Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2*

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.

III. Territorialität als Problem und Unilateralität als Lösung?

1. Eine kritische Einordnung der Entterritorialisierung der Cloud

Wie im ersten Teil dieses Beitrags deutlich wurde, hängt die Frage, wie Strafverfolger Zugriff auf in der Cloud gespeicherte elektronische Beweismittel nehmen können, entscheidend davon ab, wo diese belegen sind. Herkömmlich wurde dies, zumindest in Deutschland, ganz mehrheitlich territorial beantwortet. Die Daten sollen dort belegen sein, wo die entsprechenden Server stehen. Jedenfalls beim Zugriff auf im Ausland belegene zugangsgeschützte Daten liege, so zumindest die bisher herrschende deutsche Meinung, ein Eingriff in den völkerrechtlichen Territorialitätsgrundsatz vor.[1] In der Folge war (und ist) ein grenzüberschreitender Zugriff auf diese extraterritorialen Daten nur im Rechtshilfewege zulässig. Und ob dem Informationsrechtshilfeersuchen nachzukommen ist, hing (und hängt) dann entscheidend vom am Server- und daher Datenstandort geltenden Datenschutzrecht ab.

a) Die Entterritorialisierung der Cloud: Argumente im Schrifttum

Diese herkömmliche Position gerät heute nicht nur kriminalpolitisch (hierzu insbes. oben I. 3. b) cc) und II. 1. b), sondern auch in der Wissenschaft zunehmend unter Druck. Gegen die territoriale Verankerung von in der Cloud gespeicherten elektronischen Beweismitteln werden im Wesentlichen die zwei folgenden – nicht logisch zusammengehörenden, aber gerne zusammengezogenen – Thesen vorgebracht:[2]

- Daten sind anders („data is different“)![3] Denn die Cloud ist a-territorial![4]
- Die Nutzer kümmert das regelmäßig nicht![5] Bzw. pointierter, wenn auch regelmäßig nur hinter vorgehaltener Hand geäußert: Wer die Cloud nutzt, der muss wissen, dass seine Daten dort nicht „sicher“ sind![6]

Begründet wird die erste These – „Daten sind anders“ – zunächst mit technischen Argumenten, nämlich mit der immensen Mobilität und Volatilität von Daten im World Wide Web.[7] Und in der Tat: Technisch ist es ohne weiteres möglich, Daten in Sekundenbruchteilen von einem zum anderen Serverstandort zu transferieren.

Das führt in normativer Hinsicht zu einer Zuspitzung eines bekannten geflügelten Worts im rechtshilferechtlichen Schrifttum: Wenn die Öffnung von Landesgrenzen Kriminellen Überschallflugzeuge an die Hand gibt, denen die Strafverfolger in Postkutschen hinterhereilen müssen, weil ihre Eingriffs- und Ermittlungsbefugnisse weiterhin territorial zurückgebunden sind, so stellt die Cloud Kriminellen nunmehr Raumschiffe zu Gebote, um Strafverfolgern zu entkommen. *Daskal* hat dies wie folgt zum Ausdruck gebracht:

„Our personal data is everywhere and anywhere, moving across national borders in ways that defy normal expectations of how things and people travel from Point A to Point B. Yet,

---

* Der erste Teil dieses Beitrags ist erschienen in ZIS 2018, 190.

[1] Vgl. etwa *Brodowski*, ZIS 2012, 474 (477); *Gaede*, StV 2009, 96 (101 f.); *B. Gercke*, StraFo 2009, 272. Aus der Kommentarliteratur etwa *Hegmann*, in: Graf (Hrsg.), Beck'scher Online-Kommentar, Strafprozessordnung, Stand: 1.1.2018, § 110 Rn. 14. Ausführlich und weiterführend auch *Sieber*, Gutachten C zum 69. Deutschen Juristentag – Straftaten und Strafverfolgung im Internet, 2012, S. 144. Anders *Wicker*, MMR 2013, 765 (768 f.), die auf den Ort der Ermittlungshandlung rekurriert.

[2] Vgl. nur die bei *Woods*, Stanford Law Review 2016, 729 (754 ff.), zusammengetragenen Nachweise.

[3] Eingehend *Daskal*, The Yale Law Journal 2015, 325, und *Clopton*, Chicago Law Review 2016, 45, jeweils m.w.N. Aus dem deutschen datenschutzrechtlichen Schrifttum etwa *Ernst*, in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 1 („Beim Umgang mit personenbezogenen Daten spielen Landesgrenzen heute kaum noch eine Rolle. Es wäre angesichts der technischen Möglichkeiten zudem wenig sinnvoll, die rechtliche Anknüpfung iW an den [mittlerweile oftmals volatilen] Ort der physischen Datenverarbeitung oder gar -speicherung anzuknüpfen.“). Die Gegenposition wird eindrücklich vertreten von *Woods*, Stanford Law Review 2016, 729 (756 ff. m.w.N.).

[4] Hierzu ausführlich *Daskal*, The Yale Law Journal 2015, 325; siehe auch *Berman*, Vanderbilt Law Review 2018, 11 (23 f.).

[5] *Berman*, Vanderbilt Law Review 2018, 11 (12); *Daskal*, Vanderbilt Law Review 2018, 179 (225 f.); *Zoetekuow*, Ignorantia Terrae Non Excusat, S. 6, online abrufbar unter http://c.ymcdn.com/sites/www.iisfa.net/resource/resmgr/Slide_seminari/Convegno_Milano/c-mzoetekouw-ignorantia-terr.pdf (12.7.2018).

[6] Eindrücklich, wenn auch nicht wissenschaftlich fundiert, die Einordung von EU-Kommissar Oettinger: „Wer Nacktfotos ins Netz stellt, ist ‚blöd'.“ Berichtet in SpiegelOnline v. 30.9.2014, abrufbar unter http://www.spiegel.de/netzwelt/netzpolitik/guenther-oettingers-entlarvender-nacktbilder-kommentar-a-994547.html (25.5.2018).

[7] *Daskal*, The Yale Law Journal 2015, 325 (365 ff.); *dies.*, Vanderbilt Law Review 2018, 179 (221 ff.).

whereas data transits the globe without any intrinsic ties to territory, the governments that seek to access or regulate this data operate with territorial-based limits. This basic dichotomy between how governments and data operate is leading to an increasing number of jurisdictional conflicts, incentivizing data localization mandates as a means of asserting territorial control (and thus ensuring access to and regulatory power over sought-after data), and raising normative questions about how to draw the line between what is territorial and what is extraterritorial in the regulation of a predominantly unterritorial medium."[8]

Bezüglich der zweiten These – dass es den Nutzern ohnehin egal ist, wo ihre Daten territorial belegen sind – fällt auf, dass sie regelmäßig nur behauptet, nicht aber empirisch abgesichert wird. Gleichwohl lässt sich nicht bestreiten, dass die nachfolgenden paradigmatischen Zitate durch eingängige Evidenzappelle wirken, die durch die nicht weiter begründeten Relativierungen (im Folgenden kursiv gesetzt) noch verstärkt werden:

„Der tatsächliche Speicher- und Verarbeitungsort elektronischer Daten verliert sowohl in sozialer als auch in technischer Hinsicht zunehmend an Bedeutung. *Jedenfalls* in der *westlichen Welt* ist es dem *Durchschnitts*nutzer *in der Regel* gleichgültig, wo sich der physikalische Speicher- und Verarbeitungsort seiner Daten befindet."[9]

„[T]he territorial location of data becomes increasingly arbitrary and substantively unimportant. If I, as a U.S. citizen based in Maryland, have a g-mail account and Google, a U.S. corporation, decides to store my archived e-mails in Ireland or France or Indonesia (or indeed to split up the data fragments that make up each e-mail message among data warehouses in all three countries), that decision seems irrelevant to any question of whether I have somehow affiliated myself with any of those communities or governments for purposes of jurisdictional or choice-of-law analysis."[10]

Herauszustreichen ist, dass die hier in den Mittelpunkt gestellten Thesen für eine Entterritorialisierung der Cloud nicht zwingend strafverfolgungsfreundlich aufgestellt sind und auch nicht zwingend nationalen grenzüberschreitenden Zugriffen auf die Cloud Vorschub leisten wollen. Im Gegenteil. Das bereits im Jahre 1996 von *Johnson/Post* entwickelte Theorem „Data is different!" wollte in normativer Hinsicht gerade die Onlinewelt als Welt mit eigenem rechtlichen Gehalt jenseits von staatlicher Souveränität und Legitimität gestalten,[11] ohne dabei in die Cyberanarchie abzudriften,[12] was mit einem libertären Zungenschlag auch möglich wäre. Und *Berman* – einer der weltweit führenden Rechtstheoretiker rechtspluralistischer Provenienz – baut auf seinem Befund einer entterritorialisierten und datengetriebenen Welt ein neues und hochkomplexes Regelungsset auf, um Zuständigkeiten („jurisdiction") neu zu verteilen. Territorialität soll dabei als jurisdiktionell eindeutiger Anknüpfungspunkt durch die offene Abwägung u.a. der kommunitären Affiliation des Nutzers sowie der Marktrelevanz, Größe und ökonomischen Potenz des Diensteanbieters ersetzt werden.[13]

b) Die bewusste oder widerleglich vermutete Territorialisierung von Daten

Dass in der europäischen und US-Kriminalpolitik weder eine Entstaatlichung der Cloud noch eine gänzliche neue Bestimmung von Zuständigkeiten in der Cloud gewollt ist, liegt auf der Hand. Vielmehr werden dort wissenschaftliche Argumente „gekapert" und zu gänzlich anderen Zwecken ins Felde geführt. Eben dazu, um einer klassischen strafanwendungsrechtlichen Regeln gehorchenden nationalen Strafverfolgung Vorschub zu leisten, die durch grenzüberschreitende Zugriffe in die Cloud effektuiert werden soll. Gepaart mit dem Argument, dass die Cloud nicht zum „safe haven" für Kriminelle werden dürfe,[14] vollzieht sich so in Wahrheit eine Renationalisierung des Zwischenstaatlichen bzw. eine staatliche Landnahme des (vermeintlich) Entterritorialen der Cloud zu Strafverfolgungszwecken. Dagegen sei im Folgenden angetreten.

Vorweg ist freilich zuzugestehen, dass eine Anknüpfung an den territorialen Speicherort elektronischer Beweismittel willkürlich erscheint, wenn – wie dies der Cloudpolitik von Google entspricht (oben II. 1. c) – Daten an verschiedenen Serverstandorten in sog. „shards" zersplittert werden; oder wenn der Speicherort durch Algorithmen zur Steigerung der Netzwerkeffizienz bestimmt wird und sich daher jederzeit ändern kann. Allerdings ist das nicht die gängige Praxis aller Diensteanbieter. Wie im Microsoft Ireland Case selbst von Seite der US-Regierung konzediert wird, kann die Speicherung von Daten an einem bestimmten Ort – von Diensteanbietern, Nutzern oder Staaten – sehr wohl gewollt sein (oben II. 1. c). Und wie die Stellungnahme der Republik Irland im Microsoft Ireland Case bescheinigt, sind in solchen Konstellationen Souveränitätsansprüche über im Inland gespeicherte Daten noch lange nicht grundsätzlich passé (oben II. 1. d).

Aus all dem folgt ein Differenzierungsgebot bzw. ein Generalisierungsverbot, frei nach dem Motto: „Cloud ist nicht gleich Cloud." Die ausdrückliche und/oder gewollte Speicherung potentieller elektronischer Beweismittel an einem bestimmten Ort darf nicht der „willkürlichen" (genauer: zur bloßen Effizienzsteigerung getätigten) Speicherung an irgendeinem Ort gleichgesetzt werden. Zu paaren ist dies mit einer widerleglichen Vermutungsregel dahingehend, dass Daten in der Regel nicht willkürlich, sondern bewusst an einem bestimmten Ort abgelegt wurden.

aa) Territoriale Souveränität als Demokratie und Rechtsstaatlichkeit

Aus der Forderung, die bewusste oder widerleglich vermutete Territorialisierung elektronischer Beweismittel ernst zu neh-

[8] *Daskal*, Vanderbilt Law Review 2018, 179 (180 f.).
[9] *Warken*, NZWiSt 2017, 289 (295) (*Herv.* durch *Verf.*).
[10] *Berman*, Vanderbilt Law Review 2018, 11 (12).
[11] *Johnson/Post*, Stanford Law Review 1996, 1367.
[12] *Post*, Berkeley Technology Law Journal 2002, 1365.
[13] *Berman*, Vanderbilt Law Review 2018, 11 (22 ff.).
[14] So die von US-Strafverfolgern geäußerte Befürchtung im Microsoft Ireland Case. Hierzu BBC v. 16.6.2016, online abrufbar unter http://www.bbc.com/news/technology-36800334 (25.5.2018).

men, spricht zunächst ein relativ klassisches kontinentaleuropäisches Souveränitäts- und Völkerrechtsverständnis.[15] Diesem zufolge ist es unerheblich, ob eine Einwirkung in fremde Gebietshoheit hoheitlicher oder tatsächlicher Natur ist,[16] ob sie offen oder heimlich erfolgt,[17] ob sie mit oder ohne Zwang[18] oder – und das ist entscheidend – ob sie bewusst oder unbewusst[19] vorgenommen wird. Daher gilt: Unwissenheit schützt vor dem Eingriff in fremde Gebietshoheit nicht, schon um keiner bewussten Gleichgültigkeit gegenüber dem Gebot der Achtung fremder Gebietshoheit Vorschub zu leisten.[20]

Auf den zweiten Blick verbindet sich in Deutschland und Europa mit diesem Souveränitäts- und Völkerrechtsverständnis mehr als das „westfälische Pathos" staatlicher Unabhängigkeit und Selbstbestimmtheit in Fragen der eigenen rechtlichen Gestaltung:

Wie das Bundesverfassungsgericht in seinem Lissabon-Urteil zu Recht herausgehoben hat, steht Souveränität heute zunächst für Demokratie und Rechtsstaatlichkeit. Sie verbürgt den Schutz von Sachbereichen, die die Lebensumstände der Bürger, vor allem ihren von den Grundrechten geschützten privaten Raum der Eigenverantwortung und der persönlichen und sozialen Sicherheit prägen. Und sie verbürgt den Schutz solcher politischen Entscheidungen, die in besonderer Weise auf kulturelle, historische und sprachliche Vorverständnisse angewiesen sind und die sich im parteipolitisch und parlamentarisch organisierten Raum einer politischen Öffentlichkeit diskursiv entfalten.[21] Anders ausgedrückt: Die Gebietshoheit als Ausfluss modern gedachter Souveränität sichert die Wahrung und Kontrolle grund- und datenschutzrechtlicher Standards bei der Strafverfolgung im Ausland, wenn diese einen Inlandsbezug entfaltet. Ein demokratischer und rechtsstaatlicher Souverän darf mit anderen Worten nicht ohne Weiteres, gleichsam blind seine Hand zur Strafverfolgung im Ausland reichen.

In der EU wird überdies das nationalstaatliche durch ein gemeineuropäisches Souveränitätsdenken – hier also in der Form eines europäischen Demokratie-, Rechtsstaats- und Grundrechtsdenken – komplementiert.[22] Dies hat allemal nach außen hin zur Folge, dass der europäische Rechtsraum der Wahrung und Kontrolle grund- und datenschutzrechtlicher Standards bei der Strafverfolgung im EU-Ausland verschrieben ist. Genau dies liegt auch der DS-GVO, und hier z.B. Art. 49 DS-GVO, zugrunde. Es wäre daher aus unionsrechtlicher Sicht selbstwidersprüchlich, Clouddaten einerseits datenschutzrechtlich zu territorialisieren[23] und sie andererseits strafprozessual zu entterritorialisieren.

---

[15] Hierzu und zum Folgenden auch *Vogel/Burchard*, in: Grützner/Pötz/Kreß [Hrsg.], Internationaler Rechtshilfeverkehr in Strafsachen, Stand: Dezember 2017, Vor § 1 IRG Rn. 101, 104.

[16] Vgl. nur *Dombrowski*, Extraterritoriale Strafrechtsanwendung im Internet, 2014, S. 5; ob eine hoheitliche Maßnahme vorliegt, bemisst sich nach der Rechtsordnung des betroffenen Staates vgl. *Ipsen*, Völkerrecht, 6. Aufl. 2014, § 5 Rn. 60.

[17] Vgl. nur *Ipsen* (Fn. 16), § 5 Rn. 61; *Stein/v. Buttlar*, Völkerrecht, 14. Aufl. 2017, Rn. 541. Im Ausgangspunkt verboten sind auch verschleierte Amtshandlungen, die scheinbar privat, in Wahrheit aber mit der Zielsetzung der Förderung hoheitlicher Verfahren vorgenommen werden.

[18] Zum Teil umstritten ist, ob dies auch schlicht-hoheitliche Maßnahmen, d.h. solche ohne Zwangscharakter (z.B. eine einfache Informationsbeschaffung oder bloße „Erkundungshandlungen") betrifft, die im Grunde auch von Privaten durchgeführt werden könnten. Hierzu *Tiedemann*, in: Kaufmann (Hrsg.), Festschrift für Paul Bockelmann zum 70. Geburtstag am 7. Dezember 1978, 1979, S. 819 (821 f.).

[19] Ob allein die Unkenntnis vom Auslandsbezug – z.B. bei Internetkommunikation – einen hoheitlichen Zugriff auf fremdes Staatsgebiet rechtfertigen kann, ist umstritten, siehe hierzu *Dombrowski* (Fn. 16), S. 146 ff. m.w.N.

[20] In der Konsequenz ist die strafprozessual wohl herrschende Meinung zu § 110 Abs. 3 StPO zurückzuweisen, wonach die Sichtung von „Cloud-Daten" ohne Weiteres zulässig sein soll, wenn und weil unklar ist, ob und ggf. in welchem ausländischen Staat sich der Server befindet. So etwa *Hegmann* (Fn. 1), § 110 Rn. 15; *Meyer-Goßner/Schmitt*, Strafprozessordnung, Kommentar, 60. Aufl. 2017, § 110 Rn. 7b. Anders und wie hier *Brodowski/Eisenmenger*, ZD 2014, 119 (126); *Obenhaus*, NJW 2010, 651 (654). Vgl. auch *Kudlich*, GA 2011, 193 (208).

[21] BVerfGE 123, 267.

[22] Vgl. nur *v. Bogdandy/Bast*, in: v. Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht, 2. Aufl. 2009, S. 1; *Gerkrath*, L'émergence d'un droit constitutionnel pour l'Europe; *Peters*, Elemente einer Theorie der Verfassung Europas, 2001. – Bereits EuGH, Urt. v. 23.4.1986 – Rs. 294/83 (Les Verts), Rn. 23 sprach vom (damaligen) Gründungsvertrag der Europäischen Wirtschaftsgemeinschaft als „Verfassungsurkunde der Gemeinschaft".

[23] Gegen diese Territorialisierungsthese spricht nicht, dass Art. 3 DS-GVO den räumlichen Anwendungsbereich der DS-GVO *nicht* nach der territorialen Verarbeitung oder Speicherung von Daten im Unionsinland, sondern primär nach dem Niederlassungsprinzip (Abs. 1) und sekundär nach dem Marktortprinzip (Abs. 2) bestimmt. Da dafür jedoch unerheblich ist, „[w]o der Sitz oder Inkorporationsort des Verantwortlichen bzw. Auftragsverarbeiters belegen ist" und welche Staatsangehörigkeit die betroffene Person hat, und da für eine Unions-Niederlassung irgendeine feste Einrichtung im Unionsgebiet, die der effektiven und tatsächlichen Ausübung einer Tätigkeit dient, hinreicht, aktiviert das Betreiben von Server(farmen) im Unionsgebiet die DS-GVO und führt so über die Hintertür zu einer territorialen Aktivierung der DS-GVO. Es gilt daher dann doch: „Die DS-GVO folgt ausschließlich dem Territorialitätsprinzip. Es kommt allein auf den Ort der Niederlassung im Unionsgebiet bzw. den tatsächlichen Aufenthaltsort der betroffenen Person im Unionsgebiet an. Eine territoriale Anknüpfung an den Datenverarbeitungsort schließt Abs. 1, letzter Hs., hingegen aus." Nachweise aus *Hanloser*, in: Wolff/Brink (Hrsg.), Beck'scher Online-Kommentar, Datenschutzrecht, Stand: 1.2.2017, Art. 3 DS-GVO Rn. 1 ff., 43.

bb) Kein Grundrechtsverzicht bzw. keine datenschutzrechtliche Einwilligung durch schlichte Cloudnutzung

Angefochten wird diese Sicht der Dinge nur scheinbar durch die These, dass „es Durchschnittsnutzern in der Regel gleichgültig ist, wo sich der physikalische Speicher- und Verarbeitungsort seiner Daten befindet" (oben a), bei und in Fn. 5 f.).

Denn erstens muss hierzu die rhetorische Frage gestattet sein, was denn nun mit denjenigen ist, denen aus guten und nachvollziehbaren Gründen der Speicherort nicht gleichgültig ist. Hier sei nur an den eindrücklichen Vortrag der Presseverbände im Microsoft Ireland Case erinnert (oben II. 1. d) cc). Sind also Personen, die sich z.B. unter den europäischen Datenschutzschild begeben, weil sie penibel auf ihre Datensicherheit und informationelle Selbstbestimmung achten (müssen), nicht schutzbedürftig?

Der fehlende Schutzbedarf könnte faktisch daraus folgen, dass Nutzer schlicht wissen müssen, dass Daten in der Cloud nicht sicher sind. Und in der Tat sollte eigentlich klar sein: Wer seine Daten heute in die Cloud stellt, müsste sich eigentlich bewusst sein, dass die Cloud überwacht wird oder zumindest potentiell überwachbar ist. Freilich beginnen mit diesem „eigentlich" erst die Probleme.

In tatsächlicher Hinsicht wissen die meisten Nutzer gar nicht, welche Daten über sie gesammelt werden und wie intensiv sie überwachbar sind. Nutzer verdrängen, dass sie „gläsern" sind. Dies gilt umso mehr, als zwischen Nutzern und Diensteanbietern eine augenfällige Machtasymmetrie herrscht. Nutzer können ihr „Gläsern-Sein" also gar nicht verhandeln, wenn sie mit Diensteanbietern in vertragliche Beziehungen treten, will sagen: wenn sie Clouddienste nutzen.

Und in normativer Hinsicht folgt aus dem „Die Nutzer müssten es eigentlich wissen!" nichts, weil die Überführung in eine rechtliche Wertung fehlt. Führt man diese ein, so zeigt sich, wie schwach die These vom fehlenden Schutzbedarf qua schlichter Cloudnutzung ist. Denn entweder man verbindet mit dieser Cloudnutzung einen umfassenden Grundrechtsverzicht (was zumindest im Sinne eines Totalverzichts auf den Schutz eines oder mehrerer Grundrechte rechtlich überaus heikel wäre).[24] Oder man verbindet damit zumindest die datenschutzrechtliche (andere Verfahrens- etc. Grundrechte nicht betreffende) Einwilligung, dass personenbezogene Daten zu Strafverfolgungszwecken im Ausland Verwendung finden. Dann ist aber daran zu erinnern, dass Letztere „eine freiwillige, informierte, bestimmte und formgemäße Einverständniserklärung einer einwilligungsfähigen betroffenen Person über die Verarbeitung personenbezogener Daten"[25] voraussetzt. Daran dürfte es, zumindest ohne weitreichende Informationen seitens der Diensteanbieter, in der Regel fehlen.

cc) Die Ökonomisierung des Datenschutzes

Die Bedeutsamkeit der bewussten Territorialisierung elektronischer Beweismittel folgt auch aus der hier sog. „Ökonomisierung des Datenschutzes".[26] Denn nicht nur Daten haben ökonomischen Wert,[27] sondern zusehends auch der Datenschutz. Datenschutz und Datensicherheit verursachen nicht nur Kosten für die Diensteanbieter. Sie werden vielmehr heute auch zum Verkaufsargument. Während jedoch Unternehmen wie Apple das Thema Datensicherheit selbst in die Hand nehmen (indem z.B. iPhones mit dem Versprechen verschlüsselt werden, Hoheitsträgern keinen Zugang zu gewähren) und ansonsten libertäre Aufrufe zirkulieren, die eigenen digitalen Spuren zu verschleiern,[28] kann und sollte der ökonomische Wert der territorialen Verankerung von Datenschutzstandards nicht aus den Augen verloren werden. Paradigmatisch hierfür steht abermals der Microsoft Ireland Case, warb und wirbt Microsoft doch gerade damit, dass Nutzer den Speicherort ihrer Daten auswählen dürfen.[29]

Damit verbindet sich zweierlei: Zum einen die Erkenntnis, dass „as Internet business models mature, it will be in the interest of companies to be honest, discreet, protective, and loyal to their customers, in order to develop long-term relationships that create real value for the companies as well as their users."[30] Und zum anderen die rechtspolitische Anstrengung, Datenschutz und Datensicherheit nicht in die Hände von Unternehmen und Nutzern zu legen, sondern staatlicher Kontrolle und Gestaltung zu unterwerfen. All dies wäre nachhaltig verunmöglicht, wenn man die Cloud insgesamt für Strafverfolgungszwecke entteritorialisieren und der bewussten Territorialisierung von Daten nicht Rechnung tragen wollte. Denn dann bewahrheitete sich das dem ersten Teil dieses Beitrags vorangestellte Zitat eines Microsoft-Verantwortlichen: „If every country asserts extraterritorial jurisdiction […] then everybody gets everybody's data."

c) Addendum: Die „willkürliche" Territorialisierung von Daten

Auch aus der „willkürlichen" (zur bloßen Effizienzsteigerung getätigten) Speicherung von Daten an irgendeinem Ort folgt noch nicht, dass damit unilaterale Zugriffe (sei es durch Di-

[24] Allgemein zum Grundrechtsverzicht im Rahmen der EU-GRC *Jarass*, Charta der Grundrechte der Europäischen Union, Kommentar, 3. Aufl. 2016, Art. 52 Rn. 18, dort auch m.w.N. zu den Voraussetzungen sowie zu Grundrechten, die verzichtsfeindlich sind. Allgemein gilt: Der Verzicht darf nicht wichtigen öffentlichen Interessen widersprechen, muss eindeutig und in voller Kenntnis der Tatsachen erklärt werden und nicht durch gewichtige Umstände erzwungen worden sein. An all dem dürfte es fehlen, wenn Nutzer schlicht die Cloud nutzen.

[25] *Stemmer*, in: Wolff/Brink (Fn. 23), Art. 7 DS-GVO Rn. 32.

[26] Vgl. hierzu ein- und weiterführend *Mantelero*, International Data Privacy Law 2013, 229 (insbes. 230 f.).

[27] Hierzu etwa *Wandtke*, MMR 2017, 6.

[28] *Brunton/Nissenbaum*, Obfuscation: A User's Guide for Privacy and Protest, 2015.

[29] Siehe https://www.microsoft.com/de-de/cloud/Wahlfreiheit.aspx (12.7.2018).

[30] Erhellend *Richards/Hartzog*, Yale Law Journal 2017, 1180 (1213 ff., hier insbes. 1221).

rektzugriffe oder Beibringungsanordnungen) ohne weiteres zulässig sind. Denn damit würde man allein der normativen Kraft des Faktischen – eben der „willkürlichen" Speicherpolitik eines Diensteanbieters – Tribut zollen und damit die faktische Kraft des Normativen aus dem Auge verlieren. Anders ausgedrückt müssen aus allgemeinen Verhältnismäßigkeitserwägungen heraus komplementäre wirtschaftsverwaltungsrechtliche Steuerungsoptionen dieser Cloudspeicherpolitiken in den Blick genommen werden.

Damit wird hier keineswegs umfassenden Lokalisierungszwängen das Wort geredet, da dies die (Grundrechtsposition der) Diensteanbieter stark belasten würde. Nachgedacht werden muss aber darüber, den Nutzern mehr Verantwortung zuzuweisen. Im Mindestmaß wäre es hierfür erforderlich, dass Diensteanbieter ihre Nutzer umfassend (im Sinne von Art. 7 DS-GVO) über ihre „willkürlichen" Cloudpolitiken wie auch darüber informieren, dass eben diese Cloudpolitiken zu einer Entteritorialisierung dieser Cloud und damit dazu führen, dass Strafverfolger mit dem Argument, der territoriale Speicherort sei willkürlich und daher irrelevant, auf die in dieser Cloud gespeicherte Daten zugreifen. Entscheidet sich der Einzelne dann gleichwohl für die Nutzung dieser Cloud, so willigt er datenschutzrechtlich gleichsam darin ein, dass Daten an Strafverfolger unabhängig vom Datenstandort herausgeben werden können. Damit würde der datenschutzrechtlichen Einwilligung als „zentrale[m] Instrument zur Verwirklichung datenschutzrechtlicher Selbstbestimmung"[31] sowohl strafprozessual wie auch zusammenarbeitsrechtlich zur Durchsetzung verholfen.

2. Eine kritische Einordnung der Unilateralisierung der grenzüberschreitenden Strafverfolgung in der Cloud

Die vorstehende Skizze zeigt, dass das Territorialitätsprinzip – also die territoriale Bestimmung des Datenspeicherorts in der Cloud – keineswegs ausgedient hat. Sie mag Strafverfolger weltweit vor Probleme stellen. Diese müssen dann aber anders – z.B. wirtschaftsverwaltungsrechtlich oder durch eine Verbesserung der internationalen Zusammenarbeit in Strafsachen – überwunden werden als durch eine grundsätzliche Infragestellung völker- und zusammenarbeitsrechtlicher Fundamentalprinzipien. Zugespitzt lässt sich daher sagen, dass Territorialität kein Problem, sondern eine Lösung ist, um in der Cloud ein modernes Verständnis von Souveränität, Rechtsstaatlichkeit und Grundrechtsschutz umzusetzen, zumal all dies durch eine Ökonomisierung des territorialen Datenschutzes flankiert wird. Doch selbst wenn damit der Entterritorialisierung der Cloud beim grenzüberschreitenden Zugriff auf elektronische Beweismittel zu entsagen ist, ist damit keineswegs der vermeintlichen Lösung, namentlich der Unilateralisierung dieser Zugriffe, endgültig der Boden entzogen. Das soll nunmehr am Beispiel von hier sog. echten (unten a) und unechten (unten b) unilateralen Beibringungsanordnungen dargestellt werden.

Allgemein gilt insofern: Es kommen unterschiedliche Anknüpfungspunkte in Betracht, um die Unilateralität von Ermittlungsmaßnahmen betreffend Auslandsdaten – z.B. eine nationale Beibringungsanordnung betreffend Auslandsdaten – zu legitimieren. Zu nennen ist etwa das Marktortprinzip[32], das Ursprungslandprinzip[33], das Bestimmungslandprinzip oder das Personalitätsprinzip[34]. Es wird daher im Folgenden nicht bestritten, dass mithilfe dieser Prinzipien eine nationale „enforcement jurisdiction" begründet werden kann. Es wird jedoch im Folgenden bestritten werden, dass diese Ersetzung des Bi- und Multilateralität erforderlich machenden Territorialitätsprinzips durch andere, Unilateralität erlaubende Prinzipien kriminalpolitisch weise, aufs Ganze bezogen dem System der international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität förderlich oder „kostenlos" möglich ist.

a) Echte unilaterale Beibringungsanordnungen betreffend Auslandsdaten ohne Zustimmung des territorial betroffenen Staates

Paradigmatisch für echte unilaterale, also einseitig von einem Strafverfolgungsstaat ausgehende Beibringungsanordnungen standen – vor der Einführung des CLOUD-Act – jene nach 18 U.S. Code § 2703(a). Diese wurden ohne Zustimmung, Konsultation oder Notifikation des Staates, in dem Auslandsdaten belegen sind, erlassen und gegenüber einem in den USA tätigen oder ansässigen Diensteanbieter durch entsprechende Sanktionsdrohungen durchgesetzt.

aa) Drohende Justizkonflikte analog der „pre-trial discovery"

Ob echte unilaterale Beibringungsanordnungen extraterritorial wirken und damit den zuvor hochgehaltenen Territorialitätsgrundsatz verletzen, ist (völker-)rechtlich umstritten.[35] In der Tat tun sich hier ähnliche Konfliktlagen wie beim „discovery" des US-Zivilprozessrechts auf, die sich zu ähnlichen „Justizkonflikten" (so die herkömmliche,[36] mehr schlechte als rechte Übersetzung von „conflicts of jurisdiction") auswachsen können. Hier wie dort steht die US-Seite auf dem Standpunkt, dass die im Inland erfolgende und nur im Inland er-

[31] *Stemmer* (Fn. 25), Art. 7 DS-GVO Rn. 1.

[32] Dieses wird wohl – was wenig verwunderlich ist – von den Kommissionsdiensten präferiert, weil es europäischen Strafverfolgern Zugriff auf sämtliche Daten geben würde, die bei international tätigen Diensteanbietern liegen, wenn und weil diese im europäischen Inland Dienste anbieten.

[33] Auf dieses lässt sich unproblematisch die Position der US-Strafverfolger stützen, wenn und weil sie auf Daten Zugriff nehmen wollen, die von Diensteanbietern kontrolliert werden, die in den USA ihren (Konzern-)Sitz haben.

[34] Frei nach dem – informell immer wieder geäußerten – Motto: Inländische Strafverfolger müssen auf die Daten von Inländern Zugriff nehmen dürfen; und diesen muss es verwehrt werden, ihre Daten im Ausland „in Sicherheit" zu bringen. – Freilich ist hierzu anzumerken: Formuliert man dieses Motto als „Mitwirkungspflicht" aller Inländer, dem Staat als potentielle Beschuldigte Zugriff auf alle potentiell belastende Daten zu sichern, verliert es deutlich an Überzeugungskraft.

[35] Vgl. auch *Schaub*, ZaöRV 2011, 808 (811 ff.).

[36] Vgl. nur *Adler*, IPRax 2015, 364.

zwingbare Anordnung gegen ein sich im Inland aufhaltendes Prozessrechtsubjekt, die unter seiner Kontrolle stehenden Dokumente etc. aus dem Ausland zu beschaffen und im Inland herauszugeben, ein rein innerstaatlicher Vorgang ohne Auslandsberührung sei.[37]

Die meisten Staaten des kontinentaleuropäischen Rechtskreises lehnen diese Position im Kontext des „discovery" als Souveränitätseingriff ab.[38] Sie verweisen stattdessen auf die Notwendigkeit, dass im Inland belegene Dokumente, wenn überhaupt, im Wege der zivilprozessualen Rechtshilfe an die USA herauszugeben sind. Hier ist nicht der Ort, zu diesen kaum vereinbaren Positionen Stellung zu beziehen. Freilich ist zu betonen: Jene EU-Mitgliedstaaten, die eine US-amerikanische „zivilprozessuale discovery" ablehnen, würden sich selbstwidersprüchlich verhalten, wenn sie nun einer Art „europäischen strafprozessualen discovery" – in der Form von echten unilateralen Beibringungsanordnungen gegenüber privaten Diensteanbietern betreffend Auslandsdaten – das Wort reden würden.

bb) Drohende Dilemmata für Diensteanbieter

Abgesehen davon bringen echte unilaterale Beibringungsanordnungen die Diensteanbieter in die „Zwickmühlen" gegenläufiger Regelungsregime. Denn das Datenschutzrecht fungiert zunehmend als „blocking statute" (so die „discovery"-Terminologie),[39] die aber vonseiten des Anordnungsstaats einer Beibringungsanordnung nicht unbedingt beachtet wird. Das führt beispielhaft zu folgenden Regimekonflikten: Die Befolgung einer US-Beibringungsanordnung kann einen Verstoß gegen europäisches Datenschutzrecht darstellen, mit der Konsequenz, dass Diensteanbietern in Europa datenschutzrechtliche Sanktionen drohen.[40] Umgekehrt hat die Weigerung, einer brasilianischen Beibringungsanordnung zu entsprechen, weil sie US-amerikanisches Datenschutzrecht verletze, bereits zur Konsequenz gehabt, dass der Sich-Weigernde wegen dieser Weigerung in Brasilien strafrechtlich verfolgt wurde.[41] Solche Zwickmühlen sind in einer hochgradig vernetzten Weltwirtschaft untragbar.[42] Die DS-GVO hat hierfür zwar mit Art. 49 Abs. 1 S. 2 vorgesorgt.[43] Hiernach ist eine Übermittlung personenbezogener Daten aufgrund einer echten unilateralen Beibringungsanordnung höchst ausnahmsweise zulässig, selbst wenn kein Regelbeispiel i.S.d. Art. 49 Abs. 1 S. 1 DS-GVO, kein „Angemessenheitsbeschluss" (die einem Drittland wie den USA eine „angemessenes [datenschutzrechtliches] Schutzniveau" attestiert, Art. 45 DS-GVO) oder keine „geeignete Garantien" für eine angemessene Datenverarbeitung im Drittland vorliegen (Art. 46 DS-GVO). Allerdings setzt dies u.a. voraus, dass die „Übermittlung nicht wiederholt" erfolgt, dass sie also „einen einmaligen Vorgang darstellt."[44] Gerade bei großen Diensteanbietern, die systematisch Daten im räumlichen Anwendungsbereich der DS-GVO[45] speichern, ist freilich damit zu rechnen, dass gegen sie gerichtete Beibringungsanordnungen keine singulären Ereignisse bleiben.

cc) Drohende Erosion der internationalen Solidarität bei der international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität

Schließlich drohen echte unilaterale Beibringungsanordnungen auch die Grundlagen der international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität nachhaltig in Mitleidenschaft zu ziehen. Namentlich droht die internationale Solidarität und das Vertrauen zwischen den Hoheitsträgern verschiedener Jurisdiktionen bei der international-arbeitsteiligen Strafverfolgung grenzüberschreitender

[37] Eindrücklich die Entscheidung des US Supreme Court in Societé Nationale Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

[38] Vgl. für Deutschland *Pabst*, in: Krüger/Rauscher (Hrsg.), Münchener Kommentar zur Zivilprozessordnung, Bd. 3, 5. Aufl. 2017, Art. 23 HZPÜ Rn. 10.

[39] Vgl. nur *Metz/Spittka*, ZD 2017, 361 (363) m.w.N.

[40] So auch der Parteivortrag von Microsoft vor dem US Supreme Court im Microsoft Ireland Case, S. 16 ff., online abrufbar unter http://www.supremecourt.gov/DocketPDF/17/17-2/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf (12.7.2018). Ferner der „brief of EU data protection and privacy scholars as amici curiae in support of respondent" vor dem US Supreme Court im Microsoft Ireland Case, S. 3 ff., online abrufbar unter https://www.supremecourt.gov/DocketPDF/17/172/28272/20180118141249281_17-2%20BSAC%20Brief.pdf (12.7.2018).

[41] Siehe hierzu die Stellungnahme des „Chief Legal Officer" von Microsoft, Brad Smith, vor dem „House Judiciary Committee" des US-Kongresses v. 25.2.2016, S. 2, online abrufbar unter https://judiciary.house.gov/wp-content/uploads/2016/02/brad-smith-testimony.pdf (25.5.2018). Zur Rechtslage in Brasilien ausführlich und mit Nachweisen auch der „Brief of Internetlab and technology center am amicus curiae in support of respondent" vor dem US Supreme Court im Microsoft Ireland Case, S. 16 ff., online abrufbar unter https://www.supremecourt.gov/DocketPDF/17/172/28382/20180118203851162_172%20bsac%20Internetlab%20Law%20and%20Technology%20Center.pdf (25.5.2018).

[42] Auch *Warken*, NZWiSt 2017, 417 (422), moniert das Fehlen verlässlicher Regelungen für solche Konstellationen.

[43] Hierzu auch European Commission on behalf of the European Union as amicus curiae in support of neither party, S. 14 f., online abrufbar unter http://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf (12.7.2018); krit. bzw. differenzierend *Pauly/Dieckhoff*, CCZ 2017, 270 (271); *Metz/Spittka*, ZD 2017, 361 (365 f.).

[44] *Lange/Filip*, in: Wolff/Brink (Fn. 23), Art. 49 DS-GVO Rn. 51.

[45] Hierzu oben in Fn. 23.

Kriminalität irreparablen Schaden zu nehmen.[46] Solidarität und Vertrauen sind aber notwendig, um jene „Defizite auszugleichen, die sich aus dem Prinzip der einzelstaatlichen und damit notwendigerweise territorial beschränkten Souveränität für eine Welt ergeben, die [aufgrund des Phänomens der grenzüberschreitenden Kriminalität, Anm. d. *Verf.*, auf] einen Abbau territorialer Schranken angewiesen ist."[47]

Umso besorgniserregender sind daher die folgenden Befürchtungen, die hochrangige ehemalige nationale Sicherheitsberater, Strafverfolger und Geheimdienstmitarbeiter in ihrer amicus curiae-Intervention vor dem US Supreme Court im Microsoft Ireland Case geäußert haben. Für den Fall, dass der Gerichtshof echte unilaterale Beibringungsanordnungen auf der Grundlage von 18 U.S. Code § 2703(a) für zulässig erachten sollte, wurde Folgendes an die Wand gemalt:

„We predict that such a ruling is likely to give rise to unintended consequences that will affect law enforcement and intelligence agencies, including the following:

- conflicting legal obligations across borders that compromise the effectiveness and efficiency of law enforcement and the international intelligence community;
- increasing balkanization of the Internet – a splintering of the World Wide Web via data localization, whether forced or voluntary – that may curtail international law enforcement and inhibit intelligence cooperation; and
- an impetus for nations to move away from multilateral cooperation and toward a go-it-alone unilateralism, diminishing the cooperation of law enforcement and intelligence agencies around the world.

These risks are particularly worrisome given the critical role cooperation plays in tackling modern cross-border crime and cyberthreats – dangers that did not exist, or were not as virulent, decades ago."[48]

Dem ist in der Sache nichts hinzufügen. Ergänzend mag man sich aber die Auswirkungen vorstellen, wenn europäische gegen US-Strafverfolger Strafverfahren einleiten müssten, weil letztere einen Diensteanbieter via einer US-Beibringungsanordnung zur Verletzung des europäisierten Datenschutzstrafrechts „angestiftet" haben.

b) Unechte unilaterale Beibringungsanordnungen betreffend Auslandsdaten mit Zustimmung des territorial betroffenen Staats

Nur vermeintlich einfacher einzuordnen sind die hier sog. unechten unilateralen Beibringungsanordnungen, die mit der vorherigen Zustimmung des Staates, in dem die Daten belegen sind, erfolgen. Einfach einzuordnen sind diese aber immerhin insofern, als zumindest kein völkerrechtliches Ungemach droht, rechtfertigt diese Zustimmung doch mögliche Eingriffe in die eigene Territorialhoheit.[49]

Auf den ersten Blick sehr elegant wirkt daher eine unionsrechtliche Vereinheitlichung solcher Beibringungsanordnungen für den Raum der Freiheit, der Sicherheit und des Rechts entsprechend der oben unter **Fehler! Verweisquelle konnte nicht gefunden werden.** aa) vorgestellten Notifikationslösung der Kommissionsdienste. Dieser Lösung zufolge würden die EU-Mitgliedstaaten einander Beibringungsanordnungen betreffend auf ihrem Territorium belegener Daten gestatten,[50] wenn und weil sie darüber im Nachgang notifiziert würden. Elegant scheint diese Notifikationslösung zum einen deshalb, weil sich dieses Programm auch für außereuropäische Drittstaaten öffnen ließe, zum anderen auch deswegen, weil die Souveränität bzw. Territorialhoheit der Staaten unangetastet bliebe. Ein vereinheitlichtes System mit notifikationspflichtigen Beibringungsanordnungen reformiert also scheinbar nur das überkommene Rechtshilfewesen, um es in einen modernen Informationsaustauschverbund unter partieller Inpflichtnahme Privater zu überführen.

Auf den zweiten Blick treten jedoch, soweit es um eine unionsrechtliche Regelung geht, (insbesondere grundrechtliche) Bedenken zutage. Eingedenk seiner grundrechtlichen Schutzpflichten gegenüber den Grundrechtsberechtigten kann der Zustimmungs- dem Zugriffsstaat dessen Beibringungsanordnungen nicht rechtsgrundlos gestatten; das gilt auch und gerade im Raum der Freiheit, der Sicherheit und des Rechts.[51]

[46] Weiterführend zu diesem Prinzip *Dahm*, Völkerrecht, Bd. 1, 2. Aufl. 2002, S. 851 ff. Eingängig auch die Worte von *Lord Russel* in Arton, [1896] 1 Q.B. 108, 111 nach denen es um das „broad priciple that it is to the interest of civilized communities that crimes […] should not go unpunished, and […] that one state should afford to another every assistance towards bringing persons guilty of such crimes to justice" geht.

[47] So allg. zum völkerrechtlichen Solidaritätsprinzip *Dahm* (Fn. 46), S. 856.

[48] Brief of former law enforcement, national security, and intelligence officials as amici curiae in support of neither party, S. 3 f., online verfügbar unter http://www.supremecourt.gov/DocketPDF/17/17-2/23633/20171213113332456_17-2%20Amicus%20Brief%20in%20Support%20of%20Neither%20Party.pdf (12.7.2018).

[49] Vgl. nur *Herdegen*, Völkerrecht, 16. Aufl. 2017, § 59 Rn. 1.

[50] Man beachte freilich: Während die Kommissionsdienste die „[Member] State[s] that could be affected by the investigative measure" entlang von Faktoren wie „seat of the service provider or the habitual residence of the target of the measure" (vgl. oben Teil 1 bei und in Fn. 54) zu bestimmen suchen, wird hier entsprechend dem oben unter 1. Gesagten (auch und entscheidend) für eine Bestimmung nach Maßgabe der territorialen Belegenheit der Daten geworben.

[51] Dies folgt für Deutschland aus seinen Grundrechtsverpflichtungen aus dem GG und der EMRK. Die Solange II-Rechtsprechung (BVerfGE 73, 339) und die Bosphorus-Rechtsprechung (EGMR, Urt. v. 30.6.2005 – Rs. 45036/98 [Bosphorus v. Ireland]) des EGMR besagen – natürlich mit Unterschieden im Detail – letztlich, dass unionsrechtliche Regelungen die Grund- und Menschenrechte des GG und der EMRK nicht ersetzen, sondern diese unter der Voraussetzung eines Äquivalenzvorbehalts suspendieren. Dies hat zur Folge,

Vielmehr muss ersterer letzterem grundrechtlich vertrauen (können). Dafür ist es notwendig, dass der Zugriffsstaat ein im Wesentlichen gleichwertiges Daten- und Grundrechtsschutzniveau verbürgt[52] und er überdies die Verfassungsidentität des Zustimmungsstaates achtet.[53] Wer nun unter Hinweis auf Art. 67 Abs. 1 AEUV behaupten wollte, dass all dies im Raum der Freiheit, der Sicherheit und des Rechts bereits Realität sei, der verkennt die Erkenntnis, die wir momentan in der EU mit dem Grundsatz der gegenseitigen Anerkennung machen. Und diese Erkenntnis lautet: Postuliertes Vertrauen ist gut, aber Kontrolle ist besser, um einen einheitlichen Grundrechts- und Datenschutzraum in Europa zu schaffen, in dem sich Hoheitsträger und Bürger wahrhaftig wechselseitig vertrauen können.[54]

Diese Erkenntnis muss auch in das soeben angedeutete System mit notifikationspflichtigen Beibringungsanordnungen einfließen. Deren gegenseitige Anerkennung (und um nichts anderes geht es in der Sache) darf nicht blindlings, sondern muss (ver-)bindend verlaufen. Sie muss grundrechtlich „gemanagt" werden können.[55] Daher darf die Notifikation nicht nur informationshalber erfolgen.[56] Vielmehr müssen nachträgliche Zustimmungsverweigerungs- bzw. -rücknahmegründe vorgesehen werden (wie die Verletzung des europäischen ordre public, analog Art. 11 Abs. 1 lit. f. RL-EEA; oder die Verletzung der nationalen Verfassungsidentität, Art. 4 Abs. 2 EUV; oder ein allgemeiner Missbrauchsvorbehalt). Wird von diesen Zustimmungsverweigerungsgründen Gebrauch gemacht, muss dies im Mindestmaß zur Unverwend- und Unverwertbarkeit der erhaltenen Clouddaten im Zugriffstaat führen.[57] Und um die besagten Zustimmungsverweigerungsgründe „mit Leben zu füllen", müssen sie (zumindest wo sie grundrechtlich aufgeladen sind) vom Nutzer durch Rechtsmittel etc. erzwingbar sein, was zur Voraussetzung hat, dass die Nutzer über entsprechende Zugriffe informiert werden. Auch das mag im ersten Zugriff „teuer"

dass die grundrechtliche, dem GG und der EMRK zu entnehmende Garantieverantwortung von Deutschland als ersuchtem bzw. gestattendem Staat im Kern fortbesteht. Hierzu im Einzelnen *Burchard*, Die Konstitutionalisierung der gegenseitigen Anerkennung, 2018 (im Erscheinen), § 7 D.; sowie allgemein *Scholz*, in: Maunz/Dürig, Grundgesetz, Kommentar, 82. Lfg., Stand: Januar 2018, Art. 23 Rn. 80 ff.; *Meyer-Ladewig/Nettesheim*, in: Meyer-Ladewig/Nettesheim/v. Raumer (Hrsg.), Europäische Menschenrechtskonvention, Kommentar, 4. Aufl. 2017, Art. 1 Rn. 14; *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Kommentar, 5. Aufl. 2016, Art. 6 EUV Rn. 23.

[52] Vgl. hierzu zunächst die in Fn. 51 aufgeführten Quellen und Ausführungen. Auch der EuGH hat nach langer Verzögerung klargestellt, dass zumindest systemische Grundrechtsdefizite in einem Mitgliedstaat es rechtfertigen, die justizielle Zusammenarbeit in Strafsachen mit ihm im Einzelfall zu verweigern. Hierzu EuGH, Urt. v. 5.4.2016 – C-404/15 und C-659/15 PPU (Aranyosi und Căldăraru), u.a. mit Anm. *Epiney*, NVwZ 2017, 761; *Brodowski*, JR 2016, 415; und *Satzger*, NStZ 2016, 514. Ähnliches hat der EuGH auch im Bereich des Datenschutzes festgestellt, vgl. EuGH, Urt. v. 6.10.2015 – C-362/14 (Maximillian Schrems v. Data Protection Commissioner), u.a mit Anm. *Kuner*, German Law Journal 2017, 881.

[53] Die Beachtung der Verfassungsidentität bei der justiziellen Zusammenarbeit in Strafsachen im Raum der Freiheit, der Sicherheit und des Rechts ist zum einen unionsverfassungsrechtlich aufgegeben (Art. 4 EUV) und folgt zum anderen nationalen verfassungsrechtlichen Vorgaben; dass dabei der Umfang, im welchem Ausmaße nationale Verfassungsidentitäten bzw. -traditionen bei der Zusammenarbeit in Strafsachen in der EU zu wahren ist, je nach Perspektive anders gesehen werden kann, sei hier nur notiert, nicht aber inhaltlich kommentiert. Zur unionsrechtlichen Perspektive u.a. *v. Bogdandy/Schill*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der Europäischen Union, 62. Lfg., Stand: Juli 2017, Art. 4 EUV Rn. 13 m.w.N. Zur Perspektive des GG BVerfG, NJW 2016, 1149, u.a. mit Anm. *Meyer*, HRRS 2016, 332; *Satzger*, NStZ 2016, 514; *Sauer*, NJW 2016, 1134. Allgemein zum Topos Verfassungsidentität die Sonderausgabe Nr. 7/2017 des German Law Journal (2017, 1587 ff.).

[54] Zum Topos Vertrauen bei der Zusammenarbeit in Strafsachen im Allgemeinen und in der EU im Besonderen *Vogel/Burchard* (Fn. 15), Vor § 1 IRG Rn. 130 ff. m.w.N. Zur Frage, ob gegenseitiges Vertrauen Grundlage der gegenseitigen Anerkennung justizieller Entscheidung nach Art. 82 AEUV ist bzw. sein soll oder gar ein unionsverfassungsrechtliches Rechtsprinzip ist, vgl. ein- und weiterführend *Meyer*, EuR 2017, 163. Ich selbst vertrete in *Vogel/Burchard* (Fn. 15), Vor § 1 IRG Rn. 133, dass der (vage) Topos des zwischenstaatlichen Vertrauens eine umfassende oder auch nur eine weitreichende Suspendierung der Grundrechtsprüfung im ersuchten Staat nicht zu begründen weiß; dies gilt auch im Verhältnis zu anderen EU-Mitgliedstaaten. Dekonstruiert man die hypertrophe Vertrauensrhetorik, so wird diese keinesfalls von der Erwartung oder Hoffnung in die tatsächliche Gleichwertigkeit fremder Kriminaljustizsysteme getragen, sondern von dem realpolitischen Motto: „Spuckst Du mir nicht in die Suppe, spucke auch ich Dir nicht in die Suppe!" Um den Preis des Verzichts auf die grundrechtliche Überprüfung eingehender Rechtshilfeersuchen wird also gleichsam die Immunisierung des eigenen Kriminaljustizsystems vor grundrechtlichen Fremdkontrollen bei ausgehenden Ersuchen erkauft. Dieser Deal kann jedoch die Grundrechtsbindungen staatlicher (deutscher) Hoheitsträger nicht außer Kraft setzen.

[55] Hierzu allgemein *Nicolaïdis*, Journal of European Public Policy 2007, 682 (683), und dies auf die justizielle Zusammenarbeit in Strafsachen detailliert übertragend *Burchard* (Fn. 51), § 8 D. IV. 2.

[56] Wie dies im Technical Document der Kommissionsdienste, S. 27, in den Raum gestellt wird. Online verfügbar unter https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf (12.7.2018).

[57] Oder in Drittstaaten, an die Daten weitergereicht wurden.

wirken. Aber nur so lässt sich sicherstellen, dass die Nutzer nicht zu Objekten degradiert, sondern als europäische Bürger ernst genommen werden.

IV. Zwischenstaatlichkeit als Problem und Privatisierung als Lösung?

Kann man also die Rechnung nicht ohne den Wirt machen – indem der nationalstaatliche Zugriff auf elektronische Beweismittel in der Cloud ohne die territoriale Belegenheit der Daten in einer anderen Jurisdiktion gedacht wird – und sind auch unilaterale grenzüberschreitende Ermittlungsmaßnahmen nicht ohne Weiteres machbar, so stellt sich nichtsdestoweniger die Frage, ob die Trägheit und Schwerfälligkeit des Zwischenstaatlichen in der international-arbeitsteiligen Strafverfolgung nicht durch eine (partielle) Privatisierung derselben überwindbar ist. Eben dadurch, dass das herkömmliche Rechtshilfeverfahren im ersuchten Staat (bzw. oder das Anerkennungsverfahren im Vollstreckungsstaat einer gegenseitig anzuerkennenden justiziellen Entscheidung im Raum der Freiheit, der Sicherheit und des Rechts) auf Private ausgelagert wird. Ist also Zwischenstaatlichkeit ein Problem und Privatisierung dessen Lösung? Um hierauf eine Antwort geben zu können (unten 2.), ist zunächst zu zeigen, welche Dimension dieses Outsourcing bereits rechtstatsächlich hat (unten 1.).

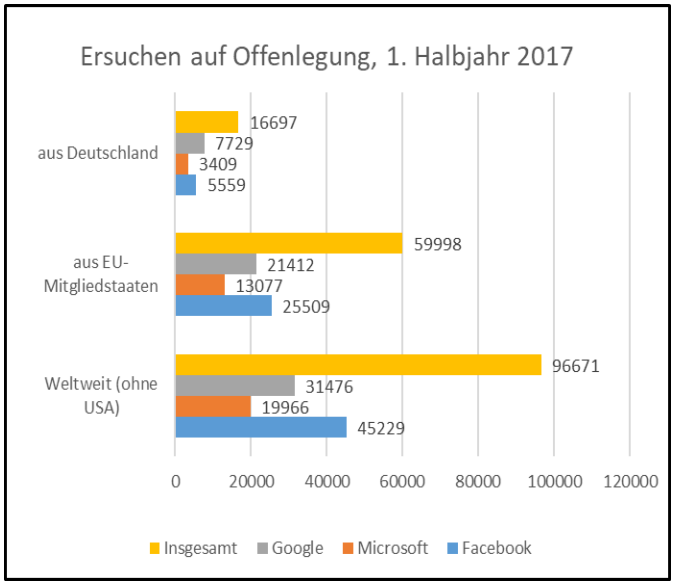
1. Vorweg: Eine summarische rechtstatsächliche Einordnung der freiwilligen Zusammenarbeit mit US-Diensteanbietern

Dass weltweit Strafverfolger private US-Diensteanbieter nach US-Recht (oben II. 2.) informell um die Beibringung von Nicht-Inhaltsdaten ersuchen dürfen, und dass dies in den Worten der Kommission paradigmatisch für ein neues Strafverfolgungskonzept im digitalen Zeitalter[58] stehen könnte, lässt nicht erahnen, wie fortgeschritten diese Zusammenarbeit mit dem privaten Sektor bereits ist. Daher seien hier vorweg einige rechtstatsächliche Einordnungen auf der Grundlage der aktuellen Transparenzberichte von Google,[59] Facebook (einschließlich WhatsApp und Instagram)[60] und Microsoft[61] vorgenommen.

a) Zahlen von Google, Facebook und Mircosoft für das erste Halbjahr 2017

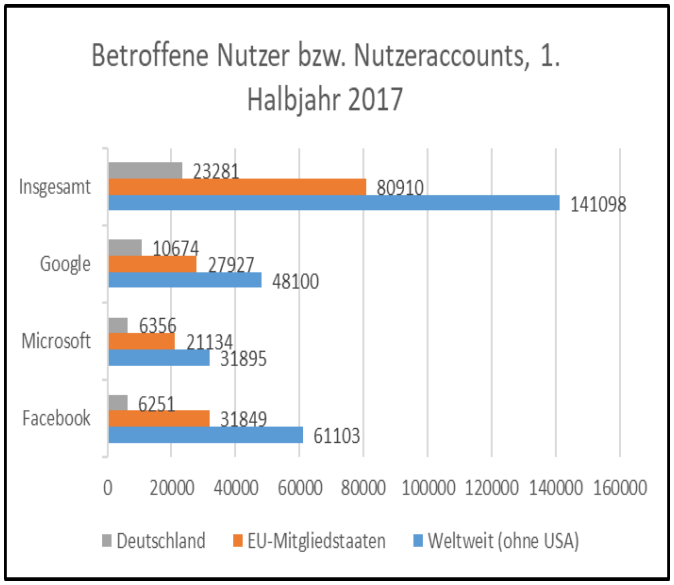
Zunächst zum Zahlenwerk.[62]

aa) Allein im ersten Halbjahr 2017 erreichten Google, Facebook und Microsoft 96.671 (sic) Ersuchen auf Offenlegung von Daten von außerhalb der USA, davon 59.998 aus EU-Mitgliedstaaten und 16.697 aus Deutschland. Weitere Diensteanbieter – wie Dropbox etc. – sind dabei gar nicht bedacht.

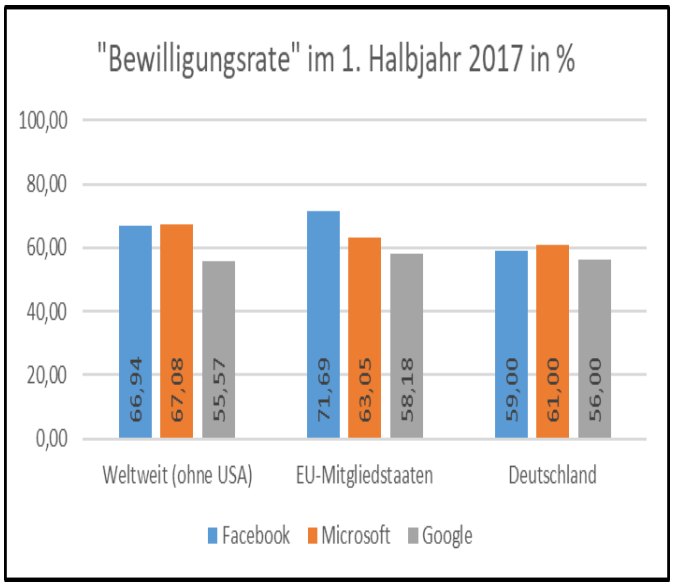


bb) Betroffen waren in diesem ersten Halbjahr bei den besagten Diensteanbietern insgesamt und weltweit nicht weniger als 141.098 Nutzer bzw. Nutzeraccounts. Die europäischen Ersuchen betrafen 80.910 und die deutschen Ersuchen 23.891 Nutzer bzw. Nutzeraccounts.

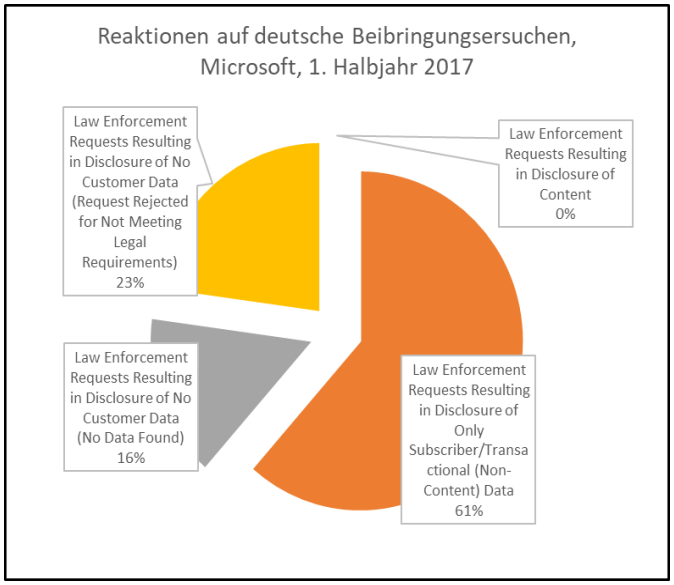
[58] Hierzu die Europäische Sicherheitsagenda, bei und in Teil 1 Fn. 29 (ZIS 2018, 194).
[59] Online verfügbar unter https://transparencyreport.google.com/user-data/overview?hl=de (12.7.2018).
[60] Online verfügbar unter https://transparency.facebook.com/government/ (12.7.2018).
[61] Online verfügbar unter https://www.microsoft.com/en-us/about/corporate-responsibility/lerr (12.7.2018).
[62] Ein kurzer Disclaimer: Die folgenden Zahlen sind empirisch lediglich richtungsweisend. Da die Erfassungsmodi der Diensteanbieter nicht harmonisiert sind, tun sich Unschärfen im Vergleich auf. Google und Facebook legen z.B. die Anzahl und Art von Auskunftsersuchen offen, die sie von Behörden erhalten haben. Ob dies in Strafsachen geschieht, ist damit nicht gesichert, wenn auch Facebook ausführt, dass sich die „überwiegende Mehrheit dieser Anfragen" auf strafrechtliche Fälle beziehe. Rechtshilfeersuchen werden bei Facebook ausdrücklich einbezogen. Microsoft legt demgegenüber offen, wie viele Ersuchen in Strafsachen eingegangen sind. Microsoft differenziert überdies nach der Offenlegung von Inhalts- und Nicht-Inhaltsdaten. Überdies zeigen sich auch Fehler in den Transparenzberichten im Detail. So führt etwa Facebook im herunterladbaren Zahlenmaterial lediglich 4,7 Auskunftsersuchen aus Frankreich im ersten Halbjahr 2017; gemeint sind aber 4.700 Ersuchen, wie eine Einzelsuche ergab. Die folgenden Zahlen umfassen auf Nutzerdaten bezogene Anfragen, jedoch keine Aufbewahrungsanfragen („preservation requests"). Bei den Google-Daten sind Notfallersuchen erfasst, bei den Microsoft-Daten hingegen nicht, was zu keinen signifikanten Verzerrungen führt, da nur wenige Notfallersuchen gestellt werden.



cc) Was die „Bewilligungsrate“ anbetrifft, also den Prozentsatz an Fällen, in denen die nachgesuchten Daten ganz oder teilweise offengelegt wurden, sticht Folgendes ins Auge: Europäische Ersuchen werden im weltweiten Durchschnitt nicht signifikant anders gehandhabt. Und Ersuchen aus Deutschland wird mitunter sogar weniger häufig nachgekommen als im europäischen oder gar weltweiten Durchschnitt.



dd) Die durchaus signifikant hohen Raten, in denen private Diensteanbieter Strafverfolgern keine Daten überlassen, lassen sich teilweise damit erklären, dass überhaupt keine Daten vorhanden sind; nach den einschlägigen Microsoft-Daten ist das etwa in gut 16 % der entsprechenden Ersuchen aus Deutschland der Fall. Dass in den übrigen Fällen keine Daten offengelegt werden, wird mit (quasi-)rechtlichen Bedenken begründet. Um abermals mit den Microsoft-Daten aus dem ersten Halbjahr 2017 zu arbeiten: Gut 22 % der deutschen Beibringungsersuchen sind statistisch mit „Request Rejected for Not Meeting Legal Requirements“ erfasst. Was damit gemeint ist, bleibt – zumal es keine empirischen Daten gibt[63] – ganz häufig unklar. Dies sorgt unter deutschen Strafverfolgern für beträchtliches Stirnrunzeln und erklärt aufs Ganze bezogen auch, warum im Rahmen der europäischen Expertenkonsultationen die Kritik laut wurde (hierzu oben I. 3. a) aa), dass die internen Prüfungsverfahren privater US-Diensteanbieter zu intransparent und unzuverlässig seien.



b) Das interne Prüfungsverfahren

In der Tat gibt es meines Wissens keine gesicherten empirischen Erkenntnisse, wie und nach welchen internen Verfahren freiwillige Beibringungsersuchen bei den großen US-Diensteanbietern abgearbeitet werden sowie mit welchen Problemen – außer den beträchtlichen Fallzahlen – sie dabei konfrontiert sind. Gesichert ist nur, dass eine Art interne Prüfung durch die Rechtsabteilung oder spezielle „Rechtshilfe“-Teams bzw. Abteilungen stattfindet.

Google beschreibt all dies sehr „selbstbewusst“ wie folgt:

„Wenn wir infolge behördlicher Ersuchen Daten offenlegen, ist es uns ein besonderes Anliegen, den Datenschutz und die Sicherheit der Daten, die Sie bei Google speichern, zu respektieren. Wenn wir ein solches Ersuchen erhalten, überprüft unsere Rechtsabteilung dieses, um sicherzugehen, dass es den gesetzlichen Anforderungen und den Richtlinien von Google entspricht. Für eine Offenlegung von Daten muss ein Ersuchen im Allgemeinen schriftlich erfolgen, von einem bevollmächtigten Beamten der Behörde, die das Ersuchen stellt, unterzeichnet und gemäß einem geltenden Gesetz aus-

[63] Anekdotisch berichtet wird z.B. über Anfragen durch deutsche Polizeibeamte, die um 23.00 Uhr deutscher Zeit von privaten Mailaccounts verschickt werden, so dass den Diensteanbietern keine Authentifizierung möglich ist. Für solche Schwierigkeiten gäbe es freilich technische Lösungen, wie digitale Signaturen.

gestellt sein. Falls wir der Ansicht sind, dass ein Ersuchen zu weit gefasst ist, versuchen wir, es einzugrenzen."[64]

Einen ähnlichen Anspruch formuliert Facebook:

„Wir setzen strenge Prozesse für den Umgang mit diesen Behördenanfragen ein. Jede Anfrage, die wir erhalten, wird auf rechtliche Hinlänglichkeit geprüft. Wir fordern von den VertreterInnen eine detaillierte Darlegung der rechtlichen und sachlichen Grundlagen ihrer Anfrage. Wir weisen diese ab, wenn wir Rechtsmängel oder eine übermäßig weit gefasste oder vage Informationsanforderung feststellen. Wir geben häufig nur allgemeine Nutzerinformationen heraus."[65]

Bemerkenswert ist schließlich, dass die Diensteanbieter „Richtlinien für Strafverfolgungsbehörden" ausgeben. Facebook gibt z.B. vor:

„Wir können keine allzu weitgefassten bzw. vagen Anfragen bearbeiten. Alle Anfragen müssen die angefragten Daten klar und deutlich benennen und Folgendes enthalten:

- Den Namen der ausstellenden Behörde, die Amts- bzw. Ausweisnummer des zuständigen Vertreters, die E-Mail-Adresse von einer Domain der Strafverfolgungsbehörde und eine Telefonnummer mit direkter Durchwahl.

- Die E-Mail-Adresse, die Nutzer-ID-Nummer […] oder den Nutzernamen […] des Facebook-Profils."[66]

2. Eine kritische Einordung der Privatisierung der Rechtshilfe

a) Primärrechtliches Verbot der umfassenden materiellen Privatisierung der Rechtshilfe

Diese Entwicklungen hin zu einer hochintensiven Zusammenarbeit europäischer und deutscher Strafverfolger mit US-Diensteanbietern, die selbstregulierend aktiv werden (müssen), muss aus deutscher und europäischer Sicht[67] die Grundlage für eine kritische Einordung des Ansinnens der Kommissionsdienste bilden, eingehende wie ausgehende Beibringungsmaßnahmen betreffend Auslandsdaten unionsrechtlich zu harmonisieren. Immerhin zielen die Kommissionsdienste auf Folgendes:

„Creating a competence for law enforcement/judicial authorities to issue cross-border production requests to service providers, and for service providers to reply to such production requests."

„Creating a competence for law enforcement / judicial authorities to issue mandatory cross-border production orders to service providers, and an obligation for service providers to reply to such requests" [68]

Diese Regelungsbestrebungen stellen sich aus der Perspektive des (so die herkömmliche Formulierung) ersuchten Staates als Privatisierung einer vormaligen Staatsaufgabe dar. Das US-Recht (hierzu oben II. 2.) illustriert diesen Wandel von Öffentlichkeit in aller Deutlichkeit: Für Beibringungsersuchen gegenüber US-Diensteanbietern betreffend Inhaltsdaten ist der Rechtshilfeweg zu beschreiten. Wird ein förmliches Rechtshilfeverfahren gestellt, wird dieses in den USA im Rahmen eines Rechtshilfeverfahren abgearbeitet, das materiellen (Stichwort: Rechtshilfevoraussetzungen und -hindernisse) wie formellen Regeln gehorcht. Für Beibringungsersuchen gegenüber US-Diensteanbietern betreffend Nicht-Inhaltsdaten stünde es den USA frei, ebenso zu verfahren. Das US-Recht begibt sich freilich dieser (potentiellen) Staatsaufgabe, Rechtshilfe betreffend Nicht-Inhaltdaten zu leisten, und delegiert es auf Private. Und da dies nicht weiter reguliert ist (man könnte gleichsam von eine Delegation ohne Regulation sprechen), liegt ein vollständiger Rückzug der USA aus der Erfüllungsverantwortung vor, sub specie der demokratischen, rechtsstaatlichen, grund- und datenschutzrechtlichen Schutzverantwortung, eingehende Ersuchen um Unterstützung fremder Strafverfolgung in demokratischer, rechtsstaatlicher, grund- und datenschutzrechtlicher Hinsicht zu überprüfen (z.B. im Hinblick darauf, ob das dem Ersuchen zugrundeliegende Strafverfahren dem eigenen ordre public entspricht, ob die ersuchende Stelle aktivlegitimiert ist und ob das Ersuchen überhaupt von einem Hoheitsträger einer anderen Jurisdiktion stammt).

Übertragen in den Unionsrechtsrahmen spricht Vieles dafür, dass ein sekundärrechtlich verfügter vollständiger Rückzug aus der rechtsstaatlichen und grundrechtlichen Erfüllungsverantwortung primärrechtlich (d.h. unionsverfassungsrechtlich) nicht tragen würde. Denn dies wäre weder mit dem Auftrag aus Art. 67 AEUV zu versöhnen, nach innen hin einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen, in dem die Grundrechte geachtet werden, noch mit dem vom EuGH unterstrichenen Anspruch vereinbar, dass es der EU verboten ist, nach außen hin den Schutz der europäischen Grundrechte auf dem Altar der internationalen Sicherheitszusammenarbeit zu opfern.[69] Anders ausgedrückt: Sollten die Kommissionsdienste eine umfassende Aufgabenprivatisierung der Rechtshilfe in dem Sinne zum Ziel haben, dass bei (bestimmten) Beibringungsersuchen keinerlei – auch parlamentarische – Kontrolle der Geschäfts- bzw. Erledigungspolitik eines Diensteanbieters mehr möglich ist,[70] so

[64] Siehe die FAQs über das Rechtsverfahren bei Auskunftsersuchen zu Nutzerdaten, online verfügbar unter https://support.google.com/transparencyreport/answer/7381738/ (12.7.2018).

[65] Online verfügbar unter https://transparency.facebook.com/government/about/ (12.7.2018).

[66] Online verfügbar unter https://www.facebook.com/safety/groups/law/guidelines/ (12.7.2018).

[67] Mir steht eine kritische Einordung aus der Sicht des US-Rechts, insbesondere des US-Datenschutzrechts nicht an.

[68] Technical Document (Fn. 56), S. 20 f.

[69] Vgl. hierzu nur die sog. Kadi-Rechtsprechung EuGH, Urt. v. 3.9.2008 – C-402/05 P und C-415/05 P (Kadi I), insbes. Rn. 360 ff.; Urt. v. 18.7.2013 – C-584/10 P, C-593/10 P und C-595/10 P (Kadi II), insbes. Rn. 125 ff. Zu den unzähligen Anmerkungen sei hier summarisch auf die Übersichten bei juris verwiesen.

[70] So die Konsequenz bei einer umfassenden Aufgabenprivatisierung, vgl. allgemein *Schmitz*, in: Stelkens/Bonk/Sachs

wäre dies nach hier zur Diskussion gestellter Ansicht primär- bzw. unionsverfassungsrechtswidrig.

b) „Kosten" der regulierten Privatisierung der Rechtshilfe, insbes. aufgrund des notwendig werdenden Privatisierungsfolgenrechts

Dies schließt freilich eine regulierte Aufgabenprivatisierung nicht eo ipso[71] aus, die durch steuernde und kontrollierende Rechtsvorschriften gelenkt wird. Dann müssen freilich die (insbesondere kriminalpolitischen) Kosten wohl bedacht werden.

Die kriminalpolitische Debatte rund um eine regulierte sowie kontrollierte Privatisierung des Zwischenstaatlichen der Rechtshilfe ist dabei in den Kontext der allgemeinen Debatte rund um die (wirtschaftlichen, politischen, rechtsstaatlichen etc.) Vor- und Nachteile der Privatisierung hoheitlicher Tätigkeiten zu stellen.[72] Dabei zeigen sich wenig erstaunliche Parallelen.

Die allgemeinen, häufig von einem tiefen Misstrauen gegen die (Modernisierungs- und Reform-)Kräfte des Staates getragenen Argumente *für* Privatisierung lauten insbesondere: Private arbeiten schneller, besser, flexibler und wirtschaftlicher; überdies sollte der Staat die Dynamik, Effizienz und Initiative privater Akteure für das Gemeinwohl nutzen. Entsprechend ließe sich für die unionsrechtliche Regelung der Zusammenarbeit mit privaten Diensteanbietern durch Beibringungsersuchen und -anordnungen kriminalpolitisch wie folgt argumentieren: Private Diensteanbieter haben die technische Kontrolle über die nachgesuchten elektronischen Beweismittel. Sie arbeiten schneller und günstiger (nämlich kostenlos!) als die (Justiz-)Behörden im herkömmlichen Rechtshilfeweg. Private können überdies schnell und unkompliziert auf die Vorstellungen und Wünsche von Strafverfolgern reagieren. Und da sie sich ständig neu erfinden müssen, um auf dem Markt zu bestehen, können sie die überkommenen Besitzstände des Rechtshilfeverfahrens ohne Weiteres hinter sich lassen. Das ist entscheidend, weil gerade diese Besitzstände den Rechtshilfeweg zu langwierig, komplex, unflexibel und schwergängig werden lassen und so einer modernen grenzüberschreitenden Strafverfolgung im digitalen Zeitalter entgegenstehen.

Umgekehrt wird *gegen* die Privatisierung von Staatsaufgaben im Allgemeinen Folgendes vorgebracht: Die Zuverlässigkeit der Aufgabenwahrnehmung und die Sozialverträglichkeit leidet, weil Private nicht das Gemeinwohl im Blick haben. Die Privatisierung staatlicher Tätigkeiten führt zu einer schädlichen Privatisierung des Öffentlichen, wodurch die regulative Idee politischer Verantwortung und der allgemeine Gemeinwohlgedanken Schaden nimmt. Entsprechend ließe sich abermals mit Blick auf die Privatisierung der Rechtshilfe vortragen: Der Grund- und Datenschutz bei der Rechtshilfe ist eine hehre Staatsaufgabe, die nicht an private Diensteanbieter delegiert werden darf. Eine Privatisierung darf weder rechtsstaatliche Verfahrensgrundsätze (Stichwort: kein rechtliches Gehör vor und keine Begründungspflichten für US-Diensteanbieter, die über eingehende Beibringungsersuchen betreffend Nicht-Inhaltsdaten entscheiden) noch grundlegende demokratische Prinzipien (Stichwort: nichtregulierte Selbstregulierung des internen Kontrollverfahrens durch US-Diensteanbieter bei besagten Ersuchen) desavouieren.

Unabhängig davon, wie man sich insofern kriminalpolitisch verhalten will (und dass ich eher letzterer Position anhänge, gebe ich gerne zu), haben Privatisierungsbefürworter die „Kosten" im Blick zu behalten, die durch ein Privatisierungsfolgenrecht verursacht werden, das notwendig wird, wenn und weil eine vollständige materielle Privatisierung der Rechtshilfe unzulässig ist:

Was *eingehende* Beibringungsersuchen bzw. -anordnungen anbetrifft, die also von europäischen Diensteanbietern zu erledigen wären (nach der hier entworfenen Konzeption, weil die Daten im territorialen Anwendungsbereich der DS-GVO sind), begäbe sich der vormals so bezeichnete ersuchte Staat seiner unmittelbaren Aufgabe, über ein Beweisrechtshilfeersuchen zu entscheiden, indem er diese Entscheidung einem Privaten gestattete; durch die Indienst- bzw. Inpflichtnahme eines Diensteanbieters wandelte sich der ersuchte zum gestattenden Staat. Da diese Gestattung nicht einem vollständigen Rückzug aus der Gewährleistungsverantwortung gleichkommen dürfte, bedürfte das interne Kontrollverfahren beim Diensteanbieter zunächst der (detaillierten) unionsrechtlichen Regulierung. Dabei wären auch rechtsstaatliche und strafverfahrensrechtliche Selbstverständlichkeiten (Beispielhaft: Anspruch auf rechtliches Gehör, außer der Untersuchungszweck wird gefährdet, Art. 47 GRC) in einen privatrechtlichen Kontext zu übersetzen. Da ausländische Strafrechtspflege stets in Grundrechtspositionen des Betroffenen einzugreifen droht, treffen den gestattenden Staat zudem Schutzpflichten. Die daraus folgende Gewährleistungsverantwortung zwänge daher dazu, ein adäquates System der „Kontrolle der Kontrolle" vorzuhalten; beispielhaft indem ein betroffener Staat über ein eingehendes Beibringungsersuchen notifiziert und ihm so die Möglichkeit gegeben würde, die (Nicht-)Bewilligung durch den privaten Diensteanbieter zu widerrufen oder zu beschränken. Schließlich müssten (insbes. Rechtsschutz-)Rechte, die der Nutzer als Bürger vormals gegen den ersuchten Staat hatte (z.B. der Rechtsschutz gegen oder auch auf die Vornahme einer Rechtshilfehandlung), auf solche gegen den Diensteanbieter übergeleitet oder als solche gegen den gestattenden Staat konzipiert werden. Kurz gesagt: So einfach, wie es sich die USA durch 18 U.S. Code § 2702 machen, kann man es sich auf EU-Ebene nicht machen. Die Regelung von eingehenden Beibringungsersuchen bzw. -anordnungen setzt als regulierte materielle Privatisierung der Rechtshilfe ein detailliertes Privatisierungsfolgenrecht voraus, das zu regeln politisch „teuer" würde.

(Hrsg.), Verwaltungsverfahrensgesetz, Kommentar, 9. Aufl. 2018, § 1 Rn. 130 m.w.N.

[71] Nicht weiter zu diskutieren ist, ob – analog der Privatisierung des Straf- und Maßregelvollzugs – bestimmte Kernfunktionen des Rechtshilfeverkehrs in staatlicher Hand bleiben müssen.

[72] Hierzu und zum Folgenden *Schmitz* (Fn. 70), § 1 Rn. 121 mit umfassenden Nachweisen.

Was *ausgehende* Beibringungsersuchen anbetrifft, mit denen z.B. US-Diensteanbieter um die freiwillige Beibringung von Auslandsdaten ersucht werden, darf die EU nicht die Augen davor verschließen, dass das oben entworfene rechtsstaatliche Programm im Ausland teilweise flagrant außer Acht gelassen wird. Daher gilt:[73] In dem Maße, in dem der ersuchte Diensteanbieter rechtsstaatlich prekär verfährt, müssen höhere Qualitäts- und Prüfungsmaßstäbe an die ausgehenden Zusammenarbeitsersuchen gestellt werden, um der transnationalen Fürsorgepflicht für die Nutzer zu genügen. Schon um der Mentalität zu begegnen, dass die zur Verfügung gestellten Daten freiwillig von Privaten beigebracht werden, und daher ohne Weiteres verwend- und verwertbar sind[74] – denn letzteres ist keineswegs gesichert.

c) Exkurs: Kompetenzrechtliche Schwierigkeiten i.R.v. Art. 82 AEUV

Abschließend sei noch kurz dazu Stellung genommen, dass die Kommissionsdienste für die Regelung von eingehenden wie ausgehenden Beibringungsersuchen bzw. -anordnungen blankettartig die Kompetenznorm des „Art. 82 AEUV“[75] ins Spiel gebracht haben, was etlichen kompetenzrechtlichen Sprengstoff birgt. Hierzu nur einige erste und tentative Überlegungen:

aa) Die Zusammenarbeit mit Privaten als Regelungsgegenstand des Art. 82 AEUV?

Erstens „passt“ für die Zusammenarbeit mit Privaten bei der grenzüberschreitenden Strafrechtspflege prima facie weder Art. 82 Abs. 1 noch Abs. 2 AEUV. Denn Art. 82 AEUV wird insgesamt vom traditionellen Leitmotiv der internationalarbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität getragen,[76] was sich schon aus der Kapitelüberschrift „Justizielle Zusammenarbeit in Strafsachen“ ergibt.[77] Dies ist der unmittelbare Regelungsgehalt des Abs. 1. Und die strafprozessualen Harmonisierungsmöglichkeiten nach Abs. 2 müssen u.a. die polizeiliche und justizielle Zusammenarbeit in Strafsachen mit grenzüberschreitender Dimension erleichtern.[78] Art. 82 AEUV scheint damit kaum geeignet, um das in der Europäischen Sicherheitsagenda geforderte, durch die Kooperation mit dem privaten Sektor zu erreichende neue Strafverfolgungskonzept im digitalen Zeitalter einlösen zu können.

Doch der Schein trügt. Die grenzüberschreitende Zusammenarbeit mit Privaten muss – allen sprachlichen Verwerfungen zum Trotz – dem Korpus der inter„nationalen“ Zusammenarbeit in Strafsachen subsumiert werden. Denn nur so kann das europäische Zusammenarbeitsrecht (das als Unterfall auch das internationale Strafprozessrecht, also das Strafprozessrecht mit grenzüberschreitenden Bezügen, mitumfasst)[79] seinem Schutz- und Regulierungsauftrag[80] und damit seinem Auftrag gerecht werden, einen einheitlichen, effektiven und grundrechtssichernden Strafverfolgungsraum in Europa zu errichten, der auf neue Herausforderungen (wie die Belegenheit elektronischer Beweismittel in einer durch private Dienstanbieter technisch kontrollierten Cloud) zu reagieren im Stande ist.[81]

Dies gilt umso mehr, als ein Rückgriff auf die Kompetenzen im Rahmen der operativen „polizeilichen Zusammenarbeit zwischen allen zuständigen Behörden der Mitgliedstaaten“ (eben nicht mit Privaten, vgl. Art. 87 Abs. 1 AEUV) ebenfalls nicht „passt“. Zudem ist ein wirtschaftsverwaltungsrechtlich begründeter Zugriff auf die allgemeinen Binnenmarktkompetenzen (arg.: Diensteanbieter, die im Binnenmarkt tätig sind, werden Zusammenarbeitspflichten aufgeben) zu verhindern. Ansonsten wären die spezifischen Garantien der justiziellen Zusammenarbeit in Strafsachen ohne Weiteres umgehbar.

bb) Die Regelung von ein- wie ausgehenden Beibringungsersuchen gemäß Art. 82 Abs. 1 oder Abs. 2 AEUV?

Doch selbst wenn damit der kompetenzrechtliche Zugang zu Art. 82 AEUV mit einigen teleologischen Verrenkungen eröffnet ist, stellt sich zweitens die Frage, ob die Regelung von ein- wie ausgehenden Beibringungsersuchen bzw. -anordnungen Abs. 1 oder Abs. 2 unterfällt.

Was eingehende Beibringungsersuchen bzw. -anordnungen von EU-Mitgliedstaaten anbetrifft, deren Erledigung privaten Diensteanbietern freigestellt bzw. verpflichtend aufgegeben wird, ist prima facie Art. 82 Abs. 1 UAbs. 2 lit. a oder d AEUV einschlägig. Die generelle Zustimmung des „ersuchten“ Mitgliedstaats hierzu müsste dann als gegenseitige Anerkennung einer justiziellen Entscheidung gedeutet werden (lit. a); alternativ müsste das „Outsourcing“ des Rechtshilfeverfahrens des ersuchten Staats auf private Diensteanbieter die justizielle Zusammenarbeit in Strafsachen beschleunigen und dadurch erleichtern (lit. d). Freilich betrifft Abs. 1 nur die Zusammenarbeit zwischen den EU-

[73] Zum Folgenden auch bereits programmatisch *Vogel/Burchard* (Fn. 15), Vor § 1 IRG Rn. 39.

[74] So dokumentiert in einem Bericht des Deutschlandfunks, abrufbar unter http://www.deutschlandfunk.de/online-ueberpruefung-potenzieller-straftaeter.862.de.html?dram:article_id=227768 (12.7.2018).

[75] So im Technical Document (Fn. 56), S. 18.

[76] So in der Sache *Böse*, in: Böse (Hrsg.), Enzyklopädie des Europarechts, Bd. 9, 2013, § 4 Rn. 27; *Schomburg/Lagodny/Schallmoser*, a.a.O., § 13 Rn. 76 ff.

[77] Dazu etwa *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der Europäischen Union, 62. Lfg., Stand: Juli 2017, Art. 82 AEUV Rn. 15.

[78] Vgl. nur *Vogel/Eisele* (Fn. 77), Art. 82 AEUV Rn. 95.

[79] Dazu eingehend *Vogel/Burchard* (Fn. 15), Vor § 1 IRG Rn. 88 ff.

[80] Hierzu *Vogel/Burchard* (Fn. 15), Vor § 1 IRG Rn. 39; ähnlich *Schomburg/Lagodny/Gleß/Hackner*, Internationale Rechtshilfe in Strafsachen, Einl. Rn. 150, die eine „[t]ransnationale Flucht in die Privatisierung“ befürchten.

[81] Ähnlich offen formuliert auch *Satzger*, in: Streinz (Hrsg.), EUV/AEUV, Kommentar, 3. Aufl. 2018, Art. 82 AEUV Rn. 1: „Art. 82 [AEUV] bildet die Grundlage für die Zusammenarbeit im Bereich der Strafverfolgung.“

Mitgliedstaaten, die als ersuchte (d.h. Rechtshilfe leistende) bzw. gestattende (d.h. die Rechtshilfeleistung auf Private delegierende) Staaten auftreten müssen. Beibringungsersuchen bzw. -anordnungen gegenüber außereuropäischen Diensteanbietern bzw. betreffend im EU-Ausland belegene Daten, wären somit vom Regelungsbereich eines nach Abs. 1 erlassenen Rechtsakts ausgenommen. Denn in diesem Fall obläge es einem Nicht-EU-Mitgliedstaat, die Erledigung von eingehenden Beibringungsersuchen bzw. -anordnungen einem Privaten zu delegieren. Da die entscheidenden Diensteanbieter (wie Google, Facebook oder Microsoft) ihren Hauptsitz in den USA haben bzw. nicht auszuschließen ist, dass Daten im EU-Ausland belegen sein werden, wäre eine Regelung von eingehenden Beibringungsersuchen bzw. -anordnungen gemäß Abs. 1 UAbs. 2 lit. a oder d wenig zielführend. Fernliegend ist es ferner auch, auf Art. 82 Abs. 1 UAbs. 2 lit. b zurückzugreifen. Treten nur EU-Mitgliedstaaten auf, namentlich als Ausstellungsstaaten von Beibringungsersuchen bzw. -anordnungen bzw. als deren Erledigung durch Private gestattende Staaten, so könnte eine unionsrechtliche Regelung zwar mit viel Phantasie[82] Kompetenzkonflikte zwischen den Mitgliedstaaten verhindern oder beilegen (darauf zielt lit. b). Damit wären aber abermals die wesentlichen Kompetenzkonflikte mit Nicht-EU-Mitgliedstaaten nicht beigelegt; im Gegenteil, solche Kompetenzkonflikte mit Nicht-EU-Mitgliedstaaten würden nachgerade provoziert (man stelle sich vor, das Unionsrecht setze die EU-Mitgliedstaten in den Stand, US-Diensteanbieter dazu zu verpflichten, 18 U.S. Code § 2703 zuwider Inhaltsdaten beizubringen).

Damit ist der Weg über Art. 82 Abs. 2 AEUV einzuschlagen. Dafür spricht, dass die Regelung von ausgehenden Beibringungsersuchen bzw. -anordnungen im Mittelpunkt stehen dürften und diese im Schwerpunkt strafprozessualer (und nicht rechtshilferechtlicher) Natur sind; und dass deren Harmonisierung zur Erleichterung (bzw. Ermöglichung) der polizeilichen und justiziellen Zusammenarbeit in Strafsachen erforderlich sein könnte (was nach Abs. 2 UAbs. 1 Voraussetzung strafprozessualer Harmonisierungsmaßnahmen ist). Diese Interpretation macht vom offenen Wortlaut des Abs. 2 UAbs. 1 Gebrauch, der gerade keine Erleichterung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten fordert,[83] sondern allgemeiner auf die Erleichterung der international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität abhebt.

cc) Die Einzelermächtigungen in Art. 82 Abs. 2 UAbs. 2 AEUV

Drittens stellt sich das Problem, welche konkrete Kompetenzgrundlage im Art. 82 Abs. 2 AEUV für welches konkrete Regelungsansinnen heranziehbar ist:

Was zunächst das Stellen von ausgehenden Beibringungsersuchen bzw. -anordungen durch europäische Strafverfolger anbetrifft, dürfte das Regelungsziel im Vordergrund stehen, dass durch Beibringungsmaßnahmen gewonnene Daten beweisrechtlich verwend- und verwertbar sein müssen. Das führt aber nicht zu Abs. 2 UAbs. 2 lit. a. Denn diese Vorschrift fokussiert „die Zulässigkeit von Beweismitteln auf gegenseitiger Basis zwischen den Mitgliedstaaten". Bei Beibringungsmaßnahmen gegenüber privaten Diensteanbietern dürfte aber auch die Zulässigkeit der von außereuropäischen Diensteanbietern bzw. der von aus dem Nicht-EU-Ausland beigebrachten elektronischen Beweismitteln im Vordergrund stehen. Es bleibt daher nur ein Rückgriff auf Abs. 2 UAbs. 2 lit. d – mit allen damit verbundenen politischen Kosten (Einstimmigkeitserfordernis im Rat etc.).

Im Hinblick auf eine Regelung, wonach – und unter welchen Voraussetzungen (z.B. analog der US-Regelung nur betreffend Nicht-Inhaltsdaten) – europäische Diensteanbieter außereuropäische Beibringungsersuchen erfüllen dürfen, kommt innerhalb des Art. 82 AEUV ebenfalls nur Abs. 2 UAbs. 2 lit. d als taugliche Kompetenznorm in Betracht. Abs. 2 UAbs. 2 lit. a scheitert ebenfalls daran, dass hier die Zulässigkeit von Beweismitteln zwischen den Mitgliedstaaten und nicht gegenüber dem Nicht-EU-Ausland gesichert werden soll. Ob es sich freilich bei der besagten Regelung um einen „sonstigen spezifischen Aspekt des Strafverfahrens" handelt, ist alles andere als klar. Es entscheidet sich an dem eigentlich für überwunden geglaubten (und gerade in Deutschland Ende des 20. Jahrhunderts erbittert geführten) Streit, ob die (hier nun teilweise privatisierte) Rechtshilfe Teil der Strafrechtspflege im (nach herkömmlicher Terminologie) ersuchten Staat ist.[84]

dd) Die Subsidiaritätshürde

Viertens und letztens ist auch die Subsidiaritätsfrage noch nicht entschieden. Ob eine Harmonisierung von eingehenden

[82] Zum „eigentlichen" Anwendungsbereich von Art. 82 Abs. 1 UAbs. 2 lit. b AEUV vgl. *Vogel/Eisele* (Fn. 77), Art. 82 AEUV Rn. 73: „Gemeint sind in erster Linie positive Kompetenzkonflikte, d.h. Situationen, in denen mehrere Mitgliedstaaten die Gerichtsbarkeit über dieselbe Tat derselben Person in Anspruch nehmen. Jedoch deckt der Wortlaut [der Vorschrift] auch negative Kompetenzkonflikte, bei denen ein oder mehrere Mitgliedstaaten jeweils die Gerichtsbarkeit über eine Tat einer Person nicht in Anspruch nehmen, sondern jeweils einen oder mehrere andere Mitgliedstaaten für zuständig halten." Im Kontext von grenzüberschreitenden Zugriffen auf die Cloud ginge es hingegen nicht um positive wie negative Straf-, sondern Kontrollgewaltkonflikte über Daten, über die der „ersuchte" Staat die Kontrolle beansprucht (z.B. weil die Daten im Inland belegen sind oder ein inländischer Diensteanbieter von einer Beibringungsmaßnahme eines anderen EU-Mitgliedstaats betroffen ist).

[83] Art. 82 Abs. 2 UAbs. 1 AEUV hingegen enger fassend *Vogel/Eisele* (Fn. 77), Art. 82 AEUV Rn. 95, die in systematischer Auslegung fordern, dass sich in „Zusammenarbeitspraxis der Mitgliedstaaten" strafprozessuale Defizite in den Mitgliedstaaten zeigen, die durch strafprozessuale Harmonisierungsmaßnahmen zu beheben sind.

[84] Zum historischen Streit zwischen der Rechtshilfe- und Rechtspflegetheorie *Vogel/Burchard* (Fn. 15), Vor § 1 IRG Rn. 75 f.

wie ausgehenden Beibringungsersuchen bzw. -anordnungen notwendig ist bzw. ob es nicht ausreichend ist, dass die Mitgliedstaaten über die Zulässigkeit solcher Maßnahmen national entscheiden, bemisst sich insbesondere danach, ob die Verwend- und Verwertbarkeit von entsprechend gewonnenen elektronischen Beweismitteln problematisch ist. Hierzu hatte das Non-Paper vom 7.12.2016 nur Folgendes behauptet: „Given that direct requests from law enforcement authorities in a EU Member State to service providers established elsewhere are not explicitly foreseen under most national laws of criminal procedure, there can be problems with the admissibility of evidence gathered through direct cooperation in a later criminal trial."[85] Wenn sich dies empirisch belegen ließe, spricht viel dafür, dass die Subsidiaritätshürde genommen wäre. Widrigenfalls spräche hingegen viel dafür, dass über die Brüsseler Bande gespielt wird, um nationale Widerstände gegen die weitreichende Einführung von eingehenden wie ausgehenden Beibringungsersuchen bzw. -anordnungen betreffend Auslandsdaten zu überwinden. Das wüsste freilich einen Harmonisierungsbedarf nach Art. 82 Abs. 2 AEUV nicht zu begründen.

V. Zusammenfassung in Kernthesen und Ausblick

Dieser Beitrag begann in Teil 1 mit dem Postulat, dass die Regelung des grenzüberschreitenden Zugriffs auf in der sog. Cloud gespeicherte Daten zu Strafverfolgungszwecken eine der drängendsten Aufgaben der Internetära ist. Dass eine solche Regelung bis dato noch nicht erfolgt ist, obwohl „die" Cloud seit vielen Jahren Realität ist, überrascht im Rückblick auf das Vorstehende nicht. Denn diese Regelung ist auch eine der komplexesten Aufgaben unserer Zeit. Die Effektivität der Strafverfolgung steht ebenso auf dem Spiel wie der Datenschutz in einem (offenen oder weiter zu fragmentierenden) World Wide Web. Hoheitliche Regulierungs- und Kontrollverantwortungen sind mit den wirtschaftlichen Interessen von transnational tätigen Anbietern von Cloud-Diensten zu praktischer Konkordanz zu bringen. Und legitime nationale Strafverfolgungs- kollidieren mit nationalen Schutz- bzw. Kontrollinteressen über im Inland belegene Daten. Zu allem Überfluss wird all dies noch unionsrechtlich überlagert und dadurch verkompliziert. Die Regelung des grenzüberschreitenden Zugriffs auf in der sog. Cloud gespeicherte Daten zu Strafverfolgungszwecken muss daher das Strafprozess-, Wirtschaftsverwaltungs- und Datenschutzrecht, das Rechtshilfe- bzw. Zusammenarbeitsrecht sowie das Staats-, Völker- und Unionsrecht im Auge behalten – und wird dementsprechend unübersichtlich.

Um dieses „Dickicht" etwas zu lichten, wurde hier dafür geworben, die etablierten Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen nicht vorschnell über Bord zu werfen. Der grenzüberschreitende Zugriff auf in der Cloud gespeicherte Daten muss also ausgehend von Territorialitätsprinzip, dem Prinzip der internationalen Solidarität bei der Verfolgung grenzüberschreitender Kriminalität und dem Prinzip des arbeitsteiligen Grund- und Menschenrechtsschutzes bei der Zusammenarbeit in strafrechtlichen Angelegenheiten gedacht werden. Das bedeutet konkret und mit wenigen Kernthesen zusammengefasst:

Nutzer sind nicht gleich Nutzer. Sie dürfen nicht allesamt als potentielle Kriminelle geführt werden. Und ihr datenschutzrechtliches Selbstbestimmungsrecht muss durch weitergehende Informationspflichten über die Speicherpolitiken von Diensteanbietern aktiviert werden (hierzu oben III. 1. b) bb) und III. 1. c).

Cloud ist nicht gleich Cloud. Die ausdrückliche und/oder gewollte Speicherung potentieller elektronischer Beweismittel an einem bestimmten Ort (z.B. in einer europäischen Niederlassung) darf nicht der „willkürlichen" (z.B. von Algorithmen bestimmten) Speicherung an irgendeinem Ort gleichgesetzt werden (hierzu oben III. 1. b).

Beim grenzüberschreitenden Zugriff auf in einer bestimmten Cloud gespeicherte elektronische Beweismittel hat das Territorialitätsprinzip noch nicht generell ausgedient. Denn dieses steht, modern gedacht, für die demokratische, rechtsstaatliche und grund- bzw. datenschutzrechtliche Garantieverantwortung des Staates, in dem Daten belegen sind, Datentransfers aus dem Inland zum Zwecke der Strafverfolgung im Ausland nicht blindlings geschehen zu lassen. Ein generelles Ende dieser Garantieverantwortung läutete das Ende von wechselseitigen, rechtsstaatlichen und grundrechtlichen Kontrollen bei der internationalen Zusammenarbeit in strafrechtlichen Angelegenheiten ein. Das ist abzulehnen (hierzu oben III. 1. b) aa).

Die Ersetzung des Territorialitäts- durch andere zuständigkeitsbegründende Prinzipien wie das Marktortprinzip führte konsequent zu Ende gedacht dazu, dass alle Clouddaten für alle Strafverfolger offen stünden. Auch das ist abzulehnen.

Die Ökonomisierung von Datenschutz und Datensicherheit führt dazu, dass rechtsstaatlich und grundrechtlich sichere Datenstandorte an Wert gewinnen. Das ist – schon zur Stärkung des Datenwirtschaftsstandorts Europa – zu unterstützen (hierzu oben III. 1. b) cc).

Eine Entterritorialisierung „der" Cloud verbreitet den Charme, die Schwerfälligkeit des Bi- oder Multilateralen (des Rechtshilfeverfahrens) durch die Leichtläufigkeit des Unilateralen (namentlich einseitig vollziehbarer strafprozessualer Zwangsmaßnahmen) zu ersetzen. Dies führte jedoch sowohl zu Jurisdiktionskonflikten, die auf dem Rücken von Diensteanbietern und Nutzern ausgetragen würden, wie auch zur einer allgemeinen Erosion der internationalen Solidarität bei der notwendigerweise international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität. Das ist kontraproduktiv (hierzu oben III. 2. a) bb) und cc).

Die Privatisierung der Zusammenarbeit in Strafsachen – durch die Inpflichtnahme transnational tätiger privater Diensteanbieter, unter ihrer technischen Kontrolle stehende Auslandsdaten beizubringen (Stichwort: Beibringungsanordnung bzw. „production order") – weist zwar einen Weg, um die internationale Zusammenarbeit in Strafsachen zu beschleunigen, indem das Rechtshilfeverfahren auf Private

[85] Non-Paper v. 7.12.2016, S. 10. Online abrufbar unter https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (12.7.2018).

ausgelagert wird. Da jedoch ein vollständiger Rückzug aus der rechtsstaatlichen und grundrechtlichen Erfüllungsverantwortung (unions-)verfassungsrechtlich nicht tunlich ist, müsste die materielle Privatisierung der Rechtshilfe mit einem Privatisierungsfolgenrecht abgefangen werden (hierzu oben IV. 2.).

Beherzigt man diese Kernthesen, ist der grenzüberschreitende Zugriff auf in der sog. Cloud gespeicherte Daten zu Strafverfolgungszwecken nicht nur eine drängende und komplexe, sondern auch eine weitgehend offene Regelungsaufgabe. Anstatt insofern an den (alles andere als perfekten, immerhin aber die derzeitige internationale Ordnung ausmachenden) Grundlagen der international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität zu rühren, sollten daher praktische Reformen (wie eine echte und sichere Vernetzung von europäischen und US-„Cyberermittlern") in den Blick genommen werden. Diese versprechen nachhaltigere und spürbarere Verbesserungen der internationalen Sicherheitszusammenarbeit als jene Neuerungen, die heute kriminalpolitisch en vogue sind.

Postskript: Eine summarische Bewertung des Kommissionsvorschlags für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (hier sog. VO-E EHSA)

Am 17.4.2018 legte die Kommission ihren VO-E EHSA vor.[86] Dieser wird im Folgenden im Weg eines sehr kurzen Postskripts im Lichte der vorstehenden Erwägungen summarisch kommentiert (und vornehmlich kritisiert):

1. Der VO-E EHSA will Regeln festlegen, nach denen eine Behörde eines Mitgliedstaats von einem Diensteanbieter, der in der Union Dienstleistungen anbietet, verlangen kann, elektronische Beweismittel herauszugeben (sog. Herausgabeanordnung) oder zu sichern (sog. Sicherungsanordnung), und zwar unabhängig davon, wo sich die Daten befinden (Art. 1 Abs. 1 VO-E EHSA). Terminologisch sollte man sich dadurch nicht täuschen lassen: Im Zentrum steht nicht die Verpflichtung zur bloßen Herausgabe (oder Sicherung) von Daten, die ein Diensteanbieter kontrolliert, sondern die Verpflichtung zum Transfer bzw. zur Beibringung etwaiger Auslandsdaten ins Unionsinland; die hier favorisierte deutsche Bezeichnung als Beibringungsanordnung wäre daher passender und ehrlicher (vgl. oben Teil 1, Einführung).

2. Der VO-E EHSA gründet auf der Annahme einer umfassenden Entterritorialisierung der Cloud.[87] Damit wird gegen das hier sog. Differenzierungsgebot bzw. Generalisierungsverbot verstoßen, weil „Cloud eben nicht gleich Cloud" ist (hierzu oben III. 1., insbes. unter b).

3. Der VO-E EHSA sieht im Territorialitätsprinzip (bei der Bestimmung der Belegenheit von Daten) ein Problem[88] und in einem qualifizierten Marktortprinzip die Lösung.[89] Entscheidend soll sein, dass ein zu verpflichtender Diensteanbieter in der EU seine Dienstleistungen anbietet (Erwägungsgrund 15, qualifiziert durch Erwägungsgrund 16, sowie Art. 3 Abs. 1 VO-E EHSA). Dann soll er zur Beibringung und Sicherung von Daten verpflichtet werden können, unabhängig davon, wo die Daten physisch gespeichert sind. Das ist ein echter Paradigmenwechsel in der grenzüberschreitenden Strafrechtspflege.[90]

a) Dagegen wurde u.a. oben erinnert: Sollte diese Abkehr vom Territorialitätsprinzip international noch weiter Schule machen[91] (wie es die USA mit dem CLOUD-Act nun auch vorexerziert haben; auch China denkt nun wohl darüber nach, gleichzuziehen, wie mir kürzlich berichtet wurde),[92] so wäre dies de facto das Ende eines auch territorial verankerten Datenschutzes. Denn es gälte dann: If every country asserts extraterritorial jurisdiction, then everybody gets everybody's data (vgl. oben III. 1.). Überdies droht eine Unilateralisierung der grenzüberschreitenden Strafverfolgung in der Cloud (vermittels unilateraler Beibringungsanordnungen) die internationale Solidarität bei der international-arbeitsteiligen Strafverfolgung grenzüberschreitender Kriminalität zu erodieren (vgl. oben III. 2., insbesondere a) cc).

[86] 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 (12.7.2018) und http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN (12.7.2018).

[87] Vgl. COM(2018) 225 final, S. 1 („Das Internet kennt keine Grenzen.") und S. 2 („Volatilität elektronischer Beweismittel").

[88] Vgl. COM(2018) 225 final, S. 15 („Die Verordnung bewegt sich auch weg vom Datenort als einem entscheidenden Anknüpfungspunkt.").

[89] Dem pflichtet bei BR-Drs. 215/18 v. 6.7.2018, S. 2 („Die damit verbundene Abkehr vom Territorialitätsprinzip bedeutet zwar einen Verzicht auf das Kriterium des Speicherorts der Daten. Dieses weist angesichts der Natur der Daten mit ihrer großen Mobilität und Volatilität aber ohnehin einen hohen Grad an Beliebigkeit auf.").

[90] BR-Drs. 215/18 v. 6.7.2018, S. 2, spricht von einem „Novum".

[91] Dies nunmehr auch befürchtend BR-Drs. 215/18 v. 6.7.2018, S. 10 f.

[92] Die Ausführungen in COM(2018) 225 final, S. 1, lassen vermuten, dass sich die Kommission ein Stück weit durch die internationalen wie auch die inner-europäischen Entwicklungen getrieben sah. Die EU soll es scheinbar jenen Staaten, die bereits unilaterale Beibringungsanordnungen kennen (USA, Brasilien, Belgien; vgl. die Nachweise in der Einführung), gleichtun. Eine selbstbewusste bzw. eigenständige europäische Kriminalpolitik sieht freilich anders aus.

b) Dass der Ansatz des VO-E EHSA zu Jurisdiktionskonflikten führen würde (hierzu oben III. 2. a), soll dadurch abgefangen werden, dass verpflichteten Diensteanbietern Rechtsbehelfe zustehen, wenn sie sich widersprechenden Verpflichtungen aus unterschiedlichen Rechtsordnungen ausgesetzt sehen (z.B. unionsrechtliche Beibringungsverpflichtung vs. US-rechtliches Beibringungsverbot, Art. 15 f. VO-E EHSA). Das ist, in der Binnenlogik gedacht, der Sache nach zu begrüßen. Die Zukunft wird weisen, ob damit den Interessen und Grundrechten der betroffenen Diensteanbieter hinreichend Rechnung getragen werden kann.

4. Der VO-E EHSA zielt auf eine weitreichende Privatisierung des klassischen Rechtshilfesystems (hierzu krit. oben IV.). Private Diensteanbieter[93] werden als die originären – und direkten – Adressaten von Beibringungs- (bzw. Sicherungs-) Anordnungen gehandelt (Art. 7 Abs. 1 VO-E EHSA).[94] Diese haben eine (oberflächliche) Rechtskontrolle durchzuführen (Art. 9 VO-E EHSA). U.a. ist vonseiten der Diensteanbieter zu prüfen, ob eine Beibringungsanordnung vollständig ist, keine offensichtlichen Fehler aufweist und die ausreichenden Informationen enthält (Art. 9 Abs. 2 VO-E EHSA).

a) Überaus modern wirkt der VO-E EHSA in Art. 9 Abs. 5 UAbs. 2, wird dort doch sowohl der Ablehnungsgrund des Verstoßes gegen den europäischen ordre public wie auch ein – wofür die Kommission im höchsten Maße zu loben ist – allgemeiner Missbrauchsvorbehalt eingeführt. Freilich sind die diesbezüglichen Prüfungsmöglichkeiten[95] der Diensteanbieter sehr begrenzt, darf ein etwaiger Grundrechtsverstoß oder Missbrauch doch ausschließlich auf der Grundlage der in der Beibringungsanordnung enthaltenen Informationen geprüft werden. Die Praxis rund um den Europäischen Haftbefehlt lehrt freilich, dass gerade „interessant" und wichtig ist, was nicht in den Formularen etc. steht. Art. 9 Abs. 5 UAbs. 2 VO-E EHSA lässt den europäischen ordre public- und den allgemeinen Missbrauchsvorbehalt damit zum zahnlosen Tiger verkümmern. Die Idee eines gemeinsamen Grundrechtsraums, in dem die europäischen Grundrechte eingehalten werden sollen, was durch gegenseitige Kontrollen in der justiziellen Zusammenarbeit in Strafsachen gesichert wird, kann so nicht befördert werden (hierzu bereits oben III. 2. b).

b) Noch grundsätzlicher ist zu kritisieren, dass der VO-E EHSA das mit der Privatisierung der Rechtshilfe notwendig werdende Privatisierungsfolgenrecht (hierzu oben IV. 2. b) nicht hinreichend abbildet und so gegen das hier zur Diskussion gestellte primärrechtliche Verbot der umfassenden materiellen Privatisierung der Rechtshilfe (hierzu oben IV. 2. a) zu verstoßen droht. Zu kritisieren ist namentlich, dass der VO-E EHSA keine hinreichende Kontrolle der Kontrolle vorsieht (also die vom sog. Vollstreckungsstaat zu verbürgende Kontrolle, dass die von ihm zu verantwortenden Diensteanbieter, die z.B. im Inland eine Niederlassung haben, eingehende Beibringungsanordnungen auch wirklich hinreichend im Hinblick auf die Einhaltung von Grund- und Menschenrechten kontrollieren bzw. kontrollieren können). Momentan sieht Art. 9 Abs. 5 UAbs. 2 VO-E EHSA lediglich vor, dass die Diensteanbieter grundrechtliche etc. Bedenken „ihrem" jeweiligen Vollstreckungsstaat melden können. Freilich ist zu fordern: Ob dies auch wirklich erfolgt und ob Diensteanbieter sich z.B. grundrechtlich hinreichend sensibilisiert zeigen (was nicht zwingend gesagt ist, da Diensteanbieter nicht die natürlichen Garanten der Grund- und Menschenrechte ihrer Nutzer sind), muss der Vollstreckungsstaat, der sich seiner rechtshilferechtlichen Prüfung eingehender Beibringungsanordnungen begibt, zu prüfen in der Lage sein. Dieser Forderung genügt der VO-E EHSA nicht.

Das ist umso bedenklicher, weil der VO-E EHSA sich mit dem Standardtextbaustein begnügt, dass Betroffenen, deren Daten im Wege einer Europäischen Herausgabeanordnung[96]

[93] *Brodowski*, NJW-aktuell 26/2018, 14, stellt in den Raum, dass der Vorschlag der Kommission auf große Dienstleister abzielt, aber auch all „jene Vereine, Kanzleien, Kleinunternehmen und Privatpersonen, die auf einem Server eine eigene kleine ‚Cloud' oder einen E-Mail-Server mit mehreren Nutzern betreiben", betrifft. Und in der Tat lässt sich Art. 4 Abs. 2 VO-E EHSA derart expansiv auslegen. Erwägungsgrund 27 indiziert freilich, dass eine engere Auslegung „im Sinne des Erfinders" ist (was freilich auch im eigentlichen Verordnungstext klargestellt werden sollte), heißt es doch dort, dass „die bloße Zugänglichkeit einer Online-Schnittstelle, beispielsweise die Zugänglichkeit der Website des Diensteanbieters oder eines Vermittlers, einer E-Mail-Adresse oder anderer Kontaktdaten in einem oder mehreren Mitgliedstaaten, für sich genommen keine ausreichende Voraussetzung für die Anwendung dieser Verordnung sein" sollte.

[94] Art. 7 VO-E EHSA behilft sich des Tricks, dass die Adressierung in der Regel (Abs. 1) an einen benannten Vertreter eines Diensteanbieters erfolgt. Der komplementäre Vorschlag über eine Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (Fn. 86) will die diesbezüglichen Regeln für die Vertreterbestimmung unionsweit harmonisieren. Was damit gewollt ist, liegt auf der Hand: Diensteanbieter sollen persönliche Ansprechpartner zur Verfügung stellen, gegen die im (Not-)Fall der Nichtbefolgung auch Druck ausgeübt werden kann. Vorbild hierfür ist das deutsche Netzwerkdurchsetzungsgesetz.

[95] Die Kommission spielt die grundrechtlichen etc. Prüfungen der Diensteanbieter in ihrer Bedeutung herunter. Und gerade kleinere Diensteanbieter sehen sich anekdotischen Berichten zufolge überdies außer Stande, solche Prüfungen konsequent durchzuführen. Es stellt sich damit die Frage, was Art. 9 Abs. 5 UAbs. 2 VO-E EHSA eigentlich ist (Prüfungsrecht, -pflicht, -obliegenheit, -möglichkeit?). Denn: Augenwischerei darf die Norm in diesem sensiblen Bereich auf keinen Fall betreiben!

[96] Für Sicherungsanordnungen soll das laut COM(2018) 225 final, S. 26, nicht gelten. Damit übersieht die VO-E EHSA das Konzept des präventiven Rechtsschutzes bzw. des Zulassungsrechtschutzes. Also den Rechtsschutz davor, dass gesi-

eingeholt wurden, allein das Recht zustehen soll, während des Strafverfahrens, für das die Anordnung erlassen wurde, wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen. Der VO-E EHSA verweist die Betroffenen hier also (für die Mitgliedstaaten „minimalinvasiv") auf die bestehenden Rechtsschutzsysteme im Anordnungsmitgliedstaat. Damit wird dem Betroffenen der herkömmliche, ohnehin schon schwach ausgeprägte rechtshilferechtliche Rechtsschutz im Vollstreckungsmitgliedstaat genommen. Auch gesonderte Informationspflichten, z.B. dass der Diensteanbieter seinen Kunden über den Eingang und die Bearbeitung einer Beibringungsanordnung aufzuklären habe, finden sich in der VO-E EHSA nicht.

c) Die Defizite im grenzüberschreitenden Rechtsschutzsystem zeigen sich gerade mit Blick auf die Garantie von Immunitäten und Vorrechten, etwa für das Recht auf Vertraulichkeit der Kommunikation zwischen Anwalt und Mandant.[97] Hierzu wollen Art. 5 Abs. 7, 18 VO-E EHSA zwar gewährleisten, dass – um die Kommissionsbegründung zu zitieren – „die Immunitäten und Vorrechte, die die im Mitgliedstaat des Diensteanbieters angeforderten Daten schützen, im Anordnungsstaat berücksichtigt werden, insbesondere, wenn zwischen diesen Mitgliedstaaten Unterschiede bestehen und es um grundlegende Interessen dieses Mitgliedstaats wie nationale Sicherheit und Verteidigung geht. Nach Artikel 18 muss das Gericht im Anordnungsstaat diese so berücksichtigen, als wären sie im nationalen Recht vorgesehen. Wegen der Unterschiede zwischen Mitgliedstaaten bei der Bewertung der Relevanz und Zulässigkeit von Beweismitteln gewährt die Bestimmung den Gerichten Flexibilität, wie dem Rechnung zu tragen ist."[98] Damit droht freilich der „Bock zum Gärtner" gemacht zu werden, weil die Gewährleistung der vollstreckungsstaatlichen Immunitäten und Vorrechte allein dem Anordnungsstaat übertragen wird (z.B. indem einer deutschen Beibringungsanordnung die Berücksichtigung des Schutzes der Verteidigerkommunikation in Bulgarien überantwortet wird, wenn und weil der angegangene Diensteanbieter seine Niederlassung eben dort hat). Das weiß so nicht zu überzeugen. Der VO-E EHSA gesteht den Betroffenen keine zureichenden Beteiligungsrechte zu. Überdies bräche der Vollstreckungsstaat als möglicher, auch politisch starker Garant „seiner" Immunitäten und Vorrechte weg.

d) Plakativ zusammengefasst: Soweit der VO-E EHSA mit der Privatisierung der Rechtshilfe auch eine „Privatisierung des Grundrechtsschutzes"[99] im Sinne hat,[100] bedürfte es allemal eines starken Privatisierungsfolgenrechts, da eine vollständige Privatisierung des inländischen Grundrechtsschutzes in grenzüberschreitenden Strafsachen nicht angeht. Sofern gar – allemal faktisch (siehe in Fn. 91) – eine Ausschaltung des inländischen Grundrechtsschutzes droht, weil Diensteanbieter nicht willens oder in der Lage sind, die Grundrechtspositionen ihrer Nutzer zu schützen, wäre dies kaum mit dem verfassungsrechtlichen Anspruch der Mitgliedstaaten vereinbar, ihre Hand nicht blindlings zu jeder, d.h. potentiell auch grundrechtsverletzenden Strafverfolgung im (EU-)Ausland zu reichen. Für Deutschland bedeutete das: Karlsruhe würde aktiv werden müssen (und ggf. auch aus anderen als grundrechtsschützenden Gründen aktiv werden wollen).

6. Waren die bisherigen Erwägungen im Wesentlichen rechtspolitischer Natur, sei zu guter Letzt noch kompetenzrechtliche Kritik am Ansinnen der Kommission geäußert, die VOEHSA als Verordnung auf der Grundlage des Art. 82 Abs. 1 AEUV[101] zu erlassen (vgl. auch die allg. kompetenzrechtlichen Ausführungen unter IV. 2. c). Hierzu dreierlei:

a) Erstens betritt die Kommission Neuland, wenn sie Maßnahmen der justiziellen Zusammenarbeit in Strafsachen im Verordnungsweg regeln will. Bis dato wurde – z.B. bei der RL-EEA – im Richtlinienwege verfahren.[102] Die Kommission will den Mitgliedstaaten nun aber jeden Ermessensspielraum bei der Umsetzung nehmen. Warum dies der Fall ist, wird nicht mitgeteilt. Es steht zu vermuten, dass die Kommission „Zähne" zeigen und die Mitgliedstaaten in ihre Schranken weisen will. Das scheint auf den ersten Blick politisch unklug. Sollte dies aber, wovon auszugehen ist, mit den relevanten Mitgliedstaaten abgestimmt sein, so nährt dies die oben geäußerte Vermutung (vgl. IV. 2. c) cc), dass auch vonseiten dieser Mitgliedstaaten über die Brüsseler Bande gespielt werden soll, um innenpolitische Widerstände zu überwinden. Das wäre europa- und rechtspolitisch prekär, weil so die europäische Idee Schaden zu nehmen droht.

b) Zweitens überzeugt Art. 82 Abs. 1 AEUV nicht als Kompetenzgrundlage für den VO-E EHSA, u.a. weil der VO-E EHSA in der Binnenlogik gedacht nicht weitreichend genug ist. Wie Erwägungsgrund 15 – konsequent – klarstellt, kann ein auf die justizielle Zusammenarbeit in Strafsachen zielender Rechtsakt für rein innerstaatliche Sachverhalte nicht gelten; z.B. wenn inländische Strafverfolger von im Inland sitzenden oder ihre Niederlassung habenden Diensteanbietern Auslandsdaten anfordern.[103] Damit droht aber ent-

cherte und alsbald herauszugebende Daten überhaupt Eingang in ein Strafverfahren finden.

[97] Kritisch nunmehr auch BR-Drs. 215/18 v. 6.7.2018, S. 5.

[98] COM(2018) 225 final, S. 27.

[99] So plakativ *Brodowski*, NJW-aktuell 26/2018, 14.

[100] Kritisch nunmehr auch BR-Drs. 215/18 v. 6.7.2018, S. 6.

[101] COM(2018) 225 final, insbes. S. 6, spricht nur von Art. 82 Abs. 1 AEUV und geht nicht auf die einzelnen Kompetenznormen in UAbs. 2 ein.

[102] Dass Verordnungen auch bei der justiziellen Zusammenarbeit in Strafsachen „in Mode kommen", zeigt u.a. der nunmehr erzielte Kompromiss über das Proposal for a Regulation of the European Parliament and of the Council on the mutual recognition of freezing and confiscation orders v. 18.6.2018, Ratsdok. 10114/18.

[103] Erwägungsgrund 15 VO-E EHSA lautet auszugsweise: „Diese Verordnung gilt in allen Fällen, in denen der Diensteanbieter in einem anderen Mitgliedstaat niedergelassen oder vertreten ist. In rein innerstaatlichen Fällen, in denen die in dieser Verordnung genannten Instrumente nicht verwendet werden können, sollte die Verordnung die bereits in den nationalen Rechtsvorschriften vorgesehenen Befugnisse der zuständigen nationalen Behörden, Diensteanbieter, die in

weder die Rechtszersplitterung in der EU erhalten zu bleiben (hierzu oben I. 3. a), weil nicht gesagt ist, dass die Mitgliedstaaten innerstaatlich nachziehen; dies konterkarierte die Verhältnismäßigkeit der VO-E EHSA. Alternativ – und wahrscheinlicher – zielt der VO-E EHSA aber gerade darauf, dass die Mitgliedstaaten innerstaatlich nachziehen. Dann wird aber der Sache nach eine Harmonisierung des Strafprozessprozessrechts der Mitgliedstaten angestrebt, für die Art. 82 Abs. 2 AEUV gilt. Der „Umweg" über die indirekte Harmonisierung nach Art. 82 Abs. 1 AEUV stellte sich dann als Umgehung der engeren Voraussetzungen des Abs. 2 dar (u.a. deswegen wurde auch oben dafür geworben, in Art. 82 Abs. 2 AEUV die richtige Kompetenznorm zu sehen; vgl. IV. 2. c) bb).

c) Drittens weiß auch die positive Kommissionsbegründung, warum Art. 82 Abs. 1 AEUV einschlägig sein soll, nicht zu überzeugen.[104] Namentlich macht die Kommission geltend, eine Europäische Herausgabe- oder Sicherungsanordnung könne zum Tätigwerden einer Justizbehörde des Vollstreckungsstaats führen, wenn dies zur Vollstreckung der Entscheidung notwendig würde,[105] wenn und weil der Diensteanbieter die Kooperation (unzulässig) verweigert. Damit wird freilich das „Pferd von hinten aufgesattelt". Daraus, dass möglicherweise in Zukunft ein Vollstreckungsstaat gegen einen in seinem Inland tätigen Diensteanbieter aktiv werden muss (z.B. indem gegen den die Kooperation verweigernden Diensteanbieter Sanktionen verhängt werden, Art. 13 f. VO-E EHSA), kann nicht folgen, dass die direkte Interaktion zwischen dem Ausstellungsmitgliedstaat und dem Diensteanbieter ein Fall der gegenseitigen Anerkennung justizieller Entscheidungen in Strafsachen ist und damit Art. 82 Abs. 1 AEUV unterfällt (zu einer alternativen, jedoch ebenfalls nicht durchdringenden Argumentation vgl. oben IV. 2. c) bb).

Wenn überhaupt müsste das Verfahren in der Kommissionslogik kompetenzrechtlich zweigeteilt werden: Art. 82 Abs. 2 AEUV erlaubt die strafprozessuale Harmonisierung von (zwischen- wie innerstaatlichen) Beibringungsanordnungen. Und im Wege der gegenseitigen Anerkennung ist zu regeln, dass und wie die Sitz- bzw. Niederlassungsstaaten von Diensteanbieter deren Sanktionierung vornehmen, wenn letztere die Kooperation verweigern. Dabei ist keineswegs gesagt, dass diese gegenseitig anzuerkennende Sanktionierung strafrechtlicher „Natur" sein muss. Nach Art. 13 VO-E EHSA sollen nämlich nationale Rechtsvorschriften, die die Verhängung strafrechtlicher Sanktionen vorsehen, unberührt bleiben; und sollen die Sanktionen gegen widerspenstige Diensteanbieter lediglich „wirksam, verhältnismäßig und abschreckend sein", was im unionsrechtlichen Jargon die Einordung als straf-, verwaltungs- oder zivilrechtliche Sanktion offenlässt.

7. Die zuvor geübte kompetenzrechtliche Kritik lenkt den Blick auf die strafprozessualen Defizite des VO-E EHSA. Während bei Art. 82 Abs. 1 AEUV die Regelungen der strafprozessualen Voraussetzungen der anzuerkennenden Maßnahmen „naturgemäß" schwach ausfallen, müsste hierzu beim eigentlich gebotenen Zugriff auf Art. 82 Abs. 2 AEUV deutlich nachgebessert werden. Anzumahnen ist etwa eine detaillierte Regelung, auf welcher Informationsgrundlage eine Beibringungsanordnung für welche Daten(typen) erlassbar ist. Reicht etwa die kriminalistische Erfahrung, dass jüngere Mitbürger regelmäßig in sozialen Netzwerken aktiv sind, um eine „fishing expedition" zu starten? Diese – nur vordergründig überzeichnete – Frage wird durch die allgemeine Regelung in Art. 3 Abs. 2 VO-E EHSA, wonach eine Europäische Herausgabeanordnung für die Zwecke eines Verfahrens „notwendig und verhältnismäßig" sein muss, nicht hinreichend klar beantwortet. Auch zu weiteren wichtigen strafprozessualen Garantien findet sich in der VO-E EHSA wenig bis nichts. Man denke an die Waffengleichheit (Unter welchen Voraussetzungen kann die Verteidigung Beibringungsanordnungen verlangen?) oder an den effektiven Rechtsschutz im Ausstellungsstaat (Wie und wann werden Betroffene über sie betreffende Beibringungsanordnungen informiert? Wie können sie sich ex ante oder ex post dagegen wehren? Wie können sie insbesondere ex post erreichen, dass rechtswidrig erlangte Informationen nicht verwendet oder verwertet werden?).

8. Trotz aller Kritik darf abschließend nicht unerwähnt bleiben, dass der Kommissionsvorschlag wichtige Impulse für eine profunde Diskussion über den Grund und die Grenzen des grenzüberschreitenden Zugriffs auf Clouddaten in Europa enthält. Meine Kritik ist so gesehen „Teil des Systems" der europäischen Kriminal- und Justizpolitik. Diese ist nun gehalten, den grenzüberschreitenden Zugang zu elektronischen Beweismitteln im Strafermittlungsverfahren unter Berücksichtigung aller konfligierender Belange rasch zu regeln. Auch und gerade angesichts des unilateralen Vorpreschens von Mitglieds- und von Drittstaaten muss sich „Europa" dabei fragen, ob es eigene Wege (z.B. in Abgrenzung zum CLOUD-Act) gehen und damit die Fundamentalprinzipien der internationalen (Sicherheits-)Ordnung erhalten will.

Abschließend muss daher dem Bundesrat Beifall gespendet werden, der sich wie folgt zum VO-E EHSA positioniert hat: „Erforderlich ist […] ein Rechtsinstrument, das effektiv, praktikabel und zeitnah die Gewinnung von elektronischen Beweismitteln bei Internet-Diensteanbietern ermöglicht, jedoch zugleich in angemessener Weise dem Grundrechtsschutz gerecht wird und die bewährten Prinzipien internationaler strafrechtlicher Zusammenarbeit fortentwickelt."[106]

dem betreffenden Hoheitsgebiet niedergelassen oder vertreten sind, zu bestimmten Maßnahmen zu verpflichten, nicht beschränken."

[104] Kritisch nunmehr auch BR-Drs. 215/18 v. 6.7.2018, S. 4.

[105] COM(2018) 225 final, S. 6.

[106] BR-Drs. 215/18 v. 6.7.2018, S. 1.