E-Evidence und CLOUD-Act – Grenzüberschreitender Direktzugriff auf Daten?

Bericht von der EAID-Veranstaltung anlässlich des Europäischen Datenschutztags am 1. Februar 2019, Berlin

Von Peter Schaar (12. 2.2019)

Peter Schaar, Vorsitzender der EAID, führt in den Gegenstand der Veranstaltung ein. Die Europäische Kommission habe am 18. April 2018 ein E-Evidence-Paket vorgelegt, bestehend aus einer „Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen“ (E-Evidence-VO - EEVO) /https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN) und einer ergänzenden Richtlinie für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN).

Wie beim 2018 vom US-Kongress beschlossenen CLOUD Act gehe es auch bei dieser EU-Initiative darum, Behörden den grenzüberschreitenden Direktzugriff auf Daten zu ermöglichen, die außerhalb des eigenen staatlichen Territoriums gespeichert werden.

Dr. Alexander Dix, LL. M., Stellvertretender Vorsitzender der EAID, stellt als Diskussionsleiter die Teilnehmer vor und erläutert den weiteren Ablauf.

Alexandra Jour-Schröder (Europäische Kommission, GD Justiz und Verbraucher, Direktorin Strafrecht) - Video-Botschaft

Frau *Jour-Schröder* führt aus, die vorgesehenen Rechtsakte dienten dazu, im Internetzeitalter effiziente Strafverfolgung zu gewährleisten und zugleich die Grundrechte der Betroffenen zu wahren.

Die Kommission habe vor Annahme der Vorschläge zwei Jahre lang die Problemlage analysiert und u.a. mit Strafverfolgern und Unternehmen diskutiert. Sie sei zu dem Ergebnis gekommen, dass die bestehenden Instrumente nicht ausreichend seien, um von den Dienstleistern elektronische Beweismittel zu bekommen.

Die Nutzung sozialer Medien und Apps, deren Anbieter im Ausland sitzen, sei heutzutage die Regel und nicht die Ausnahme und würde auch von Straftätern genutzt. So spielten in 85% der Fälle elektronische Beweismittel eine Rolle. Ohne effektive Zugriffsmöglichkeiten auf elektronische Beweismittel blieben Täter in vielen Fällen straflos und Opfer fänden keine Gerechtigkeit, etwa in den Bereichen Kinderpornographie, Passwort- und Identitätsdiebstahl und Betrug. Dies gelte auch für rein nationale Ermittlungen, in denen Opfer und Täter im Inland sitzen.

Die bisher bestehenden Instrumente — Internationale Rechtshilfeersuchen in Strafsachen und Europäische Ermittlungsanordnung — seien zu langwierig und trügen der Besonderheit elektronischer Daten, insbesondere ihrer Flüchtigkeit, nicht Rechnung. Sie bezögen sich vielmehr auf Beweismittel aller Art, die sich idR an einem bestimmten Ort befänden. Anders

gestalte sich das aber in der digitalen Welt: Die Daten befänden sich in der Regel gerade *nicht* auf dem Territorium des Staates, wo der Diensteanbieter sitze, sondern sie würden auf der Basis von Algorithmen laufend ganz oder fragmentiert immer wieder woanders über die Welt verschoben.

Die Bearbeitungszeit bei Internationalen Rechtshilfeersuchen liege zudem durchschnittlich bei einem Jahr und bei der Europäischen Ermittlungsanordnung (EEA) seien bis zu 120 Tage erforderlich, bis Beweismittel herausgegeben würden. Zudem könne letztere nicht das Problem des Umgangs mit Anbietern aus Drittstaaten lösen. Die Ermittlungsbehörden hätten sich hier an die Drittstaaten zu wenden.

Hierauf reagiere der Vorschlag der europäischen Kommission: Durch die Europäische Herausgabeanordnung könnten Strafverfolgungsbehörden unmittelbar bei den Diensteanbietern bzw. deren Vertretern die Herausgabe von Daten verlangen. Diese müssten die verlangten Daten innerhalb von 10 Tagen bereitstellen. Daneben solle die Europäische Sicherungsanordnung gewährleisten, dass die erforderlichen Daten nicht gelöscht werden. So solle verhindert werden, dass flüchtige elektronische Beweismittel verloren gingen.

Frau *Jour-Schröder* betonte, dass die im nationalen Recht des Anordnungsstaats vorgesehenen strafprozessualen Rechte vollumfänglich Anwendung fänden, gerade auch die, die gerade erst auf EU-Ebene harmonisiert wurden, aber auch die EU – Grundrechtecharta (insb. Art. 47 und 48), das in der Europäischen Menschenrechtscharta verankerte Recht auf ein faires Verfahren und die Rechte aus der gerade in Kraft getretenen Datenschutzgrundverordnung und der nun umgesetzten Polizei-Richtlinie. Zum Schutz des Betroffenen werde zudem ein Recht auf Information und die Rechtsschutzmöglichkeit des Betroffenen gegen die Herausgabe von Daten im Erlassstaat garantiert. Zudem sei die vorherige Einbindung eines Richters bei der Herausgabe von Transaktions- und Inhaltsdaten vorgeschrieben.

Die Vorschläge schüfen auch mehr Rechtssicherheit, zumal viele Diensteanbieter heutzutage die Daten lediglich auf freiwilliger Basis herausgäben.

Zudem enthielten die neuen Regelungen Vorgaben für den Fall, dass Unternehmen aus Drittstaaten sich durch die angeordnete Herausgabe von Daten in diesem Zusammenhang mit konkurrierenden Verpflichtungen aus ihrem Sitzstaat konfrontiert sähen, gerade wenn es um Grundrechte aus der Rechtsordnung dieses Staates gehe.

Frau *Jour-Schröder* betonte die Notwendigkeit für ein effizientes Instrument, das gleichzeitig die Rechte des Betroffenen, insbesondere seine Grundrechte und dabei das Grundrecht auf Privatsphäre, gewährleiste. Sie setze dabei auf die Zusammenarbeit mit den Mitgliedstaaten und dem Europäischen Parlament.

Birgit Sippel (Mitglied des Europäischen Parlaments, Berichterstatterin zu E-Evidence)

Frau *Sippel* wies darauf hin, dass der im Veranstaltungstitel verwendete Begriff „Direktzugriff“ nicht im Wortsinne so zu verstehen sei, dass etwa ausländische Behörden online auf die entsprechenden Daten in Unternehmen zugreifen könnten. Allerdings treffe es zu, dass die Behörden Anordnungen zur Sicherung und Herausgabe von Daten direkt an ausländische Unternehmen richten könnten, ohne dass von einem Gericht oder einer Behörde im Vollstreckungsstaat geprüft werde, ob die Anordnung den dortigen rechtlichen Anforderungen entspreche. Sie sieht darin ein Problem, da die strafrechtlichen Regelungen und die

strafprozessualen Schutzvorkehrungen zwischen den Mitgliedsstaaten erheblich differierten. Das gelte auch, soweit das nationale Recht EU-Richtlinien umsetze.

Ob die von den Ermittlungsbehörden angeforderten Daten tatsächlich als Beweismittel in einem Verfahren taugten, stehe zum Zeitpunkt der Anordnung vielfach nicht fest, sondern zeige sich erst in einem späteren Verfahrensstadium. Daher sei auch der in der öffentlichen Debatte verwendete Begriff der „elektronischen *Beweismittel*“ bzw. „e-*evidence*“ teils irreführend. Die Behörden erhielten auch eine Vielzahl von Daten, die letztlich nicht ermittlungsrelevant seien.

Das Problem sei weniger das Fehlen von Befugnissen, sondern die lange Verfahrensdauer. Die bisherigen Rechtsinstrumente würden bisher nicht ausgeschöpft. So gäbe es Beschleunigungsmöglichkeiten bei der Bearbeitung von internationalen Rechtshilfeersuchen. Vielfach sei die lange Bearbeitungsdauer darauf zurückzuführen, dass die Regierungen dafür nicht die erforderlichen Ressourcen zur Verfügung stellten. Über die kürzlich eingeführte Europäische Ermittlungsanordnung (EEA) lägen noch keine belastbaren Erfahrungen vor, zumal deren Implementierung in einigen Mitgliedsstaaten trotz der im Mai 2017 ausgelaufenen Umsetzungsfrist noch nicht vollständig abgeschlossen sei.

Anders als bei anderen Rechtsinstrumenten fehle bei der vorgesehenen E- Evidence-VO ein Straftatenkatalog. Sie verweise lediglich auf eine nach nationalem Recht vorgesehene Mindesthöchststrafe. Angesichts der Rechtsunterschiede zwischen den Mitgliedsstaaten könnten die nationalen Behörden des anordnenden Staates auch bei solchen Straftaten die Datenherausgabe anordnen, bei denen das Recht des Vollstreckungsstaates keine entsprechende Strafandrohung vorsehe.

Zudem stelle sich die Frage der Rechtssicherheit für die Provider. Die vorgesehene Grundrechteprüfung durch die Unternehmen sei problematisch, insb. im Hinblick auf die kurzen Herausgabepflichten, im Eilfall nur wenige Stunden. Dabei sei die Rechtsprüfung kompliziert, etwa wenn es um Straftaten gehe wie das Abtreibungsrecht, das in den Mitgliedsstaaten sehr unterschiedlich geregelt sei, oder um bestimmte Strafrechtsvorschriften, deren europarechtliche Zulässigkeit umstritten sei. Der ausstellende Staat müsse zudem Immunitätsansprüche in den Zielstaaten prüfen, z.B. bei Anwälten und Journalisten. *Sippel* bezweifelt, ob die Behörden dazu in der Lage seien.

Angesichts der Zweifel an der Rechtssicherheit bei der Vollstreckung elektronischer Ermittlungsanordnungen wolle das Europäische Parlament erreichen, dass eine zweite Behörde (möglichst eine Behörde des Ziellandes) eingeschaltet werden müsse. Zudem müsse der Umgang der Behörden mit den herausgegebenen Daten geklärt werden. Hierfür fehlten bisher klare Vorgaben.

Nach dem US-CLOUD-Act könnten US-Behörden bei einer Vielzahl von Straftaten die Herausgabe von Daten verlangen, die außerhalb des US-Territoriums gespeichert seien.

Wenn die EU mit den USA ein Abkommen schließen würde, das den jeweiligen Behörden der anderen Seite entsprechende Befugnisse einräume, müsse damit gerechnet werden, dass auch aus anderen Drittstaaten vergleichbare Forderungen erhoben würden. Es müsse vermieden werden, dass hier ein unübersichtlicher Flickenteppich mit unterschiedlichem Schutzniveau entstehe.

Frau *Sippel* erwartet, dass die Beratungen in den EU-Gremien über das E-Evidence-Paket nicht bis zum Ende der rumänischen Ratspräsidentschaft (Mitte 2019) abgeschlossen werden könnten. Im Hinblick auf die im Mai 2019 anstehenden Wahlen zum EP würden

derzeit mithilfe von Arbeitsdokumenten (Working Documents) die Beratungen zu dem Vorschlag weiter vertieft. Dies ermögliche eine Fortsetzung der Beratungen im neu gewählten EP auf Grundlage der Erkenntnisse der Working Documents.

Axel Petri (Deutsche Telekom – Senior Vice President, Group Security Governance)

Petri erklärte, für die Deutsche Telekom seien das Vertrauen der Kunden und die Harmonisierung der Vorschriften in der EU wichtig. Die Digitalisierung erfordere Vertrauen in digitale Dienste und Produkte, um erfolgreich zu sein. Ein stärker harmonisiertes europäisches Konzept für Cyber Security sei erforderlich, um mehr Rechtssicherheit und Wettbewerbsfähigkeit für den europäischen und den globalen digitalen Markt zu schaffen. Es sei zweifelhaft, ob sich diese Ziele mit der E-Evidence-VO in ihrer jetzigen Form verwirklichen ließen, auch wenn die Deutsche Telekom die initiative der Europäischen Union grundsätzlich begrüße. Im Hinblick auf die Harmonisierung sei eine Verordnung gegenüber einer Richtlinie vorzuziehen, da letztere erst nach Umsetzung in nationales Recht wirksam würde und zudem zu befürchten wäre, dass die Umsetzungsgesetze unterschiedlich wären.

Petri verwies darauf, dass die Regeln in den Mitgliedsstaaten hinsichtlich der Löschungsfristen für Telekommunikationsdaten weiterhin uneinheitlich seien. Daran würde auch die vorgesehene EEVO nichts ändern. Dies bedeute, dass der Umfang der herauszugebenden Daten stark differieren würde, je nachdem, in welchem Staat das Unternehmen ansässig sei.

Im Hinblick auf den Umfang der zu erwartenden Anordnungen ausländischer Behörden bestehe erhebliche Unklarheit. *Petri* erwartet, dass es sehr viel mehr entsprechende grenzüberschreitende Verfahren geben werde als die von der Kommission angenommenen 6 %. Nicht zuletzt deswegen sei auch eine angemessen Kostenerstattung für die Provider unabdingbar.

Auf jeden Fall seien klare Regelungen dringend erforderlich, sowohl im Hinblick auf die Herausgabebefugnisse der nationalen Behörden als auch hinsichtlich der Straftatbestände, in denen grenzüberschreitende Anordnungen erlassen werden können. Hier bestünden erhebliche Defizite, die durch die vorliegenden Entwurfsfassungen nicht beseitigt würden.

Die vorgesehenen Regelungen würden die Telekommunikationsunternehmen erheblichen Risiken aussetzen. Dies ließe sich am Fall des katalanischen Politikers Puigdemont verdeutlichen. Hier habe ein deutsches Gericht festgestellt, dass die von der spanischen Justiz behaupteten Verstöße gegen spanisches Recht nach deutschem Recht keine Straftaten darstellten und die Inhaftierung des Politikers auf Grund eines europäischen Haftbefehls dementsprechend unzulässig gewesen sei. Da bei der EEVO keine Prüfung durch ein deutsches Gericht erfolge, wären die deutschen Betreiber trotzdem verpflichtet, den spanischen Behörden in einem solchen Verfahren die angeforderten Daten herauszugeben.

Ein weiteres Defizit des Entwurfs sei für die Unternehmen die Unklarheit über die berechtigten ausländischen Behörden. Hier bestehe erheblicher Klärungsbedarf. Zumindest sei eine abschließende Liste der zum Erlass von Anordnungen berechtigten Behörden erforderlich. Auch im Hinblick auf die den Unternehmen mögliche Echtheitsprüfung der Anordnungen hätte die Telekom Zweifel. Dies gelte etwa in Bezug auf Anordnungen, die per Fax ausgestellt würden.

Petri plädierte für die Einrichtung zentraler nationaler behördlicher Anlaufstellen in jedem Mitgliedstaat. Die Anlaufstelle im Vollstreckungsstaat solle prüfen, ob eine Anordnung den rechtlichen und formalen Anforderungen entspreche. Die Unternehmen könnten dies nicht leisten.

Die in dem Entwurf vorgesehenen kurzen Herausgabefristen, insbesondere die Verkürzung der Frist in Eilfällen auf 6 Stunden, würden es den Unternehmen praktisch unmöglich machen, ihren Prüf- und Sorgfaltspflichten nachzukommen. Es müsse daher dringend ausgeschlossen werden, dass private Unternehmen für die Rechtmäßigkeit von Anordnungen verantwortlich gemacht werden können, die sie nicht selbst überprüfen können.

Schließlich müsse die Anordnung auf Daten beschränkt bleiben, die der Provider bereits gespeichert hat und über die Anordnung dürfe auch kein ansonsten unzulässiger Transport in Drittländer erfolgen. Auch hier bestehe Klärungsbedarf.

Die Regelungen müssten so formuliert werden, dass sie den betroffenen Unternehmen ein hohes Maß an Rechtssicherheit garantieren. Ansonsten würde die Wirtschaft einem doppelten Risiko ausgesetzt: Wenn ein Unternehmen die Daten nicht herausgebe, drohten die Sanktionierung wegen Strafvereitelung und hohe Bußgeldern. Wenn das Unternehmen alle verlangten Daten liefere, könnten Betroffene Schadensersatz verlangen, wenn sich herausstelle, dass die Voraussetzungen für die Herausgabe doch nicht vorgelegen hätten.

Abschließend forderte *Petri* einen transparente und gründliche Diskussion mit allen relevanten gesellschaftlichen Gruppen an der sich die Deutsche Telekom selbstverständlich weiterhin intensiv beteiligen werde. Insgesamt seien für ihn Rechtssicherheit, Praktikabilität und Schutz der Kundendaten von zentraler Bedeutung.

Klaus Landefeld (eco – Verband der Internetwirtschaft e.V., stv. Vorstandsvorsitzender, Vorstand Infrastruktur und Netze)

Landefeld wies auf die aus seiner Sicht sehr große Reichweite der geplanten Regelungen hin. Betroffen seien die vollständigen Kopien sämtlicher bei Providern vorhandener Daten. Vorgesehen sei eine umfassende Anwendbarkeit auf alle Dienste der Informationsgesellschaft. Anwendbar seien die neuen Vorschriften nicht nur für Telekommunikationsdienste sondern etwa auch bei Cloud-Diensten und sozialen Netzwerken.

Die vorgesehene Beschränkung des Anwendungsbereichs der Verordnung auf Dienste, die in mehr als einem Mitgliedstaat angeboten würden, laufe weitgehend leer. Grundsätzlich seien nahezu alle Internet-Dienste betroffen, da entsprechende Angebote auf Grund der Binnenmarktregeln der EU nur ausnahmsweise auf ein Land beschränkt werden könnten. Sogar Firmennetzwerke könnten einbezogen sein, wenn sie mehrere Mitgliedsstaaten umfassten.

Schließlich sei die Abgrenzung des Anwendungsbereichs auch im Detail sehr schwierig. So stelle sich etwa die Frage, ob Mautdaten in die Herausgabepflicht einbezogen werden sollen. Hier sei die Rechtslage in den Mitgliedsstaaten sehr unterschiedlich. Während österreichische Behörden in Österreich Mautdaten abfragen dürften, sei eine vergleichbare Befugnis deutscher Behörden, auf die in Deutschland erhobenen Mautdaten nach deutschem Recht nicht gegeben, denn hier seien sehr strikte, ausdrücklich im Gesetz formulierte Zweckbindungsbestimmungen für die erhobenen Daten zu beachten, die auch

eine Verwendung für Zwecke der Strafverfolgung ausschlössen. Im Ergebnis könne es dazu kommen, dass nach Inkrafttreten der Verordnung österreichische Behörden den Zugriff auf deutsche Mautdaten verlangen könnten, während dies deutschen Behörden versagt bleibe. Dies sei niemandem zu vermitteln.

Es stelle sich die grundsätzliche Frage, wie mit Verwertungsverboten umgegangen werden soll. Auch hier seien die Vorschriften in den Mitgliedsstaaten sehr unterschiedlich. Dies betreffe etwa Daten von Journalisten und Anwälten, aber auch von Angehörigen anderer Berufsgruppen. *Landefeld* stellte die Frage, wie die anordnende Behörde das Bestehen von Verwertungsverboten im Vollstreckungsstaat berücksichtigen solle, ohne dessen Rechtssystem gründlich zu studieren. Unternehmen seien hiermit gänzlich überfordert.

Auch im Hinblick auf die vorzuhaltenden Daten und darauf, unter unter welchen Voraussetzungen sie an Strafverfolgungsbehörden herauszugeben seien, gebe es zwischen den Mitgliedsstaaten keine Harmonisierung. Die vorgesehene minimale Maximalstrafe von 3 Jahren als Voraussetzung für den Erlass einer Sicherungs- oder Herausgabeanordnung hält *Landefeld* für eine zu schwache Hürde. Angesichts der unterschiedlichen Strafrechtssysteme in den Mitgliedsstaaten forderte er die Aufstellung eines abschließenden Straftatenkatalogs, bei denen eine Sicherungs- oder Herausgabeanordnung erlassen werden dürfe.

Es stelle sich auch die Frage, ob und wie bei von ausländischen Behörden erlassenen Herausgabeanordnungen der vom Bundesverfassungsgericht eingeforderte „Kernbereichsschutz“ durchgesetzt werden könne, wonach Behörden der Einblick in den Kernbereich privater Lebensgestaltung nicht gestattet sei. Ein vergleichbares Problem gäbe es zwar auch heute schon bei rein nationalen Verfahren, so dass es bisweilen auch zur Herausgabe von Daten komme, die dem Kernbereichsschutz unterlägen. In solchen Fällen könnten die Unternehmen aber bisher darauf vertrauen, dass der Kernbereichsschutz durch die ermittelnden deutschen Behörden, etwa mittels Verwertungssperren und nachträgliche Löschung, realisiert werde. Dies sei aber bei der Übermittlung an ausländische Behörden, in deren Rechtssystem der Kernbereichsschutz nicht vorgesehen sei, nicht zu erwarten.

Landefeld erwartet eine sehr hohe Zahl von Anordnungen und betroffenen Unternehmen — belastbare Prognosen fehlten hier gänzlich. Aufgrund der auf nationaler Ebene gemachten Erfahrungen mit Herausgabepflichten sei auch zu befürchten, dass die Eilfrist von 6 Stunden zur Regel werde und nicht etwa — wie behauptet — die absolute Ausnahme bliebe.

Nach Zählung von eco werde es EU-weit etwa 13.000 berechtigte Stellen geben. Neben Gerichten und Staatsanwaltschaften hätten auch andere staatliche Stellen nach dem Recht der Mitgliedsstaaten entsprechende Befugnisse. In den meisten Mitgliedsstaaten bestünden zwar abgestufte Befugnisse je nach Straftat und Behörde, doch unterschieden sich diese von Mitgliedsstaat zu Mitgliedsstaat sehr, etwa im Hinblick auf den „Richtervorbehalt“. Den zur Umsetzung der Anordnungen verpflichteten Unternehmen sei es nicht möglich, diese Differenzierungen nachzuvollziehen.

Auch fehlten in den Entwürfen Anforderungen an die Form der Anordnungen. Statt hier europaweit einheitliche Standards vorzusehen, etwa die nach EU-Recht normierte elektronische Signatur, könnten Behörden ihre Anordnungen auch per Fax senden. Eine Echtheitsprüfung der eingehenden Anordnungen sei den Unternehmen deshalb vielfach nicht möglich.

Ebenso fehlten Vorgaben hinsichtlich der bei der Übermittlung der angeforderten Daten an die Behörden zu treffenden Schutzvorkehrungen. Notwendig wären etwa eine Verschlüsselungspflicht für die zu übertragenden Daten und klare Vorgaben, die eine

zweifelsfreie Identifikation der berechtigten Behörden gewährleisten. Es müsse unbedingt vermieden werden, dass Daten an unberechtigte Adressaten gelangen. Die vorgesehenen Rechtsakte enthielten nicht einmal Ermächtigungen für den Erlass entsprechender technischer Richtlinien.

Auch klare Regeln hinsichtlich der Transparenz ggü. den Betroffenen suche man in dem Entwurf vergeblich, etwa im Hinblick auf deren nachträgliche Benachrichtigung über erfolgte Datenübermittlungen. Die nationalen Rechtsvorschriften und Praktiken seien auch hier sehr uneinheitlich.

Die Industrie wende sich nicht grundsätzlich gegen die Beschleunigung der grenzüberschreitenden Strafverfolgung mittels harmonisierter Vorgaben. Die Regelungen müssten jedoch Rechtssicherheit für alle Beteiligten herstellen. Unverzichtbar sei insbesondere die Einschaltung einer öffentlichen Stelle im Zielland, welche die Anordnungen ausländischer Behörden zu prüfen habe.

Auch die Haftungsrisiken für die Unternehmen müssten verringert werden, etwa für den Fall, dass irrtümlich zu viele Daten übermittelt würden. Dringlich sei auch ein striktes Verwertungsverbot für die überschüssig von den Behörden erlangten Daten. Die Weitergabe der mittels Herausgabeanordnung von ausländischen Behörden erlangten Daten an Drittstaaten müsse untersagt werden.

Die Politik müsse berücksichtigen, dass auch viele kleine und kleinste Unternehmen in den Anwendungsbereich der Verordnung fielen. Anders als den großen Providern sei es kleineren Unternehmen praktisch unmöglich, die Realisierung der Vorgaben rund um die Uhr sicherzustellen. Auch den vorgesehenen Prüfpflichten könnten sie nicht nachkommen. Dies hätte Konsequenzen für den Wettbewerb.

Schließlich seien auch bei der Kostenerstattung viele Fragen offen. Nach dem Entwurf sollten dafür offenbar die nationalen Regelungen anzuwenden sein. Allerdings stelle sich die Frage, welches nationale Recht gelte - das Recht des Landes, in dem das Unternehmen seinen Sitz habe oder das Recht des Landes, dessen Behörde die eine Anordnung erließe.

Dr. Stefanie Unzeitig (Bundesministerium der Justiz und für Verbraucherschutz)

Frau *Unzeitig*, für E-Evidence zuständige Referentin im BMJV, erläuterte die Position der Bundesregierung. Sie wies darauf hin, dass die Behandlung des Dossiers im Rat unter starkem Zeitdruck stattgefunden habe. Deutschland habe — wie einige andere Staaten auch — dem Kommissionsentwurf und dem bisher im Rat erreichten Verhandlungsstand auf dem Justizministerrat im Dezember 2018 nicht zugestimmt. Der Trilog werde erst dann beginnen, wenn das Europäische Parlament seine Position festgelegt habe.

Die Bundesregierung sehe grundsätzlich die Notwendigkeit eines neuen Instruments für die grenzüberschreitende Erlangung elektronischer Beweismittel. Dabei müssten aber die Rechtsstaatlichkeit und die Grundrechte angemessen gewahrt bleiben. Hier bestünden noch Defizite.

Es dürfe nicht übersehen werden, dass die von der Kommission vorgeschlagene Richtlinie einen größeren Anwendungsbereich habe als die Verordnung. Die Richtlinie beschränke sich nicht auf E-Evidence, sondern wäre auch auf weitere, möglicherweise künftige grenzüberschreitende Instrumente bei der internationalen Strafverfolgung anwendbar.

Angesichts der unterschiedlichen strafrechtlichen und strafprozessualen Regeln in den Mitgliedsstaaten sei die Bundesregierung stets für ein „Tandem“-Verfahren eingetreten, d.h. eine Prüfung der Herausgabeanordnung durch eine Behörde eines anderen Mitgliedstaats.

Nach dem vorliegenden Entwurf spiele der Ort der Speicherung keine Rolle. Insofern sei es auch unbeachtlich, ob die Daten auf einem Server in einem EU-Mitgliedstaat oder außerhalb der Europäischen Union gespeichert würden.

Die Bedenken der Bundesregierung bestünden fort. Insbesondere gebe es keine echte Widerspruchsmöglichkeit des Vollstreckungsstaates gegen eine Anordnung. Das BMJV trete überdies dafür ein, dass der Vollstreckungsstaat stets auch notifiziert werde, wenn eine Anordnung zur Erlangung von Transaktionsdaten erlassen werde. Ein zweiter Staat müsse die Anordnung tatsächlich prüfen können und sein Prüfergebnis müsse Einfluss haben.

Zur Frage, welcher Staat für die Prüfung zuständig sein solle, wurde erläutert, dass die Bundesregierung zunächst den Mitgliedstaats des Aufenthalts des Datennutzers favorisiert hätte, jedoch aufgrund der Mehrheitsverhältnisse nun vorgesehen sei, dass bei einer Anordnung zur Herausgabe von Inhaltsdaten der Vollstreckungsstaat, also der Mitgliedstaat, in dem der gesetzliche Vertreter des Diensteanbieters benannt sei, notifiziert werden müsse. Die Bundesregierung trete auch dafür ein, dass dem Vollstreckungsstaat eine vollumfängliche Grundrechtsprüfung möglich sei.

Immerhin sei während den bisherigen Verhandlungen erreicht worden, dass es eine Notifizierungspflicht gegenüber dem Vollstreckungsstaat bei Inhaltsdaten geben solle. Eine entsprechende Verpflichtung zur Benachrichtigung des Vollstreckungsstaates bei den ebenfalls sensiblen Transaktionsdaten sei zwar weiterhin nicht vorgesehen, jedoch sei hier die Einführung eines Konsultationsverfahrens erreicht worden. Die Bundesregierung trete auch weiterhin für ein echtes Widerspruchsrecht des Vollstreckungsstaates ein.

Leider habe es über die genannten Änderungen hinaus im Rat keine Mehrheit für die weiteren Anliegen der Bundesregierung gegeben. Kritisch sehe das BMJV auch, dass bei den Sicherungsanordnungen — anders als bei den Herausgabeanordnungen — überhaupt kein Rechtsschutz vorgesehen sei.

Das BMJV ermuntere dazu, dass die Diskussion über das wichtige Thema in der Öffentlichkeit breit geführt werde und dass diese von der Zivilgesellschaft interessiert begleitet werde.

Dr. Raphael Bossong (Stiftung Wissenschaft und Politik)

Bossong plädierte dafür, bei der Diskussion die Verbindung der E-Evidence-VO der EU zum US-CLOUD-Act nicht zu vergessen. Über ein bilaterales Abkommen zur exterritorialen Datenherausgabe fänden bereits Verhandlungen zwischen der Europäischen Kommission und der US-Regierung statt.

Bei den diskutierten Maßnahmen sei immer wieder von gegenseitigem Vertrauen die Rede. Diesen Grundsatz dürfe man jedoch nicht überstrapazieren, sowohl bei der grenzüberschreitenden Strafverfolgung in Europa als auch bei Vereinbarungen mit Drittstaaten. Schon beim europäischen Haftbefehl habe man zu viel auf das Vertrauen gesetzt, weniger auf klare Regelungen. Dies sei schiefgegangen, weshalb die Regelungen zum Europäischen Haftbefehl mehrfach hätten nachgebessert werden müssen.

Wie die Vorredner/innen ist auch *Bossong* davon überzeugt, dass ein Rechtsinstrument zur grenzüberschreitenden Erlangung elektronischer Beweismittel langfristig erforderlich sei. Allerdings bestehe hier nur geringer zeitlicher Handlungsdruck. Ein Instrument, das unter großem Zeitdruck ausgearbeitet, gravierende rechtliche Mängel aufweise, laufe Gefahr, durch den Europäischen Gerichtshof kassiert zu werden. Objektive sei der Zeitdruck bei E-Evidence nicht so groß wie vielfach behauptet.

Dringend erforderlich sei vielmehr eine gründliche Risikobetrachtung und eine sorgfältige Ausformulierung der Rechtsakte. Letztlich sei E-Evidence nur ein „Puzzle"-Teil in einem Geflecht vielfältiger Maßnahmen. Deshalb müsse auch geklärt werden, in welchem Verhältnis die neuen Instrumente zu den bereits eingeführten beziehungsweise beschlossenen und noch geplanten Rechtsinstrumenten für die Strafverfolgung stünden.

Nachfragen

Bei der anschließenden Diskussion wurden die folgenden Fragen erörtert:

Ist für die Rechtsakte eine qualifizierte Mehrheit oder - wie von Teilen der Fachöffentlichkeit angenommen - Einstimmigkeit im Rat erforderlich?

Unzeitig teilte mit, dass das ordentliche Gesetzgebungsverfahren zur Anwendung komme und bestätigte, dass die qualifizierte Mehrheit erforderlich sei.

Verhältnis Verordnung - Richtlinie?

Unzeitig erläuterte den inhaltlichen Regelungsgehalt der beiden Rechtsakte und ging auch auf die möglicherweise unterschiedlichen Zeithorizonte ein. Bei der Richtlinie gehe es insb. um die Benennungspflichten gesetzlicher Vertreter durch Unternehmen mit Sitz innerhalb und außerhalb der EU. Die Vertreter wären dann Adressaten behördlicher Anordnungen nach der VO.

Warum werden Finanzdienstleister ausgenommen?

Die Podiumsteilnehmer bestätigten, dass Diensteanbieter, die Finanzdienstleistungen erbringen, generell aus dem Anwendungsbereich herausgenommen wurden. *Unzeitig* ergänzte, dass jedoch bezüglich der Finanzdienstleistungen Daten über die Europäische Ermittlungsanordnung erlangt werden können.

Zukunft von Diensten, die dem Privacy-by-Design Prinzip Rechnung tragen?

Schaar und *Dix* gaben zu bedenken, dass angesichts angesichts der jüngsten Rechtsprechung des Bundesverfassungsgerichts zur Herausgabepflicht eines E-Mail-Providers für aus Datenschutzgründen nicht gespeicherte Daten zu prüfen sei, was darunter zu verstehen ist. *Sippel* befürchtet, dass durch E-Evidence-Verordnung durch die Hintertür wieder eine Vorratsdatenspeicherung eingeführt werde, obwohl die Richtlinie zur Vorratsdatenspeicherung vom EuGH kassiert worden sei.

Wie kann bezüglich des Vorliegens eines „Notfalls" im Strafrecht eine unmittelbare Gefahr nachgewiesen werden?

Bossong ist der Auffassung, dass es sich hier eher um Gefahrenabwehr handele. Allerdings sei die Abgrenzung zwischen Polizeirecht und Strafverfolgung in anderen Mitgliedsstaaten weniger scharf als in Deutschland. Auch der Verordnungsentwurf unterscheide hier nicht.

Zweckänderung herausgegebener Daten, speziell Verwendung durch Nachrichtendienste?

Die Unterscheidung zwischen Strafverfolgungsbehörden und Nachrichtendiensten ist nach *Bossong* in anderen Mitgliedsstaaten nicht trennscharf. Es gebe sogar Behörden, die gleichermaßen polizeiliche und nachrichtendienstliche Aufgaben und Befugnisse hätten. Dies wirke sich auch auf spätere Zweckänderungen aus. Der VO-Entwurf lasse hier viele Fragen offen.

Ist der abgestufte rechtliche Schutz von Transaktions- und Inhaltsdaten noch zeitgemäß?

Landefeld weist darauf hin, dass die Transaktionsdaten (Metadaten) im Mittelpunkt des Interesses der Behörden stünden. Sie ließen weitgehende Schlüsse auf die Verhaltensweisen und Kontakte von Personen zu. Deshalb sei auch bei diesen Daten ein hohes Schutzniveau erforderlich.

Wird die E-Evidence-Verordnung Bestand haben?

Sippel, Petri, Landefeld, Unzeitig und *Bossong* sind sich einig, dass angesichts schwerwiegender rechtlicher Bedenken die Stabilität des Systems fraglich sei. Auch *Unzeitig* betonte, dass weiterhin noch rechtliche Bedenken bestünden. Auch den Strafverfolgungsbehörden sei mit Instrumenten wenig gedient, wenn die zugrundeliegenden Regelungen keinen rechtlichen Bestand hätten und ggf. vom EuGH aufgehoben würden.