



ONLINEKOMMENTAR  
DER FREI ZUGÄNLICHE  
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

# Art. 32 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Damian K. Graf  
Herausgegeben von Damian K. Graf

Stand der Bearbeitung: 26.10.2023

PDF erstellt am: 06.10.2026

DOI: 10.17176/20231026-184317-0

## ZITIERVORSCHLAG

Damian K. Graf, Kommentierung zu Art. 32 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Graf, N. XXX zu Art. 32 CCC.

### **Art. 32 Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind**

Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei:

- a. auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden; oder
- b. auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmässige und freiwillige Zustimmung der Person einholt, die rechtmässig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.

## GLIEDERUNG

|                                                                                                                                                                                                                                   |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| I. Allgemeines.....                                                                                                                                                                                                               | 3  |
| A. Einleitung, Entstehungsgeschichte, Zweck und Kritik.....                                                                                                                                                                       | 3  |
| B. Völkerrechtliches Fundament: Territorialitäts- und Souveränitätsprinzip (Art. 31 CCC) sowie deren Durchbrechung (Art. 32 CCC)Die Ausführungen dieses Kapitels finden sich bereits in Graf, Strafverfolgung 2.0, Rz. 21 ff..... | 6  |
| C. Materialien und Auslegung.....                                                                                                                                                                                                 | 8  |
| D. Rechtsnatur .....                                                                                                                                                                                                              | 8  |
| E. Geltungsbereich.....                                                                                                                                                                                                           | 9  |
| F. Praxisrelevanz .....                                                                                                                                                                                                           | 11 |
| II. Zugriff auf in einem anderen Vertragsstaat gespeicherte öffentlich zugängliche Daten («open source») (lit. a) ..                                                                                                              | 12 |
| A. Öffentlich zugängliche Daten .....                                                                                                                                                                                             | 12 |
| B. Rechtsnatur: Qualifikation als Grundrechtseingriff? .....                                                                                                                                                                      | 14 |
| C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht .....                                                                                                                                 | 15 |
| III. Zugriff auf anderweitige, in einem anderen Vertragsstaat gespeicherte Daten (lit. b).....                                                                                                                                    | 16 |
| A. Rechtmässige und freiwillige Einwilligung der Person, die rechtmässig befugt ist, die Daten weiterzugeben .....                                                                                                                | 16 |
| 1. Weitergabeberechtigung .....                                                                                                                                                                                                   | 16 |
| 2. Einwilligung.....                                                                                                                                                                                                              | 18 |
| B. Folge einer rechtsgültigen Einwilligung .....                                                                                                                                                                                  | 20 |
| C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht .....                                                                                                                                 | 20 |
| IV. Über Art. 32 CCC hinausgehende Beweissicherung nach dem ZugriffsprinzipDie Ausführungen dieses Kapitels finden sich bereits in Graf, Strafverfolgung 2.0, Rz. 26 ff. ....                                                     | 23 |
| V. Folgen der Verletzung ausländischen Souveränitätsrechts .....                                                                                                                                                                  | 26 |
| VI. Reformbedarf.....                                                                                                                                                                                                             | 27 |
| Literaturverzeichnis.....                                                                                                                                                                                                         | 27 |
| Materialienverzeichnis .....                                                                                                                                                                                                      | 31 |

## I. ALLGEMEINES

### A. Einleitung, Entstehungsgeschichte, Zweck und Kritik

- 1 In Anbetracht der stetig zunehmenden Verlagerung der Kommunikation auf Internetdienste (wie E-Mails, soziale Medien und Internettelefonie) sowie der technologischen Entwicklung weg vom lokalen Speicher hin zu «Cloud Computing» hat sich auch der Ermittlungsfokus der Strafverfolgungsbehörden gewandelt. Deren Arbeit wird durch diese **Beweisverlagerung in die digitale Welt** zunehmend komplexer. Diese Komplexität ist zum einen darauf zurückzuführen, dass Daten von flüchtiger Natur sind, problemlos grenzüberschreitend verschoben werden können (was bspw. aus Gründen besserer Auslastung der Rechnersysteme auch automatisch geschehen kann)<sup>1</sup> sowie einer Verschlüsselung zugänglich sind. Zum anderen operieren führende Anbieter von kaum mehr wegzudenkenden Internetdiensten (wie etwa Google, Facebook bzw. Meta, WhatsApp, X oder Microsoft) gewöhnlicherweise vom Ausland aus (vor allem den USA) und bieten ihre Dienstleistungen von dort aus natürlichen und juristischen Personen in der Schweiz an, während deren Nutzerdaten im Ausland gespeichert werden. Dies führt dazu, dass die Ermittlungsbehörden ihre Aufmerksamkeit selbst in Binnensachverhalten regelmässig über die nationalen Grenzen hinaus richten müssen. In den EU-Mitgliedstaaten wird bereits in über 50 Prozent aller strafrechtlichen Ermittlungen ein grenzüberschreitendes Ersuchen gestellt, um elektronische Daten erhältlich zu machen.<sup>2</sup> Das stellt die Strafverfolgungsbehörden vor einige Herausforderungen, nicht zuletzt völkerrechtlicher Natur, da die extraterritoriale Beweiserhebung prima vista einen Eingriff in die Souveränität des anderen Staates darstellt (vgl. nachstehend, N. 10 ff.).
- 2 In diesem grenzüberschreitenden Kontext müssen den Behörden **effektive Eingriffsbefugnisse** zur Verfügung gestellt werden, die es ihnen ermöglichen, die für inländische Strafverfahren erforderlichen Beweismittel sicherzustellen.<sup>3</sup> Die Rechtshilfe als traditioneller Mechanismus internationaler Zusammenarbeit gilt derweil als ineffizient und träge, gerade wenn es um flüchtige oder ohne besondere Mühe verschiebbare, löschbare oder manipulierbare Daten geht.<sup>4</sup> Regelmässig ist den Ermittlern auch nicht bekannt, in welchem Staat die Daten gespeichert sind oder, je nachdem, bei welchem Internet-Service-Provider die Daten überhaupt aufbewahrt werden, womit sie im Zeitpunkt des Zugriffs oft weder beurteilen können, ob sie dabei die «digitale Staatsgrenze» überschreiten, noch für sie erkennbar ist, in welchem Staat überhaupt um Rechtshilfe ersucht werden soll – und selbst wenn die Ermittler einen Staat identifiziert haben, benötigen sie für die erfolgsversprechende Begründung eines Rechtshilfeersuchens ein Minimum an Informationen (bspw. ein Nutzerkonto oder eine IP-Adresse), was sich zuweilen ebenfalls als schwierig erweisen kann.<sup>5</sup>
- 3 Die **Notwendigkeit einer grenzüberschreitenden Beweissicherung** wurde bereits in den Neunzigerjahren erkannt, und am 11.9.1995 – zu einem Zeitpunkt, als die heutigen technischen Möglichkeiten erst in mancher Populärliteratur absehbar waren – verabschiedete der Europarat die Empfehlung Nr. R (95) 13 zu den Problemen des Strafverfahrensrechts im Zusammenhang mit Informationstechnologien. Deren Rz. 17 lautet wie folgt: «The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction,

---

1. Vgl. T-CY, Transborder Access, Rz. 31 und Rz. 35 ff.; Bär, Rz. 30; Karagiannis/Vergidis, S. 5.

2. Angaben des Europäischen Rates, abrufbar unter <https://www.consilium.europa.eu/de/policies/e-evidence/>, besucht am 17.10.2023.

3. Wabnitz/Janovsky-Bär, Kap. 12 N. 2.

4. Seger, S. 74.

5. Seger, S. 74.

provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.»<sup>6</sup> In Umsetzung dieser Empfehlung begannen daraufhin Verhandlungen über ein Übereinkommen über die Cyberkriminalität. Die Beschleunigung internationaler Kooperation sowie eine allfällige Einräumung grenzüberschreitender Befugnisse bar des Souveränitätsprinzips gehörten dabei zu den Kernthemen.

- 4 Der letztlich beschlossene Art. 32 der Cybercrime Convention («CCC»)<sup>7</sup> erlaubt, in Durchbrechung staatlicher Souveränität, in zwei Konstellationen den Zugriff auf in anderen Vertragsstaaten gespeicherte Daten, ohne dass ein an die Behörden des anderen Staates gerichtetes Rechtshilfeersuchen erforderlich wäre: Zum einen, wenn öffentlich zugängliche Daten betroffen sind (lit. a), sowie zum anderen, wenn die berechnigte Person ihre Einwilligung in den Zugriff erteilt hat (lit. b). Art. 32 CCC erlaubt in diesen Fällen mit anderen Worten eine **direkte Sicherstellung von im Ausland gespeicherten Daten**, ohne dass zuvor die Einwilligung des betroffenen Staates eingeholt und ohne dass vor oder nach Erhebung der (steinige) Rechtshilfeweg beschritten werden müsste. Der administrative Ballaststoff fällt gänzlich weg, da der andere Staat über die Beweiserhebung nicht informiert werden muss.<sup>8</sup> Sind die Voraussetzungen von Art. 32 CCC nicht erfüllt, namentlich falls die berechnigte Person nicht kooperiert, oder ist eine Erhebung technisch nicht möglich oder aus anderen Gründen nicht durchsetzbar, so ist in Anwendung von Art. 31 CCC **subsidiär der ordentliche Rechtshilfeweg** zu beschreiten, gegebenenfalls verbunden mit einem Ersuchen um unverzügliche Beweissicherung i.S.v. Art. 29 CCC, falls ein Beweisverlust einzutreten droht.
- 5 Im Vernehmlassungs- und Gesetzgebungsprozess zur Umsetzung der CCC in der Schweiz gab Art. 32 CCC, trotz der darin verwendeten auslegungsbedürftigen Begriffe und des damit einhergehenden Souveränitätseingriffs, zu keinerlei Bemerkungen Anlass.<sup>9</sup>
- 6 Die Stossrichtung des Art. 32 CCC ist andernorts **nicht unkritisiert** geblieben, einerseits wegen der damit einhergehenden Aufhebung des durch die territoriale Souveränität gewährleisteten Grundrechtsschutzes, ohne dass die inländischen Behörden überhaupt von solchen Grundrechtseingriffen Kenntnis erlangen.<sup>10</sup> Art. 32 CCC erlaube insoweit unkontrollierte ausländische Hoheitshandlungen auf eigenem Staatsgebiet, was in verfassungsmässige Rechte der betroffenen Personen sowie Dritter eingreife,<sup>11</sup> unverhältnismässig<sup>12</sup> sowie heikel sei, gerade hinsichtlich Staaten mit einer getrühten Menschenrechtssituation. Die mit Art. 32 CCC einhergehende Erleichterung in der strafprozessualen Beweiserhebung ist in der Verfolgung von Straftaten mit einer digitalen Komponente indes nicht mehr wegzudenken: Unser Leben – und mithin dasjenige tatverdächtiger Personen – ist digital geworden und spielt sich zunehmend nicht im dem schweizerischen Territorium zurechenbaren digitalen Raum ab. Wohl verfügen heutzutage die meisten elektronischen Geräte noch über einen eigenen, oft grosszügigen lokalen Speicher, der, sofern das Gerät in der Schweiz

---

6. Siehe dazu auch Explanatory Memorandum, Rz. 187.

7. Ähnlich der fast wortgleiche Art. 40 Abs. 2 der Arab Convention on Combating Information Technology Offences vom 21.12.2010.

8. T-CY Guidance Note # 3, S. 6; anders bspw. bei der sog. Nacheile, vgl. Art. 16 Ziff. 1 des Vertrags zwischen der Schweizerischen Eidgenossenschaft und der Bundesrepublik Deutschland über die grenzüberschreitende polizeiliche und justitielle Zusammenarbeit vom 27. 4.1999 («Schweizerisch-deutscher Polizeivvertrag», SR 0.360.136.1).

9. Vgl. Bundesamt für Justiz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens; vgl. ferner die parlamentarischen Beratungen: AB 2010 S 1020 ff. (Ständerat); AB 2011 N 97 ff. (Nationalrat).

10. BVerfGE 142, 234, Rz. 7; vgl. auch BBl 2010 4738. Eine Bekanntgabe an die Behörden des betroffenen Staates ist freilich zulässig, T-CY Guidance Note # 3, S. 6.

11. Vgl. T-CY, Transborder Access, Rz. 52 ff., Rz. 58 ff. und Rz. 62 ff.

12. BVerfGE 142, 234, Rz. 7.

sichergestellt werden kann, gestützt auf die allgemeinen strafprozessualen Regeln sichergestellt, durchsucht (Art. 246 StPO) und beschlagnahmt (Art. 263 StPO) werden kann. Der Trend geht indes weg vom lokalen Speicher hin zu cloudbasierten oder dislokalen Lösungen, deren Speicherort irgendwo auf der Welt, jedenfalls nur zu einem Bruchteil in der Schweiz liegen wird (mit Ausnahme besonderer Industrien wie des Banken- und Beratungswesens). Auch die Kommunikation erfolgt heutzutage regelmässig über soziale Medien und vergleichbare Internet-Services, wobei die Inhalte zuweilen nicht einmal mehr lokal auf dem eigenen Gerät gespeichert werden. Indem es Art. 32 CCC den inländischen Strafverfolgungsbehörden eines Vertragsstaates insbesondere erlaubt, ausländische Internet-Service-Provider direkt und unter Vermeidung des Rechtshilfewegs um Herausgabe von Daten zu ersuchen (vgl. nachstehend, N. 48, 55), wird mindestens teilweise sichergestellt, dass die materielle Wahrheitsfindung im Falle von Straftaten mit einer digitalen Komponente nicht gänzlich illusorisch wird.

- 7 Andererseits erachten insbesondere Strafverfolgerkreise den Art. 32 CCC als zu restriktiv: Art. 32 CCC stelle als «kleinster gemeinsamer Nenner»<sup>13</sup> einen letztlich wenig revolutionären Kompromiss dar. Diskussionen über die Zulässigkeit von über Art. 32 CCC **hinausgehenden grenzüberschreitenden Beweiserhebungen** scheiterten indes am fehlenden Konsens innerhalb des Europarats.<sup>14</sup> Auch in den seither weitergeführten Diskussionen fand sich weitgehend kein Einvernehmen, obschon die Beweisverlagerung über die Staatsgrenzen hinaus von der Mehrheit der Staaten als eine der zentralen Herausforderungen territorialstaatlicher Strafverfolgung qualifiziert wird. Auch mit dem am 12.5.2022 verabschiedeten und bereits von zwei Staaten ratifizierten sowie 40 weiteren Staaten unterzeichneten (Stand: Oktober 2023) II. Zusatzprotokoll zur Cybercrime Convention («ZP II-CCC») blieb der grosse Wurf aus – immerhin soll es danach erlaubt sein, Dienstleister im Ausland direkt und ohne Umweg über die Rechtshilfe verbindlich aufzufordern, Registrierungsinformationen zu Domainnamen sowie Bestandesdaten<sup>15</sup> herauszugeben (Art. 6 und 7 ZP II-CCC). Von der Schweiz wurde das ZP II-CCC noch nicht unterzeichnet oder ratifiziert, was gemäss Quellen im Bundesamt für Justiz auch in naher Zukunft nicht geschehen soll – zum einen, weil die neue Regelung wiederum das Souveränitätsprinzip tangiere, und zum anderen, weil auf Stufe der Vereinten Nationen Diskussionen zu dieser Thematik geführt würden, die abzuwarten wären. In der Tat befinden sich die Beratungen zu einer United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes («UN Treaty on Cybercrime») in einem fortgeschrittenen Stadium. Der von der Mehrheit mitgetragene aktuelle Entwurf sieht aber keine grenzüberschreitende Beweiserhebung vor,<sup>16</sup> weshalb ein Zuwarten mit der Unterzeichnung und Ratifizierung des ZP II-CCC nicht sachgerecht erscheint.
- 8 Einen Schritt weiter als Art. 32 CCC geht die unlängst in der EU verabschiedete Verordnung (EU) 2023/1543 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren vom 12.7.2023 («**e-Evidence-Verordnung**»), wonach Justizbehörden eines Mitgliedstaats elektronische Beweismittel direkt von einem Diensteanbieter in einem anderen Mitgliedstaat anfordern dürfen (Art. 1 Abs. 1 e-Evidence-Verordnung) und die Diensteanbieter rechtlich verpflichtet sind, die Daten innert 10 Tagen bzw. der angesetzten Frist zu edieren (Art. 10 e-Evidence-Verordnung). Art. 32 CCC setzt dagegen auf die Freiwilligkeit ausländischer Diensteanbieter

13. Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 4; Seitz, S. 47; BGE 141 IV 108 E. 5.3 und 5.9.

14. Explanatory Report, Rz. 293; BBl 2010 4737; Weber, S. 433.

15. Bereits heute können Bestandesdaten i.A.v. Art. 32 lit. b CCC herausverlangt werden, indes ist in Art. 7 ZP II-CCC neu keine Einwilligung mehr erforderlich, der Diensteanbieter im Ausland kann mithin verpflichtet werden.

16. United Nations, Consolidated Negotiating Document (vgl. immerhin die Minderheitsvorschläge in Art. 45 Abs. 1<sup>bis</sup> und Art. 45 Abs. 1 lit. b).

– kommen sie dem Ersuchen nicht oder nicht vollständig nach, ist der Rechtshilfeweg zu beschreiten, selbst bei willkürlicher, undurchsichtiger oder unbegründeter Kooperationsverweigerung. Wohl sieht Art. 18 Abs. 1 lit. b CCC zumindest vor, dass derjenige Internet-Service-Provider, der seine Dienste «im Hoheitsgebiet der Vertragspartei anbietet», Bestandesdaten im Zusammenhang mit diesen Diensten auf Verlangen hin herauszugeben hat. Das Bundesgericht erlaubt aber keine Editionsverfügung auf der Grundlage von Art. 18 Abs. 1 CCC an einen ausländischen Provider bzw. erachtet eine solche maximal dann als rechtmässig, wenn sie an dessen schweizerischen Ableger adressiert ist, sofern dieser die Daten entweder besitzt oder kontrolliert.<sup>17</sup>

- 9 Die vor allem in Strafverfolgerkreisen geäusserte Kritik an den Limitationen des Art. 32 CCC ist in der Schweiz etwas leiser geworden. Denn der Umstand, dass die Staatengemeinschaft bislang keine konsensuale Lösung gefunden hat, hat das Bundesgericht (wohl aus Praktikabilitätsüberlegungen, wenngleich in Missachtung des Souveränitätsprinzips) nicht davon abgehalten, auch transnationale Beweiserhebungen von Daten ohne Einwilligung der berechtigten Personen unter implizitem Rückgriff auf das sogenannte **Zugriffsprinzip** zu erlauben (vgl. nachstehend, N. 63 ff.).

## B. Völkerrechtliches Fundament: Territorialitäts- und Souveränitätsprinzip (Art. 31 CCC) sowie deren Durchbrechung (Art. 32 CCC)<sup>18</sup>

- 10 Das **Territorialitätsprinzip** stellt eine der völkerrechtlichen Souveränität entfließende Schranke staatlichen Handelns dar. Es dient nicht nur der Begrenzung der Anwendbarkeit innerstaatlichen Strafrechts auf ausländische Sachverhalte – wovon freilich Ausnahmen existieren –<sup>19</sup>, sondern limitiert zugleich staatliches Handeln auf das eigene Hoheitsgebiet.<sup>20</sup> Gänzlich verboten ist die Vornahme amtlicher Handlungen auf fremdem Territorium zwar nicht.<sup>21</sup> Sofern derartiges Verhalten aber nicht ausdrücklich durch internationale (Rechtshilfe-)Abkommen, bilaterale Verträge oder zumindest ad hoc-Genehmigungen erlaubt ist, stellt es einen unzulässigen Eingriff in die staatliche Souveränität dar und kann nach ausländischem Recht gegebenenfalls entsprechend geahndet werden. Unbewilligte amtliche Handlungen auf fremdem Territorium werden auch nach schweizerischem Recht sanktioniert (Art. 299 StGB; vgl. auch Art. 271 StGB). In Verletzung des Territorialitätsprinzips erhobene Beweise können zudem im innerstaatlichen Strafverfahren gegebenenfalls nicht verwertet werden (vgl. nachstehend, N. 69 ff.).
- 11 Insbesondere «**eigenmächtige Handlungen mit Zwangs- und Eingriffscharakter auf fremdem Hoheitsgebiet**»<sup>22</sup> verletzen die staatliche Souveränität und sind daher völkerrechtswidrig. Somit sind, sofern dafür nicht die Rechtshilfe des fremden Staats in Anspruch genommen wird, etwa Verhaftungen von Personen im Ausland durch schweizerische Beamte ebenso unzulässig wie die Durchführung von Einvernahmen, die Vornahme von Augenscheinen oder die direkte Vollstreckung von Urteilen.<sup>23</sup> Dasselbe gilt gemäss Bundesgericht für den Versand von Vorladungen an im Ausland domizilierte beschuldigte Personen, die nicht mit Zwangsandrohungen versehen sein dürfen, mithin als blosser Einladungen auszugestalten sind.<sup>24</sup> Klar erscheint damit, dass die Strafverfolgungsbehörden nicht physisch im Ausland Beweise erheben oder dort Verfahrenshandlungen vornehmen dürfen,

17. BGer 1B\_142/2016 vom 16.11.2016 E. 3.6; BGE 141 IV 108 E. 6.4; s.a. Explanatory Report, Rz. 173; T-CY, Cloud, Rz. 56; Forster, S. 619 f.; Roth, Rz. 50 ff.; a.M. Schweingruber, Rz. 21 ff.

18. Die Ausführungen dieses Kapitels finden sich bereits in Graf, Strafverfolgung 2.0, Rz. 21 ff.

19. Vgl. bspw. Art. 4-7 StGB.

20. Capus, S. 193; BGE 140 IV 86 E. 2.4; vgl. BStGer BV.2006.37 vom 13.9.2006 E. 2.

21. Vgl. BGer 1B\_87/2007 vom 22.6.2007 E. 2.7.

22. Capus, S. 193; Gless, S. 322.

23. Vgl. BSK-Omlin, Art. 299 StGB N. 14; Unseld, S. 6; differenzierend Bottinelli, S. 1329 f.

24. BGE 140 IV 86 E. 2.4; vgl. die Kritik bei Largiadèr, S. 293 f.

ohne den Rechtshilfeweg zu beschreiten resp. ohne dass solche Handlungen in einem Abkommen explizit erlaubt wären. Eigenmächtige Hausdurchsuchungen oder die Sicherstellung und Durchsuchung von elektronischen Geräten oder Unterlagen auf fremdem Staatsgebiet sind damit zweifellos untersagt.

- 12 Nicht anders gelagert sind Beweisbeschaffungssituationen, in denen sich die Strafbehörden zwar nicht physisch auf ausländischem Staatsgebiet aufhalten, aber in der Schweiz Untersuchungshandlungen vornehmen, die sich auf die fremde Gebietshoheit auswirken. Darunter fällt bspw. die Observation von Personen auf der deutschen Uferseite des Rheins durch schweizerische Polizisten von Schaffhausen aus, genauso wie die Video-Einvernahme eines im Ausland befindlichen Beschuldigten durch ein schweizerisches Gericht. Solches Verhalten verletzt das Völkerrecht ebenfalls, da es in seinen Wirkungen einem Hoheitsakt direkt auf fremdem Staatsgebiet gleichkommt.<sup>25</sup>
- 13 Auch der Zugriff auf Computersysteme im Ausland von einem Standort in der Schweiz aus und damit die **Sicherstellung von im Ausland gespeicherten Daten** sind als solche extraterritorialen Hoheitsakte zu qualifizieren.<sup>26</sup> Die Staatengemeinschaft beansprucht auch hinsichtlich auf eigenem Territorium stationierter Datenverarbeitungsanlagen und der dort gespeicherten Daten Souveränität.<sup>27</sup> Nationale Durchsuchungsbefugnisse können derartige Eingriffe in fremde Souveränitätsrechte nicht legitimieren.<sup>28</sup> Das ist vom Bundesgericht einmal grundsätzlich anerkannt worden<sup>29</sup> (vgl. indes nachstehend, N. 63 ff.) und wird insbesondere auch in den (intensiven) Diskussionen zum Inhalt bzw. zur Fortentwicklung der CCC abgebildet.<sup>30</sup>
- 14 Sobald in einem solchen Sinne in die Souveränität eines ausländischen Staates eingegriffen werden soll, muss dieser infolgedessen einwilligen, entweder indem er auf individuelles Ersuchen hin Rechtshilfe leistet oder internationalen Partnern staatsvertraglich oder ad hoc die Berechtigung einräumt, entsprechend tätig zu werden. Anwendungsbeispiele für die partielle Aufgabe der Souveränität der Schweiz finden sich in Abkommen mit Nachbarländern zur polizeilichen «Nacheile»<sup>31</sup> oder, beschränkt, im Kontext der Cybercrime Convention. Denn durch die Schaffung von Art. 32 CCC wurde in zwei Konstellationen auf die Notwendigkeit eines Rechtshilfeersuchens verzichtet: Einerseits ist der Zugriff auf öffentlich zugängliche gespeicherte Computerdaten zulässig, gleichwohl, wo sich die Daten geographisch befinden (lit. a). Andererseits – und im Vergleich zu anderen Rechtshilfeakkorden sehr weitgehend – darf eine Vertragspartei gemäss Art. 32 lit. b CCC «auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmässige und freiwillige Zustimmung der Person einholt, die rechtmässig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.» Das legitimiert nicht nur eine direkte

25. Dombrowski, S. 13 f.; vgl. Burgermeister, S. 20 f.; Grave/Barth, S. 373.

26. Zusammenfassung von BGE 141 IV 108 E. 5.3 und 5.12 in BGE 1B\_29/2017 vom 24.5.2017 E. 4.7; so auch BGE 143 IV 21 E. 3.2; ferner Roth, Rz. 30; Dombrowski, S. 12.

27. Vgl. bspw. UNGA, § 20: «[...] State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.»

28. So Brodowski/Eisenmenger, S. 122; ebenso Bär, S. 54.

29. BGE 141 IV 108 E. 5.3 und 5.9: «Vorbehältlich abweichender völkerrechtlicher Bestimmungen ist ein Staat aufgrund des Grundsatzes der Territorialität nicht berechtigt, eigene Strafverfolgungsmassnahmen auf dem Hoheitsgebiet eines anderen Staates vorzunehmen [...]. Mit Art. 32 CCC haben sich die Vertragsstaaten auf einen minimalen (restriktiven) gemeinsamen Konsens für einen grenzüberschreitenden («extraterritorialen») Zugriff geeinigt.»

30. Siehe nur T-CY, Transborder Access, Rz. 37: «If the data is stored in a foreign jurisdiction, [law enforcement authorities] would need to resort to international cooperation. The basic rule of international law regarding the exercise of coercive powers is the principle of territorial sovereignty. No State may enforce its jurisdiction within the territory of another sovereign State. As a consequence, international cooperation is dependent on international treaties [...].»

31. Auf Probleme mit Frankreich hinweisend: Stellungnahme des Bundesrats vom 29.5.2019 auf die Interpellation 19.3303 von NR Jean-Luc Addor «Grenzüberschreitende Polizeikooperation. Müssen Abkommen überprüft werden?» vom 22.3.2019.

Anfrage bei ausländischen Providern zur Herausgabe von Informationen, sondern auch den eigenhändigen Zugriff der Behörden über bestehende Benutzerkonten (vgl. nachstehend, N. 55). In der CCC wird für die Vertragsstaaten mit anderen Worten verbindlich festgelegt, unter welchen Umständen Behörden direkt auf im Ausland befindliche Daten zugreifen können (i.e. unter den Voraussetzungen von Art. 32 CCC) und wann sie ein förmliches Rechtshilfebegehren zu stellen verpflichtet sind (in allen anderen Fällen; Art. 31 CCC). Daraus erhellt, dass der **Zugriff auf ausländische Daten** unabhängig davon, dass sich Mitglieder der Strafverfolgungsbehörden bei derartigen Beweissicherungsmassnahmen nicht physisch auf ausländischem Gebiet aufhalten, als **prinzipieller Eingriff in die Souveränität** gewertet wird. Im Rahmen der Ausarbeitung der CCC stellte sich denn auch gerade heraus, «dass kein Konsens erreicht werden konnte für weitergehende Regeln, unter welchen Voraussetzungen ein unilateraler Zugriff eines Staates auf Daten, die sich in einem anderen Vertragsstaat befinden, ohne Genehmigung desselben erfolgen kann.»<sup>32</sup>

### C. Materialien und Auslegung

- 15 Die von Art. 32 CCC verwendeten Begriffe und die davon erfassten Konstellationen wurden im **Explanatory Report zur CCC** – sinngemäss die «Botschaft» des Europarats zur CCC – nur teilweise näher erläutert, was das Risiko birgt, dass die Behörden der Vertragsstaaten diese unterschiedlich auslegen. Das scheint aber ein bewusster Entscheid gewesen zu sein.<sup>33</sup> Immerhin hat eine Arbeitsgruppe zum grenzüberschreitenden Zugriff auf Daten («T-CY Transborder Group») des Komitees der Vertragsparteien («Cybercrime Convention Committee, «T-CY») am 3.12.2014 eine **Leitlinie («Guidance Note») zum grenzüberschreitenden Zugriff auf Daten unter Art. 32 CCC** erlassen, die als Auslegungshilfe herangezogen werden kann. Die Voraussetzungen des Art. 32 CCC – etwa die Frage, wer berechtigt ist, die Zustimmung nach Art. 32 lit. b CCC zu erteilen – sind aber letztlich nach inländischem Recht zu bestimmen (vgl. nachstehend, N. 41 f.); insoweit sind eine innerstaatliche Begriffsbestimmung und damit allfällige unterschiedliche Auffassungen zwischen den Vertragsstaaten unvermeidlich.
- 16 Gemäss Bundesrat soll die Bestimmung eng ausgelegt werden, «um der Gefahr des Missbrauchs unter Umgehung der Rechtshilfe oder in Verletzung der Privatsphäre Dritter entgegenzuwirken.»<sup>34</sup> Berücksichtigt man allerdings die mit Art. 32 CCC angestrebte Wirkung – die Verfahrensbeschleunigung bzw. die vereinfachte Beweiserhebung –, so gibt das Freiraum für **praxisnahe und praxistaugliche Auslegungen**.

### D. Rechtsnatur

- 17 Art. 32 CCC ist eine **«self-executing» völkerrechtliche Norm**,<sup>35</sup> die mit Ratifizierung direkt Anwendung findet. Die Vertragsparteien räumen den anderen Vertragsstaaten dadurch das Recht ein, in Umgehung des Rechtshilfewegs direkt auf Daten in ihrem Hoheitsgebiet zuzugreifen. Mit anderen Worten normiert die Bestimmung einen «Verzicht auf das innerstaatliche Verfahren im ersuchten Staat.»<sup>36</sup> Die Strafverfolgungsbehörden der Vertragsstaaten können sich unmittelbar auf Art. 32 CCC abstützen, und zwar sowohl im innerstaatlichen Strafprozess, um entsprechende Beweiserhebungen im Ausland zu legitimieren (wobei sie weiterhin die inländischen prozessualen Regeln einzuhalten haben, vgl. nachstehend, N. 56) – Art. 32 CCC stellt insoweit keine originäre Zwangsmassnahme dar –<sup>37</sup>, als auch können sie sich im Verhältnis zum betroffenen Vertragsstaat darauf berufen, dass keine

---

32. BBl 2010 4737.

33. T-CY, Transborder Access, Rz. 95; s.a. Explanatory Report, Rz. 294; BVerfGE 142, 234, Rz. 39.

34. BBl 2010 4738, allerdings unter unzutreffendem Verweis auf Drucksache 16/7218, S. 55.

35. Vgl. auch BVerfGE 142, 234, Rz. 25.

36. Walder, S. 542.

widerrechtliche Beeinträchtigung ausländischer Souveränität vorliegt. Im Verhältnis zum IRSG gehen die Bestimmungen der CCC denjenigen des IRSG jedenfalls vor (Art. 1 Abs. 1 IRSG).<sup>38</sup>

## E. Geltungsbereich

- 18 Art. 32 CCC erlaubt die Sicherstellung von Computerdaten, die in einem anderen Vertragsstaat gespeichert sind.
- 19 Als **Computerdaten** gelten nach Art. 1 lit. b CCC sämtliche Darstellungen «von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschliesslich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann.» Durch Art. 32 CCC erfasst ist damit der Zugriff auf **Bestandes-, Verkehrs- bzw. Randdaten wie auch Inhaltsdaten**, die entweder gespeichert sind oder sich im Zeitpunkt des Zugriffs im Übermittlungsstadium befinden. Aufgrund seiner rechtlichen Qualifikation als elektronischer Datenbestand kann bspw. auch Kryptovermögen in Anwendung von Art. 32 lit. b CCC sichergestellt werden, sofern die berechtigten Personen ihre Ermächtigung dazu erteilen.<sup>39</sup>
- 20 Art. 32 CCC stellt ausdrücklich auf den **Speicherort** der konkret envisagierten Daten ab (Art. 32 lit. b CCC: «[...] gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden»; vgl. auch Art. 31 CCC: «[...] die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der ersuchten Vertragspartei befindet»). Bei Daten, die an mehreren Orten gespeichert sind, ist der Speicherort des Datensatzes massgebend, der konkret sichergestellt werden soll. Ein Zugriff in Anwendung dieser Bestimmung ist folglich nur dann zulässig, wenn die CCC am **Ort der Datenhaltung** anwendbar ist.<sup>40</sup> Zumal keiner der 68 Vertragsstaaten einen Vorbehalt zu Art. 32 CCC angebracht hat, kann sich die Prüfung darauf beschränken, ob der Staat am zu tangierenden Speicherort Vertragspartei der Cybercrime Convention ist, diese mithin unterzeichnet und ratifiziert hat.
- 21 Nicht anwendbar ist Art. 32 CCC auf **rein innerstaatliche Verhältnisse**: Sind die Daten lokal auf einem sich in der Schweiz befindenden und hier sichergestellten Endgerät oder Server gespeichert, so ist diesbezüglich schweizerisches Landesrecht anwendbar (vorab Art. 246, Art. 263 und Art. 265 StPO, für Randdaten siehe Art. 273 StPO).<sup>41</sup> Das ist auch dann der Fall, wenn sich ausländische Datensätze im Zeitpunkt des Zugriffs im Zwischenspeicher des hier sichergestellten Geräts befinden. Wird das Gerät indes als «Schlüssel» bzw. «Einfallstor» verwendet, um Zugang zu Services zu erhalten, die ihre Daten im Ausland gespeichert haben (bspw. Cloud, Webmail, etc.), ohne dass diese lokal auf dem Gerät gespeichert wären, handelt es sich diesbezüglich um einen transnationalen Datenabgriff und Art. 32 CCC ist zu beachten (vgl. allerdings nachstehend, N. 63 ff.). Das schweizerische Landesrecht ist auch dann anwendbar, wenn ausländische Provider schweizerische Tochtergesellschaften oder Partner haben, die die Daten in der Schweiz speichern.<sup>42</sup> Diesfalls kann der Zugriff bei letzteren erfolgen. Datencenter werden allerdings regelmässig nicht dazu zählen, da die bei ihnen gelagerten Daten oft verschlüsselt sind und diese ohne Mitwirkung oder zwangsweise Erhebung bei den datenberechtigten Personen kaum ausgelesen werden können. Die ausländischen Personen müssen

---

37. Vgl. auch Walder, S. 542.

38. OGer ZH SB140420 vom 2.5.2015 E. 3.3.3.

39. Als einwilligungsfähig zu qualifizieren sind sowohl die Inhaberin des Wallets als auch (im Falle eines Hot Wallets) die Handelsplattform, sofern die Kooperation mit Strafbehörden nach den Nutzungsbedingungen erlaubt ist (vgl. nachstehend, N. 46 ff.). In der Praxis dürfte sich jedoch, mangels Einwilligung, oft ein «Preservation Request» (Art. 29 CCC) in Verbindung mit einem förmlichen Rechtshilfersuchen aufdrängen.

40. Bär, Rz. 29.

41. Vgl. Explanatory Memorandum, Rz. 187; T-CY Guidance Note # 3, S. 6.

42. Forster, Fn. 14.

dann entweder in Anwendung von Art. 32 lit. b CCC oder subsidiär rechtshilfeweise um die Herausgabe der Daten oder Schlüssel ersucht werden. Art. 32 lit. b CCC ist auch dann anwendbar, wenn inländische Tochtergesellschaften oder Partner ausländischer Provider von der Staatsanwaltschaft angewiesen werden, Daten auszuhändigen, die sie im Ausland gespeichert haben.<sup>43</sup> Korrekterweise darf eine inländische Person nicht unter Zwangsandrohung aufgefordert werden, für die Strafverfolgungsbehörden im Ausland verfügbare Beweismittel zu beschaffen, auch wenn es sich dabei um Daten handeln sollte, hinsichtlich derer sie zugriffsberechtigt ist.<sup>44</sup> Das Bundesgericht hielt dazu fest, eine Editionsverfügung gemäss Art. 265 StPO an einen schweizerischen Ableger eines Internet-Service-Providers sei zulässig, wenn sie hinsichtlich der gegenständlichen Daten über eine Zugriffsmöglichkeit sowie eine Zugriffsberechtigung verfüge («pouvoir de disposition, en fait et en droit, sur ces données»)<sup>45</sup> Das beisst sich nicht mit den soeben erfolgten Ausführungen, da die Editionsverfügung noch keine Zwangsmassnahme darstellt<sup>46</sup> und sie in diesem Kontext als Ersuchen nach Art. 32 CCC um freiwillige Herausgabe verstanden und gewürdigt werden kann.

- 22 Hinsichtlich von **Drittstaaten**, die sich der Konvention nicht angeschlossen haben, muss im Umkehrschluss davon ausgegangen werden, dass die staatliche Souveränität hier jedweden Online-Zugriff auf (nicht-öffentliche, vgl. nachstehend, N. 35) Daten verbietet und daher einzig die Beschreitung des Rechtshilfewegs in Frage kommt.<sup>47</sup>
- 23 Das **Abstützen auf den Speicherort** ist zwar naheliegend, weil sich die Staaten auch hinsichtlich der sich auf ihrem Territorium befindenden IT-Infrastruktur auf das Souveränitätsprinzip zu berufen vermögen.<sup>48</sup> Problematisch ist indes, dass im Zeitpunkt des Zugriffs nicht selten weder für die Strafverfolgungsbehörde noch für den Datenberechtigten oder gar für den Datengewahrsamsinhaber bekannt ist, wo die Daten in jedem Moment gespeichert sind. So speichern Internet-Service-Provider die Daten ihrer Kundinnen und Kunden zuweilen nicht in ihrem Sitzstaat, sondern anderswo. Der Speicherort kann sich aufgrund von technischen Umstrukturierungen oder Verlagerung an andere (billigere) Standorte über die Zeit auch ändern. Jedenfalls kann der Speicherort im Zeitpunkt des Datenabgriffs oft nicht abschliessend eruiert werden.<sup>49</sup> Es stellt sich damit die Frage, wie mit dem Standardfall umzugehen ist, in welchem für die Strafverfolgungsbehörde im Zeitpunkt der beabsichtigten Sicherstellung nicht bestimmbar ist, ob die Daten in einem CCC-Vertragsstaat, einem Drittstaat oder gar im eigenen Land gespeichert sind. Die Materialien zu Art. 32 CCC befassen sich nicht abschliessend damit; die T-CY Guidance Note sieht nur, aber immerhin, vor, dass die Vertragsstaaten in Situationen, in denen der Speicherort unbekannt oder unsicher ist, die Rechtmässigkeit des Zugriffs im Lichte des innerstaatlichen Rechts, der einschlägigen völkerrechtlichen Grundsätze oder mit Rücksicht auf internationale Beziehungen selbst beurteilen sollen («[...] Parties may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations»)<sup>50</sup> Bei **unbekanntem Speicherort** drängt sich was folgt auf: Würde für die Anwendbarkeit

---

43. Graf, Strafverfolgung 2.0, Rz. 28; Forster, Fn. 14.

44. Graf, Strafverfolgung 2.0, Rz. 28; Heimgartner, Strafprozessuale Beschlagnahme, S. 266; vgl. BBl 1976 II 483, worin davon gesprochen wird, dass sich sowohl die betroffene Person als auch die Gegenstände in der Schweiz befinden müssten; vgl. zum deutschen Recht auch Brodowski, S. 477, m.w.H.

45. BGer 1B\_142/2016 vom 16.11.2016 E. 3.6; BGE 143 IV 21 E. 3.4.2.

46. BGer 1S.4/2006 vom 16.5.2006 E. 1.3-1.4.

47. Jedenfalls ist Art. 32 CCC dann nicht anwendbar, siehe T-CY Guidance Note # 3, S. 6. Immerhin kann diskutiert werden, ob auch Art. 32 lit. b CCC nicht insoweit bloss deklaratorischer Natur ist, als hier die zugriffsberechtigte Person zustimmt und folglich nicht von einer eigentlichen Zwangsmassnahme gesprochen werden kann, vgl. dazu Brodowski/Eisenmenger, S. 123, m.w.H.; ferner Seitz, S. 45 f., wonach es sich dabei um das (neue) Völkergewohnheitsrecht handeln könnte.

48. United Nations, Developments, § 20; T-CY, Transborder Access, Rz. 37.

49. So kann die Standortbestimmung eines Servers ggf. durch «Trace-Routing» erfolgen, MK-Hauschild, § 110 StPO N. 18.

50. T-CY Guidance Note # 3, S. 6.

von Art. 32 CCC die sichere Kenntnis verlangt, dass der Speicherort in einem Vertragsstaat liegt, verlöre Art. 32 lit. b CCC seine Bedeutung und wäre die Sicherstellung von Cloud-Daten ad absurdum geführt.<sup>51</sup> «Allein die Möglichkeit eines Standorts in einem Drittstaat kann auch keine Rechtshilfeverpflichtung auslösen, zumal gar nicht feststeht, an welches Land man sich richten dafür soll.»<sup>52</sup> Detaillierte Abklärungen zum Speicherort sind vor dem Zugriff oft unmöglich oder nehmen zu viel Zeit in Anspruch – freilich: falls keine Dringlichkeit vorliegt und der Speicherort ohne besonderen Aufwand technisch festgestellt werden kann, sollte man sich darum bemühen.<sup>53</sup> Angesichts des Beschleunigungsgedankens der CCC wäre ein generelles Zuwarten bis zur sicheren Kenntnis aber nicht angezeigt, zumal dann, wenn Beweisverlust droht. Sollte sich im Nachhinein herausstellen, dass der Speicherort tatsächlich in einem Drittstaat lag, wird auf dem Rechtshilfeweg eine nachträgliche Genehmigung des Datenzugriffs einzuholen sein (vgl. nachstehend, N. 71).

- 24 Im Verhältnis zu den grossen **Social Media-Providern** stellt sich die Sachlage noch etwas komplizierter dar. Diese haben ihren Hauptsitz in den USA, ihren Europasitz aber oft in Irland und gemäss eigenen (angesichts des U.S. Cloud Act aber nicht unbedingt korrekten) Angaben einzig von Irland aus Zugriff auf die Daten europäischer und schweizerischer Kundinnen und Kunden (was die Provider mit der europäischen Datenschutz-Grundverordnung vom 27.4.2016 [«DSGVO»] begründen), wobei die Daten wiederum regelmässig in anderen Staaten (bspw. Schweden) gespeichert sind.<sup>54</sup> Irland hat die CCC allerdings bislang nicht ratifiziert. Entsprechend stellt sich die Frage, ob Ersuchen nach Art. 32 lit. b CCC für europäische Daten zuhanden der irischen Ableger überhaupt zulässig und die erhobenen Daten verwertbar sind. Muss alternativ Schweden als möglicher Speicherort adressiert werden, wenngleich die Daten dort zwar allenfalls abgegriffen werden können, diese aber verschlüsselt und damit unbrauchbar sein dürften? Oder ist die amerikanische Muttergesellschaft zu tangieren, die die Daten bei ihrer europäischen Tochtergesellschaft beschaffen soll? In der Praxis wird die Brisanz dieser Frage dadurch abgeschwächt, dass die Auskunftersuchen über von den Internet-Service-Providern bereitgestellte «Law Enforcement Portals» gestellt werden können – von welcher Gruppengesellschaft aus die Provider die ersuchten Daten den Behörden dann zur Verfügung stellen bzw. wie sie sich intern organisiert haben, ist ihnen überlassen und muss nicht weiter geprüft werden, zumal die Strafverfolgungsbehörden ohnehin keine Möglichkeit haben, zu überprüfen, wo die edierten Daten effektiv gespeichert gewesen sind und welche Gruppengesellschaft genau darauf Zugriff gehabt hat.
- 25 Angesichts all dieser Schwierigkeiten macht der Speicherort als massgebendes Kriterium wenig Sinn. De lege ferenda sollte daher für Art. 32 CCC auf das Anknüpfungsmerkmal des Speicherorts verzichtet und vielmehr an den **Sitz oder Aufenthaltsort** derjenigen Person geknüpft werden, die **auf die Daten rechtmässig Zugriff** hat. Alternativ (der e-Evidence-Verordnung der EU<sup>55</sup> und Art. 18 Abs. 1 lit. b CCC entsprechend) kann man auch ausreichen lassen, dass das jeweilige Unternehmen seine **Dienste im betreffenden Staat anbietet**.<sup>56</sup>

## F. Praxisrelevanz

- 26 Art. 32 CCC hat sich als **unverzichtbares Mittel** zur Verfolgung von Kriminalität mit einer digitalen Komponente entwickelt. Schweizerische Strafverfolgungsbehörden stützen sich regelmässig auf Art. 32 CCC, sei es durch die Sammlung von Open Source Information («OSINF») in Anwendung von Art.

51. Vgl. LG Koblenz, NZWiSt 2022, S. 160 ff., Rz. 22.

52. MK-Hauschild, § 110 StPO N. 18; Bär, Rz. 30.

53. S.a. MK-Rückert, § 100b StPO N. 95.

54. Siehe auch Seger, S. 77.

55. Dazu Pfeffer, Ziff. III.

56. Ähnlich Art. 18 Abs. 1 lit. b CCC.

32 lit. a CCC, sei es durch den Zugriff auf Daten bei freiwilliger Bekanntgabe der Login-Daten durch die schweizerische datenberechtigte Person gemäss Art. 32 lit. b CCC oder insbesondere durch direkte Anfragen («Information Requests») an ausländische Internet-Service-Provider zur Bekanntgabe von Bestandes-, Rand- oder Inhaltsdaten (wobei in der Praxis zumeist nur Bestandes- und Randdaten geliefert werden und für Inhaltsdaten der Rechtshilfeweg, allenfalls in Kombination mit einem «Preservation Request» nach Art. 29 CCC, beschritten werden muss). Die Zahlen direkter Auskunftersuchen sind bemerkenswert: Im ersten Halbjahr 2022 hat Google allein über 422'000 direkte Anfragen erhalten, darunter 1'357 von schweizerischen Strafverfolgungsbehörden, wovon 90 % gutgeheissen wurden.<sup>57</sup> Die Provider sind allerdings keine Rechenschaft schuldig, wenn sie eine Anfrage ablehnen; sie können die Bedingungen für eine Herausgabe eigens festlegen, verändern diese auch immer wieder und zudem variieren die Bedingungen je nach Anbieter beträchtlich.<sup>58</sup> Das ist unter dem geltenden Regime hinzunehmen, da Art. 32 CCC auf Freiwilligkeit beruht.

## II. ZUGRIFF AUF IN EINEM ANDEREN VERTRAGSSTAAT GESPEICHERTE ÖFFENTLICH ZUGÄNGLICHE DATEN («OPEN SOURCE») (LIT. A)

### A. Öffentlich zugängliche Daten

- 27 Das Sammeln und Auswerten von «open source information» wird im nachrichtendienstlichen Sektor als «**OSINT**» («**Open Source Intelligence**») bezeichnet. Die Nutzung öffentlich zugänglicher Daten hat sich auch in der Strafverfolgung als nützliche und nicht-invasive Ermittlungsmethode entwickelt. Unterstützt wird dies durch die Tech-Industrie, die Tools entwickelt hat, mit welchen die Daten nicht mehr händisch zusammengetragen werden müssen, sondern dies automatisiert erfolgt: Etwa durch Bereitstellen einer Software, mit der sämtliche öffentlich zugänglichen Informationen aus Facebook herausgezogen und in Beziehungsbäumen sowie auf der Zeitachse dargestellt werden können, oder technische Hilfsmittel, um den Geldfluss von Kryptowährungen (deren Blockchain öffentlich zugänglich ist) nachvollziehen zu können. Auch der Einsatz von künstlicher Intelligenz ist keine Zukunftsmusik mehr.
- 28 Öffentlich sind Daten dann, wenn sie **via eine Datenverarbeitungsanlage frei zugänglich**<sup>59</sup> und nicht durch besondere Sicherheitsvorkehrungen dem allgemeinen Zugriff entzogen sind.<sup>60</sup> Es reicht dabei aus, wenn sie einem unbestimmten Kreis von Nutzern zugänglich gemacht sind, selbst wenn ein Login erforderlich sein sollte, «dieses aber grundsätzlich jedem Nutzer erteilt wird, wenn ein entsprechendes Anmeldeformular ausgefüllt wurde.»<sup>61</sup> Ein System kann auch bloss teilweise öffentlich sein.<sup>62</sup> Daten,

---

57. Auswertung unter <https://transparencyreport.google.com/user-data/overview>, abgerufen am 17.10.2023. Die Gründe für eine Ablehnung sind vielfältig, und die Provider sind keine Rechenschaft schuldig. In der Praxis handelt es sich zum einen um formelle Fehler (Ersuchen nicht unterzeichnet, Rechtsgrundlagen nicht genannt, keine oder keine hinreichenden Identifikatoren mitgeliefert). Bei gewissen Internet-Service-Providern kommt zum anderen erschwerend hinzu, dass sich Geschäftskunden in den Allgemeinen Nutzungsbedingungen ausbedingen können, dass Daten ohne deren Einverständnis bzw. ohne richterliche Anordnung nicht mit Strafverfolgungsbehörden geteilt werden dürfen. Diesfalls müssen sich die Strafverfolgungsbehörden mit einem «Preservation Request» i.S.v. Art. 29 CCC und einem darauffolgenden Rechtshilfeersuchen begnügen.

58. Seger, S. 77.

59. Vgl. TPF 2018 68 E. 4.3.2 (zu Art. 320 StGB). Massgebend ist, dass «eine hohe Wahrscheinlichkeit der (redlichen) Kenntnisnahme durch Dritte besteht, mithin kein grosses Hindernis überwunden werden muss, um sie zu erfahren», BGer 6B\_56/2014 vom 16.12.2014 E. 7.1.

60. Bär, Rz. 29. Art. 13 des Bundesgesetzes vom 25.9.2015 über den Nachrichtendienst («NDG»; SR 121) subsumiert unter «öffentliche Informationsquellen» in einer nicht abschliessenden Aufzählung a) öffentlich zugängliche Medien, b) öffentlich zugängliche Register von Behörden des Bundes und der Kantone, c) von Privaten öffentlich zugänglich gemachte Personendaten, und d) in der Öffentlichkeit vorgetragene Äusserungen.

61. Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 6; T-CY Guidance Note # 3, S. 4.

auf die «nur mittels einer Schnittstelle eines im – nicht öffentlich zugänglichen – Durchsuchungsobjekt befindlichen Endgeräts zugegriffen werden kann», sind dagegen nicht «open source».<sup>63</sup>

- 29 Als öffentlich zugängliche Daten gelten **beispielhaft** – im Sinne einer nicht abschliessenden Aufzählung – frei zugängliche Massenmedien (Printmedien [selbst wenn mittels Paywall geschützt], Rundfunk), sämtliche im Internet (Clearnet wie auch Darknet) auffindbaren Informationen, webbasierte Anwendungen (wie Google Earth), Informationen auf der öffentlich einsehbaren Blockchain (bspw. bei Bitcoin), auf dem Webauftritt unter der Domainadresse einer Firma oder einer Verwaltung öffentlich abrufbare Daten,<sup>64</sup> frei zugängliche Webcams, eine jedem Interessenten offen stehende Mailingliste,<sup>65</sup> auf einer Sharing-Plattform frei verfügbare Daten,<sup>66</sup> das Abgreifen technischer Daten ab einem Webserver, die Ermittlung von Domaininformationen über «WhoIs»-Datenbanken, im Ausland frei oder gegen Entgelt zugängliche Schuldner-, Grundbuch-, Handelsregister- und Einwohnerkontrollauskünfte oder verfügbare Aufzeichnungen aus Straf-, Verwaltungs- und Zivilverfahren, das Beobachten öffentlicher Chats,<sup>67</sup> offener Internet-Foren<sup>68</sup> und öffentlich geschalteter sozialer Netzwerke (die Verwendung von öffentlichen Daten, Fotos und Beziehungen auf Facebook, Informationen ab X, Instagram, LinkedIn etc.).<sup>69</sup> Auch ein Post in einer geschlossenen Gruppe (Online-Forum, Facebook o.Ä.) kann bei Gruppen mit einer hohen Mitgliederanzahl bzw. mit faktisch unbeschränktem Zugang als öffentlich qualifiziert werden, es sei denn, der Personenkreis sei bestimmt abgegrenzt und die Personen wären persönlich untereinander verbunden.<sup>70</sup> Entsprechend nicht mehr als öffentlich können «geschlossene user groups bezeichnet werden, in denen durch Administratoren der Seite eine Einzelfallprüfung der Identität der Nutzer erfolgt und ein Ermittlungsbeamter beispielsweise nur durch Vortäuschen einer Legende Zugang erhalten würde.»<sup>71</sup>
- 30 Je nach den Umständen können nicht nur Inhaltsdaten (Personen- oder andere Daten), sondern auch Bestandesdaten (bspw. Registrierungsinformationen aus «WhoIs»-Datenbeständen) oder (selten) auch Randdaten öffentlich sein und folglich in Anwendung von Art. 32 lit. a CCC erhoben werden.
- 31 Für die Qualifikation als öffentlich zugängliche Daten spielt es keine Rolle, ob die Daten unbefugt oder mit Einwilligung der datenberechtigten Person veröffentlicht wurden. Ist die **Veröffentlichung rechtswidrig** erfolgt (bspw. durch Verletzung gesetzlicher Geheimhaltungsverpflichtungen), so sind die Daten im innerstaatlichen Strafverfahren dann verwertbar, wenn sie von den Strafverfolgungsbehörden rechtmässig hätten erlangt werden können und eine Interessenabwägung für deren Verwertung spricht.<sup>72</sup> Es gilt folglich für das erste Kriterium abzuklären, ob die Daten hypothetisch auch hätten sichergestellt werden können, wenn sie nicht öffentlich gewesen wären – also ob sie i.A.v. Art. 32 lit. b CCC oder via den Rechtshilfegeweg hätten erlangt werden können.

62. T-CY Guidance Note # 3, S. 4.

63. Grassle/Hieramente, S. 193, m.w.H.

64. BBl 2010 4737 f.; vgl. BGE 141 IV 108 E. 5.8.

65. BVerfGE 142, 234, Rz. 31.

66. Vgl. BGE 141 IV 108 E. 5.8.

67. BVerfGE 142, 234, Rz. 31.

68. BGE 141 IV 108 E. 5.8.

69. Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 6.

70. Graf, Praxishandbuch, Rz. 554; vgl. LG München 37 O 17964/17 vom 31.1.2018 (zur urheberrechtlichen öffentlichen Zugänglichmachung); ferner zum Begriff der «Öffentlichkeit» bspw. BGE 130 IV 111 E. 3.1 (zu Art. 261<sup>bis</sup> StGB).

71. Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 6; Bär, S. 58.

72. Analog zur Rechtsprechung über durch Private rechtswidrig erlangte Beweismittel: BGE 146 IV 226 E. 2.

## B. Rechtsnatur: Qualifikation als Grundrechtseingriff?

- 32 Fraglich ist, inwieweit das Sammeln und Auswerten öffentlich zugänglicher Daten als Grundrechtseingriff und in der Konsequenz als Zwangsmassnahme i.S.v. Art. 196 StPO zu qualifizieren sind. Die Beantwortung dieser Frage ist zentral, zum einen um festzulegen, inwieweit auch auf öffentliche Daten, die in einem Drittstaat liegen, zugegriffen werden kann, und zum anderen weil bejahendenfalls eine hinreichend konkrete gesetzliche Grundlage bestehen muss (Art. 197 Abs. 1 lit. a StPO). Letzteres ist durch Art. 95 StPO (Beschaffung von Personendaten) allerdings bereits verwirklicht.<sup>73</sup>
- 33 Als Zwangsmassnahmen werden gemäss Art. 196 StPO Verfahrenshandlungen der Strafbehörden definiert, die u.a. dazu dienen, Beweise zu sichern, soweit sie in die Grundrechte der betroffenen Personen eingreifen. Art. 196 StPO setzt damit (im Widerspruch zum Wortlaut [«Zwangs»-Massnahme]) nicht notwendigerweise Zwang voraus, sondern stützt vielmehr entscheidend darauf ab, ob die Massnahme als Eingriff in die Grundrechte der betroffenen Personen zu werten ist.<sup>74</sup> Im Vordergrund steht dabei, neben dem Recht auf persönliche Freiheit und der Eigentumsgarantie, der Schutz der Privatsphäre nach Art. 13 BV und Art. 8 EMRK<sup>75</sup> bzw. konkreter das darin verankerte **Recht auf informationelle Selbstbestimmung**.<sup>76</sup> Als Eingriffe in dieses verfassungsmässige Recht kommen u.a. die Telefonüberwachung,<sup>77</sup> die Erhebung von Fernmeldedaten,<sup>78</sup> die Abnahme und Analyse von DNA und Fingerabdrücken,<sup>79</sup> die Observation (inkl. systematischer Überwachung durch Privatdetektive),<sup>80</sup> Videoaufnahmen durch die Polizei,<sup>81</sup> das Einsetzen eines IMSI-Catchers<sup>82</sup> und die passwortgeschützte Onlinerecherche resp. Sicherstellung von Chat-Nachrichten<sup>83</sup> in Betracht.
- 34 Zur automatisierten Verkehrsüberwachung hielt das Bundesgericht einmal fest, der Schutz der Privatsphäre beschränke sich nicht auf private Räumlichkeiten, sondern erstrecke sich auch auf den privatöffentlichen Bereich; von Art. 13 BV erfasst würden auch Lebenssachverhalte mit persönlichem Gehalt, die sich im öffentlichen Raum ereignen.<sup>84</sup> Mit dem deutschen Bundesverfassungsgericht kann der Zugriff auf «im Internet verfügbare Kommunikationsinhalte und Informationen, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richtet», indes richtigerweise noch nicht als Eingriff in das Recht auf informationelle Selbstbestimmung charakterisiert werden.<sup>85</sup> Wohl sind Inhalte, die auf Blogs, Foren oder in sozialen Medien einem bestimmten Nutzerkreis vorbehalten und damit an durch persönliche Beziehungen oder besonderes Vertrauen geprägtes Umfeld richten, der Privatsphäre i.S.v. Art. 13 Abs. 1 BV zuzurechnen und deren Abgriff als Grundrechtseingriff zu werten. Daten, die für jeden Internetnutzer voraussetzungslos zugänglich oder für alle auf einer Plattform registrierte Nutzer (unabhängig eines Näheverhältnisses zur informationspreisgebenden Person) einsehbar sind, können derweil unbeschadet des Inhalts nicht

---

73. Vgl. Cartner/Schweingruber, S. 993 f. In anderen Bundesgesetzen ist die Erhebung von Personendaten «aus öffentlichen Quellen» vereinzelt ausdrücklich geregelt, bspw. Art. 18 Abs. 3 des Bundesgesetzes vom 25.9.2020 über Vorläuferstoffe für explosionsfähige Stoffe («VSG»; SR 941.42); Art. 13 f. NDG.

74. BGE 145 IV 42 E. 3.

75. SK-Zimmerlin, Art. 196 StPO N. 2; BSK-Weber, Art. 196 StPO N. 8.

76. BGE 145 IV 42 E. 4.2, m.w.H.

77. BGE 109 Ia 273 E. 4a.

78. BGer 1B\_26/2016 vom 29.11.2016 E. 4.2.

79. Vgl. EGMR, S. und Marper gegen das Vereinigte Königreich, Nr. 30562/04 und 30566/04, 4.12.2008 (Unzulässigkeit der unbegrenzten Aufbewahrung solcher Daten von verdächtigen, aber nicht verurteilten Personen).

80. BGE 143 IV 387 E. 4.2.

81. BGE 145 IV 42 E. 4.

82. BGer 1B\_252/2017 vom 21.2.2018 E. 6.6.

83. BGer 1B\_29/2017 vom 24.5.2017 E. 7.6.

84. BGE 146 I 11 E. 3.1.1.

mehr als «privat» eingestuft werden.<sup>86</sup> An Informationen, die bereits öffentlich bekannt sind, besteht richtigerweise kein schützenswertes Interesse mehr (mit Ausnahme des datenschutzrechtlichen «Rechts auf Vergessen»).

- 35 Ist der Zugriff auf allgemein zugängliche Daten keine Zwangsmassnahme, bedeutet das zugleich, dass Art. 32 lit. a CCC nicht konstitutiver, sondern rein **deklaratorischer Natur** ist.<sup>87</sup> Wenn der Zugriff auf öffentliche Quellen mangels eigentlicher Zwangsausübung die Staatensouveränität nicht verletzt, bedarf es auch keiner zwischenstaatlichen Vereinbarung. Demgemäss können auch **öffentlich zugängliche Daten aus Drittstaaten**, die die CCC nicht ratifiziert haben, problemlos abgegriffen werden. Letzteres wird zuweilen auch damit begründet, dass es sich beim transnationalen Zugriff auf «open source data» um Völkergewohnheitsrecht handelt, als derart unbestritten gelten solche Ermittlungshandlungen.<sup>88</sup>
- 36 Selbst wenn dem nicht in dieser Absolutheit gefolgt würde, könnte in jedem Fall das Abgreifen **freiwillig offengelegter Daten** – etwa von Kommunikationsinhalten in den sozialen Medien – nicht als Grundrechtseingriff charakterisiert werden. Denn durch die bewusste Entscheidung, persönliche Informationen zu teilen, verzichten die betroffenen Personen in Bezug auf diese spezifischen Daten auf ihre informationelle Selbstbestimmung, oder in anderen Worten: durch die Freigabe in den öffentlichen Bereich haben sie ihre informationelle Selbstbestimmung gerade ausgeübt. Dasselbe gilt für die durch eigene Inputs hinterlassene öffentliche Datenspur, etwa mit Bitcoin getätigten Transaktionen, die auf der öffentlichen Blockchain nachverfolgbar sind. Sodann sind Daten, die nicht unmittelbar einer bestimmten Person zugerechnet werden können, unter keinem grundrechtlichen Titel schützenswert. Dazu gehört etwa die Verwendung von «Google Earth» oder technischer Daten, die ein Webserver preisgibt. Folglich fällt maximal das Abgreifen und Auswerten nicht freiwillig offenbarter personenbezogener Informationen als Zwangsmassnahme in Betracht; hier könnte berechtigterweise geltend gemacht werden, die Betroffenen hätten keine Kontrolle darüber, welche Informationen über sie im Internet verfügbar sind. Allerdings wäre auch dann zu berücksichtigen, dass OSINT ein vergleichsweise wenig invasiver und damit verhältnismässiger Eingriff ist, da er sich auf Informationen beschränkt, die ohne spezielle Zugangsbeschränkung von jedermann abgerufen werden können.<sup>89</sup>

### C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht

- 37 Der Abgriff von «Open Source»-Daten ist zulässig für beliebige Straftaten (Verbrechen, Vergehen oder Übertretungen), soweit die Erhebung von in elektronischer Form vorhandenem Beweismaterial für deren Verfolgung nützlich ist (vgl. Art. 25 Abs. 1 und Art. 14 Abs. 2 lit. c CCC). Soweit das kantonale Polizeirecht es erlaubt, kann auch im Rahmen präventiver polizeilicher Tätigkeit auf öffentliche Informationen zugegriffen werden.

85. BVerfGE 142, 234, Rz. 31; BVerfGE 120, 274, Rz. 308. Ein solcher kann gemäss dieser Rechtsprechung dann in Betracht fallen, «wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und dadurch einen zusätzlichen Aussagewert erhalten, aus dem sich die für das Grundrecht auf informationelle Selbstbestimmung spezifische Gefahrenlage für die Persönlichkeit des Betroffenen ergibt», (BVerfGE 120, 274, Rz. 308). Auch danach wäre jedenfalls nicht bereits der Abgriff von allgemein zugänglichen Inhalten im Sinne von Art. 32 lit. a CCC ein Grundrechtseingriff, sondern maximal deren spätere Verwendung. Art. 32 lit. a CCC regelt nur ersteres und nicht letzteres; die spätere Verwendung spielt sich dann in der nationalen Strafprozessordnung ab.

86. Cartner/Schweingruber, S. 992.

87. Burgermeister, S. 21; Dombrowski, S. 158.

88. T-CY, Transborder Access, Rz. 93; Seitz, S. 38.

89. Vgl. auch Cartner/Schweingruber, S. 993.

- 38 Aufgrund des fehlenden Grundrechtseingriffs sind «open source»-Ermittlungen nicht als Zwangsmassnahmen i.S.v. Art. 196 ff. StPO einzustufen (vgl. vorstehend, N. 32 ff.). Als Folge dessen sind weder die formellen und materiellen Vorschriften zur Durchsuchung (Art. 246 ff. StPO) noch zur Beschlagnahme (Art. 263 StPO) anwendbar. «OSINF» bzw. «OSINT» gilt vielmehr als eine gestützt auf Art. 95 StPO zulässige Erhebung von Beweismitteln i.S.v. Art. 139 Abs. 1 StPO.<sup>90</sup>
- 39 Das Einloggen durch Angehörige von Strafverfolgungsbehörden unter einer falschen Identität in den sozialen Medien oder in einem Chat, um Zugang zu den dort veröffentlichten Inhalten erhält, ist nicht als **verdeckte Fahndung** (Art. 298a StPO) oder verdeckte Ermittlung (Art. 285a StPO) einzustufen, da hier kein direkter Kontakt mit der Zielperson aufgebaut wird.<sup>91</sup> Anders sähe es aus, wenn der Ermittler der Zielperson aktiv eine Freundschaftsanfrage o. dgl. schicken würde, um dessen (privaten) Beiträge ebenfalls zur Kenntnis nehmen zu können, oder wenn er sich durch Anlegen einer Legende Zutritt zu einem nicht allgemein zugänglichen Chat oder Forum erschleicht.
- 40 Der **Beweiswert** von öffentlich verfügbaren Daten gilt es im Rahmen der freien Beweiswürdigung (Art. 10 Abs. 2 StPO) im Detail zu prüfen.<sup>92</sup> Dabei spielen diverse Überlegungen eine Rolle, vorab die Herkunft des Beweises, dessen Authentizität und Verlässlichkeit,<sup>93</sup> das Verhältnis dessen Verfassers zu den Verfahrensparteien, vor allem aber auch, ob die Quelle anonym oder bekannt ist, zumal die Zweifel bei unbekannter Herkunft gross und Daten relativ einfach manipulierbar sind.<sup>94</sup> Bedeutend ist sodann auch, dass die Daten nach dem aktuellen Stand der Technik forensisch gesichert werden, da sich aus Metadaten allfällige Rückschlüsse auf den Beweiswert ziehen lassen; das blosses Anfertigen von Screenshots wird hierfür kaum genügen.

### III. ZUGRIFF AUF ANDERWEITIGE, IN EINEM ANDEREN VERTRAGSSTAAT GESPEICHERTE DATEN (LIT. B)

#### A. Rechtmässige und freiwillige Einwilligung der Person, die rechtmässig befugt ist, die Daten weiterzugeben

##### 1. Weitergabeberechtigung

- 41 Art. 32 CCC regelt lediglich die völkerrechtliche Zulässigkeit des Datenzugriffs; «die innerstaatlichen Vorschriften, an denen die Datenübermittlung zu messen ist, nach denen also zu entscheiden ist, ob die Zustimmung zu der Übermittlung rechtmässig durch eine dazu befugte Person erteilt worden ist, werden von dem Übereinkommen nicht berührt.»<sup>95</sup> Der Europarat hat darauf verzichtet, den Begriff der Weitergabeberechtigung in der CCC näher zu definieren. Im Explanatory Report wird dazu ausgeführt, wer sein Einverständnis erklären könne, «may vary depending on the circumstances, the nature of the person and the applicable law concerned.»<sup>96</sup>

---

90. Cartner/Schweingruber, S. 996 f.

91. SK-Hansjakob/Pajarola, Art. 298a StPO N. 4; Cartner/Schweingruber, S. 996.

92. Vgl. bspw. Sampson, S. 55 ff.

93. Entsprechend wurde vor dem Internationalen Strafgerichtshof im Verfahren gegen Jean-Pierre Bemba Gombo etwa ein NGO-Report zugelassen: «The Majority notes that the UN Report is publicly available from official UN sources. In addition, the Majority is satisfied, based on a review of the document, that it provides sufficient details of its sources of information and methodology» (ICC, Decision on the admission into evidence of items deferred in the Chamber's «Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute» [ICC-01/05-01/08-2299] vom 27.6.2013, Rz. 13).

94. Etwa durch Setzen tatsächenswidriger Geotags, Photoshop, Deepfake, IP-Spoofing, Verwendung weiterer Anonymisierungstechniken durch den Absender bzw. Ersteller, etc.

95. BVerfGE 142, 234, Rz. 39.

96. Explanatory Report, Rz. 294.

- 42 Die Frage, wer «rechtmässig befugt ist, die Daten [...] weiterzugeben», bestimmt sich nach dem **inländischen Recht des ersuchenden Staates**, also demjenigen, in dem die Ermittlungen stattfinden.<sup>97</sup> Dies erscheint auch deshalb sinnvoll, weil eine genaue Lokalisierung der Daten vor dem Zugriff oft nicht oder nicht ohne grossen Aufwand möglich ist.<sup>98</sup> Es wäre zudem nicht praktikabel und mit dem Beschleunigungsgedanken der CCC unvereinbar, von den schweizerischen Behörden die Prüfung der Berechtigungssituation für jeden Vertragsstaat separat zu verlangen, bevor sie eine Datensicherung vornehmen dürften.
- 43 Erforderlich ist die **Berechtigung, Daten weiterzugeben**. Notwendig, aber auch hinreichend ist die Einwilligung einer Person, die rechtmässig befugt ist, diese den Strafverfolgungsbehörden zu offenbaren.<sup>99</sup> Die Berechtigung kann **gesetzlicher oder obligatorischer Natur** sein.
- 44 Entgegen der Botschaft<sup>100</sup> ist es keine zusätzliche Voraussetzung, dass die Zustimmung «einer Person im Inland» vorliegen muss; Art. 32 lit. b CCC kennt kein derartiges einschränkendes Kriterium, das zudem dem Sinn und Zweck der Konvention zuwiderlaufen würde.<sup>101</sup>
- 45 Der Explanatory Report und die Botschaft nennen als einwilligungsfähig beispielhaft Personen, die ihre E-Mails bei einem Service-Provider in einem anderen Staat oder anderweitige Daten im Ausland gespeichert haben.<sup>102</sup> In der Literatur wird bei auf Cloud-Servern gespeicherten Daten der den Speicherplatz mietende Kunde als berechtigte Person bezeichnet,<sup>103</sup> bei Daten über Finanztransaktionen die Bank,<sup>104</sup> für den geschäftlichen E-Mail-Account der Arbeitgeber<sup>105</sup> und bei juristischen Personen die dafür intern als zuständig erklärten Personen, bei Fehlen ebensolcher innerbetrieblicher Regelungen der Verwaltungsrat (AG) bzw. die Geschäftsführung (GmbH); Administratoren oder sonstigen Zugangsberechtigten dürfte diese Berechtigung regelmässig abgehen.<sup>106</sup>
- 46 Ein im Explanatory Report nicht abschliessend erörterter Aspekt beschlägt die Frage, ob die Einwilligung stets durch die betroffenen Personen erteilt werden muss (**Datenherrinnen**) oder die Ermächtigung anderer Stellen, die die personenbezogenen Daten bearbeiten (allen voran der Internet-Service-Provider als **Datengewahrsamsinhaber**), ausreicht.<sup>107</sup> Eine Ausweitung auf Internet-Service-Provider wird kritisch beäugt, denn diese würden bloss das Datengewahrsam ausüben und befänden sich daher nicht in der Position, um rechtsgültig einzuwilligen zu können.<sup>108</sup>

97. T-CY, Transborder Access, Rz. 108; Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 8; a.M. BBl 2010 4738: «Die rechtmässige Befugnis der Person, über die Daten zu verfügen und sie an eine staatliche Stelle weiterzuleiten, beurteilt sich primär nach dem nationalen Recht des Staates, in welchem die betreffende Person handelt», bestätigt in BGE 141 IV 108 E. 5.10.

98. Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 8.

99. BBl 2010 4738.

100. So aber BBl 2010 4738.

101. BGE 141 IV 108 E. 5.9-5.10; Schweingruber, Rz. 13 f.; vgl. auch OGer ZH SB140420 vom 2.5.2015 E. 3.3.3; vgl. T-CY Guidance Note # 3, S. 7 f.

102. Explanatory Report, Rz. 294; BBl 2010 4738; s.a. Heimgartner, Internationale Dimension, S. 146.

103. Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 9; Brodowski, S. 478.

104. Brodowski, S. 478.

105. Graf, Strafverfolgung 2.0, Rz. 46.

106. Schomberg/Lagodny-Trautmann, Art. 32 ZP-EuCybercrimeÜbK N. 9.

107. Zu weit ginge es freilich, wie in Estland den inländischen Untersuchungsrichter als Person zu qualifizieren, der die rechtmässige Befugnis («lawful authority») zukommt, im Rahmen eines innerstaatlich strafprozessual korrekten Rahmens auf ausländische Daten zuzugreifen, vgl. dazu Osula, S. 353 und S. 363.

108. T-CY Guidance Note # 3, S. 7; differenzierend noch T-CY, Transborder Access, Rz. 113, wonach gestützt auf Art. 32 lit. b CCC einzig Inhaltsdaten betroffener Personen durch die Internet-Service-Provider nicht freigegeben werden dürften; siehe sodann auch BBl 2010 4738: «Handelt es sich um vertrauliches Datenmaterial einer Drittperson, zu deren Offenlegung diese keine Zustimmung erteilt hat, liegt keine Befugnis i.S.v. Art. 32 CCC vor.»

- 47 Die Frage der Weitergabeberechtigung ist im breiteren Kontext zu betrachten, dass in der Schweiz nach geltender Rechtslage kein eigentumsähnliches Recht an Daten existiert: Das Eigentumsrecht nach Art. 641 ZGB erstreckt sich einzig auf die «Sache», worunter die Lehre «ein körperlicher, von anderen abgegrenzter Gegenstand, der tatsächlicher und rechtlicher Beherrschung zugänglich ist»,<sup>109</sup> versteht. Da Daten immaterielle Güter darstellen, kann an ihnen (wohl aber an Datenverarbeitungsanlagen oder Datenträgern) kein Eigentum i.S.v. Art. 641 ZGB begründet werden.<sup>110</sup> Auch das Urheberrecht erstreckt sich einzig auf geistige Schöpfungen mit individuellem Charakter in Datenform und ist nur ausnahmsweise anwendbar.<sup>111</sup> Immerhin ist im Datenschutzrecht ein Zugangsrecht zu Daten anerkannt, jedenfalls in Bezug auf Personendaten,<sup>112</sup> hinsichtlich derer in Art. 25 des Bundesgesetzes über den Datenschutz vom 25.9.2020 («DSG», SR 235.1) ein Auskunftsrecht normiert ist. Art. 28 DSG räumt den betroffenen Personen bei Vorliegen bestimmter Voraussetzungen zudem das Recht auf Datenherausgabe und -übertragung von Personendaten ein (Datenportabilität), sofern sie diese Daten den Verantwortlichen bekanntgegeben haben. Ferner dürfen Personendaten «nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist» (Art. 6 Abs. 3 DSG). Die Herausgabe von Personendaten an die Strafverfolgungsbehörden stellt dabei eine Form der Datenbearbeitung dar (vgl. Art. 5 lit. d DSG). Will heissen: Die berechtigte Person kann in die Weitergabe durch die datenbearbeitende Person einwilligen.
- 48 Die Schweiz, im Einklang mit anderen Vertragsstaaten, lässt deshalb die **Einwilligung von Internet-Service-Provider** als Folge ihres privatrechtlichen Verhältnisses mit der betroffenen Person genügen, wenn die Diensteanbieter sich in ihren Allgemeinen Nutzungsbedingungen bzw. Datenverwendungsrichtlinien ein Weiterleitungsrecht an ausländische Strafverfolgungsbehörden ausbedungen haben.<sup>113</sup> Die Mehrheit der Internet-Service-Provider sieht in ihren User Agreements vor, dass Daten nicht nur bei Vorliegen eines gültigen Gerichtsbeschlusses, sondern auch auf einfache Anfrage durch Strafverfolgungsbehörden hin herausgegeben werden können bzw. dass die Provider mit Strafverfolgungsbehörden kooperieren.<sup>114</sup> Eine Weitergabe ist in diesen Fällen rechtskonform.

## 2. Einwilligung

- 49 Dass eine betroffene ausländische Providerfirma in beschriebenem Sinne grundsätzlich berechtigt wäre, ihre Zustimmung zu einer direkten Datenherausgabe zu erklären, reicht (nach dem klaren Wortlaut von Art. 32 lit. b CCC) für einen grenzübergreifenden Zugriff noch nicht aus: Vielmehr ist weiter zu prüfen, ob die anfragende Strafverfolgungsbehörde eine rechtswirksame «rechtmässige und freiwillige Zustimmung» eingeholt hat.<sup>115</sup>
- 50 **Einwilligungsfähig** ist, wie besehen, die juristische oder urteilsfähige<sup>116</sup> natürliche Person, die aufgrund gesetzlicher oder obligatorischer Berechtigung über die Daten verfügen und Dritten Zugriff darauf gewähren darf (vgl. auch vorstehend, N. 43 ff.). Bei mehreren weitergabeberechtigten Personen

---

109. Stellvertretend BSK-Wolf/Wiegand, Vor Art. 641 ff. ZGB N. 6.

110. Schmid/Schmidt/Zech, S. 627; Hürlimann/Zech, Rz. 8; BSK-Wolf/Wiegand, Vor Art. 641 ff. ZGB N. 19c-d; Hess-Odoni, Rz. 7 ff.; Fröhlich-Bleuler, Rz. 13; a.M. indes Eckert, S. 245 ff.; Kohler, S. 412.

111. Schmid/Schmidt/Zech, S. 627.

112. Für reine Sachdaten besteht indes kein derartiges Herausgabe- bzw. Auskunftsrecht, Schmid/Schmidt/Zech, S. 627.

113. BGE 141 IV 108 E. 5.10; Schweingruber, Rz. 20; Graf, Strafverfolgung 2.0, Rz. 46; Roth, Rz. 36 ff.; vgl. ferner auch Seitz, S. 44; Karagiannis/Vergidis, S. 11; Walden, S. 8 f.; Osula, S. 353 f.

114. Walden, S. 8 f. Die Allgemeinen Nutzungsbedingungen von Google etwa stellen die Weitergabe von personenbezogenen Daten an Strafverfolgungsbehörden in das pflichtgemässe Ermessen von Google, OGer ZH SB140420 vom 2.5.2015 E. 3.3.4; zu Instagram OGer SO STBER.2022.64 vom 8.3.2023 E. 4.2.2.

115. BGE 141 IV 108 E. 5.10.

116. T-CY Guidance Note # 3, S. 6.

ist die Einwilligung einer Person ausreichend. Liegt beispielsweise die Ermächtigung der Kontoinhaberin vor, bedarf es seitens der ausländischen Providerfirma keiner zusätzlichen Zustimmung.<sup>117</sup> Umgekehrt reicht es aus, wenn der ausländische Provider, gestützt auf eine entsprechende Ermächtigung des Kunden in den Allgemeinen Nutzungsbedingungen, die Daten herausgibt (zur Einwilligung durch Internet-Service-Provider vgl. vorstehend, N. 46 ff.).<sup>118</sup>

- 51 Die Einwilligung kann nach allgemeinen strafprozessualen Grundsätzen entweder **ausdrücklich** erklärt werden (wofür kein Formerfordernis gilt) **oder konkludent** erfolgen.<sup>119</sup> Letzteres liegt namentlich dann vor, wenn die von den Strafverfolgungsbehörden angefragte Person – bspw. ein Diensteanbieter oder der Inhaber des betreffenden Kontos – die Daten auf Anfrage hin herausgibt.<sup>120</sup>
- 52 Das bedeutet zugleich, dass entsprechende «**Information Requests**» ins **Ausland** gestellt werden dürfen, und zwar ohne dass dies als unzulässige Handlung in einem fremden Staat zu qualifizieren wäre. Direkte Anfragen an ausländische Provider haben sich in der Praxis denn auch international zu einem Standard entwickelt, die entweder über von den Providern eigens betriebene Strafverfolgungsportale eingegeben oder, im Falle von anderen (kleineren) Providern, auch auf dem Polizeiweg (via Interpol) zugestellt werden können. Verschiedene Staatsverträge erlauben eine direkte Zustellung amtlicher Dokumente ins Ausland zudem mindestens dem Grundsatz nach, allen voran Art. 52 Abs. 1 des Schengener Durchführungsübereinkommens vom 19.6.1990 («SDÜ»). Dieser sieht aber vor, dass jeder Staat eine Erklärung darüber abgeben kann bzw. abzugeben hat, welche Urkunden an Personen in seinem Staatsgebiet übersendet werden dürfen.<sup>121</sup> Es gilt hier folglich prinzipiell für jeden Vertragsstaat gesondert zu prüfen, ob und bejahendenfalls inwieweit eine direkte Zustellung erlaubt ist. Sofern die Angeschriebenen darauf hingewiesen werden, dass jegliche Mitwirkung freiwillig ist und an eine verweigte Mitwirkung keine direkten negativen Folgen geknüpft sind, ist allerdings nicht ersichtlich, inwieweit darin überhaupt eine Verletzung fremder Gebietshoheit und damit ein Anwendungsfall von Art. 52 Abs. 1 SDÜ erblickt werden kann – es handelt sich um blossen Einladungen ohne Zwangsandrohung und ohne an eine allfällige Kooperationsverweigerung geknüpfte negativen Folgen.<sup>122</sup> Es würde denn auch wenig Sinn machen, wenn durch die Ausnahmeregelung des Art. 32 lit. b CCC eine Effizienzsteigerung zum beschwerlichen formellen Rechtshilfeweg eingeführt werden sollte, dies aber zeitgleich durch das Erfordernis torpediert würde, auf ebendiesem formellen Rechtshilfeweg die Bereitschaft der betroffenen Personen zur freiwilligen Mitwirkung abklären zu müssen. Art. 32 lit. b CCC geht insoweit Art. 52 SDÜ vor.<sup>123</sup>
- 53 Die Einwilligung muss **freiwillig** erfolgen; die betroffene Person darf nicht getäuscht oder durch Zwang zur Datenherausgabe gebracht werden.<sup>124</sup> Wohl besteht oft eine indirekte Drucksituation, weil die Staatsanwaltschaft im Weigerungsfall die rechtshilfeweise Sicherstellung und Überstellung der betreffenden Daten verlangen dürfte. Das reicht indes für eine Beeinträchtigung der Willensbildung

117. Forster, Fn. 14.

118. A.M. wohl BBl 2010 4738. Die Kontoinhaberin wird durch den Service-Provider regelmässig nicht über die Datenlieferung informiert; bei Kollusionsgefahr können die Strafverfolgungsbehörden den Diensteanbieter auch um Aufschub einer solchen Auskunft ersuchen.

119. A.M. indes T-CY Guidance Note # 3, S. 7.

120. BGE 141 IV 108 E. 5.10; OGer ZH SB140420 vom 2.5.2015 E. 3.4; Schweingruber, Rz. 20.

121. Vgl. etwa Anlage III zu Anhang II der Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten der Bundesrepublik Deutschland: «Liste der Urkunden, die gemäss Artikel 52 Absatz 1 des Schengener Durchführungsabkommens bzw. Artikel 5 Absatz 1 des EU-Rechtshilfeübereinkommens vom 29. Mai 2000 unmittelbar durch die Post zugestellt werden können», abrufbar unter [https://www.bmj.de/DE/service/rivast/rivast\\_info/RiVaSt\\_allg\\_Info.html](https://www.bmj.de/DE/service/rivast/rivast_info/RiVaSt_allg_Info.html), besucht am 17.10.2023.

122. AK-Simon, Art. 299 StGB N. 6; vgl. BGE 140 IV 86 E. 2.4.

123. Differenzierend indes T-CY Guidance Note # 3, S. 8; T-CY, Transborder Access, Rz. 118.

124. T-CY Guidance Note # 3, S. 6.

noch nicht aus. Dasselbe gilt bspw. im Falle einer Haftsituation, wo sich die beschuldigte Person aufgrund der Umstände subjektiv dazu gezwungen sehen könnte, zu kooperieren und die im Ausland gespeicherten Daten zur Verfügung zu stellen, um möglichst schnell aus der Haft entlassen zu werden. Doch auch eine derartige allgemein gehaltene Drucksituation hindert sie nicht an der Abgabe einer rechtskonformen Einwilligung. Untersagt ist dagegen freilich die konkrete Androhung allfälliger weiterer Nachteile. Entsprechend kann auch eine in der Schweiz domizilierte Person nicht unter Zwangsandrohung dazu verpflichtet werden, im Ausland gespeicherte Daten, auf die sie Zugriff hat, zu produzieren.<sup>125</sup> Freilich kann sie aber mittels Editionsverfügung (Art. 265 StPO) darum ersucht werden.

- 54 Schliesslich ist die Einwilligung jederzeit widerrufbar, wobei der **Widerruf** bloss ex nunc gilt. Ein Widerruf nach erfolgter Datensicherung ist daher unbeachtlich.

## B. Folge einer rechtsgültigen Einwilligung

- 55 Gibt die verfügungsberechtigte Person ihre Login-Daten zu ausländischen abgeleiteten Internetdiensten freiwillig preis resp. willigt in die Online-Durchsuchung ein, steht es den Strafverfolgungsbehörden in Anwendung von Art. 32 lit. b CCC offen, direkt durch Nutzung der Zugangsdaten auf die Informationen zuzugreifen und diese sicherzustellen.<sup>126</sup> Auch steht es jeder Privatperson frei, die eigenen, bei einem ausländischen Provider gespeicherten Daten (etwa E-Mails oder Chat-Nachrichten) den Strafverfolgungsbehörden in Kopie zur Verfügung zu stellen.<sup>127</sup> Ebenfalls zulässig ist es, wenn die Strafverfolgungsbehörde einen im Ausland domizilierten Internet-Service-Provider direkt um Herausgabe von Daten ersucht (vgl. vorstehend, N. 48, 51 f.).

## C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht

- 56 Der Zugriff auf nicht-öffentliche Daten in der Schweiz ist nicht voraussetzungslos möglich. Handelt es sich um Inhaltsdaten, so sind die Daten sicherzustellen (etwa durch eine Editionsverfügung [Art. 265 StPO] oder anlässlich einer Hausdurchsuchung [Art. 244 StPO]), zu durchsuchen (Art. 246 StPO) und anschliessend, soweit beweisrelevant, zu beschlagnahmen (Art. 263 StPO). Für Verkehrsdaten ist eine rückwirkende Randdatenerhebung (Art. 273 StPO) zu verfügen und vom Zwangsmassnahmengericht genehmigen zu lassen (Art. 274 StPO). Art. 32 lit. b CCC stellt nun keine eigenständige Beweissicherungs- oder Beweiserhebungsmassnahme dar, die die innerstaatlichen Voraussetzungen überflügeln würde. Die Bestimmung regelt einzig, dass bei Vorliegen einer rechtsgültigen Einwilligung auf ein Rechtshilfeverfahren verzichtet werden kann.<sup>128</sup> Der Datenzugriff, auch wenn er transnational erfolgt, stellt daher eine **innerstaatliche Zwangsmassnahme** dar, die den innerstaatlichen Gesetzlichkeiten zu genügen hat. Die Sicherstellung von Daten im Ausland muss damit – zusätzlich zur beschriebenen Einwilligung – als notwendige Bedingung dieselben Voraussetzungen erfüllen, wie wenn die Daten in der Schweiz gespeichert gewesen wären.<sup>129</sup> Ein «Information Request» an einen Internet-Service-Provider ist mithin als Editionsverfügung i.S.v. Art. 265 StPO zu qualifizieren.
- 57 Zunächst folgt daraus, dass grundsätzlich die **Eröffnung einer Strafuntersuchung** i.S.v. Art. 309 Abs. 1 StPO und damit ein hinreichender Tatverdacht vorausgesetzt sind, wobei ein noch nicht formell

---

125. Vgl. Seitz, S. 45.

126. T-CY Guidance Note # 3, S. 5; vgl. bspw. T-CY, Benefits, S. 10: «The accused consented, logged into his/her account and provided the authorities with the password. With regard to this case, Hungary noted, without the use of Article 32 (b), obtaining the data would only have been possible through a time-consuming legal assistance procedure.»

127. Explanatory Report, Rz. 294; T-CY Guidance Note # 3, S. 4; BBl 2010 4738.

128. Walder, S. 542.

eröffnetes Strafverfahren mit dem Datenabgriff automatisch als eröffnet gilt (Art. 309 Abs. 1 lit. b StPO). Im selbständigen polizeilichen Ermittlungsverfahren darf nicht auf Art. 32 lit. b CCC abgestützt werden. Auch Nachrichtendienste können sich nicht darauf berufen.

- 58 Die CCC dient der Erhebung von in elektronischer Form vorhandenem Beweismaterial für eine Straftat (vgl. Art. 25 Abs. 1 und Art. 14 Abs. 2 lit. c CCC).<sup>130</sup> Der **hinreichende Tatverdacht** kann sich damit grundsätzlich auf eine beliebige Straftat erstrecken, sofern mindestens der kriminologische Verdacht besteht, dass diese mit einem technischen Hilfsmittel begangen wurde. Die Deliktsschwere ist unerheblich: Der transnationale Datenzugriff steht grundsätzlich für Verbrechen, Vergehen wie auch Übertretungen offen (in Bagatellfällen mag allerdings die Verhältnismässigkeit des Datenzugriffs zur Diskussion stehen).
- 59 Für die Sicherstellung von **Inhaltsdaten** ist erforderlich, dass zu vermuten ist, dass sich darin Informationen befinden, die der Beschlagnahme unterliegen (Art. 246 StPO). Gemäss Art. 263 Abs. 1 lit. a StPO können Gegenstände einer beschuldigten Person oder einer Drittperson namentlich dann beschlagnahmt werden, wenn sie als Beweismittel gebraucht werden. Für die Sicherstellung und Durchsuchung von Aufzeichnungen genügt damit eine **potentielle Beweiserheblichkeit**, die dann gegeben ist, wenn die Daten zur Aufklärung der vorgeworfenen Straftaten «von Bedeutung sein können»<sup>131</sup> bzw. nicht «offensichtlich untauglich»<sup>132</sup> erscheinen. Die Rechtsprechung stellt daran keine hohen Anforderungen.<sup>133</sup> Die Sicherstellung und Durchsuchung muss schliesslich **verhältnismässig** (Art. 197 Abs. 1 lit. c und d StPO) und damit geeignet, erforderlich und angemessen sein. Gerade bei der Verfolgung von Übertretungen kann die Verhältnismässigkeit fraglich sein.<sup>134</sup> In formeller Hinsicht ist die Sicherstellung und Durchsuchung durch die Staatsanwaltschaft im Regelfall in einem schriftlichen Befehl zu verfügen (Art. 241 Abs. 1 StPO). Für die Erhebung von **Bestandesdaten** reicht es dagegen als einzige Voraussetzung aus, dass der Verdacht besteht, dass eine Straftat über das Internet begangen worden ist (Art. 22 Abs. 1 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18.3.2016 [«BÜPF»; SR 780.1]).
- 60 Werden die **IP-History/Logdaten** oder sonstige **Randdaten** im Ausland erhoben, stellt sich die Frage, ob die Staatsanwaltschaft diese Aufzeichnungen in eigener Kompetenz erhältlich machen darf oder ob in Anwendung von Art. 273 Abs. 2 StPO eine Genehmigung durch das Zwangsmassnahmengericht einzuholen ist. Das Bundesgericht hielt einmal fest, Art. 273 StPO ermögliche lediglich eine rückwirkende Randdatenerhebung des Fernmeldeverkehrs «gegenüber dem schweizerischen Recht unterworfenen, in der Schweiz domizilierten Fernmeldedienst-Anbieterinnen bzw. Internet-Zugangsprovidern.»<sup>135</sup> Dessen Anwendbarkeit auf internationale Sachverhalte schloss es damit aus, mit der Folge, dass für die Erhebung keine Genehmigung durch das Zwangsmassnahmengericht notwendig sein sollte; Art. 32 lit. b CCC erlaube mit anderen Worten «einen erleichterten internationalen Austausch von Randdaten.»<sup>136</sup> In einem anderen Entscheid wies das Bundesgericht ein Genehmigungsgesuch der Staatsanwaltschaft allerdings mit der Begründung ab, die Voraussetzungen von Art. 32 lit. b CCC seien vorliegend nicht erfüllt gewesen, wobei es nachschob, der direkte grenzüberschreitende Zugriff wäre vom Zwangsmassnahmengericht nach Art. 273 StPO zu bewilligen gewesen.<sup>137</sup> Mehr noch, es konstatierte in einem weiteren Urteil ausdrücklich,

129. Vgl. T-CY Guidance Note # 3, S. 7.

130. Vgl. auch T-CY Guidance Note # 3, S. 5.

131. BGE 101 IV 364 E. 2.

132. BGE 142 IV 207 E. 7.1.5.

133. Eingehend Graf, Praxishandbuch, Rz. 494 ff.

134. Zur Verhältnismässigkeit bspw. Graf, Praxishandbuch, Rz. 520 ff.

135. BGE 143 IV 270 E. 4.7; s.a. BGE 141 IV 108 E. 5.13.

136. BSK-Jean-Richard-dit-Bressel, Art. 273 StPO N. 8; so auch Walder, S. 542 f.

auch für bei ausländischen Providern abgefragte IP-Histories müsse eine Genehmigung des Zwangsmassnahmengerichts eingeholt werden und weil dies im konkreten Fall nicht erfolgt sei, seien die aus den Anfragen stammenden Erkenntnisse absolut unverwertbar.<sup>138</sup> Dass sich das Bundesgericht hier mit Art. 273 StPO beschäftigt hat, mag auf den ersten Blick nachvollziehbar erscheinen, wenn man sich die Rechtsnatur von Art. 32 lit. b CCC vergegenwärtigt, der einzig den transnationalen Zugriff völkerrechtlich für zulässig erklärt, die innerstaatlichen Vorschriften, gerade was die Kompetenz zur Datenerhebung anbelangt, dagegen nicht berührt. Allerdings ist zu berücksichtigen, dass die Vorschriften über die rückwirkende Randdatenerhebung nicht allein durch die Art der zu erhebenden Daten (Verkehrs- bzw. Randdaten) aktiviert werden, sondern die Daten müssen bei einem Fernmeldeanbieter beschafft werden bzw. durch das Fernmeldegeheimnis geschützt sein (Art. 321<sup>ter</sup> StGB und Art. 43 des Fernmeldegesetzes vom 30.4.1997 [«FMG»; SR 784.10]).<sup>139</sup> Das Fernmeldegeheimnis gilt aber (soweit hier interessierend) nur für Anbieter, die einen Internetzugang bzw. eine fernmeldetechnische Übertragung anbieten.<sup>140</sup> Internet-Service-Provider bzw. Anbieter abgeleiteter Kommunikationsdienste,<sup>141</sup> die keinen Internetzugang, sondern einzig Dienstleistungen anbieten, die über das Internet erbracht werden («Over-the-Top-Dienste»), gelten nicht als Fernmeldeanbieter.<sup>142</sup> Aus diesem Grund unterliegt weder die Sicherstellung von Randdaten bei solchen Unternehmen im Inland noch im Ausland einer Genehmigungspflicht. Vielmehr reicht auch hierfür eine Editionsverfügung zuhanden des Internet-Service-Providers aus (Art. 265 StPO). Werden folglich im Ausland gestützt auf Art. 32 lit. b CCC IP-Histories und andere Randdaten bei Nicht-Fernmeldeanbietern erhoben, ist **keine Genehmigung des Zwangsmassnahmengerichts** einzuholen.

- 61 Es stellt sich schliesslich die Frage, inwieweit die **übrigen Voraussetzungen der Rechtshilfe**, namentlich Ablehnungsgründe und die Notwendigkeit einer doppelten Strafbarkeit, auch für Art. 32 lit. b CCC gelten. Art. 25 Abs. 4 CCC sieht, unter dem 3. Titel («Allgemeine Grundsätze der Rechtshilfe»), vor, dass, soweit die CCC nicht ausdrücklich etwas anderes vorsieht, «die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen einschliesslich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann», unterliegt.<sup>143</sup> Nun erlaubt Art. 32 lit. b CCC aber einen der Rechtshilfe vorgehenden direkten Zugriff; eines «Ersuchens» an den anderen Vertragsstaat, wie es Art. 25 Abs. 4 CCC zugrunde liegt, bedarf es hier gerade nicht. Für den freiwillig eingeräumten Zugriff bedarf es folglich weder einer doppelten Strafbarkeit noch sind weitere Bedingungen einzuhalten, die sonst im Rechtshilfeverfahren gelten würden.<sup>144</sup> Diese Aufweichung rechtfertigt sich zum einen durch die Freiwilligkeit der einwilligenden Personen und zum anderen angesichts der Rechtsnatur von Art. 32 lit. b CCC, der den territorialen Arm der Strafverfolgungsbehörden verlängert, während es sich weiterhin um eine inländische Beweissicherungsmassnahme handelt. Scheitert der Versuch, die Aufzeichnungen gestützt auf Art. 32 lit. b CCC sicherzustellen, so ist freilich der ordentliche Rechtshilfeweg einzuschlagen, für welchen die entsprechenden Limitationen wieder gelten.

---

137. BGE 141 IV 108 E. 5.12.

138. BGer 6B\_656/2015 vom 16.12.2016 E. 1.4.3; vgl. die Kritik bei Hansjakob, S. 252 ff.

139. Roth, Rz. 18 f.; BSK-Jean-Richard-dit-Bressel, Art. 273 StPO N. 3; Moreillon/Parein-Reymond, Art. 273 N. 3; vgl. BGE 136 II 508 E. 3.1; siehe denn auch den bereits zitierten BGE 143 IV 270 E. 4.7, der von «Fernmeldedienst-Anbieterinnen bzw. Internet-Zugangs Providern» spricht; a.M. SK-Hansjakob/Pajarola, Art. 273 StPO N. 35 f. Aus diesem Grund gilt etwa auch die Beschlagnahme eines Mobiltelefons nicht als rückwirkende Randdatenerhebung, so BBl 2006 1250 f.

140. BGer 2C\_544/2020 vom 29.4.2021 E. 4.2.

141. Vgl. zum Begriff Art. 2 lit. c BÜPF.

142. BGer 2C\_544/2020 vom 29.4.2021 E. 4.2 und 5; vgl. auch BBl 2013 2707; Biaggini, Rz. 17.

143. Wobei dort zugleich einschränkend festgehalten wird, dass Ersuchen nicht allein deswegen abgelehnt werden können, weil sie Steuerstraftaten betreffen.

144. Kritisch Seger, S. 79.

- 62 Gegen die direkte Sicherstellung als solche oder die Provideranfrage kann sich die betroffene Person nicht wehren; immerhin steht ihr gegen die Durchsuchung der Rechtsbehelf der **Siegelung** (Art. 248 StPO) offen, soweit sie ein Beschlagnahmeverbot (Art. 264 StPO) glaubhaft machen kann. Die Siegelung bewirkt, dass die Strafverfolgungsbehörden die Aufzeichnungen einstweilen nicht durchsuchen dürfen, bis das Zwangsmassnahmengericht über die Zulässigkeit der Datenerhebung und Durchsuchung befunden hat.<sup>145</sup>

#### IV. ÜBER ART. 32 CCC HINAUSGEHENDE BEWEISSICHERUNG NACH DEM ZUGRIFFSPRINZIP<sup>146</sup>

- 63 In Friktion zum Territorialitätsprinzip, das auf den Lagerungsort der Beweismittel und damit bei Daten auf den physischen Speicherort abstützt,<sup>147</sup> erlaubt das Bundesgericht einen Zugriff selbst bei **fehlender Einwilligung**, und zwar unabhängig davon, wo die Daten im Zeitpunkt des Zugriffs gespeichert sind; entscheidend sei, dass die Daten von der Schweiz aus abgerufen werden könnten: «Wer über einen Internetzugang im Inland einen abgeleiteten Internetdienst benutzt, der von einer ausländischen Firma angeboten wird, handelt nicht im Ausland. Auch der blosse Umstand, dass die elektronischen Daten des betreffenden abgeleiteten Internetdienstes auf Servern (bzw. Cloud-Speichermedien) im Ausland verwaltet werden, lässt eine von der Schweiz aus erfolgte gesetzeskonforme Online-Recherche nicht als unzulässige Untersuchungshandlung auf ausländischem Territorium (im Sinne der dargelegten Praxis) erscheinen [...]»<sup>148</sup>
- 64 Gegenstand der Beurteilung war der Zugriff auf den Facebook-Account einer wegen qualifizierten Betäubungsmittelhandels beschuldigten Person, deren Zugangsdaten die Strafverfolgungsbehörden erhältlich gemacht hatten. Die Staatsanwaltschaft liess daraufhin das Facebook-Konto unter Verwendung der ermittelten Login-Daten sichten und beweisrelevante Chat-Nachrichten sicherstellen.<sup>149</sup> Der Speicherort dieser Daten lag damals – und liegt auch heute – nicht in der Schweiz. Das Bundesgericht hielt im zitierten Urteil fest, dass direkt auf Konten von Beschuldigten oder Dritten bei ausländischen Internetdiensten zugegriffen werden darf, wenn die allgemeinen Voraussetzungen einer Durchsuchung nach schweizerischer StPO<sup>150</sup> erfüllt sind und die Ermittler «von in der Schweiz befindlichen Computern, Servern und IT-Infrastrukturen aus»<sup>151</sup> agieren, mithin physisch in der Schweiz verbleiben.
- 65 Die Praxis hat diese Rechtsprechung dankend aufgenommen. Sie ist nicht nur auf Facebook anwendbar, sondern auf eine Vielzahl von in- und ausländischen Diensten wie Host-Provider, Kommunikationsdienste, Cloud-Services, Anbieter von Datenoutsourcing, Chat-Foren, Plattformen zum Austausch von Dokumenten, Shopping-Portale und E-Mail-Dienst-Anbieter. Auch Kryptovermögen, das in einer Hot Wallet gehalten wird, kann in Anwendung dieser Rechtsprechung

145. Eingehend zu dieser Thematik Graf, Praxishandbuch, passim.

146. Die Ausführungen dieses Kapitels finden sich bereits in Graf, Strafverfolgung 2.0, Rz. 26 ff.

147. Siehe insbesondere Art. 31 («die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der ersuchten Vertragspartei befindet») und Art. 32 lit. b CCC («gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden»).

148. BGE 143 IV 270 E. 7.10; vgl. sodann auch (indes nicht derart weitgehend) Explanatory Memorandum, Rz. 187: «In the case where the data is shown on a terminal screen or is already in the computer memory without any manipulation of the computer by the investigating authority, the data is in fact directly and immediately accessible at the place where the search is taking place because it is present at the premises at this time.»

149. BGE 143 IV 270 Sachverhalt A.

150. I.e. ein Durchsuchungsbefehl oder Gefahr in Verzug (Art. 241 StPO), ein hinreichender Tatverdacht (Art. 197 Abs. 1 lit. b StPO), die Verhältnismässigkeit (Art. 197 Abs. 1 lit. c und d StPO) sowie die Vermutung, dass sich in den Aufzeichnungen Informationen befinden, die der Beschlagnahme unterliegen (Art. 246 StPO).

151. BGE 143 IV 270 E. 7.10.

sichergestellt (d.h. üblicherweise auf ein Wallet der Strafverfolgungsbehörde transferiert) werden. Die bundesgerichtliche Rechtsprechung gewinnt auch immer mehr an Bedeutung. Der allgemeine Trend für elektronische Geräte lautet: Weg von individuellem Speicher hin zur Sicherung in der Cloud. Gerade Mobiltelefone werden heute von Nutzern für verschiedene Services oft nur noch als «Schlüssel» verwendet, wobei die betreffenden Daten nicht mehr auf dem physischen Gerät gespeichert sind. Wird entsprechend ein Mobiltelefon oder ein Tablet anlässlich einer Hausdurchsuchung oder einer polizeilichen Anhaltung sichergestellt und stellt sich dabei heraus, dass die Daten nicht auf dem Gerät, sondern in der Cloud gespeichert sind, oder finden sich Apps von Kommunikationsdiensten oder Web-E-Mail-Anbietern auf dem Gerät, können gestützt auf die bundesgerichtliche Rechtsprechung all diese Daten sichergestellt werden. Erleichtert wird dieses Vorgehen in der Praxis dadurch, dass Nutzerinnen und Nutzer aus Bequemlichkeitsgründen ihre Login-Daten zu Internetdiensten oft im Passwortmanager oder in einem Internet-Browser abspeichern oder aber für verschiedene Dienste dasselbe Passwort verwenden. Auch anlässlich von Hausdurchsuchungen bei Unternehmen trifft man zunehmend an, dass diese ihre Daten nicht mehr am Sitz bzw. Ort der Geschäftsführung selber hosten bzw. gespeichert haben, sondern dass sie die Datenverarbeitung und -aufbewahrung an externe Dienstleister outgesourced haben. In derartigen Situationen hilft der zitierte Bundesgerichtsentscheid ebenfalls, da er die Datensicherung auch in solchen Fällen erlaubt.

- 66 Implizit hat sich das Bundesgericht im zitierten Entscheid auf das sog. **«Zugriffsprinzip»** berufen.<sup>152</sup> Danach wird bei Computerdaten nicht auf den Standort des Datenträgers, auf dem die Informationen gespeichert sind, abgestützt, sondern darauf, wer von wo aus Zugriff auf die verfahrensrelevanten Daten hat. Die Herrschaft über die Daten liege bei derjenigen Person, die über die Zugriffsberechtigung verfüge, und nicht bei derjenigen, die im physischen Besitze des Datenträgers sei.<sup>153</sup> Das führen einzelne Autoren als Begründung an, weshalb in der Durchsuchung und Beschlagnahme von im Ausland gespeicherten Daten durch schweizerische Behörden in der Schweiz keine Souveränitätsverletzung zu sehen sei.<sup>154</sup> Die Zulässigkeit des Online-Zugriffs soll danach mit anderen Worten allein von der Rechtmässigkeit der inländischen Ermittlungshandlung abhängen.<sup>155</sup>
- 67 Wird nun aber auf nicht öffentlich zugängliche, insbesondere passwort- oder durch sonstige Barrieren geschützte ausländische Quellen zugegriffen, wirkt sich das mit hoher Intensität auf das ausländische («digitale») Hoheitsgebiet aus. Verschiedentlich wird daher der Zugriff durch Ermittlungsbehörden auf Daten im Ausland als **Eingriff in die Souveränität des betreffenden Staates** gewertet;<sup>156</sup> an derartige Beweismittel könne man nur über die internationale Rechtshilfe bzw. bloss dann auf direktem Weg gelangen, falls dies in internationalen Übereinkommen explizit so vorgesehen sei.<sup>157</sup> In der Tat ändert das Zugriffsprinzip nichts an den Auswirkungen staatlicher Online-Zugriffe auf die fremde Souveränität, wo der eigentliche Erfolg der Massnahme eintritt.<sup>158</sup> Zwar dürfte das fehlende physische Tätigwerden von Beamten auf fremdem Staatsgebiet die durch Art. 299 StGB gezogenen Grenzen noch nicht überschreiten. Sie treten jedoch, was ihre Eingriffsintensität betrifft, keineswegs hinter die äquivalenten physischen Ermittlungstätigkeiten (die Durchsuchung des Speicherträgers im

152. Vgl. Bangerter, S. 281 f.; Burgermeister, S. 22.

153. So Burgermeister, S. 22; de lege ferenda auch angetönt bei Bottinelli, S. 1333.

154. Bangerter, S. 281 f.; Burgermeister, S. 22; im Ansatz Schmid, S. 109; vgl. zu dieser Thematik (auf europäischer Ebene) sodann Grave/Barth, S. 373.

155. So auch Wicker, S. 768.

156. Dombrowski, S. 159; Heimgartner, Strafprozessuale Beschlagnahme, S. 93; Ryser, S. 575 ff.; ferner Aepli, S. 130 f.; Heimgartner, Internationale Dimension, S. 136.

157. Abo Youssef, S. 105 f.; Bär, Transnationaler Zugriff, S. 54 f.; MK-Hauschild, § 110 StPO N. 18; Obenhaus, S. 654; Singelstein, S. 597; vgl. auch Schweingruber, Rz. 4.

158. Marberth-Kubicki, § 43 Fn. 386.

Ausland durch schweizerische Beamten) zurück, die eindeutig unzulässig wären.<sup>159</sup> Dazu kommt, dass durch den Online-Abruf Datenverarbeitungsvorgänge im Ausland ausgelöst werden;<sup>160</sup> der Zugriff hinterlässt im Zielstaat nachvollziehbare Spuren. Der ermittelnde Beamte kann sich dort schlimmstenfalls je nach nationaler Gesetzgebung wegen unbefugten Eindringens in ein Datenverarbeitungssystem, unbefugter Datenbeschaffung oder der Missachtung fremder Hoheitsrechte strafbar machen.<sup>161</sup> Digitale Beweisaufnahmen von der Schweiz aus erfolgen für den ausländischen Staat darüber hinaus heimlich, was sie – angesichts der Nachrichtendienst-Skandale der jüngeren Vergangenheit – aus dessen Sicht noch gefährlicher macht.<sup>162</sup> Bemerkenswerterweise lässt das nationale Recht diverser Staaten gemäss einer UN-Studie dessen ungeachtet eine Art direkten Zugriff auf im Ausland gespeicherte Daten zu, während der Anteil an Staaten, die einen solchen direkten Zugriff durch ausländische Strafverfolgungsbehörden erlauben, gemäss derselben Studie doch merklich kleiner ist.<sup>163</sup> Das völkerrechtliche Sensorium scheint folglich grösser zu sein, wenn die eigene Souveränität betroffen ist, als wenn man selbst auf die Beweisbeschaffung im Ausland angewiesen ist. Jedenfalls erlaubt die Cybercrime-Konvention den direkten Zugriff auf ausländische Daten in Art. 32 CCC bereits in beschränkter Weise; eine darüber hinausgehende Beweisbeschaffung – zumindest im Verhältnis der Konventionsstaaten untereinander – ist e contrario als Eingriff in die staatliche Souveränität zu werten.<sup>164</sup> Nicht umsonst hat der Europarat den subsidiären Art. 31 CCC mit dem Titel «Rechtshilfe beim Zugriff auf gespeicherte Daten» ausdrücklich vorgesehen. Ein von EU-Mitgliedsstaaten im Kontext der Verhandlungen eingebrachter Vorschlag, wonach in dringenden Fällen eine transnationale Online-Durchsuchung zulässig sein soll,<sup>165</sup> wurde denn auch nicht aufgenommen – man verzichtete mangels Konsens darauf, derartige Situationen zu regeln.<sup>166</sup> Auch die seither wieder aufgenommenen Bestrebungen sind bis anhin weitgehend fruchtlos geblieben; das 2. Zusatzprotokoll zur CCC ist in dieser Hinsicht ebenfalls kein grosser Wurf. Der direkte transnationale Zugriff auf Daten ohne Einwilligung einer berechtigten Person ist damit weiterhin nicht von einem internationalen Konsens abgedeckt, verstösst gegen die Souveränität des betreffenden Staats und ist damit **völkerrechtswidrig**,<sup>167</sup> solange keine Weiterentwicklung der aktuellen bi- oder multilateralen Übereinkommen stattgefunden hat.

- 68 Dieses Resultat ist **unbefriedigend**. Erstens gerade dann, wenn die Gefahr besteht, dass die Daten ohne sofortiges Tätigwerden verlustig gehen können. Es ist deshalb vorstellbar, in Ausnahmekonstellationen die vorläufige transnationale Sicherstellung von Daten bei Vorliegen von Kollusionsgefahr bzw. der Gefahr des Beweisverlusts zuzulassen, wenn selbst ein «Preservation Request» i.S.v. Art. 29 CCC zu spät erfolgen würde.<sup>168</sup> Diesfalls wären die gesicherten Daten separat aufzubewahren und dürften noch nicht durchsucht werden, bis nicht der betroffene Vertragsstaat um

159. Wabnitz/Janovsky-Bär, Kap. 12 N. 27; ferner Grave/Barth, S. 373.

160. Wabnitz/Janovsky-Bär, Kap. 12 N. 27.

161. Wabnitz/Janovsky-Bär, Kap. 12 N. 27; siehe auch Gercke, S. 489.

162. Marberth-Kubicki, § 43 Fn. 386.

163. UNODC, S. 219 f.

164. S.a. Explanatory Memorandum, Rz. 189.

165. Europäische Union, Common Position, Art. 1 Ziff. 7: «[A] transborder computer search for the purpose of the investigation of a serious criminal offense, to be further defined in the Convention, may be considered in exceptional cases, and in particular where there is an emergency, for example, as far as necessary to prevent the destruction or alteration of evidence of the serious offense, or to prevent the commission of an offense that is likely to result in the death of or serious physical injury to, a person.»

166. Explanatory Report, Rz. 293.

167. Ähnlich MK-Rückert, § 100b StPO N. 94; Bonnici et al., S. 222 ff.; Zerbes/El-Ghazi, S. 430. Daran ändert auch nichts, dass die Materialien zur CCC festhalten, Situationen, die in Art. 32 CCC nicht vorgesehen seien, seien «neither authorised, nor precluded» (so Explanatory Report, Rz. 293; T-CY Guidance Note # 3, S. 5; siehe auch Art. 39 Abs. 3 CCC, der festhält, dass das Übereinkommen «Rechte, Beschränkungen, Pflichten und Verantwortlichkeiten einer Vertragspartei unberührt» lässt).

168. Vgl. zum deutschen Recht Bär, Rz. 30, m.w.H.; ablehnend Zerbes/El Ghazi, S. 430; MK-Hauschild, § 110 StPO N. 18.

nachträgliche Genehmigung ersucht worden ist. Zweitens wird bei der vorstehenden Kritik vom Verständnis ausgegangen, dass die Strafverfolgungsbehörden im Zeitpunkt des Zugriffs positive Kenntnis davon haben, dass die Daten nicht im eigenen Land gespeichert sind. Oft ist jedoch nicht von vornherein klar, wo die Daten gespeichert sind, ob lokal auf dem Gerät oder doch in der Cloud. Auch in diesen Fällen muss eine Beweissicherung, gegebenenfalls mit anschliessendem Rechtshilfeersuchen bei nachträglich festgestelltem Auslandsbezug, zulässig sein (vgl. vorstehend, N. 23).

## V. FOLGEN DER VERLETZUNG AUSLÄNDISCHEN SOUVERÄNITÄTSRECHTS

- 69 Werden die Befugnisse der CCC überschritten, die Rechtshilfe in Strafsachen durch den direkten Zugriff auf ausländische Datenträger umgangen und damit das Territorialitäts- bzw. Souveränitätsprinzip verletzt, so stellt sich die Frage der Unverwertbarkeit so erlangter Beweismittel. Die Umgehung des Rechtshilfewegs kann im inländischen Strafprozess grundsätzlich gerügt werden.<sup>169</sup>
- 70 Kantonale Gerichte haben sich bislang für ein relatives **Verwertungsverbot** i.S.v. Art. 141 Abs. 2 StPO ausgesprochen, womit die betreffenden Beweise verwertet werden dürfen, soweit sie zur Aufklärung einer schweren Straftat erforderlich sind.<sup>170</sup> Fraglich ist derweil, ob das völkerrechtliche Territorialitätsprinzip und das Erfordernis des Beschreitens des Rechtshilfewegs tatsächlich bloss als Gültigkeitsvorschriften einzustufen sind oder ob angesichts ihrer Wichtigkeit nicht vielmehr von einem absoluten Verwertbarkeitsverbot ausgegangen werden muss (bspw. in der Gestalt eines Verstosses gegen den Ordre public). Das Bundesgericht hat in diese Richtung entschieden, als es eine geheime Überwachungsmassnahme (GPS-Tracker und Abhörgeräte in einem Fahrzeug, mit welchem auch Fahrten ins Ausland erfolgt waren) mit Bezug auf die Auslandsfahrten als absolut unverwertbar erachtete.<sup>171</sup> Möglich und sinnvoll erscheint hier indes die Übernahme der in Deutschland vertretenen Auffassung, wonach es für die Frage der Verwertbarkeit darauf ankommt, ob die Ermittlungsperson im Zeitpunkt der Datenerhebung erkannt hat, dass der Zugriff nicht in Übereinstimmung mit internationalem Recht erfolgen würde.<sup>172</sup> War ihr das nicht bewusst, muss die Möglichkeit bestehen, für die (objektiv in rechtswidriger Weise erlangten) Beweismittel ein **nachträgliches förmliches Rechtshilfeverfahren** (im Sinne eines Genehmigungsverfahrens) durchführen zu lassen, um die Unverwertbarkeit der Beweise abzuwenden.<sup>173</sup>
- 71 Letzteres ist insbesondere auf jene Fälle anwendbar, in denen nicht von vornherein klar ist, wo die Daten gespeichert sind: Kann ein Speicherort im Inland nicht ausgeschlossen werden, so muss ein Zugriff zur Beweissicherung erlaubt sein; eine positive Kenntnis des Speicherorts ist nicht

---

169. Siehe bspw. BGE 146 IV 36 E. 2.3; anders derweil BGHSt 37, 30 ff. (33): «Aus dem Völkerrecht ergibt sich für den Beschuldigten ein Beweisverwertungsverbot hier auch nicht als Reflexwirkung aus der Verletzung von Interessen eines anderen Staates. Vielmehr ist anerkannt, dass der einzelne, der von einer völkerrechtswidrigen Massnahme betroffen ist (insbesondere von der Verletzung eines völkerrechtlichen Vertrags, der ihm keine Rechte als Individuum gewährt), sich in einem anschliessenden gegen ihn gerichteten inländischen Strafverfahren wegen einer im Inland begangenen Straftat grundsätzlich nicht auf die vom Gewahrsamsstaat verübte Völkerrechtswidrigkeit berufen kann, um daraus strafprozessuale Vorteile für sich herzuleiten.»

170. So Vorinstanz in BGE 143 IV 270 E. 2; BezGer Uster vom 19.5.2014, EKR 2014-005N, bestätigt durch OGer ZH vom 27.4.2015, EKR 2015-048N.

171. BGE 146 IV 36 E. 2.3.

172. BeckOK-Graf, § 100a StPO N. 263.

173. Graf, Strafverfolgung 2.0, Rz. 43; s.a. Glassey Ludwiczak, S. 413; wohl auch BSK-Gless, Art. 141 StPO N. 30: «Erkenntnisse, die ein Staat eigenmächtig im Ausland ohne Einwilligung des Territorialstaates gesammelt hat, [dürfen] im inländischen Verfahren nicht (ohne förmliche Zustimmung des fremden Staats) verwertet werden»; unklar derweil BGE 146 IV 36 ff.; vgl. zum deutschen Recht Bär, Rz. 30; MK-Rückert, § 100b StPO N. 95.

vorauszusetzen. «Allein die Möglichkeit eines Standorts im Ausland kann keine Rechtshilfeverpflichtung auslösen, zumal in diesen Fällen nicht bestimmbar ist, welches Land davon eigentlich betroffen sein wird.»<sup>174</sup> Sollte sich hernach (bspw. auch auf entsprechende Rügen der Verteidigung hin) herausstellen, dass die abgegriffenen Daten nicht im Inland und auch nicht in einem Vertragsstaat gespeichert waren, wird im betreffenden Staat eine nachträgliche Genehmigung auf dem Rechtshilfeweg einzuholen sein.<sup>175</sup>

## VI. REFORMBEDARF

- 72 Der Europarat erkannte die Notwendigkeit der Aufweichung territorialer Grundsätze aufgrund der technischen Entwicklung früh und erliess in Art. 32 CCC eine im Vergleich zu traditionellen Rechtshilfeübereinkommen fortschrittliche Regelung. Weitergehende verfolgte Ideen waren ebenso visionär wie aufgrund des doch stark verankerten Souveränitätsgedankens (noch) nicht mehrheitsfähig. Will die Staatengemeinschaft indes eine effektive Strafverfolgung, die auch im 21. Jahrhundert ihre Aufgaben wahrnehmen können soll, erscheint es nötig und sinnvoll, **die Souveränität mit Bezug auf vernetzte Daten vollumfänglich aufzugeben**. Denn es geht heute nicht mehr bloss um die grenzüberschreitende Kriminalität, die für nationale Strafverfolgungsbehörden seit jeher nur schwer greifbar gewesen ist, sondern auch reine Binnensachverhalte können als Folge der Beweismittelverlagerung über die Landesgrenzen hinaus bald nicht mehr, schon gar nicht mehr in einer angemessenen Kosten-Nutzen-Relation, aufgeklärt werden.
- 73 Zugegebenermassen scheint es erfolgsversprechender zu sein, vorerst kleinere Brötchen zu backen: Erstens soll die Schweiz das **2. Zusatzprotokoll zur CCC**, auch wenn es sich dabei nicht um den ganz grossen Wurf handelt, möglichst rasch unterzeichnen und ratifizieren. Zweitens wäre schon viel getan, wenn man im Kontext von Art. 32 lit. b CCC mit der Rechtswirklichkeit Schritt halten und nicht mehr nur an den Speicherort, sondern vielmehr (auch) an den **Sitz der zugriffsberechtigten Person** oder daran anknüpfen würde, dass ein Unternehmen seine Dienste im betreffenden Staat anbietet (vgl. vorstehend, N. 25). Drittens sollte sich die Schweiz um eine **Assoziierung an das e-Evidence-System der EU** bemühen (wenngleich dies politisch schwierig umzusetzen sein wird). Viertens sind die wiederkehrenden Diskussionen zu einem **unilateralen Zugriff** auf Daten im Ausland wiederaufzunehmen und einem Abschluss zuzuführen. Mindestens sollte inskünftig ein **Zugriffsort im Inland** als hinreichend erachtet werden, um den Datenzugriff nicht mehr als die Souveränität des Staates am Speicherort verletzend einstufen zu müssen.<sup>176</sup> Dabei könnten gerade auch Schutzmassnahmen und Garantien (bspw. eine Informationspflicht über den Zugriff an den betroffenen Staat, die Notwendigkeit einer nachträglichen Genehmigung, Anforderungen an die Rechtsstaatlichkeit und die Wahrung von Grundrechten etc.) miteingeflochten werden, um die Akzeptanz einer solchen Lösung zu erhöhen.<sup>177</sup>

## LITERATURVERZEICHNIS

Abo Youssef Omar, Smartphone-User zwischen unbegrenzten Möglichkeiten und Überwachung, ZStrR 130 (2012), S. 92 ff.

---

174. So zum deutschen Recht MK-Hauschild, § 110 StPO N. 18; Bär, Rz. 30.

175. Kennt der ersuchte Staat keine solche Genehmigungsmöglichkeit, könnte im inländischen Strafverfahren auch die hypothetische Überprüfung Abhilfe schaffen, ob ein Rechtshilfeersuchen, wäre es denn ursprünglich gestellt worden, gutgeheissen worden wäre, vgl. BGH 1 StR 310/12 vom 21.11.2012.

176. Siehe dazu beispielhaft Economic Crime Division, S. 10 ff.; Karagiannis/Vergidis, S. 12 f.

177. Vgl. sodann bspw. weitere Vorschläge bei Svantesson, S. 6 ff.; Velasco, S. 344 ff.

Aeppli Michael, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Zürich 2004.

Bangerter Simon, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO, Zürich 2014.

Bär Wolfgang, Transnationaler Zugriff auf Computerdaten, ZIS 2 (2011), S. 53 ff., abrufbar unter [https://www.zis-online.com/dat/artikel/2011\\_2\\_525.pdf](https://www.zis-online.com/dat/artikel/2011_2_525.pdf), besucht am 17.10.2023.

Biaggini Elena, Strafrechtlicher Schutz des E-Mail-Verkehrs post mortem?, sui generis 2021, S. 321 ff., abrufbar unter <https://doi.org/10.21257/sg.196>, besucht am 17.10.2023.

Bonnici Jeanne Pia Mifsud et al., The European Legal Framework on Electronic Evidence: Complex and in Need of Reform, in: Biasiotti Maria Angela/Bonnici Jeanne Pia Mifsud/Cannataci Joe/Turchi Fabrizio (Hrsg.), Handling and Exchanging Electronic Evidence Across Europe, 2018, S. 189 ff., abrufbar unter [https://link.springer.com/chapter/10.1007/978-3-319-74872-6\\_11](https://link.springer.com/chapter/10.1007/978-3-319-74872-6_11), besucht am 17.10.2023.

Bottinelli Nicolas, L'obtention par l'autorité pénale des données informatiques situées à l'étranger, AJP 2016, S. 1327 ff.

Brodowski Dominik, Der «Grundsatz der Verfügbarkeit» von Daten zwischen Staat und Unternehmen, ZIS 8-9/2012, S. 474 ff., abrufbar unter [https://zis-online.com/dat/artikel/2012\\_8-9\\_703.pdf](https://zis-online.com/dat/artikel/2012_8-9_703.pdf), besucht am 17.10.2023.

Brodowski Dominik/Eisenmenger Florian, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden, Sachliche und zeitliche Reichweite der «kleinen Online-Durchsuchung» nach § 110 Abs. 3 StPO, ZD 2014, S. 119 ff.

Burgermeister Daniel, Beweiserhebung in der Cloud, Luzern 2015, abrufbar unter [https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/staak/MAS\\_Forensics/dok/Masterarbeiten\\_MAS\\_5/Burgermeister\\_Daniel.pdf](https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/staak/MAS_Forensics/dok/Masterarbeiten_MAS_5/Burgermeister_Daniel.pdf), besucht am 17.10.2023.

Capus Nadja, Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen, Basel 2010.

Cartner Anna/Schweingruber Sandra, Strafbehörden dürfen googeln, AJP 2021, S. 990 ff.

De Busser Els, Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You, Groningen Journal of International Law 2/2 (2014): Privacy in International Law, S. 90 ff., abrufbar unter [https://www.researchgate.net/publication/328962642\\_Open\\_Source\\_Data\\_and\\_Criminal\\_Investigations\\_Anything\\_You\\_Publish\\_Can\\_and\\_Will\\_Be\\_Used\\_Against\\_You](https://www.researchgate.net/publication/328962642_Open_Source_Data_and_Criminal_Investigations_Anything_You_Publish_Can_and_Will_Be_Used_Against_You), besucht am 17.10.2023.

Dombrowski Nadine, Extraterritoriale Strafrechtsanwendung im Internet, Potsdam 2011/2012.

Donatsch Andreas/Lieber Viktor/Summers Sarah/Wohlers Wolfgang (Hrsg.), Schulthess Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020 (zit. SK-Bearbeiter/in, Art. ... StPO N. ...).

Eckert Martin, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 112 (2016), S. 245 ff.

Forster Marc, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/

Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 613 ff.

Fröhlich-Bleuler Gianni, Eigentum an Daten?, Jusletter 6.3.2017.

Geiser Thomas/Wolf Stephan (Hrsg.), Basler Kommentar zum Zivilgesetzbuch II, Art. 457-977 ZGB, Art. 1-61 SchlT ZGB, 7. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... ZGB N. ...).

Gercke Björn, Straftaten und Strafverfolgung im Internet, GA 2012, S. 474 ff.

Glassey Ludwiczak Maria, Mesures de surveillance suisses et résultats obtenus à l'étranger, Remarques à propos de l'ATF 146 IV 36, forumpoenale 5 (2020), S. 410 ff.

Gless Sabine, Beweisverbote in Fällen mit Auslandsbezug, JR 2008, S. 317 ff.

Graf Damian K. (Hrsg.), Annotierter Kommentar zum Schweizerischen Strafgesetzbuch, Bern 2020 (zit. AK-Bearbeiter/in, Art. ... StGB N. ...).

Graf Damian K., Praxishandbuch zur Siegelung, StPO inklusive revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022 (zit. Praxishandbuch).

Graf Damian K., Strafverfolgung 2.0: Direkter Zugriff auf im Ausland gespeicherte Daten?, Jusletter IT 21.9.2017 (zit. Strafverfolgung 2.0).

Graf Jürgen-Peter (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 47. Edition, München, Stand: 1.1.2023 (zit. BeckOK-Bearbeiter/in, § ... StPO N. ...).

Grassle Christian/Hiéramente Mayeul, Praxisprobleme bei der IT-Durchsuchung, CB 2019, S. 191 ff.

Grave Carsten/Barth Christoph, Von «Dawn Raids» zu «eRaids», Zu den Befugnissen der Europäischen Kommission bei der Durchsuchung elektronischer Daten, EuZW 2013, S. 360 ff.

Hansjakob Thomas, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B\_656/2015 vom 16.12.2016, forumpoenale 4 (2017), S. 252 ff.

Heimgartner Stefan, Die internationale Dimension von Internetstraffällen, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 117 ff. (zit. Internationale Dimension).

Heimgartner Stefan, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen, Zürich 2011 (zit. Strafprozessuale Beschlagnahme).

Hess-Odoni Urs, Die Herrschaftsrechte an Daten, Jusletter 17.5.2004.

Hiatt Keith, Open Source Evidence on Trial, 125 Yale Law Journal Forum (2016), S. 323 ff., abrufbar unter [https://www.yalelawjournal.org/pdf/Hiatt\\_PDF\\_zxz3ufoz.pdf](https://www.yalelawjournal.org/pdf/Hiatt_PDF_zxz3ufoz.pdf), besucht am 17.10.2023.

Hürlimann Daniel/Zech Herbert, Rechte an Daten, sui-generis 2016, S. 89 ff., abrufbar unter <https://doi.org/10.21257/sg.27>, besucht am 17.10.2023.

Karagiannis Christos/Vergidis Kostas, Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal, Information 12 (2021), 181, S. 1 ff., abrufbar unter <https://www.mdpi.com/2078-2489/12/5/181>, besucht am 17.10.2023.

Knauer Christoph/Kudlich Hans/Schneider Hartmut (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Band 1: §§ 1-150 StPO, 2. Aufl., München 2022 (zit. MK-Bearbeiter/in, § ... StPO N. ...).

Kohler Patrick, Rechte an Sachdaten, sic! 2020, S. 412 ff.

Largiadèr Albert, Vorladungen ins Ausland nur Einladungen?, forumpoenale 5 (2014), S. 293 f.

Marberth-Kubicki Annette, in: Auer-Reinsdorff Astrid/Conrad Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Moreillon Laurent/Parein-Reymond Aude, Petit commentaire du Code de procédure pénale, 2. Aufl., Basel 2016.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar zum Strafrecht II, 4. Aufl., Basel 2019 (zit. BSK-Bearbeiter/in, Art. ... StGB N. ...).

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar zur Strafprozessordnung/Jugendstrafprozessordnung, 3. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... StPO N. ...).

Obenhaus Nils, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, S. 651 ff.

Osula Anna-Maria, Remote search and seizure in domestic criminal procedure: Estonian case study, International Journal of Law and Information Technology 24 (2016), S. 343 ff.

Pfeffer Kristin, Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln, abrufbar unter <https://eucrim.eu/articles/die-regulierung-des-grenzuberschreitenden-zugangs-zu-elektronischen-beweismitteln/>, besucht am 17.10.2023.

Riedi Claudio, Auslandsbeweise und ihre Verwertung im schweizerischen Strafverfahren, Zürich 2018.

Roth Simon, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Direkter Zugriff oder Rechtshilfe?, Jusletter 17.8.2015.

Ryser Dominic, «Computer Forensics», Eine neue Herausforderung für das Strafprozessrecht, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 553 ff.

Sampson Fraser, Intelligence evidence: Using open source intelligence (OSINT) in criminal proceedings, The Police Journal 90(1) 2017, S. 55 ff.

Schmid Alain/Schmidt Kirsten Johanna/Zech Herbert (Hrsg.), Rechte an Daten – zum Stand der Diskussion, sic! 11/2018, S. 627 ff.

Schmid Niklaus, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, ZStrR 111 (1993), S. 81 ff.

Schomburg Wolfgang/Lagodny Otto (Hrsg.), Internationale Rechtshilfe in Strafsachen, Beck'scher Kurz-Kommentar, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Bearbeiter/in).

Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter 10.11.2014.

Seger Alexander, «Grenzüberschreitender» Zugriff auf Daten im Rahmen der Budapest Konvention über Computerkriminalität, Praxisbericht zum Stand der Arbeiten des Europarats, Zeitschrift für öffentliches Recht 73 (2018), S. 71 ff.

Seitz Nicolai, Transborder Search: A New Perspective in Law Enforcement?, Yale Journal of Law & Technology 2004-2005, S. 24 ff., abrufbar unter <https://yjolt.org/transborder-search-new-perspective-law-enforcement>, besucht am 17.10.2023.

Singelstein Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co., NStZ 2012, S. 593 ff.

Svantesson Dan, Preliminary Report: Law Enforcement Cross-Border Access to Data, 12.11.2016, abrufbar unter <https://ssrn.com/abstract=2874238>, besucht am 17.10.2023.

Unseld Lea, Internationale Rechtshilfe im Steuerrecht, Akzessorische Rechtshilfe, Auslieferung und Vollstreckungshilfe bei Fiskaldelikten, Zürich 2011.

Velasco Cristos, Cybercrime jurisdiction: past, present, future, ERA Forum (2015) 16, S. 331 ff., abrufbar unter <https://rm.coe.int/16806b8a7a>, besucht am 17.10.2023.

Wabnitz Heinz-Bernd/Janovsky Thomas (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl., München 2014 (zit. Wabnitz/Janovsky-Bearbeiter/in).

Walden Ian, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, Queen Mary School of Law Legal Studies Research Paper No. 7 (2011), abrufbar unter <https://papers.ssrn.com/abstract=1781067>, besucht am 17.10.2023.

Walder Stephan, Grenzüberschreitende Datenerhebung: Ist und Soll, Kriminalistik 8-9/2019, S. 540 ff.

Weber Amalie M., The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal 18 (2003), S. 425 ff., abrufbar unter <https://lawcat.berkeley.edu/record/1118718>, besucht am 17.10.2023.

Wicker Magda, Durchsuchung in der Cloud, Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, S. 765 ff.

Zerbes Ingeborg/El-Ghazi Mohamad, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, S. 425 ff.

## MATERIALIENVERZEICHNIS

Botschaft des Bundesrates an die Bundesversammlung zu einem Bundesgesetz über internationale Rechtshilfe in Strafsachen und einem Bundesbeschluss über Vorbehalte zum Europäischen Auslieferungsübereinkommen vom 8.3.1976, BBl 1976 II 444 ff., abrufbar unter [https://www.fedlex.admin.ch/eli/fga/1976/2\\_444\\_430\\_443/de](https://www.fedlex.admin.ch/eli/fga/1976/2_444_430_443/de), besucht am 17.10.2023.

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, besucht am 17.10.2023.

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27.2.2013, BBl 2013 2683 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2013/512/de>, besucht am 17.10.2023.

Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21.12.2005, BBl 2006 1085 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2006/124/de>, besucht am 17.10.2023.

Bundesamt für Justiz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zum erläuternden Bericht und zum Vorentwurf über die Änderung des Schweizerischen Strafgesetzbuches und des Rechtshilfegesetzes, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Bern, 10.4.2010, abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html>, besucht am 17.10.2023.

Europäische Union, Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe, Official Journal of the European Communities, L 142/1 vom 5.6.1999, abrufbar unter <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:142:0001:0002:EN:PDF>, besucht am 17.10.2023.

Europarat, Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, Strassburg, 13.7.2020, abrufbar unter <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>, besucht am 17.10.2023 (zit. T-CY, Benefits).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, Transborder access to data (Article 32), Strassburg, 3.12.2014, abrufbar unter <https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transborder-access-to-data.pdf>, besucht am 17.10.2023 (zit. T-CY Guidance Note # 3).

Europarat, Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder Access and jurisdiction: What are the options?, Strassburg, 6.12.2012, abrufbar unter <https://rm.coe.int/16802e79e8>, besucht am 17.10.2023 (zit. T-CY, Transborder Access).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report, Strassburg, 16.9.2016, abrufbar unter <https://rm.coe.int/16806a495e>, besucht am 17.10.2023 (zit. T-CY, Cloud).

Europarat, Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Strassburg, 3.12.2014, abrufbar unter <https://rm.coe.int/16802e726c>, besucht am 17.10.2023 (zit. T-CY, Assessment Report).

Europarat, Draft Explanatory Memorandum Regarding on Draft Recommendation No. R (95) Concerning Problems of Criminal Procedural Law Connected with Information Technology vom 31.7.1995 (zit. Explanatory Memorandum).

Europarat, Economic Crime Division, Project on Cybercrime, Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?, Discussion Paper, Strassburg, 31.8.2010, abrufbar unter <https://rm.coe.int/16802fa3df>, besucht am 17.10.2023 (zit. Economic Crime Division).

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter <https://rm.coe.int/16800cce5b>, besucht am 17.10.2023 (zit. Explanatory Report).

United Nations, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, 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 vom 21.1.2023, abrufbar unter <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/>

4th\_Session/Documents/CND\_21.01.2023 - Copy.pdf, besucht am 17.10.2023 (zit. United Nations, Consolidated Negotiating Document).

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General vom 24.6.2013, UN Doc A/68/98, abrufbar unter <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf>, besucht am 17.10.2023 (zit. Developments).

United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, Draft February 2013, abrufbar unter [https://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf), besucht am 17.10.2023 (zit. UNODC).