(Inter-) Nationale Strafverfolgung in der Cloud?
Risiken unilateraler Zugriffe auf Auslandsdaten

*von Christine Untch**

Abstract
Um Strafverfolgungsbehörden einen erleichterten und schnelleren Zugang zu Cloud-Daten im Ausland zu verschaffen, schlägt die Europäische Union unilaterale Direktzugriffe bei den Anbietern solcher Dienste vor. Der folgende Beitrag zeigt die daraus resultierenden Risiken für die internationale Zusammenarbeit, Interessen der Diensteanbieter und insbesondere den Grundrechts- und Datenschutz Betroffener auf und bietet alternative Lösungsmöglichkeiten an.

In order to grant law enforcement authorities easier and faster access to cloud data stored abroad, the European Union proposes an unilateral direct access to the providers of such services. The following article hightlights the resulting risks to international cooperation, the interests of service providers and, in particular, to the privacy rights of those affected. Furthermore alternative solutions are offered.

I. Problemstellung

Internetnutzer verzichten heutzutage vielfach auf eine lokale Datenspeicherung auf dem heimischen PC und nutzen stattdessen die Möglichkeiten der virtuellen Cloud. Das Cloud Computing stellt ein über das Internet zur Verfügung gestelltes, komplexes, dynamisches Angebot von Soft- und Hardwareleistungen dar, das orts- und zeitungebunden genutzt werden kann.[1] Die hierfür erforderliche Software ebenso wie bei der Nutzung anfallende Daten werden von Diensteanbietern auf in der gesamten Welt verteilten[2] Servern vorgehalten bzw. gespeichert.[3] Für den Datenzugriff von Strafverfolgungsbehörden kann das erhebliche Schwierigkeiten aufwerfen.

1. In tatsächlicher Hinsicht

Daten können in Echtzeit übertragen, geändert oder gelöscht werden,[4] sodass für einen strafverfolgungsbehördlichen Zugriff oft nur eine sehr kurze Zeitspanne verbleibt, ehe die Daten den Standort wechseln (können).[5] Diese Flüchtigkeit der Daten[6] und ihre mangelnde physische Verkörperung binden Anbieter von Internetdiensten nicht an lokale Standorte, sodass sie Nutzerdaten oft im Ausland speichern.[7] Der Datenspeicherort kann zwar grundsätzlich mithilfe sog. Traceroute-Verfahren[8] festgestellt werden, die Nachverfolgung gerät jedoch angesichts der Speicherpolitiken einiger Cloud-Anbieter an ihre Grenzen. Während einige Cloud-Anbieter die Nutzerdaten auf Servern in einem anderen Staat speichern, setzen andere auf länderübergreifende algorithmenbasierte Speichermechanismen, durch die die Daten bzw. Datenfragmente[9] je nach Kapazität auf in mehreren Staaten belegenen Serververbunden in Sekundenbruchteilen ihren Speicherort wechseln können.[10] Durch die ständige Bewegung der Daten und ihre oft nur fragmentarische Speicherung an mehreren Standorten hilft die Nachverfolgung via Traceroute oftmals nur bedingt weiter. Eine Auskunft über die dauerhafte Lokalisierung des Datenspeicherortes stellt daher sogar den Diensteanbieter selbst vor große Schwierigkeiten und ist oft schlichtweg nicht möglich,[11] sodass der Speicherort auch für strafverfolgungsbehördliche Maßnahmen jedenfalls auf Dauer nicht bestimmbar ist (*loss of knowledge of location*).[12]

2. In rechtlicher Hinsicht

Der ausländische Speicherort der Daten hindert Strafverfolger zwar faktisch nicht, die Daten aus dem Inland abzurufen.[13] In rechtlicher Hinsicht muss sich das Verhalten

---

* Die Verfasserin ist wissenschaftliche Mitarbeiterin am Institut für ausländisches und internationales Strafrecht von *Prof. Dr. Bettina Weißer*, Universität zu Köln und arbeitet derzeit an ihrer Dissertation zum Thema Strafverfolgung im Smart Home.

1 Vgl. *Bell*, Strafverfolgung und die Cloud, 2019, S. 25 f. m.w.N.; *Obenhaus*, NJW 2010, 651.

2 Vgl. *Dalby*, Grundlagen der Strafverfolgung im Internet und in der Cloud, 2016, S. 234.

3 *Obenhaus*, NJW 2010, 651.

4 Vgl. *Sieber*, Straftaten und Strafverfolgung im Internet, 2012, S. 35 f.; *Warken*, NZWiSt 2017, 289 (296 f.).

5 *Sieber*, S. 39; *Warken*, NZWiSt 2017, 289 (297); *Daskal*, YLJ 2015, 325 (366 ff.).

6 *Dalby*, S. 233.

7 *Warken*, NZWiSt 207, 417 (419); vgl. *Brodowski*, JR 2009, 402 (410).

8 Nach *Hauschild*, in: MüKo-StPO, 2014, § 110 Rn. 18, ist hierunter „ein Computerprogramm zu verstehen, mit de[m] der Standort des Servers festgestellt werden kann, insbesondere über welche IP-Router die übermittelten Datenpakete zum Zielrechner gelangen. Das Ergebnis kann allerdings u.a. durch Firewalls, fehlerhafte Implementierungen des IP-Stacks und IP-Tunnel verfälscht werden, so dass der Standort des Servers nicht immer eindeutig bestimmbar ist".

9 Vgl. *Warken*, NZWiSt 2017, 289 (296); *Kleinhans,* Die Cloud im rechtsfreien Raum, S. 4, online abrufbar unter: https://tinyurl.com/2p83aanv, (zuletzt abgerufen am 18.8.22).

10 *Bell*, S. 174; *Dalby*, S. 244; *Warken*, NZWiSt 2017, 289 (296). So etwa Dropbox oder Google.

11 Vgl. Ratsdok 15072/1/16 REV 1, S. 14; *Bell*, S. 174; *Sieber*, S. 36; *Wicker*, MMR 2013, 765 (766); *Burchard*, ZIS 2018, 190 (197); *Warken*, NZWiSt 2017, 289 (296).

12 *Sieber*, S. 77 f.; *Warken*, NZWiSt 2017, 417 (422).

13 *Warken*, NZWiSt 2017, 417 (422).

der Strafverfolger aber auch an völkerrechtliche Vorgaben halten, vgl. Art. 25 GG. Nach dem völkerrechtlichen Territorialitätsgrundsatz beschränken sich hoheitliche Maßnahmen auf das eigene Hoheitsgebiet.[14] Kein Staat darf Strafverfolgungsmaßnahmen in fremdem Hoheitsgebiet vornehmen.[15] Dieses Territorialitätsprinzip gilt nach h.M. auch im Internet.[16] Im Falle des grenzüberschreitenden Zugriffs auf Daten liegt die Hoheitsgewalt über die Daten bei dem Staat, in dem sie gespeichert sind.[17] Der Umstand, dass inländische Strafverfolger ausländische Daten vom Inland aus, also ohne Staatsgrenzen physisch überqueren zu müssen, abrufen bzw. von Diensteanbietern verlangen können, nimmt der Maßnahme nicht den Eingriffscharakter.[18] Die physische Anwesenheit nationaler Strafverfolger ist für die Annahme eines völkerrechtlichen Eingriffs in das Territorialitätsprinzip gerade nicht erforderlich.[19] Deshalb dürfen Ermittlungsmaßnahmen, die mit Zugriffen auf ausländische Server verbunden sind, grundsätzlich nur mit Zustimmung des betroffenen Staats vorgenommen werden.[20]

II. Status Quo

De lege lata sind unmittelbare strafverfolgungsbehördliche Zugriffe auf Cloud-Daten im Ausland daher nur bei Vorliegen einer völkerrechtlichen Rechtfertigung möglich.[21] Mit Blick auf den Zugriff auf Cloud-Daten im Ausland können drei Konstellationen unterschieden werden.

1. Kenntnis des ausländischen Datenspeicherorts

Ist ein ausländischer Datenspeicherort den Ermittlungsorganen (ggfs. durch Traceroute) bekannt, so liegt im strafverfolgungsbehördlichen Zugriff auf diese Daten (im Wege des Abrufens aus dem Inland oder durch Herausgabeanordnung an den Diensteanbieter) ein bewusster Eingriff in die Gebietshoheit des betroffenen Staates.[22] Nach der Cybercrime-Convention (CCC)[23] ist ein solcher Zugriff auf Auslandsdaten jedenfalls bei öffentlich zugänglichen Daten[24] gem. Art. 32 lit. a und bei zugangsbeschränkten Daten mit Zustimmung des Betroffenen[25] gem. Art. 32 lit. b CCC völkerrechtlich legitim. Über den Anwendungsbereich der CCC[26] hinaus wie für alle weiteren Fälle kommt eine Rechtfertigung jedoch nicht in Betracht, sodass der Zugriff nur im Wege der traditionellen Rechtshilfe möglich ist.[27] Innerhalb der Europäischen Union hilft auch die Europäische Ermittlungsanordnung[28] nur bedingt weiter.[29] Es haben sich jedoch Praktiken einer freiwilligen Zusammenarbeit mit Diensteanbietern[30], insb. in den USA (mit Blick auf Nicht-Inhaltsdaten) entwickelt,[31] bei denen Strafverfolger unverbindliche Anfragen an Diensteanbieter stellen und Auskunft erhalten können.[32] Da die Kooperation informell abläuft,[33] fehlt es hierbei aber an einheitlichen Formvorschriften für Anfragen[34] und an der Verlässlichkeit der Provider-Auskunft.[35] Auch werden so Rechtshilfeabkommen unterlaufen und möglicherweise Souveränitätsrechte von Drittstaaten verletzt.[36] Solche informellen Kooperationen sind zudem nur

14 Hierzu *Dombrowski*, Extraterritoriale Strafrechtsanwendung im Internet, 2014, S. 132; *Böckenförde*, Die Ermittlung im Netz, 2003, S. 206 f.; *Seitz*, Strafverfolgungsmaßnahmen im Internet, 2004, S. 361; *Sieber*, S. 144; *Graßie/Hiéramente*, CB 2019, 191 (193); *Brodowski*, in: BeckOK-IT, 5. Ed. 2022, § 110 StPO Rn. 12, 12.1.

15 *Epping*, in: Ipsen, Völkerrecht, 7. Aufl. (2018), § 7 Rn. 59 ff., 69 ff.; *Dombrowski*, S. 5; *Seitz*, S. 361; BGHSt 45, 188 (192).

16 *Dombrowski*, S. 10; *Sieber*, S. 144; auch *Graßie/Hiéramente*, CB 2019, 191 (193).

17 *Dombrowski*, S. 10; *Dalby*, S. 247; *Burchard*, ZIS 2018, 249; *Hauschild*, in: MüKo-StPO, § 110 Rn. 18; *Graßie/Hiéramente*, CB 2019, 191 (193); a.A. *Wicker*, Cloud Computing und staatlicher Strafanspruch, 2016, S. 435.

18 *Sieber*, S. 144; *Bell*, S. 162; *Dombrowski*, S. 138, 160; *Brodowski*, in: BeckOK-IT, § 110 StPO Rn. 12, 12.1. Bei einem direkten Zugriff auf die Cloud-Daten aus dem Inland liegt der Eingriff dennoch im Auslösen von datenrechnerischen Vorgängen im Ausland, vgl. *Sieber*, S. 144; *Bell*, S. 162; *Dombrowski*, S. 138, 143 f., 160; *Warken*, NZWiSt 2017, 289 (295); a.A. etwa *Wicker*, S. 342 f., 356, 435 ff.; auch *Köhler*, in: Meyer-Goßner/Schmitt, StPO, 64. Aufl. (2021), § 110 Rn. 7b.

19 *LG Hamburg*, MMR 2008, 186 (187); *Gercke*, StraFo 2009, 271 (272).

20 *Dombrowski*, S. 133 ff.; BGHSt 45, 188 (192).

21 Eine Rechtfertigung völkerrechtlicher Eingriffe kann aus anerkannten völkerrechtlichen Rechtsquellen abgeleitet werden, *Seitz*, S. 365.

22 *Bell*, S. 177; *Sieber*, S. 144; *Burchard*, ZIS 2018, 249; *Brodowski*, ZIS 2012, 474 (477 f.); *ders.*, in: BeckOK-IT, § 110 StPO Rn. 12, 12.1.; *Gaede*, StV 2009, 96 (101 f.); *Gercke*, StraFo 2009, 271 (272).

23 Europarat Übereinkommen über Computerkriminalität vom 23.11.2001, SEV Nr 185.

24 Nach e.A. soll mangels Betroffenheit des Rechts auf informationelle Selbstbestimmung kein Eingriff in die Gebietshoheit vorliegen, vgl. *Böckenförde*, S. 208. Die h.M. hält richtigerweise eine Rechtfertigung nach Art. 32 lit. a CCC oder im Falle Nicht-Vertragspartner völkerrechtlichem Gewohnheitsrecht für erforderlich, *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110 Rn. 7a; *Gercke*, StraFo 2009, 271 (272 f.); Sieber, S. 144 f.; eingehend hierzu *Dombrowski*, S. 155–159.

25 Keiner Rechtfertigung über Art. 32 lit. b CCC bedarf es, wenn der Betroffene die Daten von sich aus kopiert und aushändigt, s. *Bell*, S. 165; *Dombrowski*, S. 161 f.; a.A. *Hegmann*, in: BeckOK-StPO, 42. Ed. (2022), § 110 Rn. 16 nach dem selbst ein Zugriff durch die Strafverfolgungsbehörden zulässig sein soll, wenn Zugangsdaten bei der Durchsuchung aufgefunden wurden. Zur freiwilligen Zustimmung berechtigt ist nur, wer rechtmäßigen Zugang zu den Daten besitzt und darüber hinaus auch die Daten an Dritte weitergeben darf – neben dem Nutzer, je nach Vertragsgestaltung daher auch der Diensteanbieter, vgl. *Bell*, S. 166 f.; *Dombrowski*, S. 161 f. Mit Blick auf Zugriffe im Verhältnis zu Drittstaaten nach h.M. völkergewohnheitsrechtlich anerkannt, vgl. *Gercke*, in: HK-StPO, 6. Aufl. (2019), § 110 Rn. 27; *Seitz*, S. 365 f.; *Köhler*, in: Meyer-Goßner/Schmitt, § 110 Rn. 7a.

26 *Sieber*, S. 148; *Gercke*, in: HK-StPO, § 110 Rn. 28.

27 *Burchard*, ZIS 2018, 249; *Brodowski*, JR 2009, 402 (410); *ders.*, in: BeckOK-IT, § 110 StPO Rn. 12; *Warken*, NZWiSt 2017, 417 (419); *Graßie/Hiéramente*, CB 2019, 191 (193); *Hiéramente/Fenina*, StraFo 2015, 365 (368); *Gercke*, in: HK-StPO, § 110 Rn. 28; *Sieber*, S. 148.

28 RiLi 2014/41/EU v. 3.4.2014, ABl. L 130/1. Sie sieht nur eine vereinfachte Rechtshilfe vor, nicht aber unmittelbare Zugriffe, vgl. *Brodowski*, ZIS 2012, 474 (478); *Warken*, NZWiSt 2017, 417 (420). Allgemein hierzu *Weißer*, in: Schulze/Janssen/Kadelbach, Europarecht, 4. Aufl. (2020), § 16 Rn. 96 ff.

29 *Brodowski*, in: BeckOK-IT, § 110 StPO Rn. 12.

30 Sie stützt sich auf 18 US Code § 2702 (a) (3) und einen sog. General Permission Letter des US-Departments (nicht öffentlich einsehbar), der deutschen Strafverfolgern wohl die direkte Kommunikation mit US-Diensteanbietern gestattet, *Burchard*, ZIS 2018, 190 (201 f.); s. auch *Warken*, NZWiSt 2017, 417 (424).

31 Mit Blick auf Inhaltsdaten bleibt es aber bei der Einhaltung des Rechtshilfewegs, *Burchard*, ZIS 2018, 190 (202).

32 *Burchard*, ZIS 2018, 190 (201 f.); *Böse*, KriPoZ 2019, 140 (141); *Niekrenz*, DuD 2020, 535.

33 Vgl. *Burchard*, ZRP 2019, 164.

34 Vgl. Ratsdok. 15072/1/16, S. 7; *Warken*, NZWiSt 2017, 417 (425).

35 *Warken*, NZWiSt 2017, 417 (425); *Böse*, KriPoZ 2019, 140 (141) m.w.N.; vgl. Ratsdok. 15072/1/16, S. 7 f.

36 *Warken*, NZWiSt 2017, 417 (425); *Bär*, ZIS 2011, 53 (54).

in einigen Staaten üblich,[37] sodass hierin auch keine ständige Übung im Sinne einer völkergewohnheitsrechtlichen Anerkennung gesehen werden kann.

2. Speicherort potenziell (auch) im Ausland

Setzen Cloud-Anbieter auf Speicherpolitiken, bei denen sich der Datenstandort ständig über Landesgrenzen hinweg verändert, so wird eine zuverlässige Bestimmung des Speicherorts auch mittels Traceroute[38] nicht zielführend sein (*loss of knowledge of location*).[39] Ein ausländischer Speicherort befindet sich dann nur potenziell im Ausland – sofern der vom Provider genutzte Serververbund auch Server im Inland beinhaltet. Während einerseits argumentiert wird, allein die Möglichkeit, dass sich die Daten irgendwo im Ausland befinden, löse ohnehin keine Rechtshilfeverpflichtung aus,[40] sehen andere in dem Zugriff auf nur potenziell im Ausland befindliche Daten keinen bzw. jedenfalls einen gerechtfertigten Eingriff in die Gebietshoheit des betroffenen Staates, da die Daten im Inland liegen könnten und für den Fall, dass sie im Ausland belegen sind, die fremde Gebietshoheit nicht willkürlich und bewusst verletzt werde.[41] Zudem lege die „breite Akzeptanz der beteiligten Staaten" in Bezug auf diese Speicherpolitiken die Annahme nahe, „dass die Staaten mit der Duldung derartiger Angebote die grenzübergreifende Datenfragmentierung akzeptieren, ohne jedoch eine Beschränkung der eigenen Ermittlungsbefugnisse zu forcieren".[42] Das Handlungsinteresse des zugreifenden Staates überwiege daher.[43] Auch wird in diese Richtung vorgebracht, solange der Zugriff vom Cloud-Nutzer aus möglich sei, sei der Datenspeicherort nicht von Bedeutung.[44] Im Ergebnis bedarf es nach diesen Ansichten also weder eines Rechtshilfeverfahrens noch einer Nachholung bei nachträglicher Kenntnis der Belegenheit der Daten im Ausland.[45]

Mit der h.M. kann hingegen grundsätzlich nicht von einer völkerrechtlichen Legitimation ausgegangen werden,[46] da der Eingriffscharakter nicht von der physischen Vornahme des Zugriffs abhängt und von privaten Geschäftspraktiken und deren „Duldung" kaum auf völkergewohnheitsrechtlich anerkannte Ermittlungskompetenzen geschlossen werden kann,[47] zumal gerade die seit Jahren währende (internationale und europäische) Debatte um den Zugriff auf Cloud-Daten im Ausland eine gegenteilige Realität verdeutlicht. Es ist zudem nicht unmöglich, den Speicherort auszumachen. Wenn Traceroute keine dauerhafte Datenlokalisierung ermöglicht, kann immer noch der Diensteanbieter Auskunft geben,[48] bzw. es bedarf rechtlicher Regelungen, die den Diensteanbieter dazu verpflichten, Auskunft geben zu können.[49]

3. Good faith-Fälle

Sind Strafverfolgungsbehörden irrtümlich von einem inländischen Speicherort ausgegangen und haben stattdessen auf Daten im Ausland zugegriffen,[50] so meinen manche, der Eingriff in die fremde Gebietshoheit sei durch das Handlungsinteresse des zugreifenden Staates gerechtfertigt.[51] Die h.M. lehnt dies jedoch mit Recht ab,[52] da völkerrechtliche Eingriffe nicht durch schlichte Unkenntnis zu legitimieren sind[53] und der Datenstandort via Traceroute ermittelbar war.[54] Schließlich ließe sich eine solche Behauptung kaum verifizieren und würde daher enormes Missbrauchspotenzial bergen.[55]

4. Zwischenergebnis

Es kann also festgehalten werden, dass der Status Quo bis auf die Ausnahmen der CCC und Erleichterungen auf Unionsebene darin besteht, dass der (wenn auch langwierige[56]) traditionelle Rechtshilfeweg beschritten werden muss.[57] Insbesondere kann keinesfalls davon ausgegangen werden, der grenzüberschreitende Zugriff auf gespeicherte zugangsgeschützte Daten sei gewohnheitsrechtlich anerkannt.[58] Mit Blick auf zugangsgeschützte, also nicht öffentlich zugängliche Daten sind unilaterale Zugriffe aktuell nicht zulässig.[59]

---

37 *Bell*, S. 170 f. Insbes. ist dies europäischen Diensteanbietern nicht gestattet, vgl. *Sieber*, S. 78; *Warken*, NZWiSt 2017, 417 (424).
38 *Bell*, S. 183.
39 Vgl. *Bell*, S. 177; *Graßie/Hiéramente*, CB 2019, 191 (193 f.).
40 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110 Rn. 7b; auch *Hegmann*, in: BeckOK-StPO, § 110 Rn. 16; *Soiné*, NStZ 2018, 497 (500); vgl. auch *Bruns*, in: KK-StPO, 8. Aufl. (2019), § 110 Rn. 8a; *Wicker*, MMR 2013, 765 (768 f.).
41 *Bell*, S. 181 m.w.N.; *Wicker*, S. 356; *Wicker*, MMR 2013, 765 (768 f.).
42 *Bell*, S. 181 f.
43 *Bell*, S. 182.
44 *Wicker*, MMR 2013, 765 (768 f.).
45 *Bell*, S. 182; *Wicker*, MMR 2013, 765 (769); *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110 Rn. 7b; *Soiné*, NStZ 2018, 497 (500); auch *Bruns*, in: KK-StPO, § 110 Rn. 8a; *Hegmann*, in: BeckOK-StPO, § 110 Rn. 16.
46 S. nur *Brodowski*, ZIS 2012, 474 (477 f.); *ders.*, in: BeckOK-IT, § 110 StPO Rn. 12, 12.1.; *Burchard*, ZIS 2018, 249; *Gercke*, StraFo 2009, 271 (272); *Sieber*, S. 144; *Schiemann*, in: Migration, Datenübermittlung und Cybersicherheit, 2016, S. 151 (160).
47 Vgl. *Brodowski*, in: BeckOK-IT, § 110 StPO Rn. 12.2.
48 *Brodowski*, in: BeckOK-IT, § 110 StPO Rn. 12.2.
49 Hierzu weiter unten (V.).
50 *Sieber*, S. 147; *Bell*, S. 182 f.; *Seitz*, S. 368.
51 Dargestellt bei Seitz, S. 368 m.w.N.
52 *Sieber*, S. 147; *Seitz*, S. 377; *Gercke*, StraFo 2009, 271 (273); *ders.*, in: HK-StPO, § 110 Rn. 28; auch *Bell*, S. 183.
53 *Sieber*, S. 147.
54 *Gercke*, StraFo 2009, 271 (273); *ders.*, in: HK-StPO, § 110 Rn. 28.
55 *Gercke*, StraFo 2009, 271 (273).
56 *Warken*, NZWiSt 2017, 289 (297); *Kleinhans,* Die Cloud im rechtsfreien Raum, S. 4 f., online abrufbar unter: https://tinyurl.com/2p83aanv (zuletzt abgerufen am 18.8.22), nennt eine übliche Verfahrensdauer von „6-18" Monaten; vgl. auch *Sieber*, S. 39.
57 *Sieber*, S. 148; *Bell*, S. 172; *Graßie/Hiéramente*, CB 2019, 191 (193); *Gercke*, in: HK-StPO, § 110 Rn. 28; *Eisenberg*, StPO, 10. Aufl. (2017), Rn. 493; *Brodowski*, JR 2009, 402 (410); *ders.*, in: BeckOK-IT, § 110 StPO Rn. 12; *Burchard*, ZIS 2018, 249; *Warken*, NZWiSt 2017, 417 (419); auch *Graßie/Hiéramente*, CB 2019, 191 (193); *Hiéramente/Fenina*, StraFo 2015, 365 (368); *Hauschild*, in: MüKo-StPO, § 110 Rn. 18.
58 Vgl. *Sieber*, S. 145, 148; *Seitz*, S. 377; *Dombrowski,* S. 165 f.; *Gercke*, in: HK-StPO, § 110 Rn. 28. Eine mögliche Rechtfertigung bei überwiegendem Abwehrinteresse des agierenden Staates kommt nur in sehr engen Ausnahmefällen in Betracht, vgl. hierzu *Dombrowski,* S. 167 f.; *Gercke*, in: HK-StPO, § 110 Rn. 27 f.
59 *Warken*, NZWiSt 2017, 417 (419); *Brodowski*, JR 2009, 402 (410); *Gercke*, StraFo 2009, 271 (273); *Sieber*, S. 148.

III. Vorschlag der E-Evidence-Verordnung

Das soll sich aber nun mit der vorgeschlagenen E-Evidence-Verordnung[60] nach dem Vorbild des US-amerikanischen CLOUD-Acts[61] ändern. Strafverfolgungsbehörden von EU-Mitgliedstaaten sollen hiernach künftig von Diensteanbietern in der Europäischen Union unmittelbar Herausgabe und/oder Sicherung elektronischer Beweismittel unabhängig von ihrem Speicherort verlangen können. Vorgeschlagen wird also nicht weniger als eine Abkehr vom völkerrechtlichen Fundamentalprinzip der Gebietshoheit betreffend gespeicherte Daten. Der Anwendungsbereich der Verordnung ist dabei sehr weit gefasst[62] und erlaubt Herausgabe- und Sicherungsanordnungen künftig unmittelbar gegenüber dem Diensteanbieter mit Datenspeicherort im Ausland. Erfasst ist damit der Zugriff auf Daten auf externen Speichern, also bei einem (potenziellen) Diensteanbieter im Ausland. Die Verordnung kann allerdings nicht Zugriffe gegen Diensteanbieter krimineller Plattformen verrechtlichen, denn insoweit helfen strafverfolgungsbehördliche Anordnungen ermittlungstaktisch gesehen regelmäßig nicht weiter, da diese Diensteanbieter nicht nur ihren Datenstandort, sondern auch ihre Identität verschleiern[63] und daher entweder gar nicht erreichbar sind oder aber auf offene Anordnungen von Strafverfolgern wohl nur mit einer Vernichtung der elektronischen Beweismittel antworten würden. Ziel der Verordnung sind also nicht Zugriffe, um gegen den Diensteanbieter selbst Strafverfolgung zu betreiben, sondern vielmehr um Verpflichtungen des Diensteanbieters, strafverfolgungsrelevante Nutzerdaten herauszugeben, zu forcieren. Das Hauptaugenmerk der Verordnung liegt damit auf den großen „seriösen" Cloud-Anbietern wie Google oder Apple.

Der Verordnungsvorschlag ist seit seiner Veröffentlichung auf große Kritik gestoßen.[64] Dabei konzentrieren sich die folgenden Ausführungen auf die Abkehr vom Territorialitätsprinzip bei strafverfolgungsbehördlichen Zugriffen auf im Ausland gespeicherte Cloud-Daten. Sie unilateral zuzulassen, ist insbesondere mit Blick auf den Grundrechtsschutz der Betroffenen hochgefährlich.[65] Die Risiken unilateraler Datenzugriffe und alternative Lösungsmöglichkeiten für das Problem des grenzüberschreitenden Zugriffs auf Cloud-Daten werden deshalb im Folgenden aufgezeigt.

IV. Risiken unilateraler Direktzugriffe bei Diensteanbietern auf Cloud-Daten im Ausland

Der vorgeschlagene europäische Datenunilateralismus birgt erhebliche Risiken für die zu berücksichtigenden Interessen. Auf der einen Seite steht dabei das Interesse des zugreifenden Staates an der Funktionsfähigkeit und Effektivität seiner Strafverfolgung.[66] Während auf der anderen Seite der von dem Zugriff betroffene Staat ein Interesse an der Wahrung seiner Gebietshoheit über im Inland gespeicherte Daten und damit letztlich seiner Souveränität hat. Auch Belange der zwischenstaatlichen Höflichkeit spielen mit Blick auf den langfristigen Erhalt internationaler Beziehungen, also auch der internationalen Sicherheitszusammenarbeit, eine Rolle.[67] In diesem Zusammenhang ist zu beachten, dass unionsrechtliche Regelungen natürlich auch international zur Kenntnis genommen und ggf. übernommen werden. Die Europäische Union sollte also nur Regelungen wählen, die sie auch seitens der Drittstaaten gegenüber sich gelten lassen will.[68] Da potenziell strafverfolgungsrelevante Daten im Wesentlichen personenbezogen sind, hat auch der von den Datenzugriffen betroffene Nutzer ein erhebliches Interesse an der Wahrung seines Grundrechts- und Datenschutzes. Die Zugriffe betreffen zudem Geschäftsmodelle privater Diensteanbieter, die ebenfalls ein Interesse an der Wahrung ihrer Grundrechte und der Wirtschaftlichkeit ihres Betriebs haben. Gesellschaftsübergreifend besteht zudem auch ein Interesse daran, die Offenheit des Internets beizubehalten.[69] Das durchaus legitime Ziel der Verordnung, den grenzüberschreitenden Datenzugriff im Sinne einer effektiven Strafverfolgung auszugestalten, darf daher nicht um jeden Preis vorangetrieben werden.[70]

1. Entterritorialisierung der Cloud

Für die Abkehr vom Territorialitätsprinzip und die damit einhergehende Entterritorialisierung der Cloud wird in erster Linie die Andersartigkeit von Daten[71] und der Cloud als eigener virtueller, aber eben nicht physisch begrenzbarer Raum[72] ins Feld geführt.[73] Durch die Flüchtigkeit von Daten und ihrer Übertragbarkeit in Echtzeit ohne Rücksicht auf Staatsgrenzen sowie Speicherpolitiken über mehrere Länder hinweg,[74] sei es willkürlich, an dem oftmals nicht bzw. nicht ohne Weiteres feststellbaren Datenspeicherort und damit am Territorialitätsprinzip hinsichtlich der Cloud festzuhalten.[75]

---

60 COM (2018) 225 final.
61 Clarifying Lawful Overseas Use of Data Act. Hierzu *Cording/Götzinger*, CR 2018, 636 ff.; *Schaar*, MMR 2018, 705 ff.
62 Vgl. *Weißer*, in: Schulze/Janssen/Kadelbach, Europarecht, § 16 Rn. 100.
63 Vgl. *Warken*, NZWiSt 2017, 289 (295).
64 *Böse*, KriPoZ 2019, 140; *Burchard,* ZRP 2019, 164, *ders.*, ZIS 2018, 249 (264); *Brodowski*, ZIS 2018, 493; *ders.*, NJW-aktuell 2018, 19; *Esser*, StraFo 2019, 404; *Weißer*, in: Schulze/Janssen/Kadelbach, Europarecht, § 16 Rn. 100; *Hamel*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren, 2020, S. 103; *von Galen*, Digitalisierung und Strafverfahren, S. 127; *Thomae*, Digitalisierung und Strafverfahren, S. 139.
65 Vgl. *Böse*, KriPoZ 2019, 140.
66 *Burchard*, ZIS 2018, 190 (192).
67 Ebd.
68 Vgl. *Burchard*, ZIS 2018, 190 (192).
69 Insgesamt hierzu *Burchard*, ZIS 2018, 190 (192).
70 Vgl. auch *Burchard*, ZRP 2019, 164.
71 *Daskal*, YLJ 2015, 325 (365 ff.); *Clopton*, Chicago Law Review 2016, 45, jeweils m.w.N. A.A. *Woods*, Stanford Law Review 2016, 729 (756 ff.).
72 *Daskal*, YLJ 2015, 325 (369 ff.).
73 *Daskal*, YLJ 2015, 325; *Clopton*, Chicago Law Review 2016, 45; a.A. *Woods*, Stanford Law Review 2016, 729 (756 ff.).
74 *Daskal*, YLJ 2015, 325 (365 ff.); *dies.*, Vanderbilt Law Review 2018, 179 (221 ff.).
75 A.A. aber *Woods*, Stanford Law Review 2016, 729 ff. m. zusammengetragenen Nachweisen für diese Entterritorialisierungs-Ansicht. So zusammengefasst, nicht aber vertreten von *Burchard*, ZIS 2018, 190 (202).

Sofern Diensteanbieter ihre Nutzerdaten auf Serververbunden über mehrere Länder hinweg rotierend speichern, erscheint es mit Blick auf diesen konkreten Fall natürlich zunächst willkürlich, zur Bestimmung des Zugriffs auf den kaum auszumachenden Datenspeicherort abzustellen. Allerdings ignoriert die pauschale Annahme, der Datenspeicherort sei bei Cloud-Sachverhalten insgesamt ein willkürliches Kriterium, dass derartige Speicherpolitiken nicht von allen, ja nicht einmal von der Mehrheit der Diensteanbieter eingesetzt werden.[76] Im Gegenteil werben viele Diensteanbieter damit, die Nutzerdaten gegen Entgelt ausschließlich an einem bestimmten Standort zu speichern, um den dort geltenden Datenschutz zu gewährleisten.[77] Auch aus ökonomischer Sicht kann es Gründe geben, einen bestimmten Standort oder selbst bei Nutzung von Serververbunden bestimmte Länder als Serverstandorte bewusst auszuwählen. Angesichts der fortschreitenden Ökonomisierung des Datenschutzes überzeugt es nicht, aus den Praktiken einiger Diensteanbieter, Nutzerdaten in mehreren Ländern verteilt zu speichern, pauschal darauf zu schließen, dass der Datenspeicherort grundsätzlich bedeutungslos sei.[78] Vielmehr sollte man gegenteilig davon ausgehen, dass der Datenspeicherort sehr wohl von Bedeutung ist[79] und bei gegenteiligen Anhaltspunkten eine Differenzierung zwischen verschiedenen Cloud-Datenspeicherungsmodellen in Betracht ziehen.[80]

Auch die Behauptung, es sei Nutzern ohnehin gleichgültig, wo ihre Daten gespeichert sind,[81] vermag daher nicht zu überzeugen. Empirische Belege liegen auch hierfür nicht vor.[82] Angesichts der asymmetrischen Machtverhältnisse zwischen Diensteanbietern und Nutzern fehlt letzteren oftmals eine hinreichende Aufklärung und Informiertheit.[83] Manche Nutzer wählen gar bewusst kostenpflichtige Cloud-Angebote mit Speicherversprechen in bestimmten Ländern aus, gerade weil ihnen der Belegenheitsort ihrer Daten wichtig ist.[84] Auch hier verbietet sich deshalb jegliche Pauschalisierung. Von dieser Argumentation auf einen Grundrechtsverzicht der dem Datenbelegenheitsort gleichgültig gegenüberstehenden Cloud-Nutzern oder eine datenschutzrechtliche Einwilligung in den Zugriff zu schließen, erscheint ohnehin fragwürdig.[85]

Entscheidend, mit Blick auf die Forderung nach einer Entterritorialisierung der Cloud, sind vielmehr ihre rechtlichen Konsequenzen. So würde dies nicht weniger als eine Abkehr von völkerrechtlichen Fundamentalprinzipien bedeuten.[86] Unilaterale Zugriffe auf Cloud-Daten im Ausland können das zwischenstaatliche Vertrauen und damit zwischenstaatliche Beziehungen und Solidarität nachhaltig beeinträchtigen und eine grenzüberschreitende internationale Sicherheitszusammenarbeit erschweren oder gar unmöglich machen.[87] Im schlimmsten Fall kann der Unilateralismus zudem zu Strafverfahren gegen ausländische Strafverfolger führen, wenn diese Diensteanbieter zur Verletzung des europäisierten Datenschutzstrafrechts „angestiftet" haben.[88]

2. Problemlösung durch Notifikationslösung der E-Evidence-Verordnung?

Die Verordnung soll die völkerrechtliche Zweifelhaftigkeit unilateraler Datenzugriffe im Ausland beheben. Sie ist zu verstehen als generalisierte Zustimmung der Mitgliedsstaaten untereinander, unilateral Daten bei Diensteanbietern erheben zu dürfen – auch weil die jeweiligen Staaten möglicherweise im Nachgang über den Zugriff informiert werden sollen.[89] Durch diese Einigung auf unechte unilaterale Beibringungsanordnungen[90] würde die Gebietshoheit jedenfalls der Mitgliedsstaaten unangetastet bleiben, da sich die Staaten einverstanden erklärt haben.[91] Um völkerrechtliche Konflikte mit Drittstaaten zu vermeiden, könnte man dieses Modell unechter unilateraler Zugriffe mit Notifikation des betroffenen Staates im Wege von Vereinbarungen auf Drittstaaten ausweiten.[92] Zweifelhaft scheint dabei aber, ob damit dem Grundrechts- und Datenschutz Genüge getan würde.

3. Grundrechts- und Datenschutz durch zugreifenden Staat und Private?

Kehrseite von Gebietshoheit und Souveränität ist die Pflicht des Staates nicht nur zum Grundrechtsschutz der auf seinem Gebiet befindlichen Personen bei Hoheitsakten im Inland, sondern ebenso auch im Rahmen der internationalen Zusammenarbeit in Strafsachen für die Einhaltung grund- und datenschutzrechtlicher Mindeststandards zu sorgen.[93] Durch die Duldung von Datenerhebungen fremder Staaten gestattet der von dem Zugriff betroffene Staat Eingriffe in die Grundrechte seiner eigenen Bürger ohne echte Nachkontrolle. Das wirft die Frage auf, ob er die ihn treffenden Schutzpflichten gegenüber seinen Bürgern überhaupt noch in angemessenem Maße erfüllen kann.[94]

a) Blindes Vertrauen in vergleichbaren Grundrechts- und Datenschutz in EU- und Drittstaaten?

Möglich wäre das nur dann, wenn der aufgrund der generellen Zustimmung zugreifende Staat ein gleichwertiges Grundrechts- und Datenschutzniveau aufweist und die

76 *Burchard*, ZIS 2018, 249 (250).
77 Ebd.
78 *Burchard*, ZIS 2018, 249 (252).
79 *Burchard*, ZIS 2018, 249 (250).
80 Ebd.; vgl. *Burchard*, ZRP 2019, 164 (165).
81 *Warken*, NZWiSt 2017, 289 (295); *Daskal*, Vanderbilt Law Review 2018, 179 (225 f.).
82 *Burchard*, ZIS 2018, 249 (250).
83 *Burchard*, ZIS 2018, 249 (252).
84 Vgl. ebd.
85 Ebd.
86 *Burchard*, ZIS 2018, 249 (253).
87 *Burchard*, ZIS 2018, 249 (254 f.); hierzu weitergehend noch Brief of former law enforcement, national security, and intelligence officials as amici curiae in support of neither party, S. 3 f., online abrufbar unter: https://tinyurl.com/4fc2w3k9 (zuletzt abgerufen am18.8.2022).
88 *Burchard*, ZIS 2018, 249 (255).
89 Ebd.
90 Vgl. hierzu ebd.
91 Ebd.
92 Ebd.
93 *Böse*, KriPoZ 2019, 140 (143); *Burchard*, ZIS 2018, 249 (251); vgl. BVerfGE 141, 220 (342); 142 (234, 254 f.).
94 *Burchard*, ZIS 2018, 249 (252, 255); *Böse*, KriPoZ 2019, 140 (143).

Verfassungsidentität des betroffenen Staates achtet.[95] Mit Blick auf Drittstaaten kann davon wohl kaum ohne Weiteres ausgegangen werden. In der Europäischen Union hingegen ist dem anhand Art. 67 Abs. 1 AEUV auf dem ersten Blick wohl Genüge getan.

Eine gegenseitige Anerkennung im Sinne eines blinden Vertrauens in den fremdländischen Grundrechtsschutz ohne jedwede Rückversicherungsmöglichkeiten, also eine vollständige Suspendierung der Grundrechtsprüfung, läge jedoch nicht im Sinne der Wahrung eines effektiven Grundrechts- und Datenschutzes.[96] Angesichts einer fehlenden Harmonisierung des Strafprozessrechts[97] und dem direkten Zugriff der ausstellenden Strafverfolgungsbehörde bei privaten Diensteanbietern kann der betroffene Staat ohne Kontrollmöglichkeiten[98] kaum seinen innerstaatlichen Schutzpflichten gerecht werden. Deshalb muss der betroffene Staat auch im unilateralen Zugriffsverfahren[99] eine echte, bestenfalls zeitgleiche Notifikation sowie Verweigerungsgründe und Missbrauchsvorbehalte beanspruchen können, die echte Konsequenzen wie eine Unverwertbarkeit nach sich ziehen.[100]

b) Privatisierung des Rechtshilfeverfahrens zu Lasten der Grundrechte

Auch die vorgeschlagene Inpflichtnahme der Diensteanbieter vermag das Schutzniveau keinesfalls zu verbessern. Problematisch erscheint die Idee unechter unilateraler Zugriffe ohnehin insbesondere wegen der damit verbundenen Privatisierung ureigenster staatlicher Aufgaben[101] wie der Prüfung von Rechtshilfeersuchen. Der dadurch gewünschte Vorteil liegt auf der Hand. Die Diensteanbieter haben die technische Kontrolle über die Daten, sodass es keines „Umwegs“ über eine inländische Behörde bedarf,[102] deren Mühlen im Zweifel deutlich langsamer als die eines flexiblen und vor allem wirtschaftlicher arbeitenden privaten Unternehmens mahlen. So scheinen Private bestens geeignet, im Sinne des Gemeinwohls für den Staat einzuspringen. Allerdings ist anzunehmen, dass Private eigene wirtschaftliche Interessen im Zweifel über das Allgemeinwohl stellen.[103] Das begründet erhebliche Zweifel daran, ob die Prüfung von Strafverfolgungsmaßnahmen ausländischer Staaten wirklich sinnvoll, zuverlässig und sozialverträglich von privaten Dienstleistern übernommen werden sollte bzw. ob der Staat diese Aufgabe an Private delegieren darf.[104] Wer diesen riskanten Weg beschreiten will, muss zumindest Regelungen dafür schaffen, wie die Privaten diese Aufgabe denn ausführen sollen. Wer (mit welcher Qualifikation) prüft die eingehenden Quasi-Rechtshilfeersuchen bei Google? Anhand welcher Kriterien? Wie läuft das Verfahren ab? Wird der Betroffene informiert? Von Google? Kann man sich gegen Googles Entscheidung wehren? Und wer prüft die Prüfung durch Google? Die Liste der aufkommenden Fragen ließe sich noch fortführen. Deutlich werden soll dadurch Eines: Die Delegation einer so grundrechtssensiblen Aufgabe wie die Prüfung von ehemals Rechtshilfeersuchen an Private ohne jedwede Regulierung missachtet sämtliche Grundlagen des Rechtsstaats- und Demokratieprinzips und liefert den Betroffenen weitgehend schutzlos an Plattformbetreiber und deren wirtschaftliche Eigeninteressen aus.[105] Will man unmittelbare Zugriffe auf Cloud-Daten bei ausländischen Diensteanbietern zulassen, so bedarf es mindestens einer detaillierten, einheitlichen Regulierung auf Unionsebene unter Einhaltung grundlegender rechtsstaatlicher Verfahrensgrundsätze und einem Zusammenspiel mit dem territorial betroffenen Staat, der sich durch verpflichtende Notifikation durch den Diensteanbieter ein Eingreifen, also das Versagen, Widerrufen oder Beschränken der Datenherausgabe, vorbehalten sollte.[106] Ohne staatliche Kontrolle des privaten Datenherausgaberechtshilfeverfahrens[107] würde der europäische Grundrechtsschutz wahrlich zugunsten einer effektiven internationalen Sicherheitszusammenarbeit geopfert und unionsrechtswidrige Zustände hervorgerufen.[108]

4. Interessen der Diensteanbieter

Last but not least müssen auch die Interessen der Diensteanbieter Berücksichtigung finden, bevor sie unfreiwillig als Ersatz-Strafverfolger Fuß fassen müssen. Nach der E-Evidence-Verordnung sollen die Diensteanbieter die Prüfung der Herausgabeanordnungen ausländischer Strafverfolger übernehmen – und zwar nach dem Willen der Verordnungsgeber völlig umsonst. Es ist aber unrealistisch, dass bei unzähligen Anordnungen, die bei Erlass der Verordnung auf die Diensteanbieter zukommen werden, man an einer entsprechenden Entschädigung der Diensteanbieter für den Dienst an dem Allgemeinwohl vorbei kommt.[109] Zumal sich Dienstanbieter das für die Prüfung erforderliche Knowhow zunächst aneignen müssten.

Auch mit Blick auf Geschäftspraktiken der Anbieter muss berücksichtigt werden, dass einige, gerade kleinere Cloud-Anbieter insbesondere durch die Ökonomisierung des Datenschutzes überhaupt erst wirtschaften können.[110]

---

95 Mit vielen w.N. *Burchard*, ZIS 2018, 249 (256).

96 Vgl. nur *Burchard*, GPKG, Int. Rechtshilfeverkehr in Strafsachen, Nov. 2021, Vor § 1 Rn. 128 ff. m.w.N. und Darstellung der vertretenen Ansichten zur Anwendbarkeit nationaler Grundrechte mit Blick auf Rechtshilfeersuchen; *ders.*, ZIS 2018, 249 (256).

97 *Burchard*, ZRP 2019, 164 (166); vgl. auch *Sieber*, NJW-Beil. 2012, 86 (90).

98 *Burchard*, ZRP 2019, 164 (165).

99 Vgl. *Burchard*, ZIS 2018, 249 (256); *ders.*, ZRP 2019, 164 (165 f.); *Brodowski*, ZIS 2018, 493 (504); *Böse*, KriPoZ 2019, 140 (144).

100 *Burchard*, ZIS 2018, 249 (256); *ders.*, ZRP 2019, 164 (167).

101 Vgl. *Burchard*, ZIS 2018, 249 (259).

102 *Burchard*, ZIS 2018, 249 (260).

103 Vgl. ebd.

104 *Burchard*, ZIS 2018, 249 (260); *Böse*, KriPoZ 2019, 140 (144); vgl. auch *Weißer*, in: Schulze/Janssen/Kadelbach, Europarecht, § 16 Rn. 100.

105 Vgl. *Burchard*, ZIS 2018, 249 (260) mit der treffenden Bezeichnung als „nicht-regulierte Selbstregulierung des internen Prüfverfahrens bei Diensteanbietern“.

106 So *Burchard*, ZIS 2018, 249 (260).

107 Vgl. *Brodowski*, ZIS 2018, 493 (504).

108 So *Burchard*, ZIS 2018, 249 (259, 260); vgl. auch *Weißer*, in: Schulze/Janssen/Kadelbach, Europarecht, § 16 Rn. 100.

109 *Burchard*, ZIS 2018, 249 (260); *ders.*, ZRP 2019, 164 (166); *Warken*, NZWiSt 2017, 417 (422); vgl. auch *Schaar*, MMR 2018, 705 (706).

110 *Burchard*, ZIS 2018, 249 (252).

Zudem kann die Zugriffsidee der E-Evidence-Verordnung Diensteanbieter in die Bredouille bringen, wenn sie strafprozessuale Mitwirkungspflichten treffen, die datenschutzrechtlichen bußgeldbewehrten Handlungsverboten gegenüberstehen.[111] In der DS-GVO bestehende Ausnahmen, insb. Art 49 Abs. 1 S. 2 DS-GVO, reichen zur Auflösung dieses Spannungsverhältnisses nicht aus.[112] Hier ist Abhilfe dringend erforderlich.

5. Zwischenergebnis

Auch wenn mit der Notifikationslösung Kollisionen nationaler Strafverfolgungsinteressen mit Interessen des betroffenen europäischen Staates hinsichtlich seiner Souveränität und Gebietshoheit durch dessen Zustimmung vermieden werden, bleibt es bei unilateralen Zugriffen auf Daten in Drittstaaten bei der festgestellten Völkerrechtswidrigkeit. Zudem drohen ohne gegenseitige staatliche Kontrollmechanismen auch mit Blick auf europäische Staaten erhebliche Nachteile für den Grundrechtsschutz der von dem Zugriff betroffenen Personen. Die Privatisierung des staatlichen Rechtshilfeverfahrens durch den unmittelbaren Zugriff bei privaten Diensteanbietern ohne zwischen- oder nachgeschaltete staatliche Prüfung begründet weitere Nachteile für den Grundrechts- und Datenschutz. Es verstößt gegen den in der Europäischen Union zu gewährleistenden Grundrechtsschutz, Private ohne jegliche Regulierung der internen Prüfverfahren und ohne Interventionsmöglichkeiten des betroffenen Staates ausländische Beibringungsanordnungen prüfen zu lassen.[113]

V. Alternative Lösungsmöglichkeiten

Der in der E-Evidence-Verordnung vorgesehene unilaterale Zugriff ist zudem nicht alternativlos. Zuzugeben ist, dass auch andere Staaten, insb. die USA, diesen Weg gewählt haben, man also unilaterale Datenzugriffe auf internationaler Ebene durch einen entgegengesetzten europäischen Weg wohl nicht gänzlich verhindern kann. Andererseits ist das kein Grund, dem blindlings zu folgen und den eigenen Grundrechts- und Datenschutz aufs Spiel zu setzen, zumal das Vorgehen der USA mit europäischen Sicherheitsinteressen kollidiert.[114] Die Erleichterung strafverfolgungsbehördlicher Zugriffe auf Cloud-Daten und damit die Sicherung einer effektiven Strafverfolgung auch im digitalen Zeitalter ist ein legitimes Anliegen. Das Interesse an einer effektiven Strafverfolgung ist aber nur eines der betroffenen Interessen, die angemessen in Ausgleich gebracht werden müssen. Eine einseitige Abwägung zugunsten der Strafverfolgung kann daher keine angemessene Lösung sein.

Rückt man vom Ansatz unilateraler Zugriffsmöglichkeiten ab und verbleibt stattdessen bei traditionellen Rechtshilfeverfahren,[115] so bietet dies den Vorteil, dass die internationale Sicherheitszusammenarbeit auch mit Blick auf Clouddaten vorangetrieben werden könnte, ohne nationale Grundrechtsstandards aufzugeben. Um die Rechthilfeverfahren zu beschleunigen, wäre ein Ausbau der personellen Kapazitäten, technischer Infrastrukturen und eine bessere Koordination und damit Zusammenarbeit internationaler Strafverfolgungsorgane wünschenswert.

Die Ermöglichung der Identifizierung des zu ersuchenden Staates könnte mit einer Verpflichtung der Strafverfolgungsorgane zu Nachforschungen über den konkreten Speicherort – also zur Nachverfolgung via Traceroute – erreicht werden.[116] Hilft Traceroute angesichts von Cloud-Speichermodellen mit ständig wechselnden, nicht dauerhaften Speicherorten nicht weiter, so sollten Diensteanbieter zur Einführung technischer Mechanismen verpflichtet werden, mithilfe derer sie in der Lage sind, auf Anfrage der Strafverfolger den Datenspeicherort preiszugeben.[117]

Andere wirtschaftsverwaltungsrechtliche Lösungen wie etwa ein Lokalisierungszwang der Daten[118] im Inland (sog. Daten-Nationalismus)[119] sollten mit Blick auf die Datensicherheit, die Interessen der Diensteanbieter und der Offenheit des Internet unterbleiben.[120] Das Vorhalten von Daten oder Spiegelungen der betroffenen Daten auf „festen“ Servern, würde in einer echten Vorratsdatenspeicherung münden, die wiederum mit Blick auf den Grundrechts- und Datenschutz zu vermeiden ist.[121] Bei grenzüberschreitender Speicherung mit ständigem Standortwechsel eine personale Anknüpfung am verdächtigen Nutzer statt am Datenstandort vorzunehmen,[122] würde wieder eine Abkehr vom Territorialitätsgrundsatz bedeuten, die nach hier vertretener Ansicht unbedingt im Sinne der Wahrung des Grundrechts- und Datenschutzes unterbleiben muss.

Damit Cloud-Nutzer wissen, wo sich ihre Daten befinden und vor allem, welchen Unterschied das für den eigenen Grundrechts- und Datenschutz haben kann, ist in jedem Fall eine echte Aufklärung der Nutzer durch die Diensteanbieter notwendig und schon lange überfällig.[123] Das gilt nicht nur für den hier vorgeschlagenen Lösungsweg, sondern gerade auch dann, wenn Zugriffe unilateral zugelassen werden sollen.[124] Nur wenn der Nutzer weiß, welche

111 *Warken*, NZWiSt 2017, 417 (422); *Burchard*, ZIS 2018, 249 (254) m.w.N. und Beispielen.
112 Vgl. *Burchard*, ZIS 2018, 249 (254) m.w.N., nach dem zwar ein einmaliger Zugriff nach Art. 49 Abs. 1 S. 2 DS-GVO erfasst wäre, nicht aber unilaterale Datenzugriffe als Grundsatz.
113 *Burchard*, ZIS 2018, 249 (259 f.).
114 *Burchard*, ZRP 2019, 164 (165.).
115 So *Chander/Lê*, Emory LJ, 2015, 677 (735) im Verhältnis zu Lokalisierungspflichten; auch *Burchard*, ZRP 2019, 164 (167); *ders.*, ZIS 2018, 190 (192).
116 Vgl. *Dalby*, S. 246; in diese Richtung auch *Gercke*, in: HK-StPO, § 110 Rn. 29; *Brodowski*, in: BeckOK-IT, § 110 StPO Rn. 12.2.
117 Das können ggf. auch mehrere Orte sein. Vgl. *Bell*, S. 221; *Dalby*, S. 245.
118 Oder auch Zwang zur Spiegelung der Daten ins Inland wie in Vietnam, s. hierzu *Chander/Lê*, Emory LJ, 2015, 677 (704 f.), um sie für Zugriffe staatlicher Akteure verfügbar zu halten.
119 Hierzu *Chander/Lê*, Emory LJ, 2015, Vol. 64, 677 ff., mit Blick auf Lokalisierungspflichten in Russland (701 f.) und Vietnam (704 ff.).
120 Vgl. hierzu ausführlich *Chander/Lê*, Emory LJ, 2015, 677 (713 ff.); s. auch *Burchard*, ZIS 2018, 249 (253).
121 So aber *Dalby*, S. 245.
122 So *Bell*, S. 223 f.
123 Vgl. *Burchard*, ZIS 2018, 249 (253).
124 *Burchard*, ZRP 2019, 164 (166 f.).

Folgen sich durch die Nutzung der gewählten Cloud inkl. ihrer Speicherpolitik für die Sicherheit seiner Daten vor Zugriffen Dritter (eben auch Strafverfolgungsbehörden) ergeben, kann er eine selbstbestimmte Wahl treffen. [125] Diese Aufklärung sollte daher nicht nur als Bestandteil einer ausgreifenden Einwilligungserklärung ausgestaltet sein, sondern vielmehr so, dass ohne große Mühe Konsequenzen nachvollziehbar sind. Denkbar wäre etwa eine Art Video (analog zu den Sicherheitsvideos im Flugzeug) oder andere Arten von Visualisierung, die obligatorisch zu durchlaufen sind, bevor der Nutzungsvertrag abgeschlossen werden kann.[126]

VI. Ausblick

Ein einheitliches internationales Vorgehen ist bei Zugriffen auf im Ausland gespeicherte Daten im Sinne einer effektiven Strafverfolgung wünschenswert.[127] Die Etablierung unilateraler Zugriffe ist dabei jedoch nicht zielführend und würde nicht weniger als den (europäischen) Grundrechts- und Datenschutz kosten.[128] Folgen andere Staaten dem Vorbild der vorgeschlagenen E-Evidence-Verordnung, was durchaus zu erwarten ist,[129] so würde auch die Europäische Union mit unzähligen Herausgabeanordnungen konfrontiert, die ihren eigenen Sicherheitsinteressen zuwiderlaufen können, die sie aber mit Blick auf ihr eigenes Vorgehen kaum ohne politische Spannungen[130] ablehnen könnte.[131] Könnten Drittstaaten wie etwa China oder Russland dann unilateral mehr oder weniger nach Belieben auf europäische Daten zugreifen, so bliebe von dem „europäischen Grundrechts- und Datenschutzschild“ nicht mehr viel übrig. Die Europäische Union müsste damit entgegen ihrer eigenen Überzeugung zugunsten internationaler Sicherheitszusammenarbeit nicht nur fundamentale Interessen ihrer eigenen Bürger, sondern letztlich auch einen Teil ihrer eigenen Souveränität für den internationalen effektiven strafverfolgungsbehördlichen Zugriff auf Cloud-Daten abgeben.[132]

Bleibt es außerdem beim Verzicht auf eine Regulierung des dann privaten Quasi-Rechtshilfeverfahrens, so entsteht eine hohe Missbrauchsgefahr hinsichtlich gefälschter Herausgabeanordnungen oder Drittzugriffen auf unregulierte, mindergut geschützte Übertragungswege. So kämen auch Kriminelle an grundrechtssensible Daten und könnten diese etwa zur Erpressung Betroffener nutzen oder verkaufen. Autoritären Staaten wäre es sogar ohne weiteres möglich, die Daten zur Destabilisierung anderer Staaten oder dazu zu nutzen, Regimegegner aufzuspüren und zum Schweigen zu bringen.

In gesellschaftlicher Hinsicht kann ein solches Vorgehen auch Auswirkungen auf das künftige Nutzerverhalten haben. Eine Vielzahl der Internetnutzer könnte sich aus Clouds zurückziehen und auf lokale Speicher setzen, sich datensparsam verhalten, sich auf den Cloud-Markt im Dark Web beschränken oder aber, was wohl wahrscheinlicher ist, stärkere Verschlüsselungsmechanismen einsetzen. Insbesondere die zu erwartende verstärkte Verschlüsselung stünde dann wieder einer effektiven Strafverfolgung entgegen.[133] Was nützen unilaterale Zugriffe, wenn sie nur noch verschlüsselte Daten hervorbringen? Auch mit Blick auf die weitere Entwicklung des Internet ist zu befürchten, dass der digitale Grundrechtsschutz zunehmend ausgehebelt wird. Man denke hier heutzutage schon an ausgelagerte Daten etwa von Krankenkassen – mit Blick auf Prognosen in Richtung E-Identities und E-Wallets wären solch höchstsensible Daten dann gar individuell zusammengeführt mit einem Klick quasi auf der gesamten Welt erhältlich.

---

125 Vgl. *Burchard*, ZIS 2018, 249 (253).

126 Auch diese Art der Aufklärung wird nicht jeden Nutzer „abholen“, die Zahl aufgeklärter Internetnutzer aber zumindest erhöhen.

127 Auch *Burchard*, ZRP 2019, 164 (167).

128 Vgl. *Weißer*, in: Schulze/Janssen/Kadelbach, Europarecht, § 16 Rn. 100.

129 Vgl. *Burchard*, ZRP 2019, 164 (165 f.); *Brodowski*, ZIS 2018, 493 (504); *Weißer*, in: Schulze/Janssen/Kadelbach, Europarecht, § 16 Rn 100. Sofern nicht als Gegenreaktion mit einer Lokalisierungspflicht geantwortet wird und unilaterale Zugriffe unilateral unterbunden werden.

130 Vgl. *Burchard*, ZRP 2019, 164 (165).

131 Vg.l ebd.; *Brodowski*, ZIS 2018, 493 (504).

132 Vgl. *Brodowski*, ZIS 2018, 493 (504).

133 Vgl. auch *Burchard*, ZRP 2019, 164 (166).