AUSWIRKUNGEN DER ENTSCHEIDUNG 17-2 DES US SUPREME COURT (US VS. MS) AUF DEN EUROPÄISCHEN DATENSCHUTZ

Ewald Scheucher / Alexander Czadilek

Mag., Rechtsanwalt, Scheucher Rechtsanwalt GmbH
Lindengasse 39 1070 Wien, AT
scheucher@scheucher.eu; www.scheucher.eu

Mag., Rechtsanwaltsanwärter, Scheucher Rechtsanwalt GmbH
Lindengasse 39 1070 Wien, AT
czadilek@scheucher.eu; www.scheucher.eu

Schlagworte: ***US Supreme Court, Cloud Computing, DSGVO, Datenschutz***

Abstract: *Der US Supreme Court wird Mitte 2018 darüber entscheiden, ob US-amerikanische Unternehmen den US-Ermittlungsbehörden Zugriff auf personenbezogene Daten gewähren müssen, die auf Servern (in der Cloud) in der EU gespeichert sind. Nachstehend werden die Problemstellungen für den europäischen Datenschutz erörtert, die sich aus einer Entscheidung, die einen unilateralen und extraterritorialen Datenzugriff von US-Behörden ohne internationale Rechtsgrundlage sanktionieren würde, ergeben.*

1. Vorgeschichte und Verfahren

Ende 2013 hatte ein New Yorker Bundesbezirksgericht einen Durchsuchungsbeschluss[1] («search and seizure warrant» gemäß 18 U.S.C. § 2703) erlassen, der den US-Konzern Microsoft verpflichtete, E-Mails eines Kunden des MSN.com – bzw. Outlook.com Services, der des internationalen Drogenhandels verdächtig ist, an US-amerikanische Ermittlungsbehörden herauszugeben. Microsoft überreichte den Ermittlungsbehörden daraufhin einen Teil der Nachrichten, weigerte sich aber, den Behörden Daten auszuhändigen, die auf Servern in Dublin, Irland «in der Cloud» gespeichert waren bzw. sind. Microsoft argumentierte, dass in diesem Fall irische Gerichte zuständig seien und bekämpfte den Beschluss vor dem Bundesberufungsgericht für den zweiten Bundesgerichtsbezirk (2nd Circuit).

Die drei Richter des Berufungsgerichts entschieden im Juli 2016 einstimmig gegen das Begehren der US-Regierung und hoben die Entscheidung des Bezirksgerichts auf, da nach der Rechtsansicht der Berufungsrichter das anzuwendende Gesetz, der Stored Communications Act 1986[2] (ein Teil des Electronic Communications Privacy Act), der die Privatsphäre von Nutzern im Zusammenhang mit der Verwendung (in den 1980er Jahren) neuer Technologien (z.B. E-Mail) schützt, nur im Inland (also den USA) gelte, weil der Gesetzgeber einen Datenzugriff auf Server außerhalb der USA nicht explizit regelte. Das Berufungsgericht[3] argumentierte dies insbesondere damit, dass vor dreißig Jahren nicht absehbar war, dass Internet Service Provider ein weltweites Netz von Hardware (cloud computing) einsetzen würden, um den Ansprüchen von Nutzern im 21. Jahrhundert im Hinblick auf einen jederzeitigen und schnellen Zugang zu ihren Daten gerecht zu werden. Vielmehr wollte der Gesetzgeber nach Ansicht des Berufungsgerichts grundsätzliche Datenschutzregelungen für inländische Internetnutzer schaffen ohne dabei jedoch das Rechtsinstrument Durchsuchungsbefehl (warrant) von seiner

---

1 Der Dursuchungsbeschluss und weitere das Verfahren betreffende Dokumente sind abrufbar unter https://blogs.microsoft.com/datalaw/about-the-case/ (alle Websites zuletzt besucht am 23. Januar 2018).

2 18 U.S.C. §§ 2701 ff. siehe https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

3 US Court of Appeals for the Second Circuit Docket No. 14-2985, 6.

ausschließlich territorialen Anwendbarkeit zu befreien. Zudem würde die im Verfahren vorgebrachte Interpretation des Gesetzes der US-Regierung, nachdem ein Durchsuchungsbeschluss einen Internet Service Provider verpflichten würde, auch Daten, die außerhalb der USA gespeichert sind, zu übermitteln bzw. offenzulegen, das völkerrechtliche Territorialitätsprinzip verletzen.

Daraufhin beantragte die US-Regierung eine erneute Anhörung vor einer erweiterten Richterbank desselben Gerichts. Nachdem nur vier von acht Richtern des 2nd Circuit für eine neuerliche Anhörung stimmten, war dieser Antrag abgelehnt.

Schließlich wandte sich die US-Regierung, unterstützt von 33 US-Bundesstaaten, an den US Supreme Court (SCOTUS)[4]. Es geht um die grundsätzliche Frage, ob § 2703 des Stored Communications Act 1986 es einem US-Gericht ermöglicht, einen Durchsuchungsbeschluss zu erlassen, der einen US-Internetprovider, der (web/cloud-basierte) E-Mail Dienste anbietet, zwingt, personenbezogene Daten, die außerhalb der USA gespeichert sind, an US-amerikanische Ermittlungsbehörden herauszugeben[5].

Der Fall wurde angenommen, weil die Klärung dieser Rechtsfrage von erheblicher Bedeutung ist. Der US Supreme Court wird nun voraussichtlich im Juni 2018 über diese Frage eine richtungsweisende Entscheidung treffen. Die Tragweite dieser Entscheidung für den internationalen und Europäischen Datenschutz wird auch durch den Umstand unterstrichen, dass u.a. die Europäische Kommission und der Sonderberichterstatter für Privatsphäre und Datenschutz der Vereinten Nationen als sogenannte *Amici Curiae* sich an dem Verfahren beteiligten und Stellungnahmen[6] abgaben.

2. Technischer Hintergrund

Microsoft betreibt unter dem Namen Outlook.com (vormals msn.com) ein weltweites kostenloses webbasiertes E-Mail Service. Die Inhalte (E-Mails, Kalender etc.) eines Nutzerkontos werden neben diversen anderen kontobezogenen Informationen (z.B. IP-Adressen) in einem Netzwerk von über einer Million Servern in einer «public cloud» gespeichert. Diese Server werden in über einhundert Datenzentren in über 40 Ländern von Microsoft bzw. ihren Tochterunternehmen betrieben. Basierend auf einem vom Nutzer bei Kontoeröffnung frei gewählten Ländercode werden die Kontodaten grundsätzlich in einem Datenzentrum nahe dem physischen Ort, den der Nutzer durch den Ländercode festgelegt hat, gespeichert bzw. dorthin migriert, um etwa Netzwerklatenzzeiten zu minimieren und das Service zu optimieren. Laut Angaben von Microsoft entscheidet das System automatisch, wann ein Nutzerkonto und dessen Inhalte in das Datenzentrum in Dublin, Irland migriert werden soll. Vor dieser Migration werden weder der tatsächliche physische Ort, an dem sich der Nutzer aufhält, noch dessen Identität verifiziert, die Migration basiert allein auf dem vom Nutzer gewählten Ländercode. Sobald das Nutzerkonto vollständig migriert ist, werden Daten, die auf US-Servern gespeichert sind, vollständig gelöscht[7]. Ab diesem Zeitpunkt hat auch Microsoft ausschließlich über das Datenzentrum in Dublin Zugriff auf Inhalts- und kontobezogene Daten eines Nutzers, wobei jedoch Microsoft die Möglichkeit hat über eine Datenbank-Management-Anwendung von jedem der weltweiten Server Daten in die USA zu transferieren.

3. Argumente der Parteien

Neben der Nichtanwendbarkeit des Stored Communications Acts 1986 auf den gegenständlichen Fall argumentierte **Microsoft** im Berufungsverfahren insbesondere, dass neben internationalen Rechtsinstrumenten zur

---

4 In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, United States of America v. Microsoft Corporation; Aktenzeichen 17-2.

5 QUESTION PRESENTED
Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad.

6 https://www.supremecourt.gov/docket/docketfiles/html/public/17-2.html.

7 US Court of Appeals for the Second Circuit Docket No. 14-2985, 9.

Zusammenarbeit in der internationalen Verbrechensbekämpfung wie der Budapest Convention[8] auch ein bilaterales Rechtshilfeabkommen (Mutual Legal Assistance Treaty, MLAT) zwischen Irland und den USA bestehe[9], das US-amerikanischen Strafverfolgungsbehörden ermögliche, die geforderten Daten im Rechtshilfeweg zu erlangen. Dieser Weg wäre nicht nur der internationalen völkerrechtlichen Gepflogenheiten entsprechende, sondern würde Microsoft auch nicht vor das Dilemma stellen entweder hohe Strafen wegen Nichtbefolgung eines Durchsuchungsbeschlusses in den USA zu riskieren oder nationale Datenschutzgesetze von Staaten, in denen Microsoft Datenzentren unterhält, zu verletzen. Microsofts oberster Jurist Brad Smith warnte[10] insbesondere vor einer Konfliktsituation mit der DSGVO. Ab Mai 2018 an werde es nämlich illegal für ein Unternehmen, Kundendaten auf eine einseitige US-Anordnung hin aus Europa in die Vereinigten Staaten zu transferieren. Dass dies alles andere als ein theoretisches Dilemma sei, unterstreichen bereits Auseinandersetzungen zwischen den USA und Brasilien.

Microsoft befürchtet auch Millioneneinbußen seines Geschäfts durch einen Wechsel zahlreicher Internetuser auf nicht US-amerikanische Services, falls der US Supreme Court nicht im Sinne Microsofts entscheidet. Seit den Snowden Enthüllungen im Jahr 2013 sei nämlich das Vertrauen der Internetnutzer in US-amerikanische Internetdienstleister wegen der mehr oder weniger unlimitierten Datenzugriffe durch US-Geheimdienste schwer erschüttert. Um dieses Vertrauen wiederzugewinnen hat Microsoft auch sehr hohe Investitionen in Datenzentren außerhalb der USA getätigt. Die Befürchtungen Microsofts, aus einer für die US-Regierung positiven Entscheidung des US Supreme Courts einen Wettbewerbsnachteil gegenüber Europäischen Diensteanbietern davonzutragen, werden von der gesamten Internetwirtschaft in den USA (Apple, Amazon, Verizon etc.) geteilt.

Die **US-Regierung** argumentierte hingegen, dass § 2703 Stored Communications Act (SCA) die Offenlegung («disclosure») von elektronischen Kommunikationsdaten durch einen Diensteanbieter regle und diese Offenlegung immer in den USA stattfinde, weshalb das Territorialitätsprinzip nicht verletzt und § 2703 SCA anwendbar sei[11]. Außerdem würde die Rechtsansicht des Berufungsgerichts, dass § 2703 SCA nicht anwendbar sei, wenn ein US-Provider entscheidet, personenbezogene Daten im Ausland zu speichern, das legitime Interesse der Ermittlungsbehörden an einer Beweissicherstellung unverhältnismäßig erschweren oder behindern. In ihrer Stellungnahme vor dem US-Supreme Court bringt die US-Regierung weiters vor, dass die Entscheidung des Berufungsgerichts bereits die Aufklärung dutzender Fälle von Menschenhandel und anderer schwerer Verbrechen verhindert hätte[12]. Zudem bestünden mit vielen Staaten gar keine Rechtshilfeabkommen und Auskunftsbegehren aufgrund von Rechtshilfeersuchen wären in vielen Fällen aufwendig und langwierig, insbesondere in zeitsensitiven Ermittlungen oder in Notfällen.

4. Ausgewählte Stellungnahmen der Amici Curiae

Die **Europäische Kommission** betont zunächst in ihrer Stellungnahme die Wichtigkeit eines Rechtsrahmens für die internationale Zusammenarbeit in der Strafverfolgung, der (völker)rechtliche Konflikte verhindern und beiderseitige Interessen der Verbrechensbekämpfung einerseits und den Schutz der Privatsphäre Betroffener andererseits respektieren soll. Im gegenständlichen Fall müsse neben dem Territorialitätsprinzip und der Völkercourtoisie die fremde Jurisdiktion, hier die (ab Mai 2018) für Microsoft Ireland Ltd. geltende DSGVO, berücksichtigt werden. Insbesondere wäre zu beachten, dass ein für die Datenverarbeitung Verantwortlicher personenbezogene Daten in Drittstaaten wie die USA nur unter den engen Voraussetzungen des 5. Kapitels der DSGVO übermitteln darf. Die EU-Kommission weist auch darauf hin, dass die unabhängigen nationalen Aufsichtsbehörden nach der DSGVO die Übermittlung von personenbezogenen Daten auch unterbinden und

8 Convention on Cybercrime, ETS No. 185.

9 Criminal Justice Mutual Assistance Act 2008.

10 https://www.heise.de/newsticker/meldung/Microsoft-Fall-US-Justizministerium-bringt-Streit-ueber-Datenzugriff-in-der-EU-vor-den-Supreme-Court-3755865.html.

11 US Court of Appeals for the Second Circuit Docket No. 14-2985, 24.

12 17-2 Reply Brief for the United States, 3.

dem Verantwortlichen im Falle einer Verletzung der einschlägigen Bestimmungen Strafen bis zu 20 Millionen Euro oder vier Prozent des Konzernjahresumsatzes auferlegen können.

Der **Sonderberichterstatter für Privatsphäre und Datenschutz der Vereinten Nationen Joseph Cannataci** weist ebenso auf die Bedeutung der Entscheidung des US Supreme Court für den Schutz der Privatsphäre von unzähligen weltweiten Kunden von Microsoft und anderer Cloud Computing Services hin und sieht in dem Umstand, dass insbesondere Staaten ohne ausreichende Rechtsschutzmöglichkeiten einen unilateralen und extraterritorialen Datenzugriff zulassen könnten, eine erhebliche Gefahr für das Grundrecht auf Datenschutz im Cyberspace.

Einige frühere **leitende Beamte der US-amerikanischen Ermittlungsbehörden, der National Security Agency sowie anderer Geheimdienste und Polizeibehörden aus den USA, dem Vereinigten Königreich und Frankreich** gaben ebenfalls eine gemeinsame Stellungnahme als Amici Curiae ab. Darin fordern diese eine Zurückhaltung des US-Supreme Court und unterstreichen, ohne eine Position für eine der Parteien einzunehmen, dass es Aufgabe des nationalen Gesetzgebers bzw. der internationalen Gesetzgeber ist, eine Rechtsgrundlage zu schaffen, die den Anforderungen einer effektiven Verbrechensbekämpfung, der Achtung der Souveränität der Staaten, der Völkercourtoise, der Offenheit des Internets, dem Unternehmertum und dem Recht auf informationelle Selbstbestimmung gerecht wird. Eine Entscheidung des US Supreme Court, die dies nicht berücksichtigt, hätte nach Ansicht der Amici eine ähnliche Auswirkung wie eine legislative Entscheidung des US-Kongresses und würde Reaktionen von Gegnern wie Verbündeten der USA hervorrufen, die die Zusammenarbeit und internationale Kooperation in der grenzüberschreitenden Verbrechensbekämpfung gefährden könnten. Eine besondere Gefahr wird darin gesehen, dass ein unilateraler Datenzugriff durch manche Staaten dazu führen könnte, dass andere Staaten dazu übergehen, weltweit tätige Unternehmen zu verpflichten, ausschließlich lokale (und eben nicht vernetzte) Datenspeicher zu betreiben («compelled data localization»). Dies würde nicht nur Nachteile für die Nutzer mit sich bringen, sondern den Gedanken der Offenheit des Internets geradezu erodieren, zu einer «Balkanisierung des Internets» führen und den internationalen Handel beeinträchtigen[13].

5. DSGVO und Rechtshilfeabkommen

Zweifellos unterliegen die hier verfahrensgegenständlichen personenbezogenen Daten ab Mai 2018 der DSGVO, da sie auf Servern im Unionsgebiet (Irland) gespeichert sind (Art. 3 Abs. 1 und Art. 4 Z 2 DSGVO). Das fünfte Kapitel (Art. 44 bis 50) der DSGVO enthält spezielle Regelungen zur Datenübermittlung aus der EU in Drittstaaten. Diese Bestimmungen sollen sicherstellen, dass die Rechte aus der EU-Grundrechte Charta auch dann gewahrt werden, wenn Daten in einen Drittstaat übermittelt werden, wobei eine Übermittlung nach diesen Bestimmungen nur dann rechtmäßig sein kann, wenn schon die Verarbeitung (vor der Übermittlung) nach den übrigen Bestimmungen der DSGVO rechtmäßig war (Art. 44 DSGVO). Gemäß Art. 45 DSGVO dürfen Datenübermittlungen in Drittländer aufgrund einer Adäquanzentscheidung der EU-Kommission, wie etwa dem aufgehobenen Safe Harbor Abkommen (C-362/14 Schrems) oder dessen Nachfolgeregelung EU-US Privacy Shield erfolgen. Gemäß Art. 46 DSGVO dürfen Datenübermittlungen in Drittländer erfolgen, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien (etwa Standardvertragsklauseln, binding corporate rules) vorgesehen hat und den Betroffenen effektive Rechtsschutzmöglichkeiten im Drittland zur Verfügung stehen. Treffen die vorgenannten Bedingungen, wie im gegenständlichen Fall, nicht zu, bleibt immer noch die Möglichkeit einer Datenübermittlung gemäß Art. 49 DSGVO, der bestimmte Ausnahmefälle regelt. Im vorliegenden Fall kommen zwei Regelungen in Betracht:

[13] 17-2 Brief amici curiae of Former Law Enforcement, National Security, and Intelligence Officials in support of neither party filed, 9 f.

- die Übermittlung aus wichtigen Gründen des öffentlichen Interesses, worunter die Strafverfolgung im internationalen Drogenhandel sicher fällt (siehe auch verbundene Rs C-293/12 und C-594/12 Digital Rights Ireland) *oder*
- die Datenübermittlung ist für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Das berechtigte Interesse wäre im vorliegenden Fall, dass Microsoft (oder allgemein jeder andere US-Diensteanbieter) in den USA im Falle einer Nichtbefolgung eines gerichtlichen Durchsuchungsbeschlusses einer Strafe ausgesetzt wäre.

Im letztgenannten Fall ist eine Datenübermittlung aber nur dann zulässig, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, die Aufsichtsbehörde in Kenntnis gesetzt wird und der Betroffene davon unterrichtet wird (unbeschadet der Informationsrechte der Art. 13 und 14 DSGVO). Nachdem aber schon die Überschrift des Art. 49 DSGVO «Ausnahmen für bestimmte Fälle» lautet und diese Bestimmung sehr restriktiv ausgelegt werden sollte, bietet sie keine hinreichende und befriedigende und handhabbare Rechtsgrundlage für eine (anzunehmende) Vielzahl von Auskunftsbegehren US-amerikanischer Ermittlungsbehörden zu Daten, die auf Servern in der EU gespeichert sind. Insbesondere kann von US-Unternehmen (auch wenn sie Tochtergesellschaften in der EU haben) nicht verlangt werden, den Begriff des «öffentlichen Interesses» in jedem Einzelfall richtig auszulegen, nachdem, das «öffentliche Interesse» im Sinne des Art. 49 Abs. 1 lit. d DSGVO entweder im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, auch anerkannt sein muss.

Art. 48 DSGVO betrifft Datenübermittlungen oder Offenlegungen (disclosure) an Drittländer, welche nicht durch Unionsrecht gedeckt sind und adressiert und verbietet Übermittlungen und Offenlegungen, die von Drittländern erzwungen werden und nicht auf einem Rechtshilfeabkommen basieren. Dies geht auch aus Erwägungsgrund 115 hervor:

> «*[...] Dies kann Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden in Drittländern umfassen, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird und die nicht auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.*»

Nachdem etwa ein Cloud-Anbieter mit Sitz in den USA auf Grundlage des US-Patriot Acts verpflichtet werden kann, personenbezogene Daten, die bei einem in der EU ansässigen Tochterunternehmen gespeichert sind, an US-Ermittlungsbehörden herauszugeben oder das FBI umfassende Zugriffsmöglichkeiten auf solche Daten aufgrund des US Foreign Intelligence Surveillance Act (FISA) hat, hatte es schon im Vorfeld der Entstehung der DSGVO Bestrebungen gegeben, solche Datenzugriffe möglichst hintanzustellen. Aus diesem Grund wird Art. 48 DSGVO auch als «Anti FISA Klausel» bezeichnet[14]. Art. 48 DSGVO stellt jedenfalls klar, dass ein Gerichtsbeschluss, der nicht auf einem internationalen Rechtshilfeabkommen basiert, eine Übermittlung personenbezogener Daten nicht rechtfertigt. Die **DSGVO sieht** demnach **in Rechtshilfeabkommen** die **präferierte Option für Datenübermittlungen**, die sonst nach der DSGVO nicht zulässig sind. Nach Ansicht der EU-Kommission[15] bieten solche internationalen Verträge die Möglichkeit einer Beweiserlangung durch bilaterale/multilaterale Zustimmung und verkörpern ein sorgfältig ausgehandeltes Gleichgewicht zwischen den Interessen verschiedener Staaten um Zuständigkeitskonflikte zu verhindern, die anderenfalls entstehen

[14] Daniel A. Paul/Boris P. Paal, Kommentar zur DSGVO, Art. 48 Rz 2.

[15] Brief amicus curiae of European Commission on Behalf of the European Union in support of neither party filed, 14.

könnten. Im Übrigen existieren sowohl zwischen der USA und der EU[16] als auch zwischen der USA und Irland[17] Rechtshilfeabkommen. Im gegenständlichen Fall kamen diese aber nicht zur Anwendung, da die US-Regierung gar keine Rechtshilfeersuchen gestellt hat. Entscheidet der US Supreme Court nun im Sinne der US-Regierung und sanktioniert unilaterale Datenübermittlungen bzw. -offenlegungen von in der EU gespeicherten personenbezogenen Daten an US-Ermittlungsbehörden, hätten Betroffene nach der DSGVO zwar ein Beschwerderecht an die jeweilige nationale Aufsichtsbehörde und ein Recht auf (im)materiellen Schadenersatz gegen das jeweilige übermittelnde Unternehmen, sie hätten aber keinerlei Rechtsschutzmöglichkeiten in den USA, wie es zumindest ansatzweise bei einer Datenübermittlung aufgrund des EU-US Privacy Shield der Fall wäre. Andererseits wären US-amerikanische Diensteanbieter bzw. deren in der EU ansässige Tochterunternehmen den hohen Strafen nach Art. 83 ff. DSGVO ausgesetzt. Dieser Umstand kann weder im wirtschaftlichen Interesse der USA noch der EU sein und beeinträchtigt jedenfalls die internationalen Beziehungen.

6. Polizei Richtlinie (EU) 2016/680

Die Problematik, dass europäische Mindestdatenschutzstandards, die sich aus der RL (EU) 2016/680 ergeben, unterlaufen werden könnten, wenn europäische Ermittlungsbehörden bzgl. bestimmter Daten, die nach nationalem oder Unionsrecht nicht verarbeitet bzw. ermittelt werden dürfen, Rechtshilfeersuchen an die USA stellen, um Daten, die US-amerikanische Unternehmen auf Servern in der Europäischen Union gespeichert und an US-amerikanische Ermittlungsbehörden herausgegeben haben, zu erlangen, ist nach Ansicht der Autoren derzeit zu vernachlässigen. Einerseits dürfen gemäß Art. 4 Abs. 1 lit. b Polizei-RL personenbezogene Daten immer nur verarbeitet werden, wenn sie rechtmäßig erhoben wurden (wobei im Falle einer Übermittlung aufgrund eines Rechtshilfeabkommens auszugehen ist), andererseits gilt auch in der Polizei-RL stets die strenge Zweckbindung und das Prinzip der Verhältnismäßigkeit.

7. Conclusio

Sollte der US Supreme Court einen unilateralen und extraterritorialen Datenzugriff von US-Ermittlungsbehörden auf personenbezogene Daten, die von US-amerikanischen Unternehmen außerhalb der USA in einer Cloud gespeichert werden, aufgrund § 2703 Stored Communications Act für zulässig erklären, hätte dies schwerwiegende und nachteilige Folgen für die internationalen Beziehungen zwischen den USA und insbesondere der EU. US-amerikanische Unternehmen, die in der EU tätig sind, wären existenzbedrohenden Strafen nach der DSGVO ausgesetzt. Betroffene in der EU, deren personenbezogene Daten an US-Behörden übermittelt werden, hätten keinerlei Rechtsschutzmöglichkeiten in den USA. Diese gravierenden Folgen einer solchen (möglichen) Entscheidung des US Supreme Court zeigen klar auf, dass es für die internationale grenzüberschreitende Verbrechensbekämpfung unumgänglich ist, einen modernen und angemessenen völkerrechtlichen Rechtsrahmen zu schaffen, der den technischen Gegebenheiten des 21. Jahrhunderts wie Cloud-Computing gerecht wird, der den Ermittlungsbehörden ermöglicht effektiv zu sein und zudem gewährleistet, dass Betroffenenrechte und Rechtsschutzmöglichkeiten gewahrt bleiben. Einen ersten Vorschlag hat Joe Cannataci, UN Sonderberichterstatter für Privatsphäre und Datenschutz im Rahmen des MAPPING Projects[18] mit dem IDAW (International Data Access Warrant) unterbreitet[19].

---

16 Agreement on Mutual Legal Assistance Between the United States of America and the European Union, 25 June 2003, OJ L 181/34 of 19 July 2003.

17 Treaty Between the United States of America and Ireland on Mutual Legal Assistance in Criminal Matters, 18 January 2001, Siehe Treaty Doc. No. 107-9 (2002).

18 https://mappingtheinternet.eu/.

19 Brief amicus curiae of U.N. Special Rapporteur on the Right to Privacy Joseph Cannataci in support of neither partyfiled, 26.