Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1*

Hintergründe des Kommissionsentwurfs zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln im Strafermittlungsverfahren wie auch zum sog. Microsoft Ireland Case

Von Prof. Dr. **Christoph Burchard**, LL.M. (NYU), Frankfurt a.M.

„If every country asserts extraterritorial jurisdiction […] then everybody gets everybody's data."[1]

Tempora mutantur. Mitte März dieses Jahres fertiggestellt, um (Vor-)Überlegungen zum anstehenden Kommissionsentwurf zum grenzüberschreitenden Zugriff auf elektronische Beweismittel wie auch zum anstehenden Urteil des US Supreme Court im sog. Microsoft Ireland Case zu liefern, wurde der vorliegende Beitrag durch die sich in der Folge überschlagenden rechtspolitischen Ereignisse scheinbar (dazu, dass der Schein trügt, sogleich) überholt. Zunächst verabschiedete der US-Bundesgesetzgeber den sog. Clarifying Lawful Overseas Use of Data Act (oder auch CLOUD-Act), der am 23.3.2018 in Kraft trat und der sogleich von US-Strafverfolgern aktiv genutzt wurde, um US-Diensteanbietern, wie Microsoft, aufzugeben, in der EU gespeicherte Daten in die USA zu transferieren und dort offenzulegen.[2] Das Inkrafttreten des CLOUD-Acts nahm der US Supreme Court zum Anlass, um den sog. Microsoft Ireland Case am 17.4.2018 per curiam für gegenstandslos („moot") zu erklären, sei doch nunmehr die entscheidende Rechtsfrage (namentlich ob inländische Internet-Diensteanbieter zur Beibringung und Herausgabe von Auslandsdaten verpflichtet werden dürfen) geklärt.[3] Ironie der Geschichte: Am selben Tag, also am 17.4.2018, lancierte auch die Kommission ihre Vorschläge, wie der „grenzüberschreitende Zugang zu elektronischen Beweismitteln im Strafermittlungsverfahren" zu regeln sei.[4]

Diese „Federstriche" entscheidender rechtspolitischer Akteure dies- wie jenseits des Atlantiks unterstreichen die Aktualität dieses Beitrags. Daher musste er in der Sache nicht verändert werden – mit der Ausnahme, dass nicht länger (wie ursprünglich intendiert) Ausblicke auf kommende rechtspolitische Entscheidungen gegeben, sondern nurmehr deren Hintergründe beleuchtet werden können.[5] Meine kritische Position ist die gleiche geblieben, weil weltweit und nun auch in der EU die Axt an die ehernen Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen gelegt wird, was sich nahtlos in die globalen Erschütterungen der bestehenden internationalen (Sicherheits-)Ordnung einfügt.

Der ZIS gilt mein großer Dank. Sowohl für die ursprüngliche Bereitschaft, diesen Beitrag schnell zu veröffentlichen, um den zuvor genannten Ereignissen zuvorzukommen, wie für die jetzige Bereitschaft, diese Ereignisse „lediglich" vermittels dieser Vor- sowie einer Nachbemerkung zu verarbeiten.

Einführung

Die (strafverfahrensrechtliche) Regelung des grenzüberschreitenden Zugriffs auf in der sog. Cloud[6] gespeicherte

---

* Der zweite Teil dieses Beitrags wird in ZIS 7-8/2018 erscheinen.

[1] John Frank, Vice President for EU Government Affairs, Microsoft. Wiedergegeben nach *Fioretti*, Europe seeks power to seize overseas data in challenge to tech giants, Reuters Business News v. 26.2.2018, online abrufbar unter https://uk.reuters.com/article/uk-eu-data-order/europe-seeks-power-to-seize-overseas-data-in-challenge-to-tech-giants-idUKKCN1GA0LN (25.5.2018).

[2] So berichtet in https://www.theregister.co.uk/2018/04/03/us_government_serves_microsoft_with_fresh_warrant_for_irishheld_emails/ (25.5.2018).

[3] Namentlich dadurch, dass solche Beibringungs- und Herausgabeanordnungen auch betreffend Auslandsdaten nach dem CLOUD-Act erlassen werden dürfen. Die entsprechende Entscheidung des US Supreme Court ist online abrufbar unter https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf (25.5.2018).

[4] Vorschlag der Kommission für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen v. 17.4.2018, COM (2018) 225 final sowie für eine „Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings" v. 17.4.2018, COM (2018) 226 final. Online abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018PC0225&from=EN (25.5.2018) und http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN (25.5.2018).

[5] Mitunter wurde der Beitrag im Duktus verändert und statt der Gegenwarts- oder Zukunfts- eine Vergangenheitsform verwendet.

[6] Unter der Cloud sind ganz abstrakt onlinebasierte Speicher- und Serverdienste zu verstehen. Wie unten noch zu zeigen sein wird (siehe unten II. 1. c), verfolgen Diensteanbieter ganz unterschiedliche Speicherpolitiken, die dem territorialen Serverstandort ganz unterschiedliche Bedeutung zumessen. Daraus wird unter III. 1. b) ein Differenzierungsgebot abgeleitet, wonach „Cloud nicht gleich Cloud" ist, wenn es um den grenzüberschreitenden Zugriff auf eben jene zu Strafverfolgungszwecken geht. Zum Begriff Cloud und Cloud Computing vgl. etwa *Andrews/Newman*, Maryland Law Review 2013, 313 (323 ff.); *Wiebe*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, § 69c UrhG Rn. 60; *Wicker*, Cloud Computing und staatlicher Strafanspruch, 2016, S. 35 ff.

Daten ist eine der drängendsten Aufgaben der Internetära.[7] Drängend aus zusammenarbeitsrechtstheoretischer Perspektive, weil das Internet für die Nutzer (für friedliebende Bürger wie auch für Kriminelle) einerseits keine[8] Territorialgrenzen kennt. Da aber andererseits die staatlichen Strafverfolgungsorgane an eben diese Grenzen gebunden sind, sind sie bis dato bei grenzüberschreitenden Zugriffen auf in der Cloud gelegene zugangsgeschützte elektronische Beweismittel auf den traditionellen Rechtshilfeweg angewiesen. Da sich dieser aber bei Cyberermittlungen als zu umständlich und langwierig herausgestellt hat,[9] stellt sich die Frage nach dem anwendbaren Recht.[10] Drängend ist eine Regelung des grenzüberschreitenden Zugriffs auf elektronische Beweismittel in der Cloud überdies aus datenschutztheoretischer Sicht deshalb, weil wir aufgrund von Big Data-Analysen – ohne alarmistisch klingen zu wollen – in den Zeiten des gläsernen Menschen angekommen sind.[11] Die Daten, die von und über uns in der Cloud verfügbar sind, sind überwältigend und beängstigend. Daher ist festzulegen, welche Strafverfolger auf diese Daten Zugriff nehmen dürfen. Drängend ist die beschriebene Regelungsaufgabe schließlich aus ganz handfesten praktischen Gründen, wenn und weil es die Reichweite der strafprozessualen lex lata (in Deutschland etwa des § 110 Abs. 3 StPO bei grenzüberschreitenden Zugriffen auf Clouddaten)[12] zu klären gilt.

In der EU wurde daher lange auf den (eigentlich bereits für Mitte Januar 2018) angekündigten Kommissionsentwurf zum grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafverfahren gewartet. Und in den USA stand bis April dieses Jahres das Urteil des US Supreme Court im berühmt-berüchtigten Microsoft Ireland Case ins Haus.[13] Ein Fall, der den Blick darauf lenkt, dass etliche Staaten bereits unilateral vorgeprescht sind.[14] So können beispielsweise bereits in Brasilien[15] und Belgien[16] im Inland aktive Diensteanbieter vermittels hier so übersetzter Beibringungsanordnungen („production orders“)[17] dazu verpflichtet werden, Auslandsdaten ins Inland zu transferieren und diese an Strafverfolger herauszugeben. Dies wollte auch die US-Regierung im besagten Microsoft Ireland Case erreichen, bis dann mithilfe eines Federstrichs des US-Gesetzgebers und dem CLOUD-Act anderweitig für Klarheit gesorgt wurde. Einen anderen Weg, jenen des „Daten-Nationalismus“[18], verfolgen etwa Russland und Vietnam mit weitreichenden Lokalisierungsverpflichtungen. Danach sind Daten im Inland zu speichern oder zumindest zu spiegeln, um diese im Fall der Fälle als Inlandsdaten an Strafverfolger herausgeben zu können.

[7] So bereits *Woods*, Stanford Law Review 2016, 729 (729).

[8] Dies gilt zumindest solange, wie das Internet nicht – wie z.B. in China – abgeschottet, sondern offen gestaltet wird. Zur (wenig politisch korrekt) „Balkanisierung“ geschimpften Fragmentierung des Internets ausführlich und m.w.N. das White Paper für das World Economic Forum von *Drake/Cerf/Kleinwächter*, Internet Fragmentation: An Overview, 2016, S. 31, online abrufbar unter http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf (25.5.2018).

[9] Siehe hierzu unten I. 3. a) bb) und II. 1. b) sowie *Sieber*, Gutachten C zum 69. Deutschen Juristentag – Straftaten und Strafverfolgung im Internet, 2012, S. 39; *Wicker*, MMR 2013, 765 (769).

[10] Hierzu aus der Perspektive des internationalen Privatrechts auch *Nordmeier*, MMR 2010, 151.

[11] Vgl. nur *Solove*, The Digital Person: Technology and Privacy in the Information Age, 2004.

[12] Hierzu etwa *Warken*, NZWiSt 2017, 329 (337 f.), sowie alle aktuellen StPO-Kommentare m.w.N.

[13] Die Parteivorträge sowie eine Vielzahl an amicus curiae briefs finden sich online unter https://www.supremecourt.gov/docket/docketfiles/html/public/17-2.html (25.5.2018). Eine erste Auswertung findet sich bei *Goeble/Scheuble*, ZD-Aktuell 2018, 06009. Siehe auch die Anmerkungen und Besprechungen des Verfahrens bei *Currie*, The Canadian Yearbook of International Law 2016, 63 (84 ff.); *Daskal*, Harvard Law Review Blog v. 28.2.2018, abrufbar unter https://blog.harvardlawreview.org/microsoft-ireland-argument-analysis-data-territoriality-and-the-best-way-forward/ (25.5.2018); *dies.*, Vanderbilt Law Review 2018, 179 (187 ff.); *Gary/Olin-Ammentorp*, Georgetown Law Technology Review 2016, 52.

[14] Vgl. die Übersicht bei *Daskal*, Vanderbilt Law Review 2018, 179.

[15] Vgl. hierzu die ausführliche Darstellung der Situation von US-Diensteanbietern in Brasilien im vor dem US Supreme Court eingereichten amicus curiae-Papier des brasilianischen „Internetlab Law and Technology Center“, S. 21 ff. m.w.N., online abrufbar unter https://www.supremecourt.gov/DocketPDF/17/17-2/28382/20180118203851162_17-2%20bsac%20Internetlab%20Law%20and%20Technology%20Center.pdf (17.3.2018).

[16] Vgl. hierzu die Entscheidungen zu Yahoo! (Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N) und zu Skype (Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12). Hierzu auch die Besprechung von *de Schrijver/Daenens*, The Yahoo! Case: The End of International Legal Assistance In Criminal Matters, 2013, online verfügbar unter http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters (25.5.2018).

[17] Die Terminologie findet sich als Überschrift zu Titel 3 und zu Art. 18 Cybercrime Convention v. 23.11.2001, ETS 185, BGBl. II 2008, S. 1242; die deutsche Übersetzung in BGBl. II 2008 S. 1242 spricht insofern von der „Anordnung der Herausgabe“, was jedoch nicht erfasst, dass im Ausland belegene Daten von Diensteanbietern zunächst ins Inland zu transferieren, also beizubringen sind. Vgl. zur Terminologie auch *Sieber* (Fn. 9), S. 114 f.

[18] Pointiert *Chander/Lê*, Emory Law Journal 2015, 677; dort auch m.w.N. zum Folgenden.

Diese wenigen Optionen[19] für den „grenzüberschreitenden“ Zugriff auf die Cloud lassen erkennen, wie komplex und facettenreich die anstehenden Regelungsaufgaben sind. Das ist wenig überraschend, gilt es doch die unterschiedlichsten Interessen zu praktischer Konkordanz zu bringen, um drohende Jurisdiktionskonflikte zu verhindern und um das Verhältnis von Freiheit und Sicherheit sowie von nationaler und internationaler Strafrechtspflege bei Ermittlungen in der Cloud neu auszutarieren. Dabei sind insbesondere zu berücksichtigen: die Effektivität der Strafverfolgung, die Wahrung der nationalen Souveränität, hier insbesondere der Territorialhoheit über im Inland gespeicherte Daten, die zwischenstaatliche Höflichkeit („international comity“), die Offenheit des Internets, die wirtschaftlichen Belange der privaten (Cloud- oder Internet-)Diensteanbieter und last but not least die Grundrechte der Nutzer, insbesondere jene auf informationelle Selbstbestimmung und Privatheit („informational privacy“).[20]

In diesem Beitrag soll dafür geworben werden, die Abwägung dieser Belange nicht zu einseitig zu gestalten. Zwar verheißt die Cloud ungeheure Datenschätze, so dass für die Innen- und Sicherheitsseite (und ihre „Lobby“) der möglichst rasche Zugriff auf verwend- und verwertbare elektronische Beweismittel für die effektive Verfolgung von Cyber- und gemeiner Kriminalität im Vordergrund stehen dürfte. Die Justizpolitik muss freilich auch das „große Ganze“ im Blick behalten. Dabei gilt es dreierlei zu beachten:

- Das Gebot der langfristigen Systemerhaltung: Kurzfristige Ermittlungserfolge in Einzelfällen dürfen das Gesamtsystem der international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität langfristig nicht unterminieren.[21]
- Die Beachtung der Reziprozität: Was heute in der EU[22] für die EU geregelt wird, kann und wird außerhalb der EU Schule machen und darf dabei der EU dann nicht „auf die Füße fallen“. Weniger flapsig ausgedrückt muss beispielsweise bedacht werden: Wer z.B. nach dem Marktortprinzip die im Inland aktiven Diensteanbieter verpflichten will, Auslandsdaten beizubringen und herauszugeben, muss damit rechnen, dass im Ausland ebenso verfahren wird, mit der Folge, dass das eigene Inland keinen sicheren Datenschutzschild für schutzbedürftige Personengruppen (wie Journalisten) versprechen kann.[23]
- Die Berücksichtigung der europäischen Raumbildung: In der EU schiebt sich der Raum der Freiheit, der Sicherheit und des Rechts zwischen das Nationale und Internationale. Nach innen verspricht[24] dieser einen einheitlichen Strafverfolgungsraum unter Achtung hoher grundrechtlicher Standards. Nach außen wirkt er jedoch als einheitlicher Datenschutzraum, der Eingriffe fremder Strafverfolger – z.B. aus den USA oder Russland – zu blockieren oder allemal zu kontrollieren sucht.[25]

[19] Systematisch sind die strafverfahrens- und wirtschaftsverwaltungsrechtlichen Optionen für den grenzüberschreitenden Zugriff auf in der sog. Cloud gespeicherte Daten wie folgt aufzufächern: 1. In Betracht kommen traditionelle Rechtshilfeformen (namentlich die sog. sonstige Rechtshilfe in Form der Beweisrechtshilfe) samt ihrer Modernisierung (z.B. durch beschleunigte Erledigungsverfahren, etwa im Wege der Anwendung des Grundsatzes der gegenseitigen Anerkennung, Art. 82 Abs. 1 AEUV). 2. In Betracht kommen ferner moderne Rechtshilfeformen, wie die Etablierung von gemeinsamen Ermittlungsgruppen oder die Eröffnung von Spiegelverfahren (hierzu allg. *Vogel/Burchard*, in: Grützner/Pötz/Kreß [Hrsg.], Internationaler Rechtshilfeverkehr in Strafsachen, Stand: Dezember 2017, Vor § 1 IRG Rn. 50 ff.). 3. Dazu gesellen sich Institute wie fakultative Beibringungsersuchen („production requests“, eine rechtliche und rechtstatsächliche Einordnung findet sich unten II. 2. und IV. 1.) bzw. verpflichtende Beibringungsanordnungen gegenüber privaten Diensteanbietern betreffend Auslandsdaten („production orders“). 4. Auch Direktzugriffe (sei es mit oder ohne Zustimmung des Nutzers bzw. mit oder ohne Zustimmung des Staates, in dem die Cloud-Daten im Zugriffszeitpunkt belegen sind) stehen zur Debatte; hierzu trifft Art. 32 Cybercrime Convention die Regelung, dass der grenzüberschreitende Zugriff auf Cloud-Daten ohne Autorisierung des Vertragsstaats, an dem die Daten belegen sind, nur statthaft ist, wenn der über die Daten Verfügungsberechtigte zustimmt, was gerade bei verdeckt geführten Ermittlungen häufig unrealistisch ist. 5. Schließlich sind auch im weiteren Sinne wirtschaftsverwaltungsrechtliche Lösungen denkbar. Beispielhaft hierfür ist der o.g. Lokalisierungszwang von Cloud-Daten im Inland oder eine echte Aufklärung der Nutzer darüber, wo und wie ihre Cloud-Daten gespeichert werden, so dass sich mit der Nutzung der Cloud eine Nutzer-Einwilligung in die Herausgabe bestimmter Cloud-Daten zu Strafverfolgungszwecken konstruieren ließe (vgl. allg. Art. 7 DS-GVO).

[20] Zu diesen Abwägungstopoi der vor dem US Supreme Court im Microsoft Ireland Case eingereichte „brief of former law enforcement, national security, and intelligence officials as amici curiae in support of neither party“, S. 2 f., online verfügbar unter http://www.supremecourt.gov/DocketPDF/17/17-2/23633/20171213113332456_17-2%20Amicus%20Brief%20in%20Support%20of%20Neither%20Party.pdf (25.5.2018).

[21] Hierzu insbesondere unten III. 2. a) cc).

[22] Gleiches gilt, wenn dies auch jenseits des Atlantiks aufgrund der dortigen politischen Großwetterlage wenig en vogue sein dürfte, entsprechend in den USA – oder in sonstigen auf internationale Zusammenarbeit setzenden Jurisdiktionen.

[23] Hierzu insbesondere unten III. 1. b).

[24] Eine andere Frage ist, ob dieses Versprechen bereits jetzt erfüllt wird oder – wie ich meine – ein umsetzungsbedürftiges Versprechen in die Zukunft ist.

[25] Der räumliche Anwendungsbereich der DS-GVO ist in Art. 3 DS-GVO geregelt. Hierzu insbesondere unten III. 1. b) aa).

Diesen Geboten werden – wie in diesem Beitrag darzulegen sein wird – die herkömmlichen Fundamentalprinzipien der Rechtshilfe in strafrechtlichen Angelegenheiten am ehesten gerecht. Sie sollten daher nicht – dem aktuellen kriminalpolitischen Zeitgeist zuwider – vorschnell über Bord geworfen werden. Der grenzüberschreitende Zugriff auf die Cloud sollte namentlich unter Achtung der souveränen Territorialhoheit der Staaten, der internationalen Solidarität bei der Verfolgung grenzüberschreitender Kriminalität sowie der Wahrung der Grundrechte der Betroffenen geregelt werden.[26] Im Einzelnen folgt daraus zweierlei:

- Erstens sollte das Territorialitäts- nicht durch andere zuständigkeitsbegründende Prinzipien ersetzt werden. Wer Zugriffsmöglichkeiten auf Daten nicht davon abhängig machen will, wo sie gespeichert sind (Territorialitätsprinzip), sondern davon, ob ein privater Diensteanbieter im Inland aktiv ist (Marktortprinzip), ob er im Inland seinen (Haupt-)Sitz hat (Herkunftslandprinzip) oder ob die Daten von Inländern betroffen sind (aktives Personalitätsprinzip), der schleift den Grundrechts- und Datenschutz bei der internationalen Sicherheitszusammenarbeit und untergräbt das Vertrauen zwischen den beteiligten Akteuren.
- Zweitens sollte das Zwischenstaatliche dieser Sicherheitszusammenarbeit nicht vorschnell durch deren partielle Privatisierung ersetzt werden, indem das Rechtshilfeverfahren im (so die herkömmliche Terminologie) ersuchten Staat auf private Diensteanbieter ausgelagert wird.

Um zu diesem Ergebnis zu gelangen, werde ich zunächst einige Hintergründe des nunmehr vorgelegten Kommissionsentwurfs zum grenzüberschreitenden Zugriff auf elektronische Beweismittel (unten I.) wie auch Hintergründe zum ehemaligen US-Recht (vor der Einführung des CLOUD-Acts), hier insbesondere zum Microsoft Ireland Case, darstellen (unten II.). Dabei wird sich zeigen, dass die territoriale Belegenheit von Cloud-Daten heute zunehmend als Problem und unilaterale Ermittlungsmaßnahmen als Lösung wahrgenommen werden, was ich in dieser Generalität bestreiten möchte (unter III.). Ebenfalls lässt sich den Hintergrunddarstellungen entnehmen, dass das Zwischenstaatliche des Rechtshilfeverfahrens zusehends als Problem und die Privatisierung desselben als Lösung verstanden wird, was ich freilich ebenfalls kritisch sehe (unten IV.). In einem Postskript soll abschließend (ziemlich) kritisch und im Lichte der vorgenannten Ausführungen zum Kommissionsentwurf zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln im Strafermittlungsverfahren Stellung bezogen werden.

[26] Zu diesen Fundamentalprinzipien eingehend *Vogel/Burchard* (Fn. 19), Vor § 1 IRG Rn. 97 ff., 114 ff., 122 ff.

I. Hintergründe des anstehenden Kommissionsentwurfs zum grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen

1. Die Europäische Sicherheitsagenda vom 28.4.2015

Seit mehreren Jahren steht das Thema „e-evidence“ weit oben auf der Agenda der europäischen Kriminalpolitik.[27] So wurde in der Europäischen Sicherheitsagenda aus dem Jahre 2015 unter dem Banner der „Bekämpfung der Cyberkriminalität“ ausgeführt:

„Cyberkriminalität macht naturgemäß nicht an Landesgrenzen halt und ist flexibel und innovativ. Bei ihrer Prävention, Aufdeckung und Verfolgung müssen die Strafverfolgungsbehörden dem Einfallsreichtum der Täter gewachsen und ihnen nach Möglichkeit einen Schritt voraus sein. Dafür ist es zudem erforderlich, dass die zuständigen Justizbehörden – auch unter Berücksichtigung aktueller und zukünftiger technologischer Entwicklungen („Cloud computing“, „Internet der Dinge“ usw.) – die Methoden der Zusammenarbeit in ihrem Zuständigkeitsbereich so umstrukturieren und die geltenden Rechtsvorschriften dahingehend ändern, dass ein

[27] Siehe hierzu und zum Folgenden auch den Internetauftritt der Kommission unter https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en (25.5.2018). Vgl. auch die Darstellungen bei *Warken*, NZWiSt 2017, 449 (453 f.) und *Zerbes*, EuCLR 2015, 304. Interessant zu beobachten ist, dass viele der heutigen Entwicklungen bereits angelegt waren in der ausführlichen Mitteilung der Kommission, Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, COM (2000) 890 final v. 26.1.2001 (sic), S. 24. Dort findet sich „zeitlos“ ausgeführt: „Noch komplizierter kann es werden, wenn eine Strafverfolgun[g]sbehörde bei der Durchsuchung eines Computers oder auch nur bei einer einfachen Ermittlung feststellt, daß ein Zugriff auf Daten in einem oder mehreren anderen Ländern erfolgt oder erforderlich ist. Diese Frage berührt wichtige hoheits-, menschen- und strafrechtliche Aspekte und erfordert ein ausgewogenes Vorgehen. In derartigen Fällen können sich die geltenden rechtlichen Instrumente der internationalen Zusammenarbeit in Strafsachen (Rechtshilfe) als ungeeignet oder unzureichend erweisen, da ihre Umsetzung in der Regel einen Zeitraum von mehreren Tagen, Wochen oder Monaten erfordert. Mithin bedarf es eines Mechanismus, der es einem Land ermöglicht, auf rasche und effiziente Weise und unter Wahrung der Grundsätze der nationalen Souveränität sowie der Verfassungs- und Menschenrechte (einschließlich der Bestimmungen zum Schutz der Privatsphäre und zum Datenschutz) strafrechtliche Ermittlungen anzustellen und Beweismaterial einzuholen oder zumindest sicherzustellen, daß bei der grenzübergreifenden Strafverfolgung keine wichtigen Beweisstücke verloren gehen.“

rascherer grenzübergreifender Zugriff auf Beweise und Informationen möglich wird."[28]

Als „[v]on entscheidender Bedeutung" wurde dabei „die Zusammenarbeit mit dem privaten Sektor" ausgeflaggt, mache doch laut der Kommission die Cyberkriminalität nicht weniger als „ein neues Konzept für die Strafverfolgung im digitalen Zeitalter erforderlich."[29]

Was die Europäische Sicherheitsagenda damit aber noch nicht hinreichend klar herausstellte: Elektronische Beweismittel spielen auch bei der Verfolgung von gemeiner wie auch exzeptioneller (Stichwort: Terrorismus) „offline"-Kriminalität eine immer größere Rolle. Sie leisten auch dort der Effektuierung der Strafrechtspflege Vorschub, bedrohen aber im gleichen Ausmaße die Privatsphäre der Bürger. Zudem kann die Gewinnung elektronischer Beweismittel auch im Hinblick auf die Verfolgung von „offline"-Kriminalität zeitkritisch sein und eine Zusammenarbeit mit Privaten erforderlich machen.[30]

2. Die Schlussfolgerungen des Rats über die Verbesserung der Strafrechtspflege im Cyberspace vom 9.6.2016

Diese Erwägungen tragen die Schlussfolgerungen des Rats über die Verbesserung der Strafrechtspflege im Cyberspace vom 9.6.2016,[31] in denen allgemein die „zunehmende Bedeutung von elektronischen Beweismitteln für die Verfolgung *aller Kriminalitätsformen*" herausgestrichen wurde.[32] Obwohl die eigentlichen Schlussfolgerungen ansonsten in der Möglichkeitsform gehalten wurden (namentlich als Aufforderung an die Kommission, bestimmte Optionen und Möglichkeiten der Gewinnung elektronischer Beweismittel zu sondieren), lassen sie doch rechtspolitische Präferenzen des Rats erkennen.

Konkret schrieb der Rat der Kommission die Sondierung folgender Optionen ins Stammbuch, um die grenzüberschreitende Gewinnbarkeit von elektronischen Beweismitteln in Strafverfahren zu verbessern:

- Erstens die Erleichterung der Zusammenarbeit mit privaten Diensteanbietern;
- zweitens die Modernisierung der Rechtshilfe, insbesondere im Wege der Anwendung des Grundsatzes der gegenseitigen Anerkennung auf die Sicherstellung und Gewinnung elektronischer Beweismittel und
- drittens die Einführung anderer Ermittlungsmaßnahmen („other measures"), um den Mitgliedstaaten Möglichkeiten zur Durchsetzung ihrer Zuständigkeit im Cyberspace an die Hand zu geben.[33]

Diese kryptische Wendung wurde vom Rat dahingehend „präzisiert", dass (unionsrechtlich vereinheitlichte) andere Ermittlungsmaßnahmen in Situationen vonnöten werden könnten, in denen sich der bisherige (Rechts-)Rahmen als unzureichend herausstelle. Beispielhaft in Situationen „[1] where a number of information systems are used simultaneously in multiple jurisdictions to commit one single crime, [2] where relevant e-evidence moves between jurisdictions in short fractions of time, or [3] where sophisticated methods are used to conceal the location of e-evidence or the criminal activity, leading to ‚loss of location'."[34] Daher mahnte der

[28] Mitteilung der Kommission, Europäische Sicherheitsagenda, COM (2015) 185 final v. 28.4.2015, S. 24. Hierzu etwa *M. Gercke*, ZUM 2015, 772 (778 ff.); *ders.*, StV 2016, 391.

[29] COM (2015) 185 final v. 28.4.2015, S. 25.

[30] Zu diesem Zeitfaktor grundsätzlich etwa *Sieber* (Fn. 9), S. 39, und *Warken*, NZWiSt 2017, 289 (289). – Ein illustratives Anschauungsbeispiel für all das lieferte der Freiburger Mordprozess gegen Hussein K. Wie medial eingehend berichtet: „Gerade" noch rechtzeitig konnte während der Hauptverhandlung das verschlüsselte und nur unter Rückgriff auf einen privaten Entschlüsselungsanbieter entschlüsselbare Smartphone des Angeklagten ausgewertet werden. Die dort gefundenen Geodaten (wie über WiFi-Logins und Daten aus einer Health-App) zeigten wohl, dass die dem Angeklagten zur Last gelegte Tötung einer Freiburger Studentin geplant war, d.h. seiner Einlassung zuwider nicht spontan erfolgte. Vgl. hierzu http://www.sueddeutsche.de/digital/prozess-wegen-vergewaltigung-und-mord-wie-polizisten-das-handy-des-freiburger-mordverdaechtigen-auslasen-1.3860870 (25.5.2018).

[31] Hierzu auch *M. Gercke*, ZUM 2016, 825 (830).

[32] Presseerklärung „Council conclusions on improving criminal justice in cyberspace" v. 9.6.2016, S. 1, „stressing the increasing importance of e-evidence in criminal proceedings in all types of crime, and in particular for terrorism" (*Hervorhebung* durch *Verf.*), online abrufbar unter https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf (25.5.2018).

[33] Presseerklärung „Council conclusions on improving criminal justice in cyberspace" v. 9.6.2016, S. 3. – Interessant ist, dass der Rat die Topoi Rechtshilfe und gegenseitige Anerkennung noch in unterschiedlichen Bulletpoints führte (a.a.O., S. 3), die Kommissionsdienste jedoch – richtigerweise, da die gegenseitige Anerkennung keinen Paradigmenwechsel, sondern eine Weiterentwicklung der Rechtshilfe darstellt; hierzu grundsätzlich *Burchard*, Die Konstitutionalisierung der gegenseitigen Anerkennung, 2018 (im Erscheinen), § 8 C. II. 1. c); anders etwa *Klip*, European Criminal Law, 3. Aufl. 2016, S. 343 f. und 356 f. – diese Topoi als einen gemeinsamen Block verstanden. Namentlich im Non-paper from the Commissions Services: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace v. 7.12.2016, Dok. 15072/1/16 REV 1, S. 2, online abrufbar unter http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf (25.5.2018).

[34] Presseerklärung „Council conclusions on improving criminal justice in cyberspace" v. 9.6.2016, S. 5 samt der instruktiven Fn. 9. – Unter dem Phänomen „loss of location" bzw. genauer: „loss of knowledge of location" versteht man schlicht, dass Strafverfolger nicht wissen, wo (in welchem Staat, ja sogar auf welchem Kontinent) bestimmte Daten belegen sind. Vgl. den Bericht des Europäischen Parlaments

Rat an, zunächst Faktoren zu bestimmen, die die Durchsetzungszuständigkeit („enforcement jurisdiction“) der EU-Mitgliedstaaten im Cyberspace begründen; und sodann der Frage nachzugehen, ob (und wenn ja) welche Zwangsmaßnahmen eines zuständigen Mitgliedstaats sich unabhängig von staatlichen Territorialgrenzen zum Einsatz bringen ließen.[35]

Auf dieser noch recht abstrakten Grundlage forderte der Rat die Kommission abschließend sehr konkret dazu auf, die folgenden beiden Ermittlungsmaßnahmen für den grenzüberschreitenden Zugriff auf elektronische Beweismittel auszuarbeiten:

- Erstens „a cooperation solution for direct trans-border access to data without technical assistance“ und
- zweitens „the use and effectiveness of domestic production orders based on […] possible connecting factors for enforcement jurisdiction in cyberspace.“[36] Als mögliche zuständigkeitsbegründende Faktoren nannte der Rat dabei einen „headquarter link“ (Stichwort: Herkunftslandprinzip) oder einen „business link“ (Stichwort: Marktortprinzip) der Diensteanbieter ins Inland.[37] Dies liefe darauf hinaus, dass ein Strafverfolgungsstaat gegen im Inland ihren Sitz habende oder im Inland Dienste anbietende Diensteanbieter verpflichtende Beibringungsanordnungen betreffend Auslandsdaten erlassen dürfte.

3. Die Non-Paper der Kommissionsdienste vom 7.12.2016 und 8.6.2017 sowie deren undatiertes Technical Document

In Umsetzung des Arbeitsauftrags des Rats veröffentlichte die Kommission Ende 2016 sowie Mitte 2017 drei Dokumente.[38] Diese zeichneten sich durch ein formales Kuriosum aus. Sie erschienen nicht als Kommissionsdokumente, sondern lediglich als Dokumente der Kommissionsdienste. Wie in den letzten beiden Papieren einleitend ausdrücklich herausgehoben wurde: „This document is a document prepared by the Commission services and cannot be considered as stating an official position of the Commission.“[39] Es bedarf keiner großen Phantasie, um zu verstehen, was das bedeutet: Die (vier, so informelle Angaben) beteiligten Kabinette konnten sich nicht auf eine einheitliche Positionierung der Kommission einigen. Das überrascht aufgrund der in der Einführung aufgerissenen Komplexität der Regelungsaufgabe – und der konfligierenden Interessen der Innen- bzw. Sicherheits-, der Justiz- sowie der Verbraucher- bzw. Datenschutz-Seite – nicht wirklich. Und es erklärt auch, warum die eigentlich für Mitte Januar 2018 angekündigte Vorlage eines Kommissionsentwurfs für einen Rechtsakt über den grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen verschoben werde musste und erst Mitte April 2018 erfolgte.

Das darf aber nicht darüber hinwegtäuschen, dass in den vorgenannten Dokumenten wichtige Weichenstellungen enthalten sind. Das Non-Paper vom 7.12.2016 trifft entscheidende – wenn auch vielfach auf tönernen Füßen stehende – rechtstatsächliche Festlegungen,[40] mit denen sich die unionsrechtlichen Subsidiaritätshürden überwinden ließen (hierzu unten a). Und das Non-Paper vom 8.6.2017 sowie das Technical Document lassen in ihren Ausführungen über mögliche

über Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, PE 583.137, 2017, S. 28, online verfügbar unter http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)583137 (11.6.2018).

[35] Presseerklärung „Council conclusions on improving criminal justice in cyberspace“ v. 9.6.2016, S. 5 („whether, and if so which investigative measures can be used regardless of physical borders“).

[36] Presseerklärung „Council conclusions on improving criminal justice in cyberspace“ v. 9.6.2016, S. 5.

[37] Presseerklärung „Council conclusions on improving criminal justice in cyberspace“ v. 9.6.2016, S. 5: „[P]ossible grounds for enforcement jurisdiction [may be] the headquarters of a service provider, the economic activity of a service provider in the investigating state i.e. when the service provider offers products or services on the territory of the investigating state […].“

[38] Non-paper from the Commissions Services: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace v. 7.12.2016, Dok. 15072/1/16 REV 1, online verfügbar unter http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf (25.5.2018); Non-paper from the Commission services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward v. 8.6.2017, online verfügbar unter https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (25.5.2018); Technical Document from the Commission Services: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, online verfügbar unter https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf (25.5.2018). Die Dokumente besprechend *Warken*, NZWiSt 2017, 449 (449). Nicht weiter eingegangen wird im Folgenden auf das inhaltlich nichts wesentlich Neues bringende Inception Impact Assessment: Improving cross-border access to electronic evidence in criminal matters v. 3.8.2017, Ref. Ares(2017)3896097. Abrufbar unter https://ec.europa.eu/info/law/betterregulation/initiative/44462/attachment/090166e5b4358fd4_en (25.5.2018).

[39] Non-paper v. 8.6.2017 (Fn. 38), S. 1; Technical Document (Fn. 38), S. 1. Diese Dokumente ziert nicht einmal ein Kommissionsbriefkopf, geschweige denn eine Dokumentennummer.

[40] Bewusst wurde nicht von Feststellungen gesprochen, da mitunter Festlegungen ohne empirische oder rechtstatsächliche Validierung erfolgten.

legislative Maßnahmen bestimmte rechtspolitische Tendenzen deutlich erkennen (hierzu unten b).[41] In der Übersicht:

a) Rechtstatsächliche Festlegungen im Non-Paper vom 7.12.2016

aa) Zusammenarbeit mit privaten Diensteanbietern

Was zunächst die Zusammenarbeit mit privaten Diensteanbietern anbetrifft, könnte die Rechtslage in den Mitgliedstaaten nach Darstellung des Non-Paper vom 7.12.2016 kaum unterschiedlicher sein.[42] Während es beispielsweise 14 EU-Mitgliedstaaten ausländischen Diensteanbietern anheimstellen, ob sie Ersuchen auf Beibringung elektronischer Beweismittel nachkommen, sehen dies sieben Mitgliedstaaten als verpflichtend an. Auch was überhaupt unter einem *ausländischen* Diensteanbieter verstanden wird, divergiert fundamental. Teils solle der Hauptsitz des Diensteanbieters entscheiden, teils der Ort, wo die Dienste angeboten werden, und teils der Serverstandort, an dem die nachgesuchten Daten gespeichert sind.

Unter dem Disclaimer, dass man die Diensteanbieter nicht über einen Kamm scheren dürfe, weil diese ganz unterschiedliche Zusammenarbeitspolitiken und -prozesse hätten (was nach anekdotischen Berichten richtig ist), wurde überdies im Non-Paper vom 7.12.2016 Kritik an der freiwilligen Kooperation privater Diensteanbieter zusammengetragen.[43] Diese Form der Zusammenarbeit sei – worauf noch unter IV. 1. a) zurückzukommen sein wird – u.a. zu intransparent und zu unzuverlässig. Strafverfolgern sei häufig weder die Bewilligung noch die Ablehnung ihrer Beibringungsersuchen durch private Diensteanbeiter erklärlich. Zudem informierten diese mitunter ihre Nutzer über eingehende Zusammenarbeitsersuchen, was verdeckte Ermittlungen gefährde.

Für die umgekehrten Fragestellungen, ob und wie nämlich inländische Diensteanbieter direkt mit ausländischen Strafverfolgern (aus anderen EU-Mitgliedstaaten oder aus Drittstaaten[44]) in Kontakt treten und diesen Daten aushändigen dürfen, sehen die Mitgliedstaaten laut dem Non-Paper mehrheitlich keine Regelungen vor.

bb) Rechtshilfe und gegenseitige Anerkennung

Im Hinblick auf die Gewinnung elektronischer Daten im Wege der Rechtshilfe mit außer-europäischen Staaten (hier insbesondere mit den USA) bestand Einigkeit unter den konsultierten Experten, dass dieser Weg rechtspraktisch zu langwierig und umständlich sei.[45] Und in der Tat stehen – so lässt sich summarisch kommentieren – Bearbeitungszeiten von einem bis 18 Monaten[46] einer wirksamen Strafverfolgung von offline wie auch online begangenen Straftaten entgegen. In dieser Zeitspanne sind die hinterlassenen digitalen Spuren regelmäßig verwischt. Und um andauernde Cyberangriffe zurückverfolgen zu können, sind Echtzeitzugriffe vonnöten.

Was die beweisrechtshilferechtliche Zusammenarbeit mit EU-Mitgliedstaaten anbetrifft, die erst seit kurzer Zeit auf die Grundlage Europäischer Ermittlungsanordnungen gestellt wurde, findet sich in den Kommissionsdokumenten wenig rechtstatsächliches Zahlenwerk. Umso bemerkenswerter ist, dass und wie die Kommissionsdienste die Tür zu neuen grenzüberschreitenden Ermittlungsbefugnissen jenseits der Europäischen Ermittlungsanordnung – die wohlgemerkt mit dem Ziel der Beschleunigung der Beweisrechtshilfe angetreten ist – aufstoßen:

„Although the use of the European Investigation Order (EIO) will considerably improve the formal cooperation between the relevant authorities of Member States for obtaining cross-border access to electronic evidence, it has not been developed specifically with the objective to improve cross-border access to electronic evidence. Compared to direct cooperation with service providers, requests on the basis of mutual recognition are expected to be *slower, more cumbersome and resource-intensive*."[47]

cc) Andere Ermittlungsmaßnahmen

Mit Blick auf alternative bzw. andere Ermittlungsmaßnahmen förderten die Expertenkonsultationen im Wesentlichen zwei rechtstatsächliche Probleme zu Tage, die in den EU-Mitgliedstaaten höchst unterschiedlich bzw. erst gar nicht gelöst werden:[48]

- Erstens das Problem, dass sich kein Diensteanbieter identifizieren lässt, der die beweiserheblichen Daten speichert oder bearbeitet.[49] Unter diesen komplexen Be-

[41] Nicht weiter eingegangen werden soll im Folgenden auf die im Non-Paper v. 8.6.2017 (Fn. 38), S. 2 ff. und dem Technical Document (Fn. 38), S. 10 ff., 14 ff. angesprochenen praktischen Vorschläge, um die zwischenstaatliche Zusammenarbeit innerhalb der EU bzw. mit dem Ausland, hier insbesondere den USA, sowie die Zusammenarbeit mit privaten Diensteanbietern zu verbessern. Im Folgenden werden mit anderen Worten die Erwägungen über „legislative measures to improve cross-border access to electronic evidence" – so das Non-Paper v. 8.6.2017 (Fn. 38), S. 4 f. – fokussiert.

[42] Hierzu und zum Folgenden Non-Paper v. 7.12.2016 (Fn. 38), S. 4 f. und 12 f.

[43] Hierzu und zum Folgenden Non-Paper v. 7.12.2016 (Fn. 38), S. 6 ff.

[44] Vgl. hierzu nun aber insbesondere die ab dem 25.5.2018 in Kraft getretenen Regelungen der DS-GVO (insbes. Art. 49 DS-GVO).

[45] Für die umgekehrte Situation, dass also ausländische Strafverfolger EU-Mitgliedstaaten um Beweisrechtshilfe ersuchen, wurde leider kein rechtstatsächliches Zahlenwerk geliefert.

[46] So die Zahlen im Non-Paper v. 7.12.2016 (Fn. 38), S. 5.

[47] Non-Paper v. 7.12.2016 (Fn. 38), S. 12 (*Hervorhebung* durch *Verf.*).

[48] Hierzu und zum Folgenden Non-Paper v. 7.12.2016 (Fn. 38), S. 4 ff.

[49] Darauf antworten manche EU-Mitgliedstaaten mit polizeilichen oder zwischen-behördlichen Zusammenarbeitsformen (gemeint sind wohl informelle Kooperationen jenseits der herkömmlichen Beweisrechtshilfe), mit Einwilligungslösungen (indem die Einwilligung in den Datenzugriff durch den Nutzer eingeholt wird, vgl. auch Art. 32 Cybercrime-

dingungen, so die Rückmeldung der meisten EU-Mitgliedstaaten, sei der Zugriff auf elektronische Beweismittel regelmäßig unmöglich.

- Zweitens das „loss (of knowledge) of location"-Problem, dass also der territoriale Speicherort elektronischer Beweismittel unklar oder nicht bestimmbar ist. Dem begegnen die EU-Mitgliedstaaten ganz unterschiedlich: teils vermittels direkter Fernzugriffe; teils mit Durchsuchungs- und Beschlagnahmeanordnungen („search and seizure techniques"; gemeint sein dürften Beibringungsanordnungen, weil und wenn der Diensteanbieter identifiziert ist, aber unklar ist, wo die Daten belegen sind); teils mit multiplen Beweisrechtshilfeersuchen (wohl ähnlich einer unbestimmten Fahndungsausschreibung, wenn unklar ist, in welchem Staat sich ein Flüchtiger aufhält); und teils mit internationalen Zusammenarbeitsinstrumenten (was recht vage bleibt). Immerhin acht Mitgliedstaaten signalisierten, dass bei einem „loss (of knowledge) of location" der Zugriff auf elektronische Beweismittel entweder unmöglich oder gesetzlich nicht geregelt sei.

b) Rechtspolitische Tendenzen im Non-Paper vom 8.6.2017 sowie dem Technical Document

Die zuvor geschilderten rechtstatsächlichen Festlegungen gaben den Kommissionsdiensten Anlass, im Non-Paper vom 8.6.2017 sowie dem attachierten Technical Document eine Reihe legislativer Maßnahmen zur Verbesserung des grenzüberschreitenden Zugriffs auf elektronische Beweismittel zur Diskussion zu stellen. Zugleich wurde an den Grundfesten der internationalen Zusammenarbeit in Strafsachen gerührt. Im Einzelnen:

aa) Zusammenarbeit mit privaten Diensteanbietern

Um Rechtsklarheit zu gewinnen und Jurisdiktionskonflikte zwischen den EU-Mitgliedstaaten abzubauen, wurde zunächst die unionsrechtliche Vereinheitlichung der fakultativen wie auch der obligatorischen Zusammenarbeit mit privaten Diensteanbietern im Ausland angedacht.[50] Namentlich durch die unionsrechtliche Regelung von freiwilligen Beibringungsersuchen („production requests", deren Bewilligung ins Belieben der Diensteanbieter fallen soll) und zwingenden Beibringungsanordnungen („production orders", deren Befolgung für die Diensteanbieter verpflichtend sein soll). Beibringungsersuchen bzw. -anordnungen wurden dabei in beide Richtungen, d.h. in ausgehender wie auch eingehender Richtung, diskutiert. Wörtlich:

„The measure would provide a harmonised legal basis at EU level to allow law enforcement authorities to make a production request to service providers located in another Member State or in a third country, and for service providers located in the EU to reply to such requests."[51]

Ergänzt werden soll dies durch komplementäre Regelungen, um die Durchführung dieser Maßnahmen sicherzustellen und etwaige Eingriffe zu kompensieren. Diskutiert wurden insbesondere ein Sanktions-, namentlich ein Geldbußen-Regime (für den Fall, dass Diensteanbieter einer Beibringungsanordnung nicht nachkommen) wie auch die Verpflichtung, dass außer-europäische Diensteanbieter einen Vertreter in einem EU-Mitgliedstaat benennen müssen (an den Beibringungsersuchen bzw. -anordnungen zu richten und gegen den die besagten Sanktionen zu vollstrecken seien).[52] Als „mitigating measure"[53] wurde ein Notifikationssystem in die Diskussion eingeführt, welches das Technical Document wie folgt umriss (wobei wir sogleich unter cc) noch sehen werden, warum der Ort, an dem elektronische Beweismittel belegen sind, nicht länger als notifikationsrelevanter Faktor geführt wurde):

„One of the ideas emerging from the expert consultation process is to provide for an obligation to notify the [Member] State that could be affected by the investigative measure. Factors to identify affected countries could e.g. be the seat of the service provider or the habitual residence of the target of the measure. The measure also would have to establish the legal consequences of the notification: it could range from a mere information to the need for the Member State notified to agree to the measure, and provide for deadlines and grounds for the Member States notified to object or refuse its agreement."[54]

Bemerkenswert ist schließlich, dass all dies in einem bloßen Nebensatz unter das kompetenzrechtliche Dach des „Art. 82 AEUV"[55] gezogen wurde – wohlgemerkt ohne die Nennung von Absätzen oder Unterabsätzen, geschweige denn Begründungen.

bb) Direktzugriffe

Als weitere Legislativmaßnahme nannten die Kommissionsdienste die Regelung von Direktzugriffen, namentlich für „loss of (knowledge of) location"-Szenarien wie auch bei Gefahr im Verzug, weil Daten verloren zu gehen drohen.[56] Entweder – so das Non-Paper vom 8.6.2017 – könnten Eingriffsvoraussetzungen und Mindeststandards für solche Direktzugriffe unionsrechtlich vereinheitlicht werden, komplementiert durch die Notifikationsverpflichtung anderer betroffener Staaten. Oder aber man könnte sich mit letzterem bescheiden, d.h. lediglich Notifikationsverpflichtungen vorsehen und die mitgliedstaatlichen Regime für Direktzugriffe unangetastet lassen.

Konvention) oder mit Durchsuchungs- und Beschlagnahmeanordnungen („search and seizure techniques") – was alles recht vage klingt und bleibt.

[50] Siehe hierzu und zum Folgenden Non-Paper v. 8.6.2017 (Fn. 38), S. 4.

[51] Technical Document (Fn. 38), S. 20.

[52] Letzteres ist aus dem Netzwerkdurchsetzungsgesetz bekannt. Hierzu *Liesching*, in: Spindler/Schmitz (Hrsg.), Telemediengesetz, 2. Aufl. 2018, § 5 NetzDG Rn. 11 ff.

[53] Non-Paper v. 8.6.2017 (Fn. 38), S. 5.

[54] Technical Document (Fn. 38), S. 24.

[55] Technical Document (Fn. 38), S. 18.

[56] Technical Document (Fn. 38), S. 25 ff.

cc) Entterritorialisierung der Cloud

Nachdem sehr kurz weitere völkerrechtliche Vereinbarungen, die die zuvor dargestellten grenzüberschreitenden Ermittlungsmaßnahmen komplettieren sollen, angesprochen wurden, legten die Kommissionsdienste zu guter (?) Letzt noch Hand an die Grundlagen der internationalen Beziehungen, namentlich an das Konzept der Territorial- oder Gebietshoheit.[57] Um in extenso aus dem Non-Paper vom 8.6.2017 zu zitieren:

„Owing to the fact that the concept of territoriality is still based largely on the place where data is stored, any cross-border access to electronic evidence that is not based on cooperation between authorities may raise issues in terms of territoriality. This applies both within the EU and where data is stored in a third (non-EU) country. Already in the EU, Member States do not always agree on when a relevant ‚cross-border element' affects the territory of another Member State. Common EU criteria could address this issue. These criteria can provide conditions to be fulfilled for certain investigative measures, and may trigger further obligations such as the notification of the other state concerned. *The experts have expressed the view that there is a need to move away from data storage location as the (only) relevant criterion.* Instead, a number of factors should be considered, including the place of main establishment of the data controller and/or the place of residence of the person targeted by the measure."[58]

Noch schärfer formuliert das Technical Document: „The expert process has shown the need to move away from data storage location as the key criterion."[59]

II. Hintergründe zur Rechtslage in den USA

Eben diese Position – dass der Datenstandort nicht länger rechtlich signifikant sein soll, so dass Zugriffe auf Auslandsdaten der Sache nach nicht extraterritorial wirken und daher gestattet sein müssen – spielt auch jenseits des Atlantiks im Microsoft Ireland Case eine zentrale Rolle. Mit diesem Argument soll dort ermöglicht werden, dass US-Strafverfolger durch Beibringungsanordnungen gegenüber US-Diensteanbietern auf von diesen im Ausland gespeicherte Daten Zugriff bekommen (hierzu unten 1.). Damit aber nicht genug. Das US-Recht legt auch Standards fest, wie bei eingehenden Ersuchen auf Datenherausgabe zu verfahren ist, insbesondere indem US-Diensteanbietern freigestellt wird, ausländischen Beibringungsersuchen betreffend Nicht-Inhaltsdaten zu entsprechen (hierzu unten 2.). Kurz gesagt findet sich im US-Recht daher reiches rechtsvergleichendes Anschauungsmaterial für die Ansinnen der Kommissionsdienste, Beibringungsersuchen und -anordnungen unionsrechtlich zu verankern.

1. Aus den USA ausgehende Beibringungsanordnungen: Der Microsoft Ireland Case (und Parallelfälle gegen Yahoo! und Google)

a) Prozessgegenstand und -geschichte

In der weithin als Microsoft Ireland Case abgekürzten Rechtssache United States v. Microsoft Corp[60] erging im April 2018 eine endgültige Entscheidung durch den US Supreme Court. Bis zum Erlass des CLOUD-Act wurde in dieser Rechtssache die Zulässigkeit von unilateral erlassenen und mit Sanktionsdrohungen erzwingbaren Beibringungsanordnungen verhandelt (wenn diese auch in den USA unter anderen Namen firmieren).[61] In Streit stand die Rechtmäßigkeit eines im Jahre 2013 gegen Microsoft in den USA erlassenen „warrant" nach 18 U.S. Code § 2703(a) des „Stored Communications Act" (SCA) a.F. Mit diesem konnten Diensteanbieter verpflichtet werden, Strafverfolgern bestimmte Inhaltsdaten ohne Benachrichtigung des Nutzers offenzulegen. Microsoft wehrte[62] sich freilich gegen diesen „warrant", weil die nachgesuchten Inhaltsdaten (konkret ging es um „sämtliche E-Mails" eines Nutzers, gegen den wegen Drogendelikten ermittelt wurde) auf irischen Servern lägen und zunächst in die USA transferiert werden müssten. Letzteres sei zwar technisch ohne Weiteres möglich, könne aber rechtlich nur durch eine „subpoena" (also durch eine verpflichtende und sanktionsbewährte Anordnung, bestimmte Informationen in bestimmter Weise beizubringen, Anm. d. *Verf.*) angeordnet werden. Die gegenständliche Ermächtigungsgrundlage in 18 U.S. Code § 2703(a) spreche jedoch lediglich von „warrants" (die traditionell keine extraterritoriale Wirkungen haben, Anm. d. *Verf.*), nicht aber von „subpoenas".[63]

Dogmatisch stand somit im Microsoft Ireland Case zur Debatte, ob das Wörtchen „warrant" in 18 U.S. Code § 2703(a) a.F. auch als „subpoena" gelesen werden durfte, gleichsam als „hybrid: part search warrant and part subpoe-

[57] Hierzu grundsätzlich *Ipsen*, Völkerrecht, 6. Aufl. 2014, § 5 Rn. 3 ff.; *Herdegen*, Völkerrecht, 16. Aufl. 2017, § 26 Rn. 4 ff.

[58] Non-Paper v. 8.6.2017 (Fn. 38), S. 6 (*Hervorhebung* durch *Verf.*).

[59] Technical Document (Fn. 38), S. 30.

[60] Die in Vorinstanzen auch als „In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation" firmierte.

[61] Die dogmatische Relevanz dieser Rechtsfrage hat sich durch den CLOUD-Act erledigt, da dort im Grundsatz der Zugriff von US-Strafverfolgern auf von US-Diensteanbietern kontrollierte Daten, unabhängig vom Speicherort, vorgesehen wird. Hierzu auch Ratsdok. 6339/18 v. 26.2.2018. Die folgenden Ausführungen dienen dazu, die rechtspolitische Brisanz dieser Rechtsfrage herauszuheben.

[62] Zum Folgenden das Vorbringen von Microsoft vor dem US Supreme Court aus dem Januar 2018, S. 20 ff., online abrufbar unter https://www.supremecourt.gov/DocketPDF/17/17-2/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf (25.5.2018).

[63] Gerade, wie ergänzt werden darf, weil in 18 U.S. Code § 2703(b)(1)(B)(i) a.F. eine „subpoena" für Inhaltsdaten vorgesehen, aber unter die Voraussetzung einer vorherigen Benachrichtigung des Nutzers gestellt war. Zu den dogmatischen Hintergründen ausführlich *Gillaspie*, University of Kansas Law Review 2017-2018, 459.

na."[64] Hintergründig ging es aber um nicht weniger als die „Natur" von Clouddaten; namentlich darum, wo sich diese Clouddaten befinden („überall und nirgendwo"; oder dort, wo sich die Server befinden, auf denen die elektronischen Beweismittel gespeichert sind); und in der Folge darum, ob der einem Diensteanbieter aufgegebene Transfer von Auslandsdaten ins Inland extraterritoriale Wirkung entfaltet und die Territorialhoheit des Staates, in dem sie belegen sind, verletzt.[65]

Der ihn ausstellende „Magistrate Judge" sowie der „District Court" verbanden mit dem SCA-„warrant"[66] keine extraterritoriale Wirkung. Immerhin werde die Verpflichtung, Daten beizubringen, nur im Inland ausgesprochen und auch durch Sanktionen erzwungen, nicht aber im Ausland durchgesetzt. In der Folge wurde 18 U.S. Code § 2703(a) weit gezogen, also als Beibringungsanordnung für Auslandsdaten angewandt. Gegenteilig, und damit zugunsten von Microsoft, urteilte[67] dann jedoch ein mit drei Richtern besetzter Spruchkörper des „Court of Appeals for the Second Circuit"[68]. Zwei dieser Richter urteilten, dass der „warrant" extraterritoriale Effekte zeitige und 18 U.S. Code § 2703(a) folglich nicht auf Auslandsdaten erstreckt werden dürfe. Eine Beibringungsanordnung betreffend Auslandsdaten sei mit der geltenden Fassung dieser Vorschrift nicht zu machen. Hierfür müsse der US-Bundesgesetzgeber nachsteuern (was nunmehr durch den CLOUD-Act erfolgte, Anm. d. *Verf.*). Diese materielle Position wurde freilich nur im Mehrheitsvotum des „Court of Appeals for the Second Circuit" geäußert. Sie beruhte auf der Sichtweise, dass der SCA die Privatsphäre der Nutzer territorial schütze und die beizubringenden E-Mails schlicht in einem Datencenter in Irland belegen waren, so dass eine diesbezügliche Beibringungsanordnung einer Datenbeschlagnahme im Ausland gleichkomme.[69] Das laufe allemal der „international comity" zuwider und könne fremde Territorialhoheit beeinträchtigen.[70]

b) Entterritorialisierung der Cloud

Wir erinnern uns: Eben diese (vermeintlich konservative) Sichtweise soll laut den Kommissionsdiensten veraltet und daher aufzugeben sein (siehe oben I. 3. b) cc). Bezeichnend ist nun, dass diese Position ebenso im Microsoft Ireland Case laut wurde,[71] hier unter dem Schlachtruf: „Electronic ‚documents' […] are different."[72] Wes Geistes Kind der (vermeintlich moderne) Ansatz der Kommissionsdienste ist, zeigt sich daher im Lichte der Argumente, die für eine weite Auslegung des 18 U.S. Code § 2703(a) im Microsoft Ireland Case ins Felde geführt wurden.

So brachte Richter Lynch in seinem zustimmenden Sondervotum („concurring opinion") zur Entscheidung des „Court of Appeals for the Second Circuit" vor, dass die Privatsphäre („privacy") der Nutzer sich nicht nach dem Datenspeicherort bestimme, wenn Daten in der Cloud abgelegt werden. Eine solche territoriale Bestimmung sei ihm „suspekt".[73] Pointiert eingeordnet: Der Datenschutz in der Cloud wird auf diesem Wege systematisch entterritorialisiert. Dazu passt, dass Richter Lynch allein die Grund- und Verfahrensrechte der US-Verfassung für maßgeblich erachtete. Wörtlich:[74] „To uphold the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment

[64] So der US Magistrate Judge Francis in seiner Entscheidung in erster Instanz, wiedergegeben im Antrag auf Zulassung des Microsoft Ireland Case vor dem US Supreme Court („Petition for a Writ of Certiorari") durch die US-Administration, S. 73a ff. (84a); online abrufbar unter https://www.justice.gov/sites/default/files/briefs/2017/09/29/17-2_microsoft_pet.pdf (25.5.2018).

[65] Ebenfalls entscheidend, hier aber nicht weiterzuverfolgen, war die – in den USA stets wichtige, mit dem CLOUD-Act entschiedene – Gewaltenteilungsfrage, ob eine solch weitgehende Entscheidung für extraterritoriale Eingriffe durch Gerichte im Wege der Auslegung erfolgen dürfe oder nicht durch den Gesetzgeber im Wege einer offenen parlamentarischen Abwägung aller in Betracht kommender Belange erfolgen müsse.

[66] Bei diesem handelt es sich im Kommissionsjargon unproblematisch um eine verpflichtende Beibringungsanordnung, die unilateral von US-Seite verfügt und durchgesetzt wird.

[67] Wenn auch denkbar knapp. Die tragende Entscheidung für Microsoft entstammt einem mit drei Richtern besetzten Spruchkörper („panel"). Der Antrag auf eine en banc-Neuanhörung wurde bei einem Patt von vier zu vier Richtern abgelehnt. Die zugunsten der US-Regierung votierenden Richter widersprachen dabei der Entscheidung ihres eigenen Spruchkörpers. Vgl. US Court of Appeals for the Second Circuit, Microsoft v. U.S., 855 F.3d 53 (2nd Cir. 2017).

[68] US Court of Appeals for the Second Circuit, Microsoft v. U.S., Urt. v. 14.7.2016, Docket No. 14-2985. Online verfügbar unter https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html (25.5.2018).

[69] US Court of Appeals for the Second Circuit, Microsoft v. U.S., Urt. v. 14.7.2016, Docket No. 14-2985, Majority Opinion, Circuit Judge Carney, S. 38.

[70] US Court of Appeals for the Second Circuit, Microsoft v. U.S., Urt. v. 14.7.2016, Docket No. 14-2985, Majority Opinion, Circuit Judge Carney, S. 42.

[71] Vgl. die Zusammenfassung der Position der US-Regierung in US Court of Appeals for the Second Circuit, Microsoft v. U.S., Urt. v. 14.7.2016, Docket No. 14-2985, Concurring Opinion, Circuit Judge Lynch, S. 9: „[A]s the government points out, this case differs from that classic scenario with respect to both the nature of the legal instrument involved and the nature of the evidentiary material the government seeks."

[72] US Court of Appeals for the Second Circuit, Microsoft v. U.S., Urt. v. 14.7.2016, Docket No. 14-2985, Concurring Opinion, Circuit Judge Lynch, S. 13.

[73] US Court of Appeals for the Second Circuit, Microsoft v. U.S., Urt. v. 14.7.2016, Docket No. 14-2985, Concurring Opinion, Circuit Judge Lynch, S. 14 in Fn. 7.

[74] Zum Folgenden US Court of Appeals for the Second Circuit, Microsoft v. U.S., Urt. v. 14.7.2016, Docket No. 14-2985, Concurring Opinion, Circuit Judge Lynch, S. 1 und 2.

and in the libertarian traditions of this country." Und weiter: „[T]he government complied with the most restrictive privacy-protecting requirements", eben jenen der US-Verfassung. Auch hierzu eine kurze Einordnung: Ob der Nutzer am Datenstandort einen anderen oder höheren Grund- und Datenschutz genießt, wird durch diese Argumentation (bewusst oder unbewusst) ausgeblendet, was bestenfalls einer Art Grund- und Verfahrensrechtssolipsismus Vorschub leistet. Frei nach dem Motto: „[I]f [domestic] statutory and constitutional standards are met, it should not matter where the ones-and-zeroes are stored."[75]

Zu diesen grund- und datenschutztheoretischen Erwägungen gesellten sich solche, die auf die Effektuierung der nationalen Strafverfolgung grenzüberschreitender Kriminalität zielen:[76] Im Falle einer territorialen Verankerung der Cloud-Daten könnten Nutzer die Cloud dazu „missbrauchen", Daten im Ausland zu speichern und damit vor inländischen Strafverfolgern zu „verstecken". Der herkömmliche Rechtshilfeweg (der nun reziprok von US-Seite lamentiert wird, Anm. d. *Verf.*) sei beim grenzüberschreitenden Zugriff auf elektronische Beweismittel überdies zu schwerfällig. Und bestünden schließlich keine Rechtshilfebeziehungen mit bestimmten Staaten, so wären dort gespeicherte elektronische Beweismittel gänzlich unzugänglich, wenn der Datenstandort maßgeblich sei. All dies begünstige (so dürfen die politisch korrekt gehaltenen Aussagen in politisch weniger korrekter Terminologie fortgeschrieben werden) die Entstehung von „digital paradises"[77] und „safe havens" – was nicht sein dürfe!

c) Exkurs: Parallelfälle gegen Yahoo und Google; gleichsam zu den unterschiedlichen Speicher- bzw. Cloud-Politiken der Diensteanbieter

Diese Argumente haben dazu beigetragen, dass das Mehrheitsvotum des „Court of Appeals for the Second Circuit" in den USA singulär geblieben war. In Entscheidungen gegen Yahoo![78] und Google[79] wurde 18 U.S. Code § 2703(a) in anderen US-Bundesgerichtsbezirken als zulässige Rechtsgrundlage für Beibringungsanordnungen betreffend Auslandsdaten erachtet. Dabei wurde nicht „nur" die zuvor genannte grundsätzliche Kritik an einer territorialen Verankerung von auf ausländischen Servern gespeicherten Daten laut. Zudem wurde auch deutlich, dass die großen US-Diensteanbieter fundamental unterschiedliche Speicher- bzw. Cloud-Politiken verfolgen, wie dies etwa in einer Entscheidung gegen Google zu Tage trat:

„Unlike Microsoft, where storage of information was tethered to a user's reported location […] there is no storage decision here. The process of distributing information is automatic, via an algorithm, and in aid of network efficiency."[80]

Dies nahm die US-Regierung im Parteivortrag vor dem US Supreme Court im Microsoft Ireland Case wie folgt auf, um den Datenspeicherort als willkürlich und damit als irrelevant für grenzüberschreitende Zugriffe auf Clouddaten zu geißeln:

„Microsoft, at least, currently stores emails for a single account in a particular location that it can divine through a few keystrokes. […] Google, by contrast, stores the emails of U.S. users all over the world, sometimes breaking an account into multiple ‚shards'; even a single email may be divided into pieces, with the text stored in one location and attachments in another. […] Because it also moves the location of the data frequently and without human intervention, Google's compliance with a Section 2703 warrant would depend on the happenstance of where the data is located at the precise moment when the warrant is served or the provider accesses its network. And that is assuming that the precise location is knowable; some providers may not even be able to determine whether they currently store the requested data in the United States or abroad."[81]

d) Die amicus curiae-Papiere der Republik Irland, der EU-Kommission und von Presseverbänden

Der in den USA damit von der Regierungs- wie auch teilweise der Justizseite eingeleitete Abgesang auf das Territorialitätsprinzip in der Cloud ist nicht unwidersprochen geblieben. In den – die Bedeutung des Falls unterstreichenden – dutzenden amicus curiae-Papieren, die den US Supreme Court im Microsoft Ireland Case erreichten, sprachen sich etliche (wenn natürlich längst nicht alle) Akteure offen oder versteckt[82] gegen die Zulässigkeit unilateraler US-Beibringungsersuchen aus. Hier seien exemplarisch nur die Papiere der

[75] So US Court of Appeals for the Second Circuit, Microsoft v. U.S., Dissenting Opinion, Circuit Judge Jacobs, 855 F.3d 53, 62 (2nd Cir. 2017).

[76] Zum Folgenden US Magistrate Judge Francis (Fn. 64), S. 90a ff.; Parteivortrag der US-Administration vor dem US Supreme Court, S. 44 f., online verfügbar unter https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf (25.5.2018).

[77] So die Position der US-Administration im Microsoft Ireland Case einordnend *Christakis*, Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence, S. 24 f., online verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3086820 (25.5.2018).

[78] US District Court, E.D. Wisconsin, Urt. v. 21.2.2017, In re: Information associated with one Yahoo email address that is stores at premises controlled by Yahoo, No. 17-M-1234.

[79] US District Court, N.D. California, Urt. v. 25.4.2017, San Francisco Division, In the Matter of Search of Content that is Stored at Premises Controlled by Google, No. 16-MC-80263-LB, 2017 WL 1487625.

[80] US District Court, N.D. California, Urt. v. 25.4.2017, No. 16-MC-80263-LB, 2017 WL 1487625, S. 4.

[81] Parteivortrag der US-Administration (Fn. 76), S. 43 f., dort auch mit im Zitat nicht wiedergegebenen Nachweisen aus der US-Rechtsprechung.

[82] Die Tatsache, dass weder Irland noch die Kommission Partei für Microsoft ergriffen haben, sondern neutral geblieben sind, dürfte im Wesentlichen der politischen Höflichkeit sowie taktischen Erwägungen geschuldet sein.

Republik Irland, der EU-Kommission und von Presseverbänden herausgegriffen. Sie verdeutlichen, dass die Sachlage in der Cloud längst nicht so eindeutig ist, wie gerne im auffälligen Gleichklang dies- wie jenseits des Atlantiks behauptet wird.

aa) So trug die Republik Irland kurz und trocken vor, dass sie ein Rechtshilfeersuchen als das angemessene Mittel zur Erlangung der auf ihrem Territorium gespeicherten Daten ansehe. Überdies seien US Gerichte dazu verpflichtet, die irische Souveränität und die aller souveränen Staaten zu respektieren.[83] Trotz des respektvollen Tons machte die Republik Irland damit relativ unverblümt deutlich, dass sie eine auf 18 U.S. Code § 2703(a) gestützte unilaterale US-Beibringungs-anordnung zu in Irland gespeicherten Daten als Verletzung ihrer Territorialhoheit und damit als Völkerrechtsverletzung verstehen würde.[84]

bb) Bemerkenswert ist ferner, wie sich die EU-Kommission stellvertretend für die Europäische Union verhielt. Um sie selbst zu Worte kommen zu lassen:

„In the European Union's view, any domestic law that creates cross-border obligations should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. […] The relevant foreign law here is the GDPR, a comprehensive EU framework for regulating privacy of personal data. […] There is thus no doubt that the European Union is actively regulating the issues at this case's heart, including how data stored in the European Union must be protected, and when such data may be transmitted abroad."[85]

Diese Einlassung steht im augenfälligen Widerspruch zu den grundstürzenden Bestrebungen der Kommissionsdienste in ihren Papieren über den grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen. Während hier – wenn es um Eingriffe ausländischer Hoheitsträger in den europäischen Datenschutzraum geht – der Speicherort in Irland für maßgeblich erachtet wurde, weil er die DS-GVO (engl. General Data Protection Regulation, GDPR) aktiviere, wurde dort – im Kontext möglicher grenzüberschreitender Zugriffe europäischer Strafverfolger auf außereuropäisch gespeicherte Daten – die Notwendigkeit betont, den Speicherort als maßgeblichen Faktor zu verabschieden.[86]

cc) Um die Diskussion abzurunden, ist schließlich noch auf das gemeinsame Vorbringen von Presseverbänden (u.a. den Reportern ohne Grenzen) hinzuweisen. Es verdeutlicht zunächst, dass es zu kurz gegriffen wäre, alle Nutzer – Normalbürger, Kriminelle, institutionelle Nutzer etc. – in einen Topf zu werfen oder sie gar als potentielle Kriminelle zu führen, die ihre Clouddaten im Ausland dem legitimen Zugriff von Strafverfolgern entziehen wollen. Denn gerade Journalisten müssten – so die Presseverbände – ihre sensiblen Recherchematerialien, die in modernen digitalen Nachrichtenredaktionen und damit in der Cloud eingestellt sind, vor Zugriffen weltweit schützen können.[87] Zudem wurde betont, dass die langfristigen Auswirkungen nicht aus dem Blick verloren werden dürften. Denn: „Expanding the U.S. government's ability to reach electronic records stored outside its borders sets a dangerous international example that foreign governments hostile toward journalists may exploit."[88]

2. In den USA eingehende Ersuchen auf Datenherausgabe

Die in den EU-Dokumenten immer wieder herausgehobene Notwendigkeit der Zusammenarbeit mit dem privaten Sektor (oben I.) ist insbesondere auf US-Diensteanbieter gemünzt, da allein die „big six"[89] (also Google, Microsoft, Apple, Facebook, Twitter und Yahoo!; Amazon scheint mir noch „unterschätzt" zu werden) den Großteil der potentiell interessanten elektronischen Beweismittel unter ihrer technischen Kontrolle haben. Für die freiwillige Zusammenarbeit europäischer Strafverfolger mit US-Diensteanbietern fand sich im US-Recht, konkret im Electronic Communication Privacy Act (ECPA), ein Rechtsrahmen, der freilich sehr rudimentär ausfiel und schnell erzählt ist.[90]

a) Freiwillige Zusammenarbeit mit US-Diensteanbietern zur Erlangung von Nicht-Inhaltsdaten

Den US-Diensteanbietern stand – und steht es wohl noch – frei, ausländischen Strafverfolgern auf freiwilliger Basis Zugang zu Nicht-Inhaltsdaten (also zu Bestands- und Verkehrsdaten) außerhalb eines förmlichen Rechtshilfe- etc. -verfahrens zu geben. Grundlage hierfür ist 18 U.S. Code § 2702(a)(3), der mit „voluntary disclosure of customer communications or records" überschrieben ist und vorsieht:

"[A] provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a sub-

[83] Brief for Ireland as amicus curiae in support of neither party, S. 3, online abrufbar unter http://www.supremecourt.gov/DocketPDF/17/172/23732/20171213152516784_172%20ac%20Ireland%20supporting%20neither%20party.pdf (25.5.2018).

[84] So auch *Christiakis* (Fn. 77), S. 24 ff.

[85] Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither party, S. 5 f., online abrufbar unter http://www.supremecourt.gov/DocketPDF/17/172/23655/20171213123137791_172%20ac%20European%20Commission%20for%20filing.pdf (25.5.2018).

[86] Siehe oben bei und in Fn. 58 und 59.

[87] Brief amici curiae of the Reporters Committee for Freedom of the Press and 40 Media Organization, in Support of Respondent, S. 4 ff., online abrufbar unter http://www.supremecourt.gov/DocketPDF/17/17-2/28270/20180118140903639_Microsoft%20Word%20-%20Microsoft%20Amicus%20Draft_1.18.18_v4.0_Clean.docx.pdf (25.5.2018).

[88] Brief amici curiae of the Reporters Committee for Freedom of the Press and 40 Media Organization, in Support of Respondent, S. 9.

[89] Technical Document (Fn. 38), in Fn. 46.

[90] Ausführlich zu diesem Electronic Communication Privacy Act *Kerr*, University of Pennsylvania Law Review 2014, 373. Zu aktuellen Reformvorhaben in den USA *Pauly/Dieckhoff*, CCZ 2017, 270.

scriber to or customer of such service […] to *any governmental entity*." (*Hervorhebung* durch *Verf.*)

Da nun aber ausländische Strafverfolger keine „governmental entity" i.S.d. dieser Vorschrift sind, trifft die US-Diensteanbieter schlicht kein Preisgabeverbot. Das Kuriose daran: Ausländische Strafverfolger können informell an Bestands- und Verkehrsdaten gelangen, während US-Strafverfolger hierfür in der Regel einen förmlichen Beschluss benötigen (vgl. 18 U.S. Code § 2702[b][2]; für eine Ausnahme bei akuter Lebens- oder Leibesgefahr vgl. § 2702[b][8]).

Komplementiert wird dies aus deutscher Sicht wohl durch einen General Permission Letter des US-Department of Justice[91], der deutschen Strafverfolgern den direkten Kontakt mit US-Diensteanbietern gestattet. Die Relativierung „wohl" war notwendig, weil eine Einsichtnahme in diesen General Permission Letter für wissenschaftliche (oder für Verteidigungs-) Zwecke nicht möglich ist. Denn der General Permission Letter wurde von US-Seite mit der Erwartung und Vorgabe ausgegeben, dass er ausschließlich für nationale Strafverfolgungsbehörden Verwendung finden und nicht an Dritte herausgegeben wird. Aus dieser Erwartungshaltung wie auch daraus, dass sich deutsche Stellen strikt daran halten, spricht eine eigentlich für überwunden geglaubte „zweidimensionale" Konzeption der internationalen Zusammenarbeit in Strafsachen, die berechtigten Individualinteressen wenig Raum zumisst.[92]

b) Notwendigkeit der förmlichen Rechtshilfe für die Erlangung von Inhaltsdaten

Anderes gilt für Inhaltsdaten. Denn für deren Herausgabe ist – nach der uns aus dem Microsoft Ireland Case bekannten Vorschrift des 18 U.S. Code § 2703 – ein förmlicher Beschluss („court order", „subpoena", „warrant") notwendig, den lediglich eine „governmental entity" erlangen kann. Und da abermals ausländische Strafverfolger oder Gerichte keine „governmental entity" im Sinne dieser Vorschrift sind, können sie direkt keinen förmlichen Beschluss nach 18 U.S. Code § 2703 erwirken, sondern müssen dafür indirekt vorgehen und den Rechtshilfeweg beschreiten.

3 Zwischenfazit

Lässt man die oben unter I. und II. ausgeführten Hintergründe des nunmehr vorgelegten Kommissionsentwurfs zum grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen wie auch jene zum US-Recht Revue passieren und bedenkt zu allem Überfluss dabei, dass Vieles nur summarisch angerissen werden konnte, so bestätigt sich die in der Einführung angesprochene Komplexität der Regelungsaufgabe. Diese wird von den Kommissionsdiensten wie auch von aktivistischen Akteuren in den USA mit nachgerade revolutionärem Elan angegangen, wird doch an den ehernen Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen gerührt, um den grenzüberschreitenden Zugriff auf Clouddaten durch neue Konzepte zu effektuieren:

Das Territorialitätsprinzip wird dies- wie auch jenseits des Atlantiks zunehmend als Problem identifiziert (Stichwort: Die territoriale Zuordnung von Clouddaten soll willkürlich und suspekt sein). Die Lösung soll in der Unilateralität von Ermittlungsmaßnahmen liegen (Stichwort: Direktzugriffe; nationale Beibringungsanordnungen betreffend Auslandsdaten), deren Zulässigkeit mit anderen jurisdiktionsbegründenden Prinzipien wie dem Marktort- oder dem Ursprungslandprinzip begründet wird.[93]

Überdies wird die Zwischenstaatlichkeit der Strafverfolgung grenzüberschreitender Kriminalität als weiteres Problem ausgemacht (Stichwort: Sowohl die Rechtshilfe wie auch die gegenseitige Anerkennung sollen zu langwierig und schwerfällig sein). Hiergegen wird die Zusammenarbeit mit dem privaten Sektor (auf freiwilliger oder mit Zwang durchsetzbarer Basis) als neues Konzept der Strafverfolgung im digitalen Zeitalter in Stellung gebracht (Stichwort: Beibringungsersuchen oder -anordnungen).

Da diese Wechselspiele aus vermeintlichen Problemen und vermeintlichen Lösungen den Kern des grenzüberschreitenden Zugriffs auf Clouddaten zu Strafverfolgungszwecken betreffen, sind sie in Teil 2 dieses Beitrags eingehender unter die Lupe zu nehmen. Um also den sprichwörtlichen Wald vor lauter Bäumen nicht aus dem Blick zu verlieren, wird der zweite Teil des Beitrags darauf verwendet, nicht den Details[94]

[91] Auf solche nimmt Bezug Rats-Dok. 13982/16, ANNEX, S. 6.

[92] So bereits *mein* kritischer Kommentar in *Vogel/Burchard* (Fn. 19), Vor § 1 IRG Rn. 38.

[93] Wie vor kurzem in der Presse berichtet: „The European Union is preparing legislation to force companies to turn over customers' personal data when requested even if it is stored on servers outside the bloc, a position that will put Europe at loggerheads with tech giants and privacy campaigners." Vgl. https://uk.reuters.com/article/uk-eu-data-order/europe-seeks-power-to-seize-overseas-data-in-challenge-to-tech-giants-idUKKCN1GA0LN (25.5.2018).

[94] Dass diese Details ebenfalls entscheidend sind, wird nicht bestritten. Im Gegenteil. Die Grundsatz- darf die (hier nicht zu leistende) Detailarbeit nicht überflüssig machen. Ein wichtiges „Detail" sei hier nur exemplarisch angesprochen: Die hinlänglich bekannte Unterscheidung zwischen Bestands-, Verkehrs- bzw. Meta- und Inhaltsdaten als Datentypen mit vermeintlich aufsteigender Privatheitsintensität. Insofern ist zweierlei zu bedenken zu geben:
Erstens muss eine unionsrechtliche Regelung weitere Datentypen wie Big-Data-Analysen bedenken, da diese Big-Data-Analysen ein präzises Profiling von Nutzern erlauben und daher für Strafverfolger von großem Interesse sind. Die Möglichkeit des Big-Data-Profilings kommt im Zusammenhang mit der Wahl von Donald Trump zum US-Präsidenten zusehends an die Öffentlichkeit; vgl. nur The Guardian v. 17.3.2018, online abrufbar unter https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (25.5.2018).
Zweitens ist die Sichtweise, dass Inhaltsdaten (z.B. dass eine SMS einen Smiley zum Inhalt hat) die höchste und andere Datentypen eine geringere Privatheitsintensität hätten,

der grenzüberschreitenden Strafverfolgung in der Cloud nachzuspüren, sondern sich ihrer rechtsprinzipiellen Grundlagen zu versichern. Zur Verdeutlichung werde ich dies am Beispiel von Beibringungsanordnungen bzw. -ersuchen durchexerzieren, d.h. Sonderprobleme wie ein „loss of (knowledge of) location“ und Sondermaßnahmen wie Direktzugriffe ohne Einwilligung des Nutzers nicht weiter beachten.

schlicht veraltet. Gerade Verkehrs- und Meta-Daten können eine radikale Grundrechtsbedeutung entfalten, so wenn sie präzise Bewegungsprofile oder etwa Rückschlüsse auf das Sexualverhalten der Nutzer erlauben; ein „schönes“ Beispiel für Letzteres liefert das Beförderungsunternehmen Uber, das das „Fahrverhalten ihrer Kunden ausgewertet und Stadtkarten erstellt [hat], die beliebte Gegenden für One-Night-Stands zeigen.“ Hierzu Die Welt v. 8.1.2015, online verfügbar unter https://www.welt.de/wirtschaft/article136146346/Uber-veroeffentlicht-One-Night-Stand-Karten.html (25.5.2018). Die EU wäre daher gut beraten, bei der Regelung des grenzüberschreitenden Zugriffs auf elektronische Beweismittel nicht an der klassischen Einteilung in Bestands-, Verkehrs- bzw. Meta- und Inhaltsdaten festzuhalten.