Autoren: Sarah Rachut, Ass. jur., Wissenschaftliche Mitarbeiterin,
Julian Walter Maurer, Studentische Hilfskraft

Erscheinungsdatum: 17.11.2023
Quelle: juris

Normen: § 94 StPO, § 95 StPO, § 100a StPO, EURL 2023/1544, EURL 2017/541
... mehr

Fundstelle: jurisPR-ITR 23/2023 Anm. 2
Herausgeber: Prof. Dr. Dirk Heckmann, Technische Universität München
Zitiervorschlag: Rachut/Maurer, jurisPR-ITR 23/2023 Anm. 2

Die E-Evidence-Verordnung der Europäischen Union im Spannungsfeld zwischen Datenschutz und notwendiger Gewährleistung grenzüberschreitender Sicherheit

A. Einleitung

Elektronische Beweismittel sind in knapp 85% der strafrechtlichen Ermittlungen innerhalb der Europäischen Union von besonderer Bedeutung, stammen jedoch zu 65% regelmäßig aus dem innereuropäischen Ausland (https://www.europarl.europa.eu/news/de/press-room/20230609IPR96203/elektronische-beweismittel-neue-regeln-fur-schnelle-eu-weite-strafermittlungen, zuletzt abgerufen am 13.10.2023).

Insbesondere im Rahmen von Antiterrorermittlungen, aber auch im Bereich der Verfolgung von Betrugs- und Sexualdelikten sind die Ermittlerinnen und Ermittler der Mitgliedstaaten auf möglichst vollständige und belastbare Beweismittel angewiesen. Oftmals befinden sich diese jedoch im digitalen Raum, mithin außerhalb des direkten Zugriffs der deutschen Strafverfolgungsbehörden. Mit der im Juni 2023 verabschiedeten E-Evidence-Verordnung (Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12.07.2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32023R1543, zuletzt abgerufen am 13.10.2023) hat die Europäische Union einen Rechtsrahmen für die Erleichterung der grenzüberschreitenden Kooperation zwischen Ermittlungsbehörden und innerhalb der EU operierenden Diensteanbietern geschaffen – unabhängig davon, ob Letztere die Daten ihrer Nutzer als mögliche Verdächtige auf Servern innerhalb oder außerhalb der EU speichern. Das Vorhaben wurde indes insbesondere aufgrund der damit verbundenen datenschutzrechtlichen Herausforderungen und Bedenken im Vorfeld der Verabschiedung umfangreich kritisiert. Neben dem Blick auf den konkreten Regelungsinhalt der E-Evidence-VO lohnt auch der Vergleich mit dem verwandten US-amerikanischen CLOUD Act, um die an den Regelungen geübte Kritik einordnen zu können.

B. Hintergrund und Entwicklungsgeschichte der E-Evidence-VO

Im Kontext der Bedrohungen durch den internationalen islamistischen Terror in Europa (z.B. in Paris, Nizza oder Barcelona) wurde deutlich, dass Onlinekommunikationskanäle von den Tätern vor und während der Taten intensiv genutzt wurden, so dass der Schaffung von Maßnahmen zur effizienten und wirksamen Beschaffung und Sicherung elektronischer Beweismittel eine immer größere Bedeutung zukommt.

Konkret regte der Rat für Justiz und Inneres bereits 2016 an, die Kooperation zwischen Providern und Sicherheitsbehörden auszubauen, Rechtshilfeverfahren zu straffen und die Regelungen in Hinblick auf die Rechtsdurchsetzung im Cyberspace zu überarbeiten (vgl. Council of the European Union, Council conclusions on improving criminal justice in cyberspace, 09.06.2016, abrufbar unter: https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf, zuletzt abgerufen am 13.10.2023).

Der Entwurf für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (kurz: E-Evidence-VO), welchen die Europäische Kommission am 18.04.2018 vorlegte, wurde am

13.06.2023 mit wenigen Änderungen schließlich vom Europäischen Parlament verabschiedet (https://www.europarl.europa.eu/news/de/press-room/20230609IPR96203/elektronische-beweismittel-neue-regeln-fur-schnelle-eu-weite-strafermittlungen, zuletzt abgerufen am 13.10.2023). Ergänzend zur E-Evidence-VO wurde am 12.07.2023 im Rahmen des E-Evidence-Pakets auch die sog. Vertreterrichtlinie (Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12.07.2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32023L1544, zuletzt abgerufen am 13.10.2023) verabschiedet, welche die Benennung von Niederlassungen und die Bestellung von Vertretern bestimmter Diensteanbieter regelt. Diese müssen im Sinne der Erleichterung des Vollzugs der E-Evidence-VO zur Entgegennahme, Befolgung und Durchsetzung von Entscheidungen und Anordnungen der Ermittlungsbehörden dafür verantwortliche Vertreter bzw. Niederlassungen innerhalb der Europäischen Union bestimmen.

C. Regelungsinhalt und Instrumente der E-Evidence-VO

Kern der verabschiedeten E-Evidence-VO ist die Einführung der Instrumente einer bindenden Europäischen Herausgabeanordnung einerseits sowie Sicherungsanordnung andererseits, wobei diese nach dem Vorschlag in ihrer konkreten Anwendung jeweils durch die zuständige Justizbehörde eines Mitgliedstaates erlassen oder validiert werden müssen. Art. 2 Nr. 1 E-Evidence-VO definiert die Europäische Herausgabeanordnung dabei als „eine verbindliche Entscheidung einer Anordnungsbehörde eines Mitgliedstaats, mit der ein Diensteanbieter, der in der Union Dienstleistungen anbietet und in einem anderen Mitgliedstaat niedergelassen oder vertreten ist, zur Herausgabe elektronischer Beweismittel verpflichtet wird“. Die Europäische Sicherungsanordnung hingegen ist „eine verbindliche Entscheidung einer Anordnungsbehörde eines Mitgliedstaats, mit der ein Diensteanbieter, der in der Union Dienstleistungen anbietet und in einem anderen Mitgliedstaat niedergelassen oder vertreten ist, im Hinblick auf ein späteres Ersuchen um Herausgabe zur Sicherung elektronischer Beweismittel verpflichtet wird“ (Art. 2 Nr. 2 E-Evidence-VO).

Anwendung finden sollen diese Anordnungen vor allem dann, wenn Daten von einem Diensteanbieter aus einem anderen Staat gespeichert wurden, die wiederum als Beweismittel im Rahmen von strafrechtlichen Ermittlungen bzw. Strafverfahren von Relevanz sein könnten. Diensteanbieter i.S.d. E-Evidence-VO sind dabei nach Maßgabe des Art. 2 Nr. 3 jene natürlichen oder juristischen Personen, welche eine der in den Buchst. a) bis c) näher definierten Dienstleistungen anbieten (u.a. elektronische Kommunikationsdienste, soziale Netzwerke, Online-Marktplätze, Hosting- und Domaindienste). Dabei ist zu berücksichtigen, dass eine solche Herausgabe- bzw. Sicherheitsanordnung nur dann zulässig ist, insofern in einer vergleichbaren hypothetischen Situation innerhalb der Landesgrenzen des Anordnungsstaates eine ähnliche Maßnahme möglich wäre (in Deutschland kämen diesbezüglich je nach Sachverhaltskonstellation die §§ 94, 95, 100a Abs. 4 StPO in Betracht, vgl. Brodowski in: BeckOK IT-Recht, 11. Edition, § 94 StPO Rn. 5 m.w.N.; Ferner, jurisPR-StrafR 11/2023 Anm. 4; Braun, jurisPR-ITR 1/2017 Anm. 2; Nadeborn/Friedrich, NZWiSt 2023, 48, 54). In diesem Zusammenhang ist außerdem darauf hinzuweisen, dass die E-Evidence-VO keine konkreten Überwachungsmaßnahmen vorsieht oder vielmehr gar Regelungen zur Vorratsdatenspeicherung umfasst. Der Fokus des Vorhabens liegt auf der einzelfallbezogenen Erleichterung der Arbeit der Strafverfolgungsbehörden ab dem Ermittlungsstadium, weshalb sich der Anwendungsbereich der vorgesehenen Instrumente entsprechend auf die Phasen vom vorgerichtlichen Ermittlungsstadium bis hin zum jeweiligen Abschluss des Verfahrens, beispielsweise durch Einstellung oder ein entsprechendes rechtskräftiges Urteil, erstreckt. Die Herausgabe von Teilnehmer- und Zugangsdaten kann dabei in sämtlichen Strafermittlungen erwirkt werden, wohingegen die Herausgabe von Transaktions- und Inhaltsdaten zunächst lediglich dann möglich ist, soweit Straftaten im Raum stehen, welche im Anordnungsstaat mit einer Mindestfreiheitsstrafe von drei Jahren geahndet werden (vgl. Art. 5 Abs. 3, 4 Buchst. a E-Evidence-VO). Ausnahmen stellen im Vorschlag explizit hervorgehobene Straftaten dar, bei denen eine hinreichende Verbindung zwischen der Verwendung von Informationssystemen und der jeweiligen Straftat herzustellen ist (v.a. in Bezug auf die Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie oder aber Angriffen auf Informationssysteme; vgl. Art. 5 Abs. 4 Buchst. b E-Evidence-VO) und darüber hinaus auch Straftaten, welche unter die Richtlinie der Europäischen Union zur Terrorismusbekämpfung (Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15.03.2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32017L0541, zuletzt abgerufen am 13.10.2023) fallen (Art. 5 Abs. 4 Buchst. c E-Evidence-VO).

In Bezug auf die Ausführung einer Europäischen Herausgabeanordnung sieht der Vorschlag der Kommission vor, dass die angeforderten Daten spätestens innerhalb einer Frist von zehn Tagen nach Erhalt der Anordnung an die Anordnungsbehörde bzw. die zuständige Verfolgungsbehörde übermittelt werden sollen, wobei in Ausnahmefällen auch eine frühere Offenlegung angezeigt sein kann (Art. 9 Abs. 1 E-Evidence-VO). In Notfällen sind die angeforderten Daten sogar unverzüglich, jedoch spätestens innerhalb von sechs Stunden nach Erhalt der Anordnung zu übermitteln (Art. 9 Abs. 2 E-Evidence-VO). Bei bloßen Sicherungsanordnungen sind die angeforderten Daten nach Maßgabe des Art. 10 Abs. 1 E-Evidence-VO unverzüglich zu sichern, wobei diese Sicherung nach 60 Tagen endet, sofern die Anordnungsbehörde dem Diensteanbieter nicht bestätigt, dass ein Ersuchen um Herausgabe in die Wege geleitet wurde. Sollte dies der Fall sein, hat der Diensteanbieter die Daten so lange zu sichern, wie es erforderlich ist, um die Daten nach Eingang des Herausgabeersuchens herauszugeben (Art. 10 Abs. 2 E-Evidence-VO). Die Sicherungsanordnung dient im zweigliedrigen Anordnungssystem folglich lediglich der anlassbezogenen Sicherung von Daten, deren Herausgabe im weiteren Fortgang des Verfahrens nachträglich angeordnet werden könnte.

D. Die E-Evidence-VO im Kontext transatlantischer Initiativen

Als transatlantisches Gegenstück der E-Evidence-VO kann gewissermaßen der US-amerikanische CLOUD Act (Clarifying Lawful Overseas Use of Data Act, abrufbar unter: https://www.justice.gov/criminal-oia/page/file/1152896/download, zuletzt abgerufen am 13.10.2023) aus dem Jahr 2018 gesehen werden (vgl. hierzu auch Abra, Regulating law enforcement access to electronic evidence across borders: The United States approach, Information & Communication Technology Law, 2020, 324, 324).

Tatsächlich geht der Ansatz der Europäischen Union noch etwas über das hinaus, was das US-amerikanische Pendant zur E-Evidence-VO vorsieht. Während der CLOUD Act nämlich lediglich vorsieht, dass US-amerikanische Diensteanbieter im Falle einer US-amerikanischen Herausgabeanordnung die jeweils gespeicherten Daten auch dann offenlegen müssen, wenn sich diese auf einem Server außerhalb der USA befinden, sieht der europäische Vorschlag der E-Evidence-VO vor, dass Diensteanbieter die fraglichen Daten immer herausgeben müssen, ohne danach zu unterscheiden, wo und von wem sie gespeichert werden. Diese Auskunftspflicht besteht vollumfänglich und für alle in der Europäischen Union tätigen Diensteanbieter, unabhängig davon, ob es sich auch um originär europäische Unternehmen handelt oder nicht. Die Herausgabepflicht gegenüber den Behörden europäischer Mitgliedstaaten träfe somit auch US-amerikanische Unternehmen, welche ihre Daten nicht in Europa speichern, und stellt diese vor weitere datenschutzrechtliche Herausforderungen. Datenschutzrechtliches Konfliktpotenzial entsteht in diesem Zusammenhang dadurch, dass es US-amerikanischen Unternehmen grundsätzlich nicht erlaubt ist, in den USA gespeicherte Inhaltsdaten an Strafverfolgungsbehörden ausländischer Staaten herauszugeben (vgl. hierzu ausführlich Meißner, Verfassungsblog v. 28.06.2023, abrufbar unter: https://verfassungsblog.de/digitale-beweise-im-eu-us-datenschutzkonflikt/, zuletzt abgerufen am 13.10.2023). Per dato würde von US-amerikanischen Unternehmen folglich ein Verhalten gefordert werden, welches ihnen nach den Regelungen ihres Sitzlandes verboten ist. Aufgrund der großen Bedeutung US-amerikanischer Unternehmen und der von ihnen angebotenen Dienste in der EU gefährdet dies letztlich die Wirksamkeit der E-Evidence-VO und die mit dieser verfolgten Ziele. Maßgebliche Einschränkungen in den Strafverfolgungsmöglichkeiten wären die Folge, die sich jedoch durch ein Abkommen zwischen der EU und den USA ausgleichen ließen. Gleichwohl wird befürchtet, dass eine Lockerung der einschlägigen datenschutzrechtlichen US-Bestimmungen nur durch ein Entgegenkommen in anderen datenschutzrechtlichen Streitfragen auf Seiten der EU umgesetzt werden könnte (für eine tiefgehende Beleuchtung der Verhandlungen zwischen EU und USA wird verwiesen auf Meißner, Verfassungsblog v. 28.06.2023, abrufbar unter: https://verfassungsblog.de/digitale-beweise-im-eu-us-datenschutzkonflikt/, zuletzt abgerufen am 13.10.2023).

E. Kritik

Die Kritik an der E-Evidence-VO bezieht sich insbesondere auf datenschutzrechtliche Bedenken. Darüber hinaus sind vereinzelte Regelungen jedoch auch im Lichte der in einigen Mitgliedstaaten sinkenden Rechtstaatsqualität bedenklich (Burchard, ZRP 2019, 164, 167; Rojszczak, The Modern Law Review, 4/2022, 997, 1028; Garsztecki, ZfP 2020, 86, 101). Dies betrifft ganz besonders auch den Zugriff auf Internetverkehrsdaten, welche unter Umständen präzise Schlüsse über das (Intim-)Leben einer Person zulassen (vgl. Monroy, Netzpolitik.org v. 04.03.2022, abrufbar unter: https://netzpolitik.org/2022/e-evidence-woran-die-eu-verordnung-zu-elektronischen-beweismitteln-hakt/, zuletzt abgerufen am 13.10.2023). So kann durchaus in Anbetracht der Erfahrungen aus dem Pegasus-Abhörskandal, bei dem unter anderem aufgedeckt wurde, dass Ungarn, Polen, Spanien und Griechenland politisch unliebsame Bürgerinnen und Bürger ausspionierten, (Vgl. Rudl, Netzpolitik.org v. 14.06.2023, abrufbar unter: https://netzpolitik.org/2023/e-evidence-elektronische-beweismittel-stellen-den-rechtsstaat-auf-die-probe/, zuletzt abgerufen am 13.10.2023) eine zu einfache Möglichkeit des länderübergrei-

fenden Datenzugriffs kritisch gesehen werden. Eine wesentliche Änderung, welche maßgeblich auch der kritischen Auseinandersetzung mit dem ersten Kommissionsentwurf aus dem Jahre 2018 zu verdanken ist, ist in der Etablierung des Benachrichtigungserfordernisses aus Art. 13 Abs. 1 E-Evidence-VO zu sehen. Personen, über welche Daten seitens staatlicher Stellen angefordert wurden, sind nunmehr grundsätzlich unverzüglich hierüber zu informieren (vgl. Basar, Die „E-Evidence-VO“ tritt in Kraft - Update zu jurisPR-StrafR 5/2019 Anm. 1: Verordnung (EU) 2023/1543 vom 12.07.2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, Basar, jurisPR-StrafR 14/2023 Anm. 1). Ausnahmen hiervon sind lediglich für Fälle vorgesehen, in denen die Benachrichtigung aus Gründen der Gewährleistung der Ermittlungen oder zum Schutze der nationalen Sicherheit unzumutbar erscheint (Art. 13 Abs. 2 E-Evidence-VO). Auch hier stellt sich die Frage, wie diese Ausnahmeregelungen von den einzelnen Mitgliedstaaten künftig ausgelegt werden.

Aus rechtspolitischen Erwägungen ist zudem zu berücksichtigen, dass Rechtsakte der EU durchaus zu Nachahmungen durch Drittstaaten anregen. Diese unter dem Begriff des „Brussels Effect“ diskutierte Entwicklung (Grundlegend hierzu Bradford, The Brussels Effect: How the European Union Rules the World, 2020) ist oftmals positiv konnotiert und soll z.B. im Bereich des Datenschutzrechts durch einen Orientierungseffekt an den Regelungen der DSGVO zu einem ansteigenden Datenschutzniveau beigetragen haben. Im Kontext der E-Evidence-VO ist indes fraglich, inwieweit ein Nachahmungseffekt zu begrüßen wäre. So wird angemerkt, dass die Verordnung als „Blaupause“ für Nicht-EU-Staaten dienen könnte, analoge Regelungen einzuführen und EU-Mitgliedstaaten möglicherweise mit Herausgabeanordnungen konfrontiert wären, die zur Verfolgung von Straftaten uns fernliegender Rechtstraditionen beitragen würden (vgl. hierzu auch die Erwägungen der Datenschutzkonferenz v. 07.11.2018, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20181107_EntschliessungE_Evidence.pdf?__blob=publicationFile&v=7, zuletzt abgerufen am 13.10.2023).

F. Ausblick

Der Verfolgung von Straftäterinnen und Straftätern im digitalen Raum kommt in der zunehmend digitalen Welt eine zentrale Bedeutung zu. Insbesondere, nachdem das Internet und die damit verbundenen Kommunikationskanäle eine immer wichtigere Rolle im Zusammenhang mit der Vorbereitung, Durchführung und Nachbereitung von Gewaltverbrechen und Terrorakten auf der ganzen Welt spielen, müssen den Strafverfolgungsbehörden effektive und effiziente Instrumente an die Hand gegeben werden. Ob dies mit der nun verabschiedeten Verordnung gelingen wird, bleibt abzuwarten und wird maßgeblich auch davon abhängen, wie die neuen Möglichkeiten von den Strafverfolgungsbehörden der Mitgliedstaaten tatsächlich genutzt werden (können). Insbesondere bei der Handhabe gegenüber US-amerikanischen Unternehmen bedarf es noch einer Abstimmung auf politischer Ebene, um bestehende Widersprüche zwischen den Rechtsordnungen aufzulösen.

Mit der E-Evidence-VO werden den Strafverfolgungsbehörden umfassende Zugriffsmöglichkeiten auf Daten eingeräumt. Die Implementation der Regelungen sollte in Anbetracht der Eingriffsintensität und des damit verbundenen Missbrauchspotentials daher von einem kritischen Evaluationsprozess begleitet werden.