Präventive Datenerhebung in informationstechnischen Systemen bei grenzüberschreitenden Sachverhalten – aktuelle Rechtslage und Reformvorschlag

Matthias Haag

I. Einleitung

Der Beitrag befasst sich mit der Rechtmäßigkeit der Datenerhebung in informationstechnischen Systemen durch die gefahrenabwehrrechtlichen Ermittlungsbehörden bei grenzüberschreitenden Sachverhalten, wenn Daten physisch-geographisch nicht im Inland lokalisiert sind. Dabei werden besonders Cloud-Dienste in den Blick genommen, bei welchen die Server ihren Standort nicht in einem Mitgliedsstaat der EU haben. Abschließend wird ein Reformvorschlag aufgezeigt.

Große Datenmengen werden häufig auf Cloud-Servern von Dienstanbietern im In- und Ausland ausgelagert.[1] Unzählige alltägliche Programme arbeiten mit Cloud-Softwarekomponenten, insbesondere auch Sprachassistenz-Systeme. Aufgrund von Datenschutzbedenken gab es diesbezüglich auch Überlegungen einer sog. „Deutschland"-Cloud.[2] Diese hat sich im alltäglichen Gebrauch von Cloud-Diensten jedoch bisher nicht durchgesetzt. Aufgrund dessen, dass „aus" dem Internet heraus weitere Gefahrenkomplexe resultieren, ist das Internet im digitalen Zeitalter auch ein „Zuständigkeitsraum" von Gefahrenabwehrbehörden.[3] Auf Legislativebene ist aktuell der bayerische Landesgesetzgeber Vorreiter mit einer Regelung in Art. 25 III PAG.[4] Nachdem Cloud-Dienste weltweit eingesetzt werden und scheinbar keine geographischen Grenzen kennen, ergeben sich im Rahmen der Datenerhebung durch die Gefahrenabwehrbehörden signifikante rechtliche Fragestellungen. Nachdem erst wenige Gesetzgebungsakteure die Besonderheiten von grenzüberschreitenden Cloud-Diensten aufgegriffen haben, unternimmt dieser Beitrag einen Versuch, genauer den Stand de lege

1 *Liebig,* Zugriff auf Computerinhaltsdaten im Ermittlungsverfahren, Cloud Computing, Trier 2015, S. 47; *Bär* ZIS 2011, 53 (53).
2 *Steidle* in Jandt/Steidle (Hrsg.), Datenschutz im Internet, S. 256 Rn. 75.
3 *Hsieh,* E-Mail-Überwachung zur Gefahrenabwehr, Stuttgart 2011, S. 34 f.
4 Siehe *Michl* NVwZ 2019, 1631 (1631).

lata aufzuzeigen. Im repressiven Bereich wurden die dahinterstehenden Fragestellungen bereits umfangreich disputiert. Jedoch ergeben sich im Recht der Gefahrenabwehr möglicherweise Differenzen im Vergleich zur Datenerhebung zum Zwecke der Strafverfolgung. Diesbezüglich könnten sich Besonderheiten durch die Cybercrime-Konvention[5] (CCC) und ferner durch das Unionsrecht, insbesondere durch die JI-RL[6], ergeben.

II. Grundlagen

Im Rahmen von Cloud-Computing werden mehrere Server als sog. Cloud[7] i. e. S. verbunden, welche über ein Netzwerk erreichbar ist, damit der Nutzer auf „den" Cloud-Server zugreifen kann, um die dortige Hardware und Software verwenden zu können,[8] welche von einem Provider zur Verfügung gestellt werden.[9] Der Cloud-Server kann letztlich wie ein zusammenhängender Server verwendet werden.[10] Ein Vorteil von Cloud-Angeboten ist, dass mit zahlreichen netzwerkfähigen Geräten ein Zugriff auf Cloud-Systeme stattfinden kann.[11]

Eine eng umrissene Definition für Cloud-Dienste selbst findet sich jedoch nicht.[12] Folgt man der Definition des National Institute of Standards and Technology (NIST),[13] werden Cloud-Dienste in Software as a Service

---

5 Europarat, Vertrag Nr. 185, Übereinkommen über Computerkriminalität, Budapest, 23.XI.2001.

6 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABL. L 119/89 v. 4.5.2016.

7 Zur Entstehung des Begriff desCloud Computing siehe: *Hentschel/Leyh*, in Reinheimer (Hrsg.), Cloud Computing, Wiesbaden 2018, S. 4.

8 *Giedke*, Cloud Computing, München 2013, S. 43 f.; siehe auch die Differenzierungen bei: Schuster/Reichl, CR 2010, 38.

9 *Schulz/Rosenkranz* ITRB 2009, 232 (232 f.).

10 *Lehmann/Giedke* CR 2013, 608 (609).

11 *Lehmann/Giedke* CR 2013, 608 (608).

12 *Heckmann/v. Lucke/Hennrich/Maisch*, C3-Studie, Sicheres IT-Outsourcing, S. 8; vgl. *Hennrich*, Cloud Computing, Berlin 2015, S. 56.

13 National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Special Publication 800-145, September 2011, abrufbar unter: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf; weitgehend überzeugende Vorschläge einer Reform dieser Definition finden sich bei:

(SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) unterteilt. Im Rahmen von IaaS wird lediglich die Hardware zur Verfügung gestellt und der Nutzer muss selbst notwendige Softwarekomponenten implementieren und ausführen.[14] PaaS-Dienste stellen zwar eine Softwareumgebung zur Verfügung, der Nutzer verwendet innerhalb dieser Softwareumgebung jedoch weitere eigene Softwareanwendungen.[15] Im Rahmen von SaaS-Diensten wird auch die für den Nutzer des Dienstes notwendige Software über eine Cloud-Infrastruktur zur Verfügung gestellt, wobei der Nutzer jedoch die Anwendungen selbst kontrolliert.[16]

Weiterhin wird zwischen Public, Community, Private und Hybrid Clouds differenziert, abhängig davon, wem die jeweilige Cloud zur Verfügung steht (einer einzelnen Organisation, einer Gemeinschaft, der Öffentlichkeit oder einem Konglomerat von z. B. einer Cloud für Privatpersonen und einer Cloud für die Öffentlichkeit).[17]

Auch wenn diesen Cloud-Diensten unterschiedliche Servicemodelle zugrunde liegen, besteht eine Gemeinsamkeit darin, dass letztlich die vom Nutzer gespeicherten Daten auf einem Server des Cloud-Dienstanbieters gespeichert sind.

1. Virtualisierung

Der technische Hintergrund für die Aufteilung auf mehrere Server ist zu untersuchen, um analysieren zu können, inwieweit dies Auswirkungen auf die rechtlichen Fragestellungen hat.[18]

Um Cloud-Dienste technisch umsetzen zu können, bedarf es der sog. Virtualisierung.[19] Mit Hilfe der Virtualisierung werden Hardware-Systeme miteinander verbunden und für die logische Nutzung von physischen Res-

---

den Haan, The cloud landscape described, categorized, and compared, abrufbar unter: http://www.theenterprisearchitect.eu/blog/2013/10/12/the-cloud-landscape-described-categorized-and-compared, sowie: *Miyachi*, What is "Cloud"? It is time to update the NIST definition?, in: IEEE Cloud Computing, vol. 5, no. 03, pp. 6-11, 2018.

14 NIST a.a.O.

15 NIST a.a.O.

16 NIST a.a.O.

17 NIST a.a.O.; vgl. *Liebig,* a.a.O., S. 49 f.

18 Siehe auch: *Lehmann/Giedke* CR 2013, 608 (611).

19 *Giedke,* a.a.O., S. 48 m.w.N.

sourcen abstrahiert.[20] Die Virtualisierungstechnik ermöglicht einerseits, dass mehrere Server, die an physisch verschiedenen Standorten verteilt sind, als ein umfassender virtueller Server funktionieren.[21] Im Umfang der Berechtigung zur Nutzung der Cloud-Komponenten dient die Virtualisierung auch der Aufteilung dieses umfassenden virtuellen Servers an die jeweiligen Nutzer.[22] Der Cloud-Anbieter weist dem jeweiligen Cloud-Nutzer, dann insbesondere in Abhängigkeit der Intensität der Nutzung, einen Ressourcenanteil zu.[23] Erfolgt ein Zugriff auf die Daten, werden die auf den Servern gespeicherten fragmentierten Datensätze wieder zusammengeführt.[24] Von „außen" betrachtet ist der finale Speicherort quasi zufällig.[25]

2. *Standortbestimmung der Cloud-Daten*

Selbst mit einer möglichen IP-Adresse der Cloud-Server ist eine Lokalisierung des (geographischen) Serverstandortes nicht ohne weiteres möglich, weil mit dieser nicht zwingend auf den Serverstandort geschlossen werden kann.[26] Zu beachten ist weiter, dass die Daten nicht zwingend auf einem bestimmten Server lokalisiert sind, sondern dass Datenpakete verschiedenen Servern der Cloud zugeteilt sind.[27] Teilweise setzen Unternehmen auch KI-Systeme zur Optimierung der Speicherprozesse ein, was dazu führt, dass den Unternehmen zunehmend selbst der Ort der gespeicherten Daten unbekannt ist.[28] Von außen kann u. U. nicht exakt der Datenstandort lokalisiert werden. Diesbezüglich besteht ein Problem darin, dass auf Daten zugegriffen werden soll, die nicht geographisch einem Server und damit auch nicht einem Land zugeordnet werden können.

---

20 *Bedner*, Cloud Computing, Kassel 2013, S. 39 m.w.N.; vgl. *Pohle/Ammann* CR 2009, 273 (274).
21 *Lehmann/Giedke* CR 2013, 608 (611).
22 *Lehmann/Giedke* CR 2013, 608 (611 f.); BSI, IT-Grundschutz-Kompendium, Stand: Februar 2020, SYS. 1.5.
23 *Schneidereit,* Haftung für Datenverlust im Cloud Computing, Baden-Baden 2017, S. 46.
24 *Bell*, Strafverfolgung und die Cloud, Berlin 2019, S. 175 u. S. 194.
25 *Bell*, a.a.O., S. 176 u. S. 194.
26 *Bär* ZIS 2011, 53 (54); vgl. *Hoeren* MMR 2007, 3 (5 f.); *Mitsdörffer/Gutfleisch* MMR 2009, 731 (732).
27 *Giedke*, Cloud Computing, München 2013, S. 44.
28 College van procureurs-generaal (2019A001) Staatscourant 2019, 10277 vom 26.2.2019 (abrufbar unter: https://zoek.officielebekendmakingen.nl/stcrt-2019-10277.html); vgl. auch *Pohle/Ammann* CR 2009, 273 (277); *Bär* ZIS 2011, 53 (54).

3. Zeitpunkt der Datenerhebung

Im Rahmen einer Datenerhebung durch die Gefahrenabwehrbehörden muss differenziert werden, zu welchem Zeitpunkt auf die Daten zugegriffen wird. Dies kann zum einen während des Übertragungsvorganges der Daten an die Cloud-Server sein, während der Nutzer die Daten auf seinem Endgerät bearbeitet oder jedoch während diese bereits auf einem Cloud-Server gespeichert sind. Für die hier relevanten Fragestellungen wird – im Schwerpunkt – der Zeitpunkt, zu dem die Daten auf dem Cloud-Server gespeichert sind, betrachtet.

4. Präventive Datenerhebung

Im Rahmen dieses Beitrages meint die Erhebung von Daten im Internet, wenn Daten von einem Datenspeichermedium über das Internet abgerufen werden.[29]

Das deutsche Recht unterscheidet zwischen der präventiven und repressiven Zwecksetzung eines Einschreitens durch die Behörden. Dabei können jedoch sog. doppelfunktionelle Maßnahmen auftreten.[30] Bei diesen Maßnahmen, die sowohl präventiven als auch repressiven Zwecken dienen, ist im Rahmen der Abgrenzung auf den jeweiligen Einzelfall abzustellen und der objektiv erkennbare Zweck der Maßnahme zu betrachten.[31] Im Rahmen einer Schwerpunktbetrachtung ist beim Abruf von Daten auf externen Servern zu untersuchen, ob die Behörde weitere Indizien für eine Täterschaft finden möchte oder, ob die Verhinderung einer weiteren Verbreitung im Vordergrund steht. Im letztgenannten Fall liegt ein präventives Einschreiten der Sicherheitsbehörde vor.[32] Der Fokus dieses Beitrages liegt auf dem präventiven Einschreiten der Behörden.

---

29 Vgl. *Perry*, Gefahrenabwehr und Internet, Berlin 2003, S. 74.

30 *Götz/Geis*, Allgemeines Polizei- und Ordnungsrecht, 16. Aufl., München 2017, S. 210 ff.; *Keller/Braun/Hoppe*, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, 2. Aufl., Stuttgart u.a. 2015, S. 120.

31 *Bär*, in Wabnitz/Janovsky WirtschaftsStrafR-HdB, 28. Kapitel, EDV-Beweissicherung Rn. 127; vgl. differenzierter bei *Götz/Geis,* a.a.O., S. 210 ff.

32 *Bär*, a.a.O., Rn. 127; vgl. auch *Keller/Braun/Hoppe*, a.a.O., S. 119 f.

III. Landesrechtliche und bundesrechtliche Ermächtigungsgrundlagen

Im bayrischen Landespolizeirecht findet sich nicht nur eine Regelung zur Datenerhebung durch die Polizeibehörden (Art. 32 PAG), sondern seit 2018 auch eine Norm, welche es im Rahmen der Durchsuchung von Sachen (Art. 22 II PAG) ermöglicht, auf einen von der Sache entfernten Speicherort – wie einen Cloud-Server – zuzugreifen, wenn dieser von dem zu durchsuchenden Objekt als Endeinrichtung benutzt wird.[33]

Neben der offenen Maßnahme des Art. 22 II PAG, haben die Polizeibehörden weiterhin in Art. 45 PAG eine Ermächtigungsgrundlage für einen verdeckten Eingriff in ein informationstechnisches System. Zudem kann von diesem auch eine Datenerhebung auf ein davon getrenntes, aber vom Betroffenen genutztes weiteres informationstechnisches System erfolgen. Weiterhin besteht nach Art. 25 III PAG die Möglichkeit, Daten sicherstellen zu können.

Auch in anderen Bundesländern finden sich Regelungen zur Erhebung von Daten auf informationstechnischen Systemen, insbesondere die Regelungen in Baden-Württemberg zur Datenerhebung nach §§ 19 ff. PolG BW oder die Regelung in Rheinland-Pfalz in § 31c POG R-P zur Datenerhebung in informationstechnischen Systemen. Auf Ebene des Bundesrechts findet sich insbesondere noch § 49 BKAG.[34]

Es bleibt zu berücksichtigen, dass eine nationale Rechtsgrundlage nicht zu einem Zugriff auf Daten ermächtigt, welche im Ausland gespeichert sind, sondern dies zu einer Verletzung fremder Souveränitätsrechte führen kann.[35] Deswegen kann im Rahmen des Ermessens der jeweiligen Gefahrenabwehrbehörde zu berücksichtigen sein, ob die Zugriffsmöglichkeiten auf die jeweiligen Daten aufgrund eines extraterritorialen Sachverhaltes, begrenzt sind.[36]

---

33 BeckOK PolR Bayern/*Grünewald*, 11. Ed. 10.11.2019, PAG Art. 22 Rn. 22; vgl. *Weinrich*, NVwZ 2018, 1680 (1680).

34 Allerdings erfüllen wohl wenige gefahrenabwehrrechtliche Regelungskomplexe die Anforderungen der Entscheidung vom BVerfG, NJW 2016, 1781 (1794 f., Rn 211 ff.) (siehe hierzu *Roggenkamp*, in Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 21 Rn. 47). Nach der Entscheidung des BVerfG zu § 20k BKAG sind auch vernetzte fremde IT-Systeme wie eine Cloud umfasst (BVerfG, NJW 2016, 1781 (1794, Rn. 209)).

35 *Bär* ZIS 2011, 53 (54) (zur StPO); a.A. wohl *Wicker* MMR 2013, 765 (768 f.).

36 *Michl* NVwZ 2019, 1631 (1634).

IV. DS-GVO und JI-RL

Es ist zu untersuchen, welche Besonderheiten aus dem Unionsrecht folgen. An die gefahrenabwehrrechtliche Datenverarbeitung ergeben sich insbesondere Anforderungen aus der DS-GVO und der JI-RL.

Im Rahmen der DS-GVO ist zu beachten, dass die DS-GVO nach Art. 2 II lit. d DS-GVO nicht sachlich anwendbar ist, wenn es u. a. um Zwecke der Strafermittlung und Strafverfolgung „einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" geht. Hinsichtlich eines solchen Schutzes ist die JI-RL anwendbar (vgl. Art. 1 JI-RL). Es ist zu berücksichtigen, dass gefahrenabwehrrechtliche Maßnahmen der DS-GVO unterliegen sollen, wenn diese nicht im Zusammenhang mit einer Straftat fallen. [37] Allerdings unterfallen unter den Begriff der Straftaten nach dem Unionsrecht auch Ordnungswidrigkeiten.[38] Insoweit kann die JI-RL auch im Rahmen des (deutschen) Gefahrenabwehrbegriffes Berücksichtigung finden.[39] Demnach ist im Rahmen einer deutschen Rechtsanwendung zu unterscheiden zwischen Maßnahmen der Gefahrenabwehr, welche im Zusammenhang mit einer Straftat (oder Ordnungswidrigkeit) stehen und somit unter den Anwendungsbereich der JI-RL fallen und Gefahrenabwehrmaßnahmen, die keinen Zusammenhang zu einer Straftat (oder Ordnungswidrigkeit) haben und daher dem Anwendungsbereich der DS-GVO unterliegen.[40]

Hieraus resultiert, dass u. U. im Rahmen der Übermittlung von Daten Art. 35 ff. JI-RL oder Art. 44 ff. DS-GVO beachtet werden müssen.

V. Völkerrecht

Der Zugriff von Daten auf Auslandsservern hat möglicherweise völkerrechtliche Implikationen. Die innerstaatliche Anwendung des Völkerrech-

37 *Roßnagel*, in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 2 Rn. 40.

38 *Sysdow*, in Sydow, Bundesdatenschutzgesetz, Einleitung Rn. 19; *Roggenkamp*, a.a.O., § 21 Rn. 8 m.w.N.

39 *Schröder*, in BeckOK PolR BW, Einführung JI-RL Rn. 25.

40 Siehe auch: *Roggenkamp*, a.a.O., § 21 Rn. 8 m.w.N. Weiterhin Bedarf es einer einschränkenden Auslegung (vgl. Art. 2 II lit. b DS-GVO), daneben ist die JI-RL nicht im Bereich der GASP anwendbar (*Schröder*, in BeckOK PolR BW, Einführung JI-RL Rn. 16).

tes in Deutschland regeln Art. 25 GG und Art. 59 II GG.[41] Nach Art. 25 GG sind die allgemeinen Regeln des Völkerrechts vorrangig, zumindest vor dem einfachen Recht, zu berücksichtigen. Art. 59 II GG regelt die Inkorporation von völkerrechtlichen Verträgen in das Bundesrecht.

Aus der Souveränität eines Staates leitet sich dessen Gebietshoheit ab.[42] Der jeweilige Staat hat die umfassende Regelungsgewalt auf seinem Territorium und die exklusive Befugnis zur Ausübung von Hoheitsakten.[43] Aufgrund des Gebotes der Achtung der Gebietshoheit ist grundsätzlich kein Staat berechtigt, auf ein fremdes Territorium einzuwirken und dort hoheitlich tätig zu werden.[44] Fremde Staaten benötigen eine Erlaubnis, wenn sie Hoheitsgewalt in einem anderen Staat ausüben möchten.[45] Ein völkerrechtliches Delikt liegt dabei vor, wenn ein Hoheitsakt eines anderen Staates auf einem fremden Staatsgebiet einwirkt und einem Hoheitsakt dort gleichkommt.[46]

1. Virtueller Grenzübertritt

Es ist dabei nicht unumstritten, ob ein sog. virtueller Grenzübertritt[47] ein Handeln auf dem Territorium eines anderen Staates darstellt, weil bei diesem „Übertritt" der jeweilige Beamte seine Ermittlung aus dem Inland unternimmt und nie das Hoheitsgebiet verlässt.[48] Ein staatliches Handeln auf fremden Hoheitsgebiet ist nicht zwingend unter ein „hoheitliches" Han-

41 *Maunz/Dürig/Herdegen*, 88. EL August 2019, GG Art. 25 Rn. 3.
42 BVerfG, Bes. v. 5.11.2003 - 2 BvR 1506/03, BeckRS 2003, 2507, Rn. 46.
43 *Herdegen*, Völkerrecht, 19. Aufl., München 2020, § 23 Rn. 1 ff.; vgl. *Maunz/Dürig/Herdegen*, a.a.O., GG Art. 25 Rn. 47.
44 *Greve,* Access-Blocking - Grenzen staatlicher Gefahrenabwehr im Internet, Berlin 2012, S. 176; *Dombrowski,* Extraterritoriale Strafrechtsanwendung im Internet, Berlin u.a. 2014, S. 5 m.w.N.; vgl. auch *Altwicker* in Kugelmann (Hrsg.) Migration, Datenübermittlung und Cybersicherheit, Baden-Baden 2016, S. 120.
45 *Stelkens/Bonk/Sachs*, VwVfG, 9. Aufl. 2018, 2. Teil, Europäisches Verwaltungsrecht u. a. Rn. 246; vgl. *Ewer/Thienel* NJW 2014, 30 (31) m.w.N.; *Maunz/Dürig/Herdegen*, 88. EL August 2019, GG Art. 25 Rn. 47.
46 *V. Münch*, Das völkerrechtliche Delikt, S. 65; vgl. *Bell,* a.a.O., S. 160.
47 Siehe zum Begriff: *Warken* NZWiSt 2017, 289 (295). Siehe ferner zu Unterscheidung zwischen extraterritorialem Hoheitsakt und einem Hoheitsakt auf fremdem Staatsgebiet: *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.
48 Zu repressiven Ermittlungen: *Bell,* a.a.O., S. 158 f.; *Warken* NZWiSt 2017, 289 (295).

deln zu subsumieren; erst wenn dieses in Konkurrenz zur Gebietshoheit eines anderen Staates tritt, liegt ein hoheitliches Handeln vor.[49]

Nach einer Auffassung liegt auch bei einem Zugriff auf einen ausländischen Server durch einen Hoheitsträger ein extraterritorialer hoheitlicher Eingriff auf ein fremdes Hoheitsgebiet vor.[50] Es wird dabei angeführt, wenn bereits bei einer telefonischen oder postalischen Kontaktaufnahme ein Eingriff auf fremdes Territorium vorläge, läge erst Recht ein Eingriff bei einem Zugriff über das Internet vor.[51] Insofern würde auch bei einem Zugriff auf einen Cloud-Server – auch wenn dieser zum Zweck der Gefahrenabwehr durchgeführt wird – ein Eingriff vorliegen.

Nach einer anderen Auffassung liegt bereits kein Eingriff vor, weil sonst die jeweiligen Staaten nicht mehr handlungsfähig seien; vielmehr liegt durch die Duldung von Cloud-Diensten auf dem eigenen Staatsgebiet auch eine Einwilligung in mögliche Eingriffe auf das Hoheitsgebiet in Form von grenzüberschreitenden Behördenzugriffen vor, denn das Handlungsinteresse des zugreifenden Staates überwiege das Abwehrinteresse des Staates, auf dem sich ein Server befindet.[52]

Letztere Ansicht vermag jedoch nicht zu überzeugen. Auch ein nicht unmittelbar plastisch-physischer Übertritt eines Hoheitsgebietes durch einen Hoheitsträger, der auf einen Server zugreift, welcher nicht im Hoheitsgebiet des Staates belegen ist, stellt trotzdem ein Tätigwerden auf fremdem Hoheitsgebiet dar. Ein Datenabruf ist fundamentaler Bestandteil der eigenen Gebietshoheit. Dies leitet sich aus der physisch-geographischen Hoheitsmacht ab, die sich nicht danach festmacht, ob ein körperlicher Gegenstand bewegt wird, sondern ob direkte erhebliche Einwirkungen stattfinden. Solche erheblichen Einwirkungen liegen vor, wenn durch Hoheitsträger Daten auf einem fremden Staatsgebiet abgerufen werden.

---

49 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000, S. 642.

50 *Bär* CR 1995, 227 (234); *Bär* MMR 1998, 577, (579); *Moritz* CR 1998, 500 (509); *Schaumburg*/Englisch, Europäisches Steuerrecht, 2. Aufl. 2020, Grenzüberschreitende Amts- und Rechtshilfe, Rn. 25.2 m.w.N.; vgl. auch: *Schlochauer*, a.a.O., S. 68; *Bär* CR 1995, 227 (234); *Ziebarth*, Online-Durchsuchung, Hamburg 2013, S. 150; *Bell*, a.a.O., S. 192.

51 *Bell*, a.a.O., S. 162.

52 *Bell*, a.a.O., S. 181 f.

2. Unbekannter Standort des Servers

Ein sog. potentieller virtueller Grenzübertritt[53] liegt vor, wenn nicht sicher ist, aber davon ausgegangen werden kann, dass Daten in einem anderen Staat gespeichert sind. Diese Fallkonstellationen sind vergleichbar mit sog. Good Faith-Fällen, bei welchen ein Hoheitsträger irrtümlich davon ausgeht, dass sich das Speichermedium im Inland befindet. Teilweise wird bezüglich eines lediglich möglichen Standortes des Servers im Ausland ein Eingriff abgelehnt.[54]

Bei einer vergleichenden Betrachtung mit einem Polizeibeamten, der ohne Kenntnisse der Ortslage fremde Ländergrenzen überschreitet, würde sich diese Frage nur bedingt stellen. Die Besonderheit eines virtuellen Grenzübertrittes ist, dass dieser schwieriger vorhersehbar ist. Eine tatsächliche Unvorhersehbarkeit sollte aber nicht zu einer Differenzierung bei der rechtlichen formalen Wertung führen. Deswegen liegt auch bei der Nichtlokalisierbarkeit von Daten oder eines potentiellen Grenzübertritts, bei Überschreitung von Staatengrenzen, ein völkerrechtlicher Eingriff vor.[55]

3. Rechtfertigung eines Eingriffes

Ein völkerrechtlicher Eingriff kann jedoch gerechtfertigt sein und damit kein völkerrechtswidriges Handeln eines Staates vorliegen.[56] Die Staatenverantwortlichkeit kann z. B. bei höherer Gewalt ausgeschlossen sein.[57] Dabei kommt eine Rechtfertigung auch aus völkerrechtlichen Verträgen oder aus Völkergewohnheitsrecht in Betracht.

a) Cybercrime-Konvention

Im repressiven Bereich greift die CCC ein. Es ist dabei insbesondere zu untersuchen, ob diese auch im präventiven Bereich anwendbar ist. Sollte

---

53 Zum Begriff siehe *Warken* NZWiSt 2017, 289 (295).
54 Siehe hierzu *Germann*, a.a.O., S. 644 u. S. 654; *Bell*, a.a.O., S. 183.
55 Siehe auch: *Liebig*, a.a.O., S. 61; *Burchard* ZIS 7-8/2018, 249 (251); vgl. *Bell*, a.a.O., S. 183.
56 *Herdegen*, Völkerrecht, a.a.O., § 56 Rn. 1; vgl. auch *Dobrwoski*, a.a.O., S. 11 f. m.w.N.
57 *Schröder* in Völkerrecht (Hsg. v. Vitzthum/ Proelß), 8. Aufl., Berlin u.a. 2019, VII. Abschnitt, Rn. 28, S. 709.

diese nicht anwendbar sein, können möglicherweise Regelungen der CCC für den präventiven Bereich adaptiert werden.

Die CCC ist als völkerrechtlicher Vertrag über Art. 59 II 1 GG i. V. m. dem Transformationsgesetz[58] anwendbar,[59] soweit sie keine Regelungen enthält, welche „allgemeine Regeln" des Völkerrechtes sind und als solche bereits wegen Art. 25 GG beachtet werden müssen.[60]

Art. 32 der CCC enthält eine Regelung hinsichtlich des Zugriffs auf Daten ohne die Genehmigung einer anderen Vertragspartei, wenn die Daten öffentlich zugänglich[61] sind oder wenn die Zustimmung einer Person vorliegt, welche befugt ist über die Daten zu verfügen. Darüber hinaus trifft die CCC keine Regelung hinsichtlich eines Zugriffs auf grenzüberschreitende Daten – außerhalb eines Rechtshilfeersuchens – weil nach Nr. 293 des Erläuternden Berichts[62] zur CCC eine weitergehende Regelung nicht vereinbart werden sollte.[63] Nach Art. 19 II CCC ist nur ein Zugriff auf ein Computersystem, welches auf dem eigenen Hoheitsgebiet des Staates liegt, zulässig.[64] Auch im Bereich von vorläufigen Maßnahmen (bzw. bei einem sog. Quick-Freeze-Verfahren) nach Art. 16, 25 i. V. m. 29 CCC wird der Serverstandort benötigt, um ein Ersuchen an die ermittelnde Behörde weiterzuleiten, weswegen diese Maßnahmen kaum relevant sind.[65]

Die Cybercrime-Konvention regelt nach ihrem expliziten Worten nur den Zugriff auf Daten im Rahmen von Straftaten[66]. Eine umfassende Anwendung im Bereich der Gefahrenabwehr findet sich nicht. Nachdem die CCC erste Minimalstandards setzten wollte (vgl. Nr. 293 Erläuternder Bericht), können auch nicht ohne Weiteres deren Regelungen unmittelbar analog angewandt werden.[67]

---

58 BGBl II/2008 S. 1242; BGBl II/2010 S. 218.

59 *Liebig,* a.a.O., S. 193.

60 Dies ausschließend *Liebig,* a.a.O., S. 193.

61 Können die Daten auf einer Cloud nur von einem bestimmten Endgerät abgerufen werden, so sind diese Daten – auch wenn das Endgerät keinen Passwortschutz hat – nicht öffentlich zugänglich, (*Bell,* a.a.O., S. 204).

62 Erläuternder Bericht zur Cybercrime Konvention vom 23.11.2001.

63 *Bell*, a.a.O., S. 168.

64 Nr. 193 Erläutender Bericht zur Cybercrime Konvention vom 23.11.2001; siehe auch *Miquelon-Weismann*, J. Marshall J. Computer & Info. L. (23/2005), 329 (343).

65 *Bell*, *a.a.O.,* S. 173.

66 In der offiziellen englischen Textfassung: „offences".

67 Vgl. auch *Spannbrucker*, Convention on Cybercrime, Regensburg 2004, S. 3 f.

b) Rechtfertigung aus Völkergewohnheitsrecht

Eine Rechtfertigung kommt jedoch aus Völkergewohnheitsrecht in Betracht. Das Vorliegen von Völkergewohnheitsrecht im Bereich des Internets wird kontrovers disputiert; hauptsächlich aus dem Beweggrund, dass nach völkerrechtlichen Kategorien das Internet tatsächlich ein eher „jüngeres" Phänomen ist.

Der in Art. 32 lit. a CCC geregelte Tatbestand – nämlich der Zugriff auf öffentlich zugängliche Daten – wird als gemeinsame Rechtsauffassung der an der CCC beteiligten Staaten gesehen, weswegen insofern auch außerhalb der CCC von einer gewohnheitsrechtlichen Übung dergestalt auszugehen ist, dass keine Verletzung der Territorialhoheit bei einem Zugriff auf öffentlich gespeicherte Daten vorliegt.[68]

Umstrittener ist eine Rechtfertigung aus Völkergewohnheitsrecht, bei dem in Art. 32 lit. b CCC geregelten Tatbestand in Form des Zugriffs auf Daten auf fremdem Hoheitsgebiet, wenn eine Zustimmung einer verfügungsberechtigten (nicht-staatlichen) Person vorliegt. Nach einer Auffassung gibt es gerade keine Überzeugung der Nichtunterzeichnerstaaten, dass eine Privatperson eigenständig über das Hoheitsgebiet disponieren könne; es bedürfe eines völkerrechtlichen Vertrages und einer Regelung wie Art. 32 lit. b CCC.[69] Diese Auffassung wird auch dadurch bekräftigt, dass bei einem wertungsmäßigen Vergleich mit einer ähnlichen Konstellation, nämlich mit der „Nacheile", eine solche Nacheile nämlich nicht völkergewohnheitsrechtlich anerkannt ist.[70]

Dem wird entgegnet, dass die Regelung in Art. 32 lit. b CCC bereits als völkerrechtlich notwendig angesehen werde und insoweit gewohnheitsrechtlich anerkannt sei.[71]

Im Moment scheint eine völkerrechtliche Übung vordringlich, nach welcher Staaten auf die Daten zugreifen dürfen, wenn eine verfügungsberechtigte Person zugestimmt hat. Ob sich diese Auffassung durchsetzen wird, ist aktuell nicht absehbar. Diese Ansicht ist aber überzeugender, weil die Staatengemeinschaft ein Interesse an ihrer Handlungsfähigkeit hat. Vor diesem Hintergrund ist von der Bildung von Völkergewohnheitsrecht und

68 *Seitz*, Strafverfolgungsmaßnahmen im Internet, Köln u.a. 2004, S. 365 f.; *Dombrowski*, Extraterritoriale Strafrechtsanwendung im Internet, Berlin u.a. 2014, S. 158 m.w.N.; vgl. *Bell*, a.a.O., S. 164; *Blechschmitt* MMR 2018, 361 (364) m.w.N.; a.A. wohl *Ditz* DStR 2004, 2038 (2042).

69 *Dombrowski*, a.a.O., S. 163.

70 *Cremer* ZaöRV 2000, 103 (119) m.w.N.

71 *Bell*, a.a.O., S. 167 u. S. 193.

damit einer deklaratorischen Regelung in Art. 32 CCC auszugehen. Demnach würden aufgrund von Völkergewohnheitsrecht die Regelungen von Art. 32 CCC entsprechend auch für ein präventives Einschreiten gelten. Diesbezüglich läge eine Rechtfertigung aus Völkergewohnheitsrecht vor. Eine solche Regelung würde insoweit auch eingreifen, wenn nicht bekannt wäre, in welchem Land ein Serverstandort ist.

c) Rechtfertigung aufgrund einer Interessenabwägung

Nachdem sich zeigt, dass lediglich im Bereich von öffentlich zugänglichen Daten und bei der Zustimmung eines Verfügungsberechtigten (nach der hier vertretenen Auffassung) eine völkerrechtliche Übung vorliegt, ist zu untersuchen, ob eine Rechtfertigung auch aus anderen Gründen vorliegen kann. Eine weitergehende Rechtfertigung kommt in Betracht, wenn das Interesse des eingreifenden Staates das Abwehrinteresses des betroffenen Staates überwiegt oder die Interessen gleichwertig sind.[72]

Im Rahmen der Rechtfertigung eines Eingriffes muss es sich insoweit um ein hinreichendes Eingriffsinteresse handeln.[73] Ein solches hochwertiges Interesse liegt nur in Fällen vor, in denen es um Bestandsinteressen des Staates geht, etwa bei einer Gefahr für die innere Stabilität.[74] Bei grenzüberschreitenden Maßnahmenwirkungen liegt im Bereich der Internet-Kommunikation keine Verletzung eines fremden Hoheitsgebietes vor, wenn ein Staat auf die Ausübung seiner eigenen Gebietshoheit übermäßig verzichten müsste.[75] Weiterhin kann der Schutz von Individualinteressen ausreichend sein, soweit gewichtige staatliche Schutzpflichten bestehen, wie bei der unmittelbaren Bedrohung des Lebens[76] einer natürlichen Person.[77]

Anders als im Rahmen der Strafverfolgung besteht aufgrund des Gefahrenabwehrzweckes häufig ein höheres Interesse, dass bei der Bedrohung von höherrangigen Rechtsgütern das Territorialitätsinteresse überwiegt. Dies begründet sich vor allem darauf, weil – im Vergleich mit dem Einschreiten zum Zwecke der Strafverfolgung – eine Gefahrenquelle noch besteht und nicht bereits in der Vergangenheit liegt. Allerdings muss es sich

72 *Dombrowski*, a.a.O., S. 167.
73 *Dombrowski*, a.a.O., S. 167.
74 *Dombrowski*, a.a.O., S. 167.
75 *Germann*, a.a.O., S. 644.
76 Eine Schutzpflicht für das Leben kann sich insbesondere aus der EMRK ergeben.
77 *Dombrowski*, a.a.O., S. 167; *Bell*, a.a.O., S. 171 f.

um eine erhebliche Gefahr handeln. Im Einzelfall kommt daher eine Rechtfertigung aus völkerrechtlicher Sicht auch bei präventiven Zugriffen auf Daten bei einer Gefahr für gewichtige Interessen des jeweiligen Staates in Betracht.

VI. Aktuelle Entwicklungen

1. Aktuelle Herangehensweisen

Im belgischen Recht werden Beibringungsanordnungen verwendet, um Dienstanbieter zu verpflichten Daten herauszugeben, auch wenn diese keinen physischen Sitz im Inland haben, sofern diese lediglich im Inland aktiv sind.[78] Die USA gehen mit dem sog. CLOUD-Act in eine ähnliche Richtung.[79] In Vietnam wurde 2013 eine Regelung verabschiedet, aus welcher eine Verpflichtung zur Spiegelung der Daten auf einem Server in Vietnam folgte.[80] Denkbar ist insoweit also auch ein Lokalisierungszwang von Daten, sodass Daten zumindest auch im Inland gespeichert werden müssen.[81]

2. Aktuelle Entwicklungen im Rahmen der Cybercrime-Konvention

Aktuell gibt es Entwürfe einer Reform der CCC. Dabei bestehen Überlegungen ein zweites Zusatzprotokoll zu ratifizieren,[82] welches Regelungen zur gegenseitigen Unterstützung in Notfällen, der direkten Offenlegung von Bestandsdaten und der Ausführung von Anordnungen einer anderen Partei zur beschleunigten Herausgabe von Daten umfasst. Hierbei zeigt sich, dass auf internationaler Ebene im repressiven Bereich vor allem eine Reform in Form eines direkten Vorgehens des ersuchenden Staates gegen-

78 *Daskal*, Vanderbilt Law Review 2018, 179 (191) m.w.N.; *Burchard* ZIS 6/2018, 190 (191) m.w.N.

79 Clarifying Lawful Overseas Use of Data Act, (sec. 105 H.R.1625).

80 *Chander/Lê* Emory Law Journal (Vol. 64 in 2015), 677 (704) m.w.N.; vgl. *Burchard* ZIS 6/2018, 190 (191) m.w.N.

81 *Burchard* ZIS 6/2018, 190 (192, Fn. 19).

82 Cybercrime Convention Committee T-CY (2018)23, Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, Strasbourg, v. 8.11. 2019, (abrufbar unter: https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff).

über einem Dienstanbieter geplant ist, wenn der ersuchte Staat dem Ersuchen stattgibt.

3. Aktuelle Entwicklungen im Unionsrecht

Seit 2018 gibt es einen Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (e-Evidence-VO)[83]. Der e-Evidence-VO-Entwurf legt Regeln für eine Beibringungsanordnung gegenüber Dienstanbietern fest und trifft Regelungen für eine „Privatisierung" des Rechtshilferechts, sowie einer Abkehr vom klassischen Territorialitätsprinzip zum Marktortprinzip.[84] So sieht insbesondere Art. 1 I e-Evidence-VO für den repressiven Bereich vor, dass es ausreichend ist, wenn ein Dienstanbieter Dienstleistungen anbietet, um verpflichtet sein zu können, Beweismittel herauszugeben, unabhängig davon, wo deren jeweiliger Standort ist.

Die aktuellen Entwicklungen gehen insoweit in verschiedene Richtungen.

VII. Reformvorschlag

Aufgrund der vorhergehenden Ausführungen bedarf es aus Gründen der Rechtssicherheit eines multilateralen Vertrages zwischen den Staaten der internationalen Staatengemeinschaft, weil eine Divergenz vorliegt zwischen dem was für Hoheitsträger nötig ist und dem, was nach der aktuellen Rechtslage explizit geregelt ist, um zur Gefahrenabwehr tätig zu werden. Im Nachfolgenden werden nun Überlegungen angestellt, welche Regelungen in einem solchen Vertrag enthalten sein sollten.

---

83 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM(2018) 225 final 2018/0108(COD), Straßburg, den 17.4.2018. In Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, COM(2018) 226 final 2018/0107(COD), Straßburg, den 17.4.2018 wird weiterhin eine Vertreterregelung gleichsam wie in Art. 27 DS-GVO geregelt.

84 *Burchard* ZIS 7-8/2018, 249 (264); *Burchard* ZRP 2019, 164 (165).

1. Widerspruchslösung

Unter dem Ziel ein effizientes Handeln der Gefahrenabwehrbehörden sicherstellen zu können, bedarf es einer Regelung, die mit Hilfe von Fristen, zeitliche Vorgaben an die Dauer der Bearbeitung eines Rechtshilfeersuchens statuiert.

Demnach ist eine Regelung notwendig, die einem Rechtshilfeersuchen im Bereich der digitalen Datenerhebungen gleichsam im Sinne einer Fiktion stattgibt, wenn innerhalb einer Frist von zwei Wochen keine inhaltliche Rückmeldung des ersuchenden Staates erfolgt. Der um Rechtshilfe ersuchende Staat darf auf die Daten eigenständig zugreifen, wenn der ersuchte Staat keine Antwort auf eine Anfrage innerhalb der Frist erteilt. Dieser Reformvorschlag adaptiert dabei das Aufnahmeverfahren aus Art. 21 f. Dublin III-VO[85]. Im Rahmen von Art. 22 VII Dublin III-VO kann ein Mitgliedsstaat verpflichtet sein, eine Person – welche einen Antrag auf internationalen Schutz gestellt hat – aufzunehmen, wenn der ersuchte Mitgliedsstaat auf ein Gesuch dem ersuchenden Mitgliedsstaat nicht innerhalb einer bestimmten Frist eine Antwort erteilt.

Dieses Fristensystem ist auch im Rahmen von grenzüberschreitenden Datenerhebungen zielführend, weil es zur Rechtsklarheit und Effektivität von Rechtshilfeabkommen beiträgt. Durch dieses Umstellen des Systems auf klare Fristen und einer Möglichkeit zu einem Vorgehen bei einer fehlenden Reaktion, wird die Proaktivität gesteigert und die beteiligte Staatengemeinschaft bleibt handlungsfähig. Gleichzeitig sind die Staaten verpflichtet, ihre internen Regelungen an eine zügigere Bearbeitung auszurichten und Bearbeitungsabläufe zu entschlacken, um dem Fristerfordernis nachkommen zu können.

Dabei ist es auch denkbar, dass es einen Widerspruchs-Pool von mehreren Staaten gibt, weil die relevanten Daten zwar in einer Cloud gespeichert sind, die zugrundeliegenden Cloud-Server sich jedoch in mehreren Staaten befinden.

Weiterhin ist es für ein Funktionieren des Systems notwendig, dass der ersuchende Staat auch gegenüber dem jeweiligen Privaten (insb. dem Cloud-Dienstanbieter) direkt eine durchsetzungsfähige Anordnung hat, falls der ersuchte Staat nicht widersprochen hat. Eine vergleichbare Rege-

85 Verordnung (EU) Nr. 604/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist, ABl. L 180 vom 29. Juni 2013, S. 31 ff.

lung (ohne die hier vorgeschlagene Widerspruchslösung) befindet sich insoweit bereits für den repressiven Bereich in dem Entwurf vom 08.11.2019 für ein Zusatzprotokoll zur Cybercrime-Konvention. Hierdurch bedarf es nach einem fehlenden „Widerspruch" keines Mitwirkungserfordernisses des ersuchten Staates und ein weiteres Vorgehen wird nicht durch die Beteiligung eines weiteren Behördenapparats verzögert.

2. Zweigliedriger Widerspruch

Um den besonderen Prüfungserfordernissen eines Staates Rechnung zu tragen, bedarf diese „Widerspruchsregelung" einer Modifikation: Es ist einmal ein endgültiger Widerspruch des ersuchten Staates vorzusehen und weiterhin ein vorläufiger Widerspruch des ersuchten Staates bis zu einer endgültigen Prüfung des Ersuchens. Dieses abgestufte System würde dadurch bei Bedarf eine intensivere Prüfung ermöglichen, insbesondere, wenn eine Abwägung von Grundrechten (und dabei u. a. auch von Datenschutzrechten) in Frage stehen.

3. Geographische Nichtlokalisierbarkeit der Daten

Die hier vertretene Lösung findet hinsichtlich einer Widerspruchsregelung keine Anwendung, wenn nicht lokalisiert werden kann, wo sich die „Daten" überhaupt befinden. Allerdings muss dabei differenziert werden: Sind die Daten unzweifelhaft auf Servern in mehreren bestimmten Staaten gespeichert, wobei aber nicht geklärt werden kann, in welchem Staat sich die Daten befinden, dann kommt diese Widerspruchslösung in Form eines Staaten-Widerspruch-Pools in Betracht.. Um das Funktionieren des Systems zu gewährleisten und die Übersichtlichkeit zu wahren, darf der jeweilige Staaten-Pool jedoch nicht die Anzahl von drei Staaten überschreiten. Soweit mehr als drei Staaten in Betracht kommen muss auch die nachfolgende Gefahr-im-Verzug-Regelung greifen.

4. Gefahr-im-Verzug-Regelungen im Völkerrecht

Nicht nur in Fallkonstellationen, in denen vor der Zwei-Wochen-Frist dieser Widerspruchslösung auf die Daten zugegriffen werden muss, weil dies

zur Gefahrenabwehr notwendig ist, sondern auch in Fällen in denen Daten nicht lokalisierbar sind, bedarf es einer Gefahr-im-Verzug-Regelung[86].

Eine solche Regelung auf internationaler Ebene entsprechend einer physischen „Nacheile“[87] von Polizeibeamten bei der Verfolgung von Personen, ist im virtuellen Raum elementar, um die Handlungsfähigkeit der jeweiligen Staaten zu gewährleisten. Diese „digitale Nacheile“ ist dabei mit einer Anzeigenpflicht (bzw. „Notifikationspflicht“[88]) gegenüber dem Staat, auf dessen Hoheitsgebiet ein virtueller Eingriff vorgenommen wird, zu verbinden, soweit bekannt ist oder nachträglich ohne erheblichen Aufwand ermittelbar ist, gegenüber welchem Staat ein Eingriff vorlag.

Aufbauend auf dieser Anzeigenpflicht einer „digitalen Nacheile“ muss der dann (nachträglich) „ersuchte“ Staat dieser zustimmen. Teilt der ersuchte Staat dabei explizit mit, dass er nicht zustimmt, dann war der Eingriff völkerrechtlich rechtswidrig, es sei denn, der ersuchte Staat darf seine Zustimmung nicht verweigern.[89] Einer Zustimmungsverweigerung kann insbesondere ein überwiegendes Interesse an dem Zugriff auf die Daten durch den ersuchenden Staat entgegenstehen.

5. Problemfelder und Fazit

Eine Problematik besteht, wenn die Folge der Stattgabe eines Ersuchens die Preisgabe von grundrechtlich geschützten Informationen ist. Hierbei können die unterschiedlichen Grundrechtsregimie u.U. kollidieren. Auch kann ein Widerspruchs-System nur durch das (auch passive) Mitwirken der teilnehmenden Staaten funktionieren. Würden sich Staaten beteiligen, die ausschließlich widersprechen oder, die ohne weitere eigene Prüfung ein Rechtshilfeersuchen stellen, dann würde dieses System ad absurdum geführt werden.

Eine mögliche Alternative zu den hier vorgeschlagenen Regelungen stellen die Überlegungen dar, private Cloud-Dienstanbieter im Rahmen des Marktortprinzips zu verpflichten, Daten herauszugeben oder deren Verpflichtung Daten auf Inlandsservern „spiegeln“ zu müssen. Durch diese Verpflichtungen kann das „trägere“ Rechtshilfeersuchen-Verfahren umgangen werden. Allerdings zeigt sich, dass auch private Dienstanbieter

86 Siehe bereits *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society, Würzburg 1998, S. 107, Fn. 239; vgl. *Seitz*, a.a.O., S. 373.
87 Vgl. Art. 41 SDÜ.
88 *Burchard* ZIS 7-8/2018, 249 (256).
89 Vgl. auch: *Burchard* ZIS 7-8/2018, 249 (256).

nicht immer ohne jegliche Prüfung Daten herausgeben.[90] Gleichzeitig stellt es einen erheblichen Eingriff[91] in die jeweiligen Unternehmensrechte dar, wenn Privatunternehmen verpflichtet werden, deren Daten im Inland zu spiegeln.

Auch wenn aufgrund der internationalen Verflechtungen weiterhin eine Widerspruchslösung nicht zu einer Lösung aller Konflikte führen könnte, so wäre diese ein erster Schritt in Richtung einer international geregelten Datenerhebung von Gefahrenabwehrbehörden. Ein möglicher Schutz der Rechte von Betroffenen wird auf völkerrechtlicher Ebene – wie im Rahmen der traditionellen Mediatisierung[92] von Völkerrechten – mit Hilfe dieser Widerspruchslösung (zumindest auch) durch den Staat des Standortes des Cloud-Servers[93] gewährleistet. Gegen diesen Standortstaat eröffnen sich insoweit i. d. R. einfachere Rechtsschutzmöglichkeiten – nicht nur aus der Sicht des jeweiligen Cloud-Dienstanbieters.

Zwar können diese Regelungen nicht allein das Problemfeld der grenzüberschreitenden Datenerhebung lösen. Die hier vorgeschlagenen Regelungen führen aber zu einem völkerrechtlich geregelten Vorgehen, welches die Interessen des ersuchten Staates an seinem Hoheitsgebiet in eine Konkordanz mit dem Interesse des ersuchenden Staates, auf einem fremden Territorium Daten erheben zu können, führt. Dabei können weiterhin auch die Betroffenenrechte optimal gewahrt werden, weil der Betroffene dadurch nicht nur die Möglichkeit hat gegenüber dem ersuchenden Staat Rechtsschutz zu suchen, sondern auch gegenüber dem ersuchten Staat, z. B. im Rahmen der Verletzung seiner Grundrechte vorgehen kann. Im Übrigen kann der Cloud-Dienstanbieter gegenüber dem Staat vorgehen, welchen er selbst für seinen Serverstandort ausgesucht hat und der Dienstanbieter muss nicht Rechtsschutz gegenüber einem Staat suchen, in welchem er möglicherweise keinen Serverstandort hat.

Es wird auch notwendig sein, dass sich neben den einzelnen Mitgliedsstaaten, auch die EU selbst an einem multilateralen Vertrag beteiligt, um eine Kollision[94] mit Unionsrecht zu verhindern.

---

90 Siehe hierzu *Burchard* ZIS 7-8/2018, 249, (258 f.).

91 Ein solcher kann jedoch gerechtfertigt sein.

92 Siehe zur Mediatisierung des Einzelnen *Kau*, in Völkerrecht (Hrsg. Vitzthum/Proelß), 8. Aufl., Berlin u.a. 2019, Abschnitt 3, Rn. 15.

93 Bzw. unter Umständen auch durch den Heimatstaat.

94 Wobei die nach Art. 72 AEUV eingeschränkte Kompetenz der EU zu berücksichtigen ist (*Breitenmoser/Weyeneth* in Groeben/Schwarze/Hatje, Europäisches Unionsrech, Baden-Baden 7. Aufl. 2015, AEUV Art. 72 Rn. 10 ff.).

Gleichzeitig muss aus der Perspektive der EU differenziert werden, ob es sich um ein Rechtshilfeersuchen zwischen den Mitgliedsstaaten handelt, bei welchen zukünftig zumindest im repressiven Bereich eine umfangreichere Zusammenarbeit geplant ist. Insofern ist zu überlegen, „unionsintern" den e-Evidence-VO-Vorschlag[95] auch im präventiven Bereich aufzugreifen.[96]

Die hier vorgeschlagene Lösung führt allerdings dazu, dass am Territorialitätsprinzip festgehalten wird. Es führt nicht zu einer partiellen Privatisierung, indem Rechtshilfeverfahren auf private Dienstanbieter ausgelagert werden.[97] Der heutige Telos der „Territorialität" ist, dass indem eine Zuordnung eines Gebietes zu einem Staat und der gleichzeitigen Zuordnung von Personen zu diesem Staat, dieser „Zuordnungs"-Staat die Interessen dieser Personen am besten schützen kann.[98] Eine Auflösung des Territorialitätsprinzips würde im derzeitigen System der Staatengemeinschaft dazu führen, dass kein Staat mehr unmittelbar für Privatpersonen eintreten kann und eine Verletzung von (innerstaatlichen) Rechten von Individuen (bzw. soweit subjektive Rechte auch außerhalb des innerstaatlichen Rechts verletzt werden) ein geringeres Rechtsschutzniveau erfährt, weil einer Privatperson in grenzüberschreitenden Sachverhalten häufig die Rechtsdurchsetzung erschwert ist.

Möchten die staatlichen Stellen autonom von privaten Dritten (und von deren Wirtschaftsinteressen) handlungsfähig bleiben, ist der hier vertretene Vorschlag in Form einer Widerspruchslösung und der Gefahr-in-Verzug-Regelung – zumindest kumulativ neben (möglichen) weiteren Regelungen zur Verpflichtung von Privaten – notwendig.

95 Siehe Fn. 83.

96 Vielen Dank für die Gespräche bei der ATÖR, insb. an Odey Hardan (wissenschaftlicher Mitarbeiter, Universität Bielefeld), welcher auf diesen Punkt hingewiesen hat und auch auf die Ermächtigung der Kommission zum CLOUD-Act (siehe: Rat der EU, Brüssel, Bes. v. 21.5.2019 - 9114/19). Damit einhergehend auch die Ermächtigung zum CCC-Zusatzprotokoll (Bes. - 9116/19).

97 Vgl. ausführlich zur Strafverfolgung *Burchard* ZIS 7-8/2018, 249 (259 ff.).

98 Siehe auch *Burchard* ZIS 7-8/2018, 249 (251) mit Verweis auf BVerfGE 123, 267.