Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln

Aktuelle nationale, europa- und völkerrechtliche Entwicklungen

Kristin Pfeffer

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

This article provides an overview of current national, European, and international legal efforts to regulate cross-border access to electronic evidence. At the level of the EU, it was recently decided to harmonise the legal systems of the Member States by means of regulations and directives, which is to be flanked by an agreement between the EU and the USA in the future. In addition, there are already agreements under international law, such as the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) of the Council of Europe. Meanwhile a future UN Cybercrime Convention is being negotiated in the UN. This article outlines these developments.

AUTHOR

Kristin Pfeffer

Professur für Öffentliches Recht
Hochschule der Akademie der Polizei Hamburg, University of Applied Police Sciences

CITE THIS ARTICLE

Pfeffer, K. (2023). Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln : Aktuelle nationale, europa- und völkerrechtliche Entwicklungen. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-012

Published in eucrim 2023, Vol. 18(2) pp 170 – 174

https://eucrim.eu

ISSN:

I. Einleitung

Die Fallzahlen im Bereich der Internetkriminalität steigen im Zuge der weltweiten Digitalisierung auch in Europa stetig an. Laut Europäischem Rat lag der Anteil strafrechtlicher Ermittlungen, die digitale Daten zum Gegenstand hatten, bereits 2018 bei 85 Prozent, gegenwärtig ist der Prozentsatz noch höher.[1] Zur Verfolgung dieses regelmäßig grenzüberschreitenden Phänomens[2] sind die Strafverfolgungsbehörden bei ihren Ermittlungen auf die Zusammenarbeit mit ausländischen Stellen angewiesen. Somit werde, so heißt es weiter in dem Bericht des Europäischen Rates, in über 50 Prozent aller strafrechtlichen Ermittlungen ein Rechtshilfeersuchen gestellt, um elektronische Beweismittel zu erhalten.[3]

Doch obwohl es durchaus erfolgreiche Ermittlungen gegen grenzüberschreitend agierende Täter im Internet gibt, werden die meisten Verfahren eingestellt, weil die dafür erforderlichen justiziellen Rechtshilfeersuchen-Prozesse zu lange andauern und häufig im Sande verlaufen.[4] Deshalb werden sowohl auf nationaler als auch europäischer und völkerrechtlicher Ebene neue rechtliche Lösungen gesucht: So wurden von deutschen Gerichten vereinzelt die vorhandenen nationalen Ermächtigungsgrundlagen weit ausgelegt (dazu unter II.). Auf der Ebene der EU-Mitgliedstaaten wurde jüngst eine Harmonisierung der mitgliedstaatlichen Rechtsordnung im Verordnungs- und Richtlinienwege beschlossen, was künftig mit einem Abkommen zwischen der EU und den USA (dazu unter III.) flankiert werden soll. Daneben gibt es bereits völkerrechtliche Abkommen, wie das zweite Zusatzprotokoll zur Cybercrime-Konvention des Europarates (siehe IV). Inzwischen wird auch in der UN eine künftige UN-Cybercrime-Konvention ausgehandelt (siehe V).

II. Weite Auslegung vorhandener nationaler Vorschriften (Beispiel Deutschland)

Ein Ansatz, zeitaufwendige Rechtshilfegesuche zu vermeiden, ist die extensive Auslegung der Erlaubnis zur Online-Durchsicht elektronischer Speichermedien im Strafprozessrecht nach § 110 Abs. 3 StPO.[5]

Dem Wortlaut nach erlaubt § 110 Abs. 3 StPO den offenen Zugriff auf räumlich getrennte Speichermedien. Die Regelung dient dazu, den Verlust beweiserheblicher Daten zu vermeiden, die von dem durchsuchten Computer aus zwar zugänglich sind, sich aber auf einem räumlich getrennten Speichermedium, wie etwa dem Server im Intra- oder Internet, befinden.

Nach Auffassung des LG Koblenz etwa stellt der Zugriff auf Daten von Cloud-Nutzern stets eine rein inländische Ermittlungsmaßnahme im Sinne des § 110 Abs. 3 S. 2 StPO dar, unabhängig vom Speicherort. Jedenfalls bei Cloud-basierten Speicherdiensten sei ein Ermitteln des aktuellen Speicherorts regelmäßig nicht zielführend, sodass ein Zugriff inländischer Ermittler:innen auch auf im Ausland gespeicherte Daten erfolgen könne. Infolge des regelmäßig nicht bekannten Speicherorts sei jedenfalls keine willkürliche Missachtung ausländischer Hoheitsrechte anzunehmen und damit kein Beweisverwertungsverbot die Folge.[6]

Die herrschende Ansicht in der Rechtswissenschaft sieht in einer solchen Maßnahme hingegen eine Überschreitung der Grenzen des § 110 Abs. 3 S. 2 StPO und einen Verstoß gegen das Recht des Beschuldigten auf ein faires Verfahren, welches zu einem Beweisverwertungsverbot führe.[7]

III. E-Evidence-Gesetzgebungspaket der EU und Abkommen mit den USA

Im Juni 2023 hat die EU das Gesetzgebungspaket zur grenzüberschreitenden Sicherung und Herausgabe elektronischer Beweismittel verabschiedet, das seit Vorlage durch die Europäische Kommission im Jahr 2018 heftig diskutiert wurde. Vollständig in Kraft treten werden die Regeln erst in rund drei Jahren. Das Paket besteht aus der Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[8] und der Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.[9]

Die neuen Vorschriften ermöglichen es nationalen Strafverfolgungsbehörden, Beweismittel direkt von Diensteanbietern in anderen Mitgliedstaaten anzufordern (sog. "Herausgabeanordnungen") oder die Aufbewahrung von Daten für bis zu 60 Tage zu verlangen, damit relevante Daten nicht zerstört werden oder verloren gehen (sog. "Sicherungsanordnung"). Es wird auch eine verbindliche Frist von 10 Tagen für die Beantwortung einer Herausgabeanordnung eingeführt; in Notfällen ist die Frist auf 8 Stunden reduziert.

Diese Anordnungen können sich auf alle bei den Online-Diensten gespeicherten Daten beziehen, z.B. auf Teilnehmer-, Verkehrs- und Inhaltsdaten. Für Verkehrsdaten (außer für Daten, die ausschließlich zur Identifizierung der Nutzer angefordert werden) und für Inhaltsdaten wurde eine Einschränkung vorgesehen. Diese Daten können nur bei Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, oder bei bestimmten Straftaten in Verbindung mit Cyberkriminalität, Kinderpornografie, Fälschung im Zusammenhang mit unbaren Zahlungsmitteln oder Terrorismus angefordert werden.

Die bisher üblichen Rechtshilfegesuche zwischen den Mitgliedstaaten werden danach nicht mehr erforderlich sein. Die Behörden im Land des Online-Dienstes müssen nach Inkrafttreten der neuen Regelung nicht mehr benachrichtigt werden, wenn eine „Sicherungsanordnung“ das Einfrieren von Daten für bis zu 60 Tage anordnet, auch dann nicht, wenn mittels einer Herausgabeanordnung Verkehrsdaten wie unter anderem IP-Adressen, angewählte Rufnummern oder auch Bestandsdaten angefragt werden, um die Identität von Nutzern festzustellen.

Behörden, die sensible Daten anfordern (z.B. Inhaltsdaten und Verkehrsdaten, die nicht nur zur Identifizierung verwendet werden), müssen die Behörden des Ziellandes benachrichtigen. Die benachrichtigte Behörde hat dann 10 Tage Zeit, die Anfrage zu überprüfen und gegebenenfalls Widerspruch einzulegen, wenn die Anfrage den Vorgaben des Gesetzes nicht genügt. Reagiert sie innerhalb dieser Frist nicht, muss der Diensteanbieter die Daten übermitteln. Bei grundrechtlichen Bedenken können die benachrichtigten Behörden dann Beweisanfragen an Dienstleister in ihrem Land auch ablehnen. Diensteanbieter selbst können ebenfalls rechtliche Bedenken gegen Anfragen äußern.

Die begleitende Richtlinie über gesetzliche Vertreter verpflichtet Unternehmen, die in der EU Dienstleistungen anbieten, Niederlassungen oder rechtliche Vertreter in der EU zu benennen, an welche die Behörden der Mitgliedstaaten Anfragen zur Übermittlung elektronischer Beweismitteln richten können.

Eine weitere erhebliche Neuerung, neben der Tatsache, dass die üblichen Rechtshilfegesuche nicht mehr nötig sind, birgt ein erhebliches Konfliktpotential mit Drittstaaten: Nach der neuen Verordnung ist es irrelevant, wo die Daten, die im Rahmen einer Europäischen Herausgabeanordnung zu übermitteln sind, tatsächlich gespeichert sind: Dies kann der Fall sein a) in dem Staat, in dem der benannte Vertreter sitzt, b) in einem anderen EU-Staat, aber eben auch c) in einem Drittstaat außerhalb der Europäischen Union. Dass die Verpflichtung zur Herausgabe unabhängig vom Datenspeicherort gilt, ergibt sich aus verschiedenen

Regelungen der Verordnung.[10] Damit Anordnungen an die Diensteanbieter adressiert werden können, ist es lediglich relevant, dass das jeweilige Unternehmen seine Dienste in der Europäischen Union anbietet, was insbesondere auf die großen Unternehmen aus den USA zutrifft. US-Diensteanbietern ist es aber grundsätzlich verboten, Inhaltsdaten, die auf Servern in den USA gespeichert sind, an ausländische Strafverfolgungsbehörden herauszugeben (18 U.S.C. § 2702). Die US-Diensteanbieter könnten dann zwar nach Art. 17 VO als Adressaten von Herausgabeanordnungen von der Möglichkeit Gebrauch machen, einen „Einwand" gegen die Herausgabeanordnung zu erheben. Soweit die Anordnungsbehörde die Anordnung aufrechterhalten will, entscheidet nach Art. 17 Abs. 3 VO ein Gericht des Anordnungsstaates anhand einer umfangreichen Abwägung, deren Wertungen sich aus einem ausführlichen Kriterienkatalog (Art. 17 Abs. 6 VO) ergeben, darüber, ob die Anordnung dennoch aufrechtzuerhalten ist: In die Abwägung ist etwa das Datenschutzinteresse des anderen Staates bzw. des die Herausgabe verhindernden Staates sowie der Grad der Verbindung der Strafsache mit der Europäischen Union zu berücksichtigen. Schon 2019 wurde die Europäische Kommission daher damit beauftragt, ein Abkommen zwischen der Europäischen Union und den USA über digitale Beweise auszuhandeln. Ziel aus EU-Sicht ist dabei, dass das US-Datenschutzrecht es den US-Diensteanbietern nicht mehr verbietet, Europäischen Herausgabeanordnungen, die sich auf in den USA gespeicherte Daten beziehen, nachzukommen. Auf der anderen Seite möchten auch die Regierungsvertreter:innen aus den USA verhindern, dass sich die US-Diensteanbieter gegenüber US-Anordnungen nach dem sog. US CLOUD Act[11] zur Herausgabe von Daten, die auf Servern in der Europäischen Union gespeichert sind, auf das EU-Datenschutzrecht und dabei insbesondere die Art. 44 ff. DSGVO berufen dürfen. Danach ist die Herausgabe von in der EU verarbeiteten Daten ohne ein Abkommen zwischen der Europäischen Union und dem jeweiligen Drittstaat, an den die Daten übermittelt werden sollen, grundsätzlich verboten. Geregelt werden soll daher die Geltung der E-Evidence-Verordnung für US-Diensteanbieter auf der einen und der Zugriff der US-Ermittler:innen auf in der Europäischen Union gespeicherte Daten auf der anderen Seite.[12]

Nachdem die Verhandlungen lange ausgesetzt waren, wurden sie im März 2023 aus Anlass der bevorstehenden Verabschiedung des E-Evidence-Gesetzespakets wieder aufgenommen. Nach einer am 21. Juni 2023 veröffentlichten gemeinsamen Erklärung der EU- und US-Innen- und Justizminister:innen soll zur Sicherstellung von hinreichenden Verfahrens- und Grundrechten eine im vergangenen Jahr auf OECD-Ebene verabschiedete Erklärung als eine Grundlage für das E-Evidence-Übereinkommen dienen. Durch diese Erklärung werden bestimmte Mindeststandards festgeschrieben, etwa, dass es für den Zugriff auf Daten einer rechtlichen Grundlage bedarf und ein solcher nur für legitime Zwecke zulässig ist. Außerdem wird ein Gebot der Zweckbindung formuliert sowie ein gewisses Maß an Transparenz vorgegeben. Angesichts der vagen Formulierungen erscheint es jedoch fraglich, ob hierdurch den Art. 44 ff. DSGVO hinreichend Rechnung getragen wird.[13]

IV. Zweites Zusatzprotokoll zur Cybercrime-Konvention des Europarates

Der Europarat hat am 17. November 2021 ein zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität angenommen. Es enthält Bestimmungen für eine effizientere Rechtshilferegelung, Bestimmungen über die direkte Zusammenarbeit mit Diensteanbietern in anderen Ländern, die Vertragsparteien des Übereinkommens sind, und einen Rahmen und Garantien für die Ausweitung grenzüberschreitender Abfragen. Das Protokoll enthält strikte Garantien und Datenschutzanforderungen. Da nur Staaten Vertragsparteien sein können, konnte die EU das Protokoll nicht unterzeichnen oder ratifizieren. Aus diesem Grund wurden die Mitgliedstaaten von der EU am 5. April 2022 zur Unterzeichnung und am 14. Februar 2023 zur Ratifizierung des Protokolls ermächtigt.

Ziel des Zusatzprotokolls ist die Ergänzung der Cybercrime-Konvention und ihres ersten Zusatzprotokolls. Der Anwendungsbereich umfasst jegliches elektronische Beweismaterial.

Auch für Verkehrsdaten ist lediglich ein beschleunigtes Rechtshilfeverfahren in Art. 8 des zweiten Zusatzprotokolls geregelt. Gem. Art. 8 können die Behörden einer Vertragspartei die Behörden einer anderen Vertragspartei um Übermittlung von Bestands- und Verbindungs-/Verkehrsdaten ersuchen. Art. 8 Abs. 6 gibt konkrete Fristen für die Weiterleitung der Anfrage an Diensteanbieter vor (45 Tage) sowie für die Beantwortung durch die Diensteanbieter (20 bzw. 45 Tage).

Für den grenzüberschreitenden Zugang zu Inhaltsdaten bei Telekommunikations- und Telemedienprovidern enthält Art. 9 einen beschleunigten Weg der Rechtshilfe über die nationalen Kontaktstellen des sog. 24/7-Netzwerks nach Art. 35.

Ein Direktzugriff ist im zweiten Zusatzprotokoll nur für Bestandsdaten im Sinne von Art. 18 Abs. 3 des Übereinkommens über Computerkriminalität (siehe Art. 7 des zweiten Zusatzprotokolls) und für Informationen bezüglich der Registrierung von Domänennamen im Internet (siehe Art. 6 des zweiten Zusatzprotokolls – auch hierbei handelt es sich der Sache nach um Bestandsdaten des Domain-Inhabers) vorgesehen.[14]

V. UN-Cybercrime-Konvention

Während die USA und ihre Verbündeten der Auffassung sind, dass die Budapester Konvention das beste Abkommen ist, um Cybercrime zu bekämpfen, argumentieren Russland, China und viele Entwicklungsländer, dass die Budapester Konvention nur eine begrenzte Anzahl von Staaten repräsentiere und weit von einem globalen Konsens entfernt sei. Ein solcher könne nur auf der Ebene der UN erreicht werden.[15]

Nachdem Ansätze zur Aufnahme von Verhandlungen über eine UN-Cybercrime-Konvention immer wieder scheiterten, nicht zuletzt aufgrund der Intervention des Europarates bzw. einiger Mitgliedstaaten des Europarates, beschloss die UN-Generalversammlung am 27. Dezember 2019, ein Ad-hoc-Komitee zur Erarbeitung einer umfassenden Konvention zum Thema Cybercrime zu schaffen.

Die ersten fünf Treffen des Ad-Hoc-Komitees fanden 2021 und 2022 in Wien und New York statt. Am 26. Mai 2021 beschloss die UN-Generalversammlung bereits erste Details der Konvention. Die Generalversammlung regte eine breite Beteiligung von Nichtregierungsorganisationen an und betonte sowohl die Prinzipien der Transparenz als auch die geografische Ausgewogenheit und Geschlechterparität ausdrücklich.[16] Nach weiteren Treffen in diesem Jahr wird mit einer Verabschiedung der UN-Cybercrime-Konvention Anfang 2024 gerechnet.[17]

Eine erste veröffentlichte Gliederung der Konvention zeigt, dass folgende Kapitel vorgesehen sind: Grundsätzliche Vorschriften, Strafbarkeit, Prozessrecht, Internationale Zusammenarbeit, Technische Unterstützung, Prävention, Implementierung und Schlussbestimmungen. Da vor allem Russland und China brisante Vorschläge eingebracht haben, ist eine Debatte entbrannt. Ein russischer Vorschlag sieht unter anderem eine Pflicht für Provider vor, Strafverfolgungsbehörden weltweit beim Abhören in Echtzeit zu unterstützen, *"subversive oder bewaffnete Aktivitäten, die auf den gewaltsamen Sturz des Regimes eines anderen Staates gerichtet sind"*, sollen verboten werden.[18] Das Verbreiten terroristischer und extremistischer Inhalte inklusive "politischer Hassrede" soll nach dem Willen Russlands global strafbar werden.[19] NGOs kritisieren insbesondere die in Art. 46 IV geregelten Verpflichtungen gegenüber Dritten, wie z.B. Diensteanbietern, entweder Sicherheitslücken in bestimmter Software offenzulegen oder den zuständigen Behörden Zugang zu verschlüsselter Kommunikation zu gewähren. Widerspruch regt sich auch gegen die in Art. 47 geregelte Erhebung von Verkehrsdaten in Echtzeit.[20] Mehr als 80 NGOs fordern, die UN solle dafür

Sorge tragen, dass die Konvention „nicht das Hacken von Netzwerken und Endgeräten“ ermöglicht.[21]. Das Abkommen habe das Potenzial, Millionen von Menschen auf der ganzen Welt tiefgreifend zu beeinflussen. Es müsse daher deutlich gemacht werden, dass der Kampf gegen die globale Cyberkriminalität nicht die Menschenrechte gefährdet oder untergräbt.[22]

VI. Fazit

Der schnelle grenzüberschreitende Zugang zu digitalem Beweismaterial ist von entscheidender Bedeutung für eine erfolgreiche Bekämpfung der Cyberkriminalität. Zugleich gilt es hier, den Grundrechtsschutz und die staatliche Souveränität der betroffenen Staaten zu respektieren.

Während eine Überdehnung der existierenden strafprozessualen Befugnisse nicht zur Lösung beitragen kann, dürfte künftig die schnellste Lösung in der Anwendung des E-Evidence-Gesetzespakets der EU liegen. Vorausgesetzt ist freilich, dass die erwähnten noch notwendigen Verhandlungen mit den USA erfolgreich abgeschlossen werden. Das EU-Gesetzespaket tritt allerdings erst in drei Jahren in Kraft.

Eine deutliche Beschleunigung der Verfahren dürfte auch bei einer Ratifizierung des zweiten Zusatzprotokolls zum Übereinkommen über Computerkriminalität des Europarates erfolgen. Dieses Zusatzprotokoll wurde bisher von 42 Staaten unterzeichnet; 2 davon haben es ratifiziert. Deutschland hat es am 27. Januar 2023 unterzeichnet, jedoch bis dato noch nicht ratifiziert.

Mit Inkrafttreten der UN-Cybercrime-Konvention, sofern sie, wie angekündigt, im nächsten Jahr verabschiedet wird, wird es zwei Konventionen zu demselben Thema geben, sodass über die jeweilige Anwendung gem. Art. 30 des Wiener Übereinkommens über das Recht der Verträge zu entscheiden wäre. Es besteht hier die Gefahr, dass das Vorhandensein zweier allgemeiner Rechtsrahmen für ein und dasselbe Thema nicht zur Vereinfachung der Rechtshilfe zwischen den Staaten beitragen wird. Positiv ausgewirkt hat sich hier bisher die breite Beteiligung der NGOs an den Verhandlungen zur UN-Cybercrime-Konvention, welche zu einer notwendigen und breiteren Debatte in der Öffentlichkeit über die hier betroffene Souveränität der Staaten und den Grundrechtsschutz der Bürger:innen geführt hat.

---

1. Angaben des Europäischen Rates <https://www.consilium.europa.eu/de/policies/e-evidence/> (Zugriff: 15.9.2023).↩
2. Keyser, Journal of Transnational Law & Policy Vol. 12 (2), 289; A. Sofaer und S. Goodman, “Cyber Crime and Security-The Transnational Dimension”, in: A. Sofaer und S. Goodman (Hrsg.), *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, S. 1 ff.↩
3. Angaben des Europäischen Rates <https://www.consilium.europa.eu/de/policies/e-evidence/ > (Zugriff: 15.9.2023).↩
4. Dazu M. Gercke, „Die Entwicklung des Internetstrafrechts 2021/2022“, (2022), *Zeitschrift für Urheber- und Medienrecht (ZUM)*, 893.↩
5. LG Koblenz, Beschluss vom 24.8.2021 – 4 Qs 59/21.↩
6. LG Koblenz, a.a.O.↩
7. Bechtel, Anmerkung zu LG Koblenz vom 24.8.2021 - 4 Qs 59/21, NZWiSt 2022, 160, 162 ff.; M. Gercke, (2022) *ZUM, op. cit*. (n. 4), 893; M. Gercke und P. Brunst, *Praxishandbuch Internetstrafrecht*, 2009, 371 f.; W. Bär, „Transnationaler Zugriff auf Computerdaten“, (2011), *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)*, 54; W. Bär, *Handbuch der EDV-Beweissicherung*, 2007, Rn. 372 ff. insbes. 375; G. Trüg und M. Mansdörfer, „Strafprozessuale Maßnahmen zur Ermittlung in der Cloud“, in: M. Hilber (Hrsg.) *Handbuch Cloud Computing*, 2014, S. 559 f.; G. Borges und J. Meents und M. Gercke, Cloud Computing, 2016, Kap. 8 Rn. 40; Hegemann, BeckOK StPO, 44. Ed. Stand: 1.7.2022, StPO § 110 Rn. 14 mwN.↩
8. Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, ABl L 191, 28.7.2023, 118.↩
9. Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren, ABl L 191, 28.7.2023, 181.↩
10. Art. 1 Uabs. 1 , Art. 17 Abs. 2 lit. b, Erwägungsgrund 21 der VO 2023/1543.↩
11. „Clarifying Lawful Overseas Use of Data Act (CLOUD Act)“ <https://www.justice.gov/criminal-oia/page/file/1152896/download> (Zugriff: 15.9.2023). Dazu J. Daskal, “Unpacking the CLOUD Act”, eucrim 2018, 220.↩
12. Zum Ganzen P. Meißner, „Digitale Beweise im EU-/USDatenschutzkonflikt“, (2023), *Verfassungsblog*, <https://verfassungsblog.de/digitale-beweise-imeu-us-datenschutzkonflikt/> (Zugriff: 15.9.2023).↩
13. P. Meißner, (2023) *Verfassungsblog, op. cit.* (n. 12).↩

14. MüKo StPO/Rückert, 2. Aufl. 2023, § 100a StPO Rn. 46a.↩
15. A. Segura-Serrano, „Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development“, (2021), *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV),* 701 ff.↩
16. Dazu M. Gercke, (2022) *ZUM, op. cit*. (n. 4), 893.↩
17. So Human Rights Watch, „Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights“, 28. April 2022, <https://www.hrw.org/news/2022/04/28/opening-stages-un-cybercrime-treaty-talks-reflect-human-rights-risks> (Zugriff: 15.9.2023).↩
18. Art. 26 Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, A/AC.291/16, 7. November 2022, Englische Version, <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/A_AC291_16_Advance_Copy.pdf> (Zugriff: 28.09.2023).↩
19. Art. 27, *op. cit.* (n. 18).↩
20. Offener Brief von mehr als 80 NGOs „Civil Society Letter on the Proposed Cybercrime Treaty“, <https://epicenter.works/sites/default/files/cndletter-14.12.2022_0.pdf> (Zugriff: 15.9.2023).↩
21. Electronic Frontier Foundation (EFF), "Global Cybercrime and Government Access to User Data Across Borders: 2022 in Review", 2. Januar 2023, <https://www.eff.org/de/deeplinks/2022/12/global-cybercrime-and-government-access-user-data-across-borders-2022-year-review> (Zugriff: 15.9.2023).↩
22. Offener Brief von mehr als 80 NGOs, *op. cit.* (n. 20).↩

COPYRIGHT/DISCLAIMER
© 2023 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union