Probleme des transnationalen Zugriffs auf elektronische Beweismittel im Lichte der europäischen Beweisrechtshilfe

von Luca Alexander Petersen

Der technische Fortschritt im Bereich der Kommunikations- und Informationstechnologie hat in den vergangenen Jahrzehnten nicht nur Veränderungen des materiellen Strafrechts (u.a. §§ 200a ff. StGB) hervorgebracht, sondern stellt ebenso die Strafverfolgung vor aktuelle Herausforderungen. Durch die fortschreitende Digitalisierung des Alltags stellen elektronische Beweismittel (sog. *e-evidence*) als elektronische Daten von beweissicherungsrechtlicher Relevanz[1] mittlerweile einen essentiellen Teil der relevanten Beweismittel dar[2] und lösen die herkömmlichen, körperlichen Beweismittel immer weiter ab. Ihre effektive Gewinnung ist daher als von zentraler Bedeutung für das Strafverfahren anzusehen.[3]

Bereits seit der StPO-Reform im Jahr 2008[4] sind in den §§ 100a ff. StPO nationale Erhebungsregelungen vorgesehen. Durch die Formulierung von Voraussetzungen, Umfang und Zuständigkeit wird eine für das Strafverfahren effektivere Gewinnung der Daten in ebenso klaren wie – aufgrund der Sensibilität der Daten – umstrittenen Grenzen sichergestellt[5]. Der größte Teil der relevanten Daten befindet sich dabei jedoch nicht innerhalb der deutschen Territorialgrenzen, sondern auf ausländischen Servern[6]. Aufgrund der grenzüberschreitenden Sachverhalte wirft dies völkerrechtliche und europarechtliche, insbesondere die staatliche Souveränität betreffende, Fragen auf.[7] So ist immer noch umstritten, inwiefern Ermittlungsmaßnahmen, die den Zugriff auf Daten betreffen, die sich auf Serverfarmen im Ausland befinden, während sie von ausländischen, inländischen oder inländisch ansässigen Firmen auch auf den Endgeräten (PC, Smartphone, etc.) des Verbrauchers zugänglich gemacht und insofern auch im Inland genutzt werden, mit dem Territorialprinzip vereinbar sind.[8] Der für die ermittelnde Strafverfolgungsbehörde durch das grenzüberschreitende Auseinanderfallen von Daten und Inhaber notwendig werdende transnationale Zugriff auf beweiserhebliche Daten stellt diese vor erhebliche Schwierigkeiten, die – nach heutigem Stand – im Regelfall nicht über den Weg der traditionellen Rechtshilfe lösbar sind.[9] Die bestehenden, auch auf dem Prinzip gegenseitiger Anerkennung beruhenden, Instrumente zeigen sich nämlich dem schnellen Datenstrom nicht gewachsen.[10] Um eine effektive Gewinnung der Daten zu ermöglichen, wird die Zeit als wichtigster Faktor zu berücksichtigen

---

[1] *Warken,* Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 1, NZWiSt 2017, 289 (291 ff.).

[2] *Wicker*, Cloud Computing und staatlicher Strafanspruch, Nomos 2016, S. 283, m.w.N; *Warken,* (Fn. 1), NZWiSt 2017, 289 ff.

[3] *Warken,* Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2, NZWiSt 2017, 329 ff.

[4] Gesetz vom 21.12.2007, mit Wirkung vom 01.01.2008, BGBl I, S. 3198.

[5] Vgl. *Bruns*, in: KK-Kommentar-StPO, C.H. Beck, 8. Aufl. 2019, § 100a Rn. 1; ausführlich dazu: *Bell*, *S.*, Strafverfolgung und die Cloud, Duncker & Humblot, 2019, S. 75 ff.

[6] *Bell*, (Fn. 5), S. 157.

[7] *Fahrner,* Handbuch Internationale Ermittlungen, C.H. Beck, 2020, § 7 Rn. 1; *Bell*, (Fn. 5), S. 191 ff.

[8] *Bell*, (Fn. 5), S. 157 ff.

[9] *Burchard,* Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen, Teil 1, ZIS 2018, 190 (191).

[10] *Wörner,* in: Ambos/König/Rackow, IRG, Vor §§ 91 ff. Rn. 511.

sein.[11] Dies scheint vorauszusetzen, dass es eines grundlegend anderen Rechtshilfeinstrument bedarf, das territoriale Grenzen und die staatliche Souveränität weiter aufweicht.[12]

Seit der Implementierung der Richtlinie über die Europäische Ermittlungsanordnung[13] (im Folgenden „EEA") besteht ein weiteres Instrument i.R.d. europäischen Rechtshilfe auf Grundlage der gegenseitigen Anerkennung gem. Art. 82 Abs. 1 AEUV. Dieses kontrovers diskutierte Instrument[14] soll durch die gegenseitige Anerkennung die Beweisrechtshilfe innerhalb der Grenzen der Europäischen Union vereinfachen und beschleunigen.[15] Die EEA umfasst dabei grds. auch elektronische Beweismittel.[16] Dennoch scheinen die erwarteten Beschleunigungen, insbesondere durch kurze Vollstreckungsfristen nicht auszureichen, um die elektronischen Beweismittel rechtzeitig zu erlangen.[17] Doch eine weitere Verkürzung, ggf. sogar eine automatische Übermittlung der Daten ohne zwischengeschaltete Vollstreckungsbehörde[18], droht zu Lasten der im Prozess betroffenen Personen zu gehen, denn in einem solchen Fall wäre eine Überprüfung der Anordnung durch den Vollstreckungsstaat nur noch stark eingeschränkt oder gar nicht mehr möglich und würden damit auch entsprechende Rechtsmittel nicht eingreifen können.[19] Damit einhergehend stellt sich die Frage, inwiefern ein solcher Mechanismus noch mit dem Grundsatz gegenseitiger Anerkennung vereinbar ist.[20] Bei einem direkten Durchgriff wird nämlich nicht mehr nur auf einen Anerkennungsakt verzichtet, sondern die *nationale* Ermittlungskompetenz vielmehr auf das gesamte EU-Gebiet erstreckt.[21] Ansatzpunkte für eine solche Regelung könnten im Grundsatz der Verfügbarkeit von Informationen innerhalb der Europäischen Union zu verorten sein, auch wenn dabei zunächst nicht die Erhebung von

[11] *Warken,* (Fn. 1), NZWiSt 2017, 289 (296 f.).
[12] *Wörner,* in: Ambos/König/Rackow (Hrsg.), IRG, Vor §§ 91 ff. Rn. 511, m.w.N. in Fn. 47.
[13] Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates v. 3.4.2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl EU Nr. L 130 v. 1.5.2014, S. 1.
[14] Vgl. *Böse,* Die Europäische Ermittlungsanordnung – Beweistransfer nach neuen Regeln, ZIS 2014, 152 ff. m.w.N.
[15] Vgl. ausführlich *Ambos,* Internationales Strafrecht, 5. Auflage, C.H. Beck 2018, § 12 Rn. 88 ff.
[16] *Blažič und Klobučar,* Removing the barriers in cross-border crime investigation by gathering e-evidende in an interconnected society, I&CTL (29) 2020, 66 (71).
[17] Commission Services, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 7.12.2016, Doc. No. 14711/16, 10007/16, S. 12; *Wörner,* in: Ambos/König/Rackow (Hrsg.), IRG, Vor §§ 91 ff. Rn. 511.
[18] So erschöpft sich bspw. schon jetzt der Anerkennungsakt gem. § 91g Abs. 6 IRG im Verstreichenlassen der Frist, vgl. BT-Drs. 18/9757, S. 75.
[19] *Esser,* Grenzüberschreitende Ermittlungen innerhalb der EU: neuer Rechtsrahmen für E-Evidence, StraFo 2019, 404 (408 f.).
[20] *Wörner,* in: Ambos/König/Rackow (Hrsg.), IRG, Vor §§ 91 ff. Rn. 511; *Böse,* An assessment of the Commission's proposals on electronic evidence, Study, 2018, abrufbar unter <https://op.europa.eu/de/publication-detail/-/publication/be0532d4-c5ee-11e8-9424-01aa75ed71a1> (zuletzt aufgerufen am 07.09.2020), S. 36.
[21] *Wörner,* in: Ambos/König/Rackow (Hrsg.), IRG, Vor §§ 91 ff. Rn. 511. Insofern ist jedoch auch allgemeiner festzuhalten, dass nach derzeitigem Verständnis der gegenseitigen Anerkennung eine automatische Anerkennung, ohne jegliche Überprüfungsmöglichkeiten des Vollstreckungsstaates, fernliegend erscheint, dazu *Nalewajko*, Grundsatz der gegenseitigen Anerkennung, Duncker & Humblot, 2010, S. 90 f. Aus der EEA-Richtlinie eine Distanzierung von einer automatischen Anerkennung schließend, *Zimmermann,* Die Europäische Ermittlungsanordnung: Schreckgespenst oder Zukunftsmodell für grenzüberschreitende Strafverfahren?, ZStW 2015, 143 (162).

Beweisen im Vordergrund steht.[22] Die EEA stößt jedenfalls immer dann an Grenzen, sobald es um die Erlangung von Daten geht, die sich außerhalb des mitgliedsstaatlichen EU-Raums befinden oder im maßgeblichen Erhebungszeitpunkt gar nicht örtlich zuordnungsfähig sind.[23] Letzteres ist insbesondere dann der Fall, wenn aufgrund der Speicherung in einer Cloud im maßgeblichen Zeitpunkt gar kein Speicherort ermittelbar ist.[24]

Während der Umfang und die Auswirkungen der EEA noch nicht hinreichend erforscht sind[25], scheint die Europäische Kommission diese bestehende Lücke bzw. fehlende Anpassbarkeit der bestehenden Instrumente jedoch nicht, wie teilweise befürwortet, über eine Erweiterung der EEA schließen zu wollen.[26] So greift der Kommissionsentwurf über die Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (*European Production Order and Preservation Order*)[27], geprägt durch den U.S. amerikanischen „Cloud-Act" vom 23.03.2018[28], die angesprochenen Probleme auf.[29] Ansatzpunkt ist dabei eine unmittelbare Übermittlung der Daten durch die Unternehmen an den Anordnungsstaat. Ob sich auch eine solche Übermittlung ohne das Zwischenschalten einer Vollstreckungsbehörde, wie es auch im Rahmen der Beweisrechtshilfe basierend auf dem Grundsatz gegenseitiger Anerkennung angestrebt ist, auf Art. 82 Abs. 1 AEUV stützen lässt, erscheint fraglich.[30] Der Entwurf knüpft daran an, dass private Unternehmen zur unmittelbaren Herausgabe der Daten an die Behörden verpflichtet werden sollen, ohne auf Landesgrenzen und die damit zusammenhängenden Souveränitätsansprüche Rücksicht zu nehmen.[31] Auch wenn man davon ausgeht, dass ein Zugriff auf physikalisch im Ausland befindliche Daten unter den Besonderheiten im Cyberraum nicht schon per se eine Souveränitätsverletzung darstellt[32], gilt es, die Souveränität und die damit zusammenhängenden Grundrechtsgarantien dennoch hinreichend zu wahren.[33] Augenscheinlich wird dieser Konflikt, sofern Provider und Ressource, wie es beim „*cloud-computing*"[34] regelmäßig der Fall ist, territorial auseinanderfallen.[35] Auch in diesem Fall ist der Staat innerhalb seiner territorialen Grenzen zur Wahrung der Grundrechte von Providern und Nutzern verpflichtet.[36] Dabei gilt es auch berücksichtigen, dass es sich regelmäßig um besonders

---

[22] Dazu *Satzger*, Internationales und Europäisches Strafrecht, 8. Auflage, C.H. Beck 2018, § 10 Rn. 75 ff.; *Esser,* 'Daten- und Informationsaustausch', in: Böse (Hrsg.), Europäisches Strafrecht, Nomos, 2013, § 19 Rn. 43.

[23] *Schaar,* EAID: E-Evidence und CLOUD-Act – Grenzüberschreitender Direktzugriff auf Daten?, ZD-Aktuell, 2019, 04362.

[24] *Hackner*, in: Schomburg/Lagodny (Hrsg.), Int. Rechtshilfe, C.H. Beck, 2020, Vor § 68 IRG, Rn. 37e.

[25] Vgl. *Esser*, (Fn. 19), StraFo 2019, 404 (404); Zum derzeit laufenden Projekt zur Erforschung der Auswirkungen s. <https://eio-lapd.eu/de/ueber-das-projekt/> (zuletzt aufgerufen am 07.09.2020).

[26] Ausdrücklich gegen eine Änderung der EEA spricht sich die Kommission im Entwurf COM (2018) 225 aus; dafür dagegen *Esser*, (Fn. 19), StraFo 2019, 404 (412).

[27] Vorschlag der Europäischen Kommission, COM (2018) 225 und 226.

[28] *Burchard,* (Fn. 9), ZIS 2018, 190 (190).

[29] Zusammenfassend auch *Wahl et al.*, eucrim 2018, 35.

[30] *Böse,* Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel – Rückzug des Staates aus der Rechtshilfe?, KriPoZ 2019, 140 (141 f.).

[31] *Esser*, (Fn. 19), StraFo 2019, 404 (406).

[32] Dazu *Fahrner,* (Fn. 7), § 7 Rn. 33.

[33] *Wörner,* in: Ambos/König/Rackow (Hrsg.), IRG, Vor §§ 91 ff. Rn. 511; *Böse,* (Fn. 30), KriPoZ 2019, 140 (143); *Burchard,* (Fn. 9), ZIS 2018, 190 (192).

[34] Zur umstrittenen Begriffsbestimmung s. *Müller,* Cloud Computing, Duncker & Humblot, 2020, S. 33 ff.

[35] Vgl. *Böse,* (Fn. 30), KriPoZ 2019, 140 (143).

[36] *Ibid.*

sensible und grundrechtsrelevante Daten handeln wird. Durch die Datenschutz-Grundverordnung[37] (DSGVO) ist in diesem Bereich bereits ein Rahmen für ein einheitliches Datenschutzniveau auf europäischer Ebene geschaffen worden, mit dem auch ein entsprechendes Instrument zur strafprozessualen Datenerhebung vereinbar sein muss.[38]

Kritisch ist der Entwurf über die Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen weiter insoweit zu betrachten, als dass eine solche Umsetzung zu einer weiteren „Privatisierung der Rechtshilfe“ im Bereich der elektronischen Beweisrechtshilfe führen kann.[39] Gerade in einem solch sensiblen Bereich wie der Erhebung personenbezogener Daten erscheint es höchst bedenklich, staatliche Kernaufgaben auf Private zu übertragen und damit sogar die Grundrechtskontrolle diesen Privaten zu überlassen.[40] Zumindest kann auf entsprechende Rechtsschutzmöglichkeiten nicht verzichtet werden.[41] Auch lässt der Entwurf in der Tendenz erkennen, dass sich die Kommission damit von der derzeit praktizierten "eingeschränkten"[42] zu einer "automatischen" gegenseitigen Anerkennung begeben will.[43]

Neben diesen Aspekten stellt sich – wie bereits angedeutet – vorrangig die Frage, ob sich ein solches Kooperationsinstrument überhaupt auf eine bestehende Kompetenzgrundlage stützen lässt. Der Entwurf über die Herausgabe- und Sicherungsanordnung wird auf Art. 82 AEUV und die dort niedergelegte gegenseitige Anerkennung gestützt.[44] Die Inanspruchnahme dieser Kompetenzgrundlage ist jedoch fraglich, weil die Anordnungen für den Adressaten unmittelbar verbindlich sein sollen und gerade keine Anerkennungsakt des Vollstreckungsstaates vorgesehen ist.[45] Eine Unsicherheit der Kommission scheint insoweit auch darin zu erkennen zu sein, dass, anders als noch im Falle der EEA[46], auf eine explizite Bezugnahme auf Art. 82 Abs. 1 *Buchstabe a)* AEUV verzichtet wird. Es bedarf also genauer Prüfung, ob der Entwurf tatsächlich auf den Grundsatz gegenseitiger Anerkennung und, wenn ja, auf welche konkrete Rechtsgrundlage gestützt werden kann.

Ziel der Arbeit ist es, nach einer Darstellung der technischen und rechtlichen Besonderheiten der Gewinnung elektronischer Beweise die aktuellen und in der wissenschaftlichen Betrachtung noch wenig berücksichtigten Entwicklungen im Rahmen der europäischen Beweisrechtshilfe aufzugreifen und kritisch zu hinterfragen. Damit soll zum wissenschaftlichen Diskurs in diesem sensiblen, da datenschutzrechtlich besonders relevanten, wie bedeutsamen Bereich der Strafverfolgung beigetragen werden. Die Untersuchung der skizzierten Probleme soll der Feststellung dienen, unter welchen Voraussetzungen eine effektivere Strafverfolgung im europäischen Raum durch die Erhebung elektronischer Beweismittel im Rahmen der

[37] Verordnung (EU) 2016/679 des Europäischen Parlament und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119, 4.5.2016; ber. ABl. L 127, 23.5.2018.
[38] *Bell*, (Fn. 6), S. 190 f.
[39] *Esser*, (Fn. 25), StraFo 2019, 404 (408 f.); *Gleß*, in: Schomburg/Lagodny (Hrsg.), Int. Rechtshilfe, C.H. Beck, 2020, III. B. 3a. Rn. 6.
[40] *Esser*, (Fn. 19), StraFo 2019, 404 (408 f.); *Böse,* (Fn. 30), KriPoZ 2019, 140 ff.
[41] *Böse,* (Fn. 20), S. 26 f.
[42] *Nalewajko*, (Fn. 21), S. 91.
[43] *Esser*, (Fn. 19), StraFo 2019, 404 (410 f.).
[44] Vorschlag der Europäischen Kommission, COM (2018) 225 und 226.
[45] *Böse,* (Fn. 30), KriPoZ 2019, 140 (142 f.); Im Ansatz auch schon im Antrag der Fraktion DIE LINKE vom 20.05.2019, BT Drs. 19/10281, S. 2.
[46] ABl. L EU 2014, 130/1.

Beweisrechtshilfe gewährleistet werden kann, ohne dabei die aufgeführten völkerrechtlichen und europäischen Grundprinzipien sowie Grundrechtsgarantien der Betroffenen außer Acht zu lassen. Im weiteren Verlauf soll der Kommissionsvorschlag kritisch gewürdigt werden, wobei die rechtliche Legitimation, insbesondere die Grenzen des Prinzips der gegenseitigen Anerkennung im Mittelpunkt stehen und ggf. entsprechende Anpassungsvorschläge erarbeitet werden sollen. Dabei bedarf es ebenfalls der Berücksichtigung von Entwicklungen, die über die territorialen Grenzen der EU hinausgehen, insbesondere im Zusammenhang mit dem schon erwähnten U.S. „*Cloud Act*“. Aber auch innerhalb der EU könnte eine vergleichende Betrachtung der Rechtshilfe unter den Mitgliedsstaaten, die die EEA nicht umgesetzt haben (Irland und Dänemark), weitere Erkenntnisse für ein entsprechendes Rechtshilfeinstrument liefern.

Gliederung: