DEUTSCHER RICHTERBUND
Bund der Richterinnen und Richter,
Staatsanwältinnen und Staatsanwälte

Stellungnahme

**Nr. 6/18**
Juni 2018

# Stellungnahme des Deutschen Richterbundes zum Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)

**Deutscher Richterbund**
Haus des Rechts
Kronenstraße 73
10117 Berlin

T +49 30 206 125-0
F +49 30 206 125-25

info@drb.de
www.drb.de

**Verfasser der Stellungnahme:**
Dr. Peter Schneiderhan, Oberstaatsanwalt
Mitglied des Präsidiums

## A. Tenor der Stellungnahme

Der Deutsche Richterbund begrüßt den Ansatz der Kommission, die Sicherstellung und Beschlagnahme von elektronischen Beweismitteln im Strafverfahren unionsweit zu regeln. Er lehnt allerdings die grenzüberschreitende Erhebung von Inhaltsdaten bei Providern ohne Prüfung der Rechtmäßigkeit durch ein Gericht im Vollstreckungsmitgliedstaat ab. Er sieht die hierfür notwendige Harmonisierung der rechtlichen Vorgaben in den Mitgliedstaaten als (noch) nicht ausreichend an.

## B. Allgemein

Der Deutsche Richterbund begrüßt den Ansatz der Kommission, die Sicherstellung und Beschlagnahme von elektronischen Beweismitteln im Strafverfahren unionsweit zu regeln. Er sieht auch den Ansatz der Kommission als richtig an, für die Sicherung von Daten beim Provider mit der Europäischen Sicherungsanordnung (EPOC-PR) und für die Herausgabe dieser Daten an die Ermittlungsbehörden mit der Europäischen Herausgabeanordnung (EPOC) zwei unterschiedliche Ermittlungsmaßnahmen vorzusehen. Aus seiner Sicht bedarf es einer weiteren, gesonderten Regelung für die Erhebung von Verkehrsdaten durch eine EPOC-AC (access data).

Für die Herausgabe von Inhaltsdaten ist aus Sicht des Deutschen Richterbundes ein Richtervorbehalt im Vollstreckungsmitgliedstaat einzuführen, der unter engen Vorgaben für die Datenverwendung durch ein Notifikationsverfahren mit Klagemöglichkeit ersetzt werden kann. Wie der Richterbund bereits im Oktober 2017 (Stellungnahme 20/17) ausgeführt hat, handelt es sich bei der Erhebung von Inhaltsdaten um einen schwerwiegenden Grundrechtseingriff, der grundsätzlich nur nach Prüfung durch ein Gericht im Vollstreckungsmitgliedstaat erfolgen kann.

Die vorliegende Stellungnahme kann nur eine erste Prüfung des Verordnungsvorschlags darstellen. Eine vertiefte Prüfung der praxisrelevanten Fragen zum Anwendungsbereich, zu den mit der Vertretung bzw. der Niederlassung von Providern verbundenen Rechtsfragen, aber auch zu den Rechtsbehelfen der Art. 15 und 16 VO-E konnte bisher nicht erfolgen, ist aber für eine Bewertung des Vorschlags aus der Sicht der Rechtspraxis notwendig.
Der Deutsche Richterbund geht davon aus, dass die Beratungen zu diesem komplexen Rechtsinstrument mit der gebotenen Gründlichkeit erfolgen, um auch den betroffenen Verbänden ausreichend Zeit zu lassen, die Fragen vertieft zu beleuchten. Es wäre nicht hinnehmbar, wenn auf der einen Seite der Datenschutz europäischer Bürger, auf der anderen Seite die Möglichkeit der Strafverfolgungsbehörden zur Erhebung relevanter Daten unter einem Rechtsinstrument leiden würden, welches nicht ausreichend durchdacht ist und bei dem die gegenläufigen Interessen auf Grund einer zu hastigen Verabschiedung nicht überzeugend und praxistauglich austariert wurden. Der Deutsche Richterbund steht für eine Praxisbewertung des gesamten Vorhabens jederzeit zur Verfügung.

## C. Gegenseitige Anerkennung erfordert Angleichung des Rechts

I. Rechtsgrundlage der Verordnung ist Art. 82 Abs. 1 AEUV. Die Verordnung basiert somit auf dem Prinzip der gegenseitigen Anerkennung gerichtlicher Entscheidungen, welches durch die Angleichung der Rechtsordnungen in den Mitgliedstaaten gefördert werden soll.

Inhaltliche Voraussetzung für den Erlass einer EPOC ist gemäß Art. 5 Abs. 1, 2 VO-E die Möglichkeit ihrer Anordnung im Ausstellungsmitgliedstaat in einem Ermittlungsverfahren wegen einer Straftat, deren Mindesthöchststrafe drei Jahre beträgt, sowie ihre Notwendigkeit und Verhältnismäßigkeit. Die europarechtlichen Vorgaben der Verordnung an den Erlass einer EPOC beschränken sich darauf, dass diese notwendig und verhältnismäßig sein muss, Art. 5 Abs. 2 VO-E, und die Grundrechte zu beachten sind, Art. 1 Abs. 2 VO-E. Ihre Anordnung, so die Kommission, soll auf das beschränkt bleiben, was notwendig und verhältnismäßig ist, um den „Bedürfnissen der Strafverfolgungs- und Justizbehörden im digitalen Zeitalter Rechnung zu tragen“ (VO-E, S. 8). Eine weitergehende Rechtsharmonisierung, wie dies Art. 82 Abs. 1 AEUV vorsieht, erfolgt nicht.

II. Einheitlich geregelt wird jedoch, neben Verpflichtungen für Provider, der Wegfall der Prüfung im Vollstreckungsmitgliedstaat. Dies ist der wesentliche Inhalt der Verordnung. Materiell-rechtlich abgesichert wird dieser Wegfall der Prüfung nur – wie oben ausgeführt – durch das Erfordernis der Verhältnismäßigkeit der Maßnahme, ohne dass eine diesen Begriff harmonisierende Definition in die Verordnung aufgenommen wird.

Dabei geht die Kommission davon aus, dass der Grundrechtsschutz der Betroffenen durch das vorherige Einschalten einer Justizbehörde beim Erlass der Anordnung gewährleistet werde (VO-E, S. 11). Dieses Gericht – im Falle einer EPOC-PR eine Staatsanwaltschaft – prüft jedoch ausschließlich nach nationalem Recht und unter Beachtung der dürftigen europarechtlichen Vorgaben der Verordnung zur Notwendigkeit und Verhältnismäßigkeit der Maßnahme. Eine EPOC wird daher im Wesentlichen nach den jeweiligen nationalen Regelungen zur Datenerhebung im Strafverfahren erlassen.

III. Der Deutsche Richterbund sieht die Voraussetzungen für eine so weitgehende gegenseitige Anerkennung zumindest in Bezug auf die Herausgabe von Inhaltsdaten ohne Prüfung im Vollstreckungsmitgliedstaat als (noch) nicht vorhanden an. Gegenseitige Anerkennung als Ergebnis gegenseitigen Vertrauens benötigt weitgehend angeglichene Prüfungsmaßstäbe für Richter und Staatsanwälte in allen Mitgliedstaaten. Eine Prüfung einer EPOC im

Vollstreckungsmitgliedstaat könnte nur dann entfallen, wenn die materiellrechtlichen Voraussetzungen für deren Erlass weitgehend harmonisiert sind.

Eine solche Angleichung als Grundlage der gegenseitigen Anerkennung nimmt die Verordnung nicht vor. Auf eine solche könnte aus Sicht des Deutschen Richterbundes nur dann verzichtet werden, wenn durch Fallstudien dargelegt werden könnte, dass die Möglichkeit und Grenzen zum Erlass einer EPOC in den einzelnen Mitgliedstaaten gleich ausgestaltet sind. Praxiserfahrungen lassen eher vermuten, dass der Ansatz der Kommission, von einer „Zersplitterung der mitgliedsstaatlichen Rechtsrahmen“ (VO- E, S. 7) auszugehen, zutreffen dürfte. Diese Unterschiede müssen – unter besonderer Berücksichtigung der Rechtsprechung des EuGH zum Schutz der Privatsphäre (vgl. Urteil vom 21. Dezember 2016 i. S. Tele2 Sverige AB (C-203/15)) – beseitigt werden, bevor Inhaltsdaten ohne Prüfung im Vollstreckungsmitgliedstaat grenzüberschreitend herausgegeben werden können.

## D. Ansatz des Verordnungsentwurfs

Dabei übersieht der Deutsche Richterbund nicht, dass die grenzüberschreitende Sicherung und Erhebung von Daten geregelt werden muss. Die Erhebung von Daten bei einem Provider ist eines der wesentlichen Ermittlungsinstrumente der Strafverfolgungsbehörden, dessen Bedeutung in der Zukunft noch zunehmen wird. Der Umfang der elektronischen Kommunikation wird weiter zunehmen, außerdem dürfte die Auslagerung von Daten auf externe, von einem Provider unterhaltene Speicher zum Regelfall werden. Die Verordnung über die Europäische Herausgabeanordnung für elektronische Beweismittel wird zu einem zentralen Rechtsinstrument der grenzüberschreitenden Strafverfolgung werden. Sie muss daher den rechtstaatlichen Anforderungen an ein solches Rechtsinstrument vollumfänglich genügen.

Mit der Europäischen Herausgabeanordnung (EPOC) und der Europäischen Sicherungsanordnung (EPOC-PR) sollen wesentliche Elemente der Beweiserhebung – die Sicherung und Herausgabe von Verbindungs- und Inhaltsdaten durch den Provider – auf ein neues Niveau der gegenseitigen Anerkennung gehoben werden. Es soll auf die Prüfung der Rechtmäßigkeit der Anordnung des Ausstellungsmitgliedstaates im Vollstreckungsmitgliedstaat im Regelfall verzichtet werden. Dies führt dazu, dass sich die Herausgabe von Daten bei einem Provider nach dem Recht desjenigen Staates richtet, der Zugriff auf diese Daten begehrt.

Der Schutz des (eigenen) Rechts am Sitz des Providers, welches häufig das Recht des Dateninhabers ist, wird aufgegeben bzw. greift nur noch gegenüber den Ermittlungsbehörden des Staates, in dem der Provider seinen Sitz hat. Die Provider werden damit bei den von der Verordnung umfassten Ermittlungsmaßnahmen der Strafverfolgungsbehörden vollständig aus der Rechtsordnung des Staates, in welchem sie ihren Vertreter oder ihre Niederlassung (im Sinne von Art. 7 Abs. 1-3 VO-E) haben, herausgelöst. Der Provider wird für eine Datensicherung oder -herausgabe jeweils derjenigen Rechtsordnung unterstellt, welche eine EPOC erlässt. Dieser Verlust des Schutzes der eigenen Rechtsordnung am Sitz des Providers in einem sehr sensiblen Bereich, der zu einem Vertrauensverlust der Bürger in die eigene Rechtsordnung führen kann, wird vom Deutschen Richterbund kritisch gesehen. Dabei sieht der Deutsche Richterbund, dass der Erlass einer EPOC, einer EPOC- PR oder einer von ihm vorgeschlagenen EPOC-AC jeweils eine Justizbehörde – Gericht oder Staatsanwaltschaft - im Ausstellungsmitgliedstaat den Erlass der Maßnahme geprüft hat.

Notwendig ist daher die Prüfung, inwiefern die Besonderheit der Daten und der damit verbundenen Probleme bei der Datensicherung im Ermittlungsverfahren den von der Kommission vorgelegten Ansatz zur Schaffung einer EPOC und einer EPOC-PR rechtfertigt.

I. Diese Notwendigkeit besteht zunächst wegen der Flüchtigkeit der Daten, die schnell umsetzbare Maßnahmen zur Sicherung der Daten erforderlich macht. Dies wird aus Sicht der Praxis weitgehend zufriedenstellend mit der EPOC-PR umgesetzt (siehe dazu unter E.). Die eigentliche Herausgabe der Daten unterliegt dann einer gesonderten Herausgabeanordnung.

II. Gespeicherte Daten bestehen aus Verkehrs- und Inhaltsdaten. Diese enthalten Informationen, deren Erhebung mit einer unterschiedlichen Eingriffstiefe in die Rechte von Betroffenen verbunden ist. Die Erhebung von Verkehrsdaten stellt – auch wenn der EuGH zutreffend feststellt, dass „aus der Gesamtheit dieser Daten … sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden (können) …“ (Urteil C 203/15, aao, Rdnr 99) und daher nicht nur deren Speicherung, sondern auch deren Herausgabe nur unter den engen Vorgaben der Art. 7, 8 und 11 der Charta möglich ist – einen weniger schweren Eingriff als die Herausgabe von Inhaltsdaten dar. Ihre Erhebung ist im Regelfall beschleunigt erforderlich, um feststellen zu können, mit wem ein Beschuldigter Kontakt hatte. Die inhaltliche Bewertung dieses Kontaktes muss dann über Inhaltsdaten erfolgen, deren Herausgabe einer gesonderten Herausgabeanordnung unterliegt.

Daher dürfte die Erhebung von Verkehrsdaten gegenüber dem Provider ohne Entscheidung eines Gerichts im Vollstreckungsmitgliedstaat auch grundrechtlich zu rechtfertigen sein. Dazu müsste jedoch sichergestellt werden, dass diese Daten ausschließlich für das Ermittlungsverfahren selbst genutzt werden und nicht weitergegeben werden dürfen (dazu noch unten). Gesondert zu prüfen ist, ob auch Standort- und Bewegungsdaten unter diese erleichtert zu erhebenden Verkehrsdaten fallen können.

III. Anders ist die Situation bei Inhaltsdaten. Die Erhebung von Inhaltsdaten ohne gerichtliche Entscheidung im Vollstreckungsmitgliedstaat kann nicht wegen der Besonderheit der Daten gerechtfertigt werden. Diese können, über eine EPOC-PR, vor Verlust gesichert werden. Kontakte des Beschuldigten mit Dritten können über eine EPOC-AC erhoben werden. Eine Herausgabe ohne gerichtliche Entscheidung im Vollstreckungsmitgliedstaat lässt sich mit der Flüchtigkeit der Daten oder besonderer Eilbedürftigkeit im Ermittlungsverfahren im Regelfall nicht begründen.

Soweit die Besonderheit der Datenerhebung darin begründet ist, dass sich die zu erhebenden Daten in Datenspeichern an einem beliebigen Ort getrennt von der Niederlassung des Providers befinden, begegnet die Verordnung diesem Umstand überzeugend mit einer Herausgabepflicht des Providers, Art. 9 Abs. 1 VO-E. Dieser wird verpflichtet, die Daten in seinen Datensystemen festzustellen, auf sie zuzugreifen und herauszugeben. Dieser Ansatz ist richtig und beendet die Probleme der Strafverfolgungsorgane, festzustellen, wo gerade welche Daten gespeichert werden und über welchen Server in welchem Staat Zugriff genommen werden kann. Es handelt sich bei dieser Pflicht der Provider, weltweit verstreut abgespeicherte Daten zu sammeln und herauszugeben, auch um keinen Eingriff in staatliche Souveränität, da die Speicherung dieser Daten dem Staat, in welchem der Server (zufällig) steht, im Regelfall unbekannt war. Auch Rechte des Betroffenen sind nicht berührt, da dieser keinen Anspruch darauf hat, dass die Daten nicht am Ort des Providers – und damit dem Zugriff der Ermittlungsbehörden ausgesetzt – gespeichert werden.

Die Notwendigkeit dieses Datenzugriffs über den Provider lässt jedoch, entgegen der Ansicht in Erwägungsgrund 17 des VO-E, die Bedeutung des Standorts des Providers nicht entfallen. Dem Nutzer ist im Regelfall nicht gleichgültig, wer seine Daten verwaltet und unter welcher Rechtsordnung Datenschutz und Schutz vor Zugriff durch Strafverfolgungsorgane gewährt wird. Gerade bei sensiblen Daten, wie dies bei Betriebs- und Geschäftsgeheimnissen der Fall ist, dürfte dieser Schutz durch die örtliche Rechtsordnung maßgeblich für die Wahl des Providers sein.

Eine Aufgabe dieses Standortprinzips des Providers – nicht der von ihm herauszugebenden Daten – und damit die Auflösung von dessen örtlicher Rechtsgebundenheit bedarf daher einer Rechtfertigung, die über die – durch die Herausgabepflicht des Providers gelöste – fehlende örtliche Verortung der Daten hinausgeht. Eine solche Rechtfertigung sieht der Deutsche Richterbund nicht. Es ist unerheblich, ob ein Verpflichteter bei ihm gesammelte Daten oder dort verwahrte Papiere herausgibt – für beide Beweismittel reicht eine Europäische Ermittlungsanordnung (EEA). Für die Herausgabe von Inhaltsdaten sollte daher die EEA dahingehend ausgebaut werden, dass dort eine Verpflichtung von Providern aufgenommen wird, an einem beliebigen Ort von ihm gespeicherte Daten herauszugeben.

## E. Die Europäische Sicherungsanordnung

Wie bereits ausgeführt ist der Ansatz der Kommission, über eine Europäische Sicherungsanordnung (EPOC-PR) unionsweit Daten einfrieren zu können, durch die Notwendigkeit der schnellen Datensicherung und der geringen Eingriffstiefe zu rechtfertigen. Eine solche Anordnung entspricht auch dem Bedürfnis der Praxis, Daten zu sichern.

Zu prüfen wäre, ob die im VO-E vorgesehene Speicherfrist von 60 Tagen (Art. 10 Abs. 1) ausreicht oder ob nicht eine längere Frist vorgesehen werden sollte. In umfangreichen Verfahren wird es oft kaum möglich sein festzustellen, auf welche Daten tatsächlich zugegriffen werden muss und auf welche verzichtet werden kann. Die kurze Frist von 60 Tagen könnte Ermittlungsbehörden dazu bringen, frühzeitig die Herausgabe in die Wege zu leiten, nur um der Löschung vorzubeugen.

## F. Die Europäische Herausgabeanordnung

### I. Einleitung eines Strafverfahrens

Neben den bereits erwähnten Vorgaben zum Erlass einer EPOC wirkt beschränkend, dass diese nur im Rahmen eines Strafverfahrens und beim Vorliegen einer konkreten, bereits begangenen Straftat (VO- E, Erwägungsgrund 24) erlassen werden darf. Dabei werden auch hier die Voraussetzungen für die Einleitung eines Ermittlungsverfahrens – in Deutschland die auf konkreten Tatsachen basierte, auf kriminalistischer Erfahrung beruhende Möglichkeit einer Straftat – nicht harmonisiert. Es wird der Rechtsprechung des EuGH überlassen bleiben müssen, Kriterien für das Vorliegen eines Er-

mittlungsverfahrens, welches den Erlass einer EPOC rechtfertigt, zu entwickeln.

II. Weitergabe von Daten

Um die Verhältnismäßigkeit sicherzustellen, müsste ein Verbot der Verwertung der Daten außerhalb des Ermittlungsverfahrens und insbesondere ein Verbot der Weitergabe der Daten an Ermittlungsbehörden, welche nicht mit dem Fall befasst sind, eingeführt werden. Die Weitergabe der Daten zur Gefahrenabwehr müsste klar geregelt werden. Dies ist notwendig, um Rechtsmittel, welche ein Betroffener nach Abschluss der Ermittlungen gegen eine EPOC einlegen kann ( Art. 17 VO-E), nicht ins Leere laufen zu lassen. Sind die Daten, welche rechtswidrig erhoben wurden, weitergegeben, ist ihre Löschung kaum noch durchzuführen.

Für die Verwertung und die Weitergabe müssten gesonderte Verfahren geschaffen werden, in denen zumindest dann, wenn die Maßnahme noch verdeckt durchgeführt wird, die Gerichte des Vollstreckungsmitgliedstaates die Entscheidungen treffen. Insbesondere vor einer Weitergabe der Daten an Behörden von Drittstaaten muss diese gerichtliche Entscheidung im Vollstreckungsmitgliedstaat unabdingbar sein.

III. Rechtsschutz der Betroffenen: Notifikation als Mindeststandard

Im Regelfall führt der Provider die EPOC aus und übermittelt die Daten, Art. 9 Abs. 1, 2 VO-E. Nur dann, wenn sich die EPOC nicht umsetzen lässt, muss dieser gegenüber der Behörde des Ausstellungsmitgliedstaates aktiv werden, Art. 9 Abs. 3, 4 VO-E. Kommt der Provider seiner Verpflichtung nicht nach, müssen die Behörden im Vollstreckungsmitgliedstaat eingeschaltet werden, Art. 14 VO-E. Die Maßnahme ist verdeckt, der Inhaber der Daten erfährt erst nach Abschluss der Ermittlungen von der Maßnahme, Art. 11 VO-E. Der Betroffene kann dann im Ausstellungsmitgliedstaat Rechtsmittel einlegen, Art. 17 VO-E, nachdem er im Regelfall von der dortigen Ermittlungsbehörde nach Abschluss der Ermittlungen (Art. 11 Abs. 2 VO-E) von der Maßnahme unterrichtet wurde.

Dies führt in der Praxis zu einer weitgehenden Rechtlosigkeit der Betroffenen. Dagegen ist der Schutz des Providers gut ausgebaut, Art. 15, 16 VO-E (siehe dazu unter F. IV). Dies wird vom Deutschen Richterbund sehr kritisch gesehen, da bereits durch den in der Verordnung vorgesehenen Wegfall der Prüfung der EPOC im Vollstreckungsmitgliedstaat ein erheblicher Rechtsverlust für den betroffenen Dateninhaber eingetreten ist. Dieser, in dessen Rechte durch eine EPOC in ganz erheblichem Maße eingegriffen wird, ver-

liert den Schutz durch die eigene Rechtsordnung und erhält kein angemessenes Rechtsmittel als Ausgleich.

Es ist daher unabdingbar, sofern nicht die vom Deutschen Richterbund für Inhaltsdaten geforderte Prüfung einer EPOC durch ein Gericht des Vollstreckungsmitgliedstaates eingeführt wird, die Rechte der Betroffen zumindest über ein Notifikationsverfahren sicherzustellen. Dazu müssten die Grundentscheidungen des Ausstellungsmitgliedstaates an eine Justizbehörde des Vollstreckungsmitgliedstaates übermittelt werden. Dort sollte diese Stelle, die auch als Ombudsstelle eingerichtet werden kann, die eingehenden Grundentscheidungen prüfen und ggf. die vollständigen Akten, welche zum Erlass der EPOC geführt haben, anfordern können. Diese Stelle soll, sofern sie Bedenken hinsichtlich der Rechtmäßigkeit der Anordnung hat, diese Anordnung von einem Gericht im Vollstreckungsmitgliedstaat überprüfen lassen können. Es könnte eine Verschweigensfrist vorgesehen werden, nach deren Ablauf der Provider die Daten herausgeben darf. Dieses Verfahren sollte, sofern der Ermittlungszweck gefährdet ist, auch ohne Beteiligung des betroffenen Dateninhabers durchgeführt werden können.

IV. Rechtsbehelfe der Provider

Der Rechtsschutz des Providers gegen Anordnungen auf Datenherausgabe, welche seiner Ansicht nach mit Grundrechten Dritter oder Interessen eines Drittstaates kollidieren ( Art. 15, 16 VO-E), bedarf einer vertieften Analyse. Soweit er dem Schutz individueller Rechte dient, wäre zu prüfen, ob dieser nicht über Art. 9 Abs.5 VO-E ausreichend und im Gleichklang mit dem Schutz der Rechte von Unionsbürgern gewährt werden kann. Soweit die Vorschriften dazu dienen sollen, „diplomatische Gepflogenheiten zu gewährleisten“ (VO-E, S. 24), wäre sicherzustellen, dass Provider, welche Dienste innerhalb der Europäischen Union anbieten, auch die hier geltenden Rechtsvorschriften über die Datenherausgabe an Ermittlungsbehörden einhalten können. Ansonsten würde die Regelung dazu führen, dass Provider am Markt tätig sind, gegenüber denen eine EPOC nicht vollstreckt werden kann. Dies würde das Ziel der Verordnung, zu europaweit einheitlichen Zugriffsmöglichkeiten auf Daten für Ermittlungsbehörden zu kommen, konterkarieren.

V. Anpassung des deutschen Rechts

Aufgabe des deutschen Gesetzgebers muss es sein, die deutsche Strafprozessordnung an die Vorgaben der Verordnung (sofern sie wie von der Kommission vorgeschlagen verabschiedet wird) anzupassen, um zu vermeiden, dass deutsche Ermittlungsbehörden gegenüber in Deutschland niederge-

lassenen Providern „weniger“ dürfen als gegenüber Providern mit Sitz in einem anderen Mitgliedstaat. Dies ist notwendig, um sicherzustellen, dass in Deutschland ansässige Provider auch gegenüber den deutschen Ermittlungsbehörden Daten, welche weltweit gespeichert sind, zuziehen und herausgeben müssen. Diese Pflicht ist bisher nicht eindeutig normiert. Außerdem müsste sichergestellt werden, dass auch aus deutscher Sicht die Erhebung von Daten über einen deutschen Provider, welche im Ausland gespeichert sind, keinen Eingriff in die Souveränität eines ausländischen Staates darstellt.

*Der Deutsche Richterbund ist mit mehr als 16.000 Mitgliedern in 25 Landes- und Fachverbänden (bei bundesweit 25.000 Richtern und Staatsanwälten insgesamt) der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland.*