnung einer ausländischen Behörde mitteilt, sofern der US-Justizminister hierüber mit dem betroffenen ausländischen Staat eine Regierungsvereinbarung („Executive Agreement“) abgeschlossen hat, die neben einer Reihe von weiteren Vorgaben sicherstellt, dass die ausländische Ermittlungsmaßnahme sich nicht direkt oder indirekt gegen Personen richtet, die die US-Staatsangehörigkeit besitzen oder sich in den USA aufhalten.

15. Der Bundesrat sieht hierin eine Unilateralisierung grenzüberschreitender Strafverfolgung, die den Geltungsanspruch von auf den Sachverhalt ebenfalls anwendbaren Rechtsordnungen nicht oder nur eingeschränkt anerkennt und letztlich die Gestaltung der Datenschutzrechte einseitig auf eigene, nationale Interessen ausrichtet. Damit bricht die US-Gesetzgebung mit den bisherigen Prinzipien, nach denen hoheitliche Maßnahmen, die in ausländische Rechtsordnungen eingreifen, nur erfolgen dürfen, wenn dies völkerrechtlich zulässig ist. Eine solche einseitige Ausgestaltung von grenzüberschreitenden Sachverhalten bedeutet eine gefährliche Erosion des in den internationalen Beziehungen bislang geltenden Grundsatzes der gegenseitigen Rücksichtnahme („international comity“),

ohne den letztlich eine alle Interessen berücksichtigende und befriedende Gestaltung der internationalen Beziehungen nicht möglich ist.

16. Der Bundesrat nimmt daher zur Kenntnis, dass die vorgeschlagene EU-Gesetzgebung Gefahr läuft, Strafverfolgungsmaßnahmen zuzulassen, die im Widerspruch zum US-Recht nach dem CLOUD-Act stehen. Dieser kann folglich nur aufgelöst werden, wenn die EU das danach vorgesehene „Executive Agreement“ abschließt, dessen Inhalt aber durch die Vorgaben des CLOUD-Act weitgehend vorbestimmt und nicht das Ergebnis bilateraler Verhandlungen auf Augenhöhe ist. Die mit dem Verordnungsvorschlag vorgesehene Erleichterung der Strafverfolgung wird faktisch durch die Vorgaben des CLOUD-Act konterkariert, da davon auszugehen ist, dass in der überwiegenden Anzahl der Fälle dem US-Recht unterworfene Diensteanbieter betroffen sein werden. Diese werden dann den in Artikel 15 des Verordnungsvorschlags vorgesehenen Einwand der Nichtvereinbarkeit mit dem Recht eines Drittstaates – hier der USA – vortragen. Diese Beschränkung des EU-Rechts durch die US-Gesetzgebung wiegt umso schwerer, als die US-Seite ihrerseits sich Beschränkungen, die sie für die Übermittlung für Daten an ausländische Stellen vorsieht, selbst in keiner Weise auferlegt, sondern ein umfassendes Beauskunftungsrecht von jedem Diensteanbieter fordert, der dem US-Recht in irgendeiner Weise unterworfen ist.

17. Er ist sich daher klar darüber, dass der Abschluss eines solchen „Executive Agreements“ der EU mit den USA zugleich die Zugriffe von US-Behörden auf EU-Datenschutzrecht unterfallende Sachverhalte – positiv – sanktionieren würde, so dass ihre Vereinbarkeit mit EU-Recht nicht mehr zu prüfen wäre. Der Bundesrat bittet daher die Bundesregierung, dafür Sorge zu tragen, dass Maßnahmen von US-Behörden, die das EU-Datenschutzrecht berühren, den gleichen Voraussetzungen unterliegen wie vergleichbare Maßnahmen in einem rein innereuropäischen Fall. Dies ist im Rahmen der vorgesehenen Verhandlungen sicherzustellen, die die Kommission demnächst mit dem Ziel des Abschlusses eines „Executive Agreements“ aufnehmen will.

18. Der Bundesrat ist der Auffassung, dass der Anwendungsbereich des Verordnungsvorschlag sich auf die Herausgabe und Sicherstellung von bereits gespeicherten Daten beschränken und nicht auf die Ausleitung von Echtzeit-Kommunikation erweitert werden sollte. Die Überwachung der Echtzeit-Kommunikation ist eine Maßnahme von hoher Grundrechtsrelevanz, die insbe-

sondere den Kernbereich persönlicher Lebensgestaltung betreffen kann. Ein grenzüberschreitender Zugriff kann daher nur nach sorgfältiger Abwägung und in einem Verfahren erfolgen, das die ausreichende Beachtung der betroffenen Grundrechte gewährleistet. In Anbetracht des Zeitrahmens, in dem die Verhandlungen zu Ende gebracht werden sollen, ist eine sorgfältige Prüfung und diese Vorgaben berücksichtigende Anpassung des Gesetzgebungsvorschlags nicht zu erwarten.

19. Er gibt zu bedenken, dass eine Regelung des sogenannten Direktzugriffs, also des Zugriffs auf im Ausland gespeicherte Daten zum Beispiel mittels eines im Inland sichergestellten Endgeräts, zumindest zum jetzigen Zeitpunkt nicht opportun erscheint. Der von der Kommission vorgelegte Verordnungsvorschlag enthält bereits in seiner jetzigen Fassung zahlreiche kontrovers zu diskutierende Punkte. Um einen Abschluss der Verhandlungen auf europäischer Ebene vor dem Ende der Legislaturperiode des Europäischen Parlaments nicht zu gefährden, sollte man sich auf den bereits bestehenden Vorschlag konzentrieren. Die Aufnahme weiterer kontroverser Themen würde die Verhandlungen weiter verlangsamen. Darüber hinaus besteht die Befürchtung, dass durch eine einheitliche europäische Regelung dieser Thematik eine Verschlechterung des Status quo in der Bundesrepublik Deutschland eintreten könnte. Gemäß § 110 Absatz 3 der Strafprozessordnung ist nach deutschem Recht derzeit ein Zugriff auf extern inländisch gespeicherte Daten zulässig. Soweit rein tatsächlich auf im Ausland gespeicherte Daten zugegriffen wird, ist hinsichtlich der gewonnenen Beweismittel solange kein Beweisverwertungsverbot anzunehmen, als bei der Erhebung der Daten der (ausländische) Speicherort der Daten nicht bekannt war.

20. Der Bundesrat fordert die Bundesregierung auf, die weiteren Verhandlungen in diesem Sinne zu führen.

21. Der Bundesrat übermittelt diese Stellungnahme direkt an die Kommission.