



ONLINEKOMMENTAR
DER FREI ZUGÄNLICHE
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

Art. 18 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

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

Stand der Bearbeitung: 29.04.2025

PDF erstellt am: 06.10.2026

DOI: 10.17176/20250429-193729-0

ZITIERVORSCHLAG

Damian K. Graf, Kommentierung zu Art. 18 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Graf, Art. 18 CCC N. XXX.

Titel 3: Anordnung der Herausgabe

Art. 18 Anordnung der Herausgabe

¹ Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen:

- a. dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat; und
- b. dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat.

² Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

³ Im Sinne dieses Artikels bedeutet der Ausdruck «Bestandsdaten» alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann:

- a. die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Massnahmen und die Dauer des Dienstes;
- b. die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen;
- c. andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.

GLIEDERUNG

I. Allgemeines.....	4
II. Anordnung zur Herausgabe von Computerdaten (Abs. 1 lit. a)	5
III. Anordnung zur Herausgabe von Bestandesdaten bei Providern (Abs. 1 lit. b)	7
IV. Verweis auf Art. 14–15 CCC (Abs. 2)	10
V. Definition von Bestandesdaten (Abs. 3)	10
VI. Voraussetzungen für eine zulässige Datenerhebung nach schweizerischem Strafprozessrecht	11
Literaturverzeichnis.....	13
Materialienverzeichnis.....	13

I. ALLGEMEINES

- 1 Im 2. Abschnitt («Verfahrensrecht») des 2. Kapitels («Innerstaatlich zu treffende Massnahmen») befasst sich Art. 18 CCC unter dem 3. Titel («Anordnung der Herausgabe») mit der **Edition von Daten** durch die zuständigen Strafbehörden. Dabei werden zwei Konstellationen unterschieden: Einerseits die Herausgabe von Computerdaten durch eine Person, die sich im Hoheitsgebiet des betreffenden Vertragsstaates befindet (Abs. 1 lit. a), andererseits die Edition von Bestandesdaten von Diensteanbietern, die ihre Dienste im Vertragsstaat anbieten (Abs. 1 lit. b). Indem Letztere ihren Sitz nicht im betreffenden Vertragsstaat haben und die Bestandesdaten auch nicht dort gespeichert sein müssen, enthält Art. 18 CCC ein **extraterritoriales** Element (vgl. N. 9 f.).
- 2 Der Erlass einer Anordnung zur Herausgabe von Daten stellt das **mildere Mittel** im Verhältnis zu Zwangsmassnahmen dar, die tiefgreifender in die Rechte der betroffenen (oft nicht selbst beschuldigten) Personen eingreifen.¹ Im Einklang mit dem Verhältnismässigkeitsgrundsatz muss die Möglichkeit einer Editionsverfügung stets geprüft werden, bevor zu weiterreichenden Zwangsmassnahmen (wie etwa einer Hausdurchsuchung) gegriffen wird (vgl. auch Art. 265 Abs. 4 StPO). Ein wesentlicher Gesichtspunkt bei dieser Interessenabwägung ist die Gefahr von Kollusion und Beweismittelverlust, wenn die Daten nicht umgehend durch Mitglieder der Strafverfolgungsbehörden sichergestellt werden.
- 3 Inhaltlich ist Art. 18 CCC auf die Herausgabe von **konkret bestimmten oder bestimmbaren, bereits existierenden bzw. gespeicherten² Daten im Rahmen eines Strafverfahrens** beschränkt.³ Dabei muss es sich nicht zwingend um eine Cyberstraftat i.S.v. Art. 2–11 CCC oder eine andere Straftat, die mit einem Computersystem begangen wurde, handeln; es genügt, dass mit den in elektronischer Form vorliegenden Beweismitteln der Nachweis einer beliebigen Straftat geführt werden soll (Art. 14 Abs. 2 CCC).⁴ Das bedeutet zugleich, dass das ersuchte Beweismaterial zumindest **potentiell beweiserheblich** sein muss, also für die Strafuntersuchung von Bedeutung sein kann bzw. nicht offensichtlich untauglich erscheinen darf,⁵ was sich bereits aus dem allgemeingültigen Verhältnismässigkeitsgrundsatz (Voraussetzung einer «geeigneten» staatlichen Massnahme) ergibt.
- 4 Aufgrund des Wortlauts der Konvention («jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um ihre zuständigen Behörden zu ermächtigen»; ähnlich auch Art. 14 Abs. 1 CCC) ist Art. 18 CCC **keine «self-executing»-Norm**, die mit Ratifizierung des Übereinkommens unmittelbar Anwendung findet. Vielmehr begründet er eine völkerrechtliche Verpflichtung zum Erlass entsprechender innerstaatlicher Vorschriften.⁶ Art. 18 CCC kann daher – im Gegensatz zu Art. 32 CCC – nicht direkt als Grundlage für eine strafprozessuale Massnahme herangezogen werden.
- 5 Allerdings erklärte der Bundesrat in der Botschaft, **das schweizerische Recht entspreche bereits den Anforderungen von Art. 18 CCC.**⁷ Insofern können sowohl der Wortlaut von Art. 18 CCC als auch die dazugehörigen Materialien – insb. der Explanatory Report zur CCC sowie die Guidance Note # 10 des Cybercrime Convention Committee («T-CY») des Europarates – als **Auslegungshilfen**

1. Vgl. Explanatory Report, Rz. 171.

2. **Nicht erfasst sind im Zeitpunkt der Anordnung noch nicht existierende Daten wie Verbindungs- oder Inhaltsdaten im Zusammenhang mit zukünftiger Kommunikation**, Explanatory Report, Rz. 170.

3. Vgl. Explanatory Report, Rz. 182.

4. Vgl. auch T-CY Guidance Note # 10, S. 3.

5. So, in anderem Zusammenhang, BGE 142 IV 207 E. 7.1.5; BGE 101 IV 364 E. 2.

6. So auch Roth, Rz. 45; Walder, S. 545.

7. BBl 2010 4721.

für die Anwendung der inländischen Bestimmungen, vorab Art. 265 StPO, herangezogen werden. In der Schweiz entspricht es zudem einem allgemeinen Grundsatz, dass Normen soweit möglich konventionskonform auszulegen sind.⁸

- 6 Art. 18 CCC legt nicht fest, wie die Massnahmen im jeweiligen Binnenrecht genau umzusetzen sind; vielmehr umreist er lediglich den Mindestgehalt der nationalen Befugnisnormen und überlässt es den einzelnen Vertragsstaaten, die konventionsrechtlichen Vorgaben in ihre Beweiserhebungsmassnahmensystem zu integrieren. Art. 18 Abs. 2 CCC verweist immerhin auf die weiteren Mindestgarantien der Art. 14–15 CCC, die auch in diesem Kontext beachtet werden müssen.
- 7 Ebenso wenig regelt Art. 18 CCC, ob und bejahendenfalls in welchem Umfang Daten gespeichert werden müssen, noch bestimmt er Aufbewahrungsfristen.⁹ Insbesondere enthält er keine Verpflichtung für Provider, Aufzeichnungen über ihre Abonentinnen und Abonenten zu führen, deren Richtigkeit sicherzustellen, die Identität von Nutzerinnen und Nutzern zu überprüfen oder die Verwendung von Pseudonymen zu unterbinden.¹⁰ Solche Pflichten können sich ggf. aus innerstaatlichen Regelungen auf Gesetzes- oder Verordnungsebene ergeben.¹¹

II. ANORDNUNG ZUR HERAUSGABE VON COMPUTERDATEN (ABS. 1 LIT. A)

- 8 In **sachlicher Hinsicht** kann sich die Herausgabeaufforderung auf «Computerdaten» erstrecken, die in Art. 1 lit. b CCC als «jede Darstellung 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», definiert werden. Dieser Begriff schliesst **sämtliche Datentypen** ein, insb. Bestandes-, Verbindungs- sowie Inhaltsdaten (vgl. N. 24 ff.).¹² Dabei setzt Art. 18 CCC einzig voraus, dass die betreffenden Daten herausverlangt werden dürfen, ohne sich jedoch zur Zuständigkeit oder zum spezifischen innerstaatlichen Verfahren zu äussern. Aus diesem Grund ist es bspw. mit Art. 18 und Art. 15 CCC ohne Weiteres vereinbar, dass die Herausgabe von Verbindungsdaten nach schweizerischem Recht strengeren Anforderungen als eine Edition von Bestandes- oder Inhaltsdaten unterliegt und zudem eine Genehmigung des Zwangsmassnahmengerichts eingeholt werden muss (vgl. N. 27 f.).
- 9 **Persönlich** erstreckt sich Art. 18 Abs. 1 lit. a CCC gemäss seinem ausdrücklichen Wortlaut auf alle juristischen und natürlichen Personen, die zum Zeitpunkt der Anordnung ihren Sitz, Wohnsitz oder auch nur ihren vorübergehenden Aufenthaltsort im Vertragsstaat aufweisen. Die souveränitätsrechtlich erforderliche Binnenbeziehung wird hier – im Gegensatz zu Art. 32 CCC – nicht über den Speicherort der Daten definiert, sondern **an die Person geknüpft, in deren Besitz oder unter deren Kontrolle sich die zu erhebenden Daten befinden**. Art. 18 Abs. 1 lit. a CCC erfasst auch in der Schweiz ansässige **Provider**; von diesen können nicht nur Bestandesdaten (vgl. Art. 18 Abs. 1 lit. b CCC), sondern auch Inhalts- und Verbindungsdaten erhältlich gemacht werden.
- 10 Der Speicherort der Daten ist in diesem Kontext m.a.W. irrelevant. Demnach können auch **im Ausland gespeicherte Daten** bei einer inländischen Person ediert werden, sofern diese Daten «in ihrem Besitz oder unter ihrer Kontrolle befinden» («computer data in that person's possession or control»). Art. 18 Abs. 1 lit. a CCC erlaubt daher, wie Art. 32 CCC, eine Form von extraterritorialer

8. Vgl. bspw. BGE 134 IV 297 E. 4.3.5.

9. Vgl. Explanatory Report, Rz. 172 und 181; BBl 2010 4721.

10. Explanatory Report, Rz. 181.

11. Vgl. bspw. Art. 21 Abs. 2, Art. 22 Abs. 2 und Art. 26 Abs. 5 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18.3.2016 («BÜPF»; SR 780.1).

12. T-CY Guidance Note # 10, S. 6; Seger, S. 80.

Beweiserhebung. Dies steht im Einklang mit der bundesgerichtlichen Rechtsprechung zu Art. 18 CCC bzw. Art. 265 StPO, wonach diese Bestimmungen **die Edition sämtlicher Daten erlauben, auf die der Verfügungsadressat zugreifen kann bzw. darf** («avoir un pouvoir de disposition, en fait et en droit, sur ces données»¹³).

- 11 Das Begriffspaar «Besitz oder Kontrolle» bezieht sich zum einen auf den **physischen Besitz** der betreffenden Daten im Hoheitsgebiet des anordnenden Vertragsstaats (Datenherrschaft), zum anderen auf Situationen, in denen sich die interessierenden Daten zwar nicht in der Gewahrsamssphäre der Editionsadressatin befinden, diese die Herausgabe jedoch **frei kontrollieren** kann (Verfügungsberechtigung).¹⁴ Dies umfasst bspw. eine Person, die Daten bei einem Drittanbieter, etwa in einer Cloud, gespeichert hat¹⁵ – der Drittanbieter ist diesfalls im Besitz und die Nutzerin in Kontrolle der Daten, und beide können je einzeln als Verfügungsadressaten in die Pflicht genommen werden. Besitz und Kontrolle können insoweit auseinanderfallen.¹⁶ Laut dem Explanatory Report reicht es jedoch nicht aus, lediglich die technische Fähigkeit zu besitzen, auf remote gespeicherte Daten zuzugreifen; vielmehr müssen die Daten unter der legitimen Kontrolle («legitimate control») des Verfügungsadressaten stehen.¹⁷ «Kontrolle» setzt damit kumulativ die Möglichkeit des Zugriffs als auch die Berechtigung voraus, auf diese Daten zuzugreifen.¹⁸ Dies gilt es im Einzelnen abzuklären. Der Verfügungsadressat muss an der Beweisführung **mitwirken**, wenn er die fehlende Kontrolle bzw. den fehlenden Zugang zu den angeforderten Informationen geltend macht.¹⁹
- 12 In **Konzernstrukturen** kann nicht ohne Weiteres davon ausgegangen werden, dass eine Konzerntochtergesellschaft auf Daten der Mutter- oder von Schwesterngesellschaften zugreifen kann.²⁰ Umgekehrt dürften Konzernobergesellschaften, zufolge ihrer Stellung, oft entweder faktisch oder rechtlich konzernintern über die Daten verfügen oder diese kontrollieren. Wenn Daten aus regulatorischen oder datenschutzrechtlichen Gründen bei Ländergesellschaften verbleiben, und fehlt es der Muttergesellschaft nachweislich an einem Zugriff, so können die Daten derweil nur bei der Ländergesellschaft herausverlangt werden. Werden firmeninterne oder -externe Speicher- bzw. Archivierungslösungen bzw. Datenzentren genutzt, so verbleibt die Kontrollberechtigung bei der outsourcenden Person,²¹ während das aufbewahrende Unternehmen die Daten «besitzt», da sie sich in ihrem Herrschaftsbereich befinden.²² Daher unterliegen bspw. auch in der Schweiz ansässige Tochter- oder Partnergesellschaften ausländischer Provider, die Daten in der Schweiz speichern (z.B. in Serverfarmen), einer Herausgabepflicht.²³
- 13 Entscheidend ist die faktische oder rechtliche Zugriffsfähigkeit **im Zeitpunkt der Anordnung**. Eine Kappung des Zugriffs nach Erhalt einer Aufforderung wäre nicht nur rechtsmissbräuchlich, sondern

13. BGer 1B_142/2016 vom 16.11.2016 E. 3.6.

14. Explanatory Report, Rz. 173.

15. Explanatory Report, Rz. 173.

16. Verkürzt BBl 2010 4720, der nur von Besitz spricht und die Kontrolle unerwähnt lässt.

17. Explanatory Report, Rz. 173; s.a. T-CY Guidance Note # 10, S. 6: «if the person has no physical possession, that person freely controls the computer data to be submitted under Article 18.1.a from within the Party's territory»; BGer 1B_142/2016 vom 16.11.2016 E. 3.6: «un pouvoir de disposition, en fait et en droit, sur ces données».

18. Irrelevant sind derweil etwaige Datenbearbeitungs- und Herausgabebeschränkungen im Innenverhältnis zwischen Datenherr und Datenverarbeiterin.

19. BGer 1B_142/2016 vom 16.11.2016 E. 3.6.

20. So offenbar die Tochtergesellschaften von Social Media Providern oder Virtual Asset Service Providern, die zuweilen für Werbung oder Lizenzen Ländergesellschaften gründen, welche jedoch nicht auf Daten zugreifen können sollen. Extensiver derweil Walder, S. 545.

21. Vgl. auch Walder, Fn. 81.

22. Explanatory Report, Rz. 173. Wohl werden solche Daten verschlüsselt sein, weshalb eine Edition bei den Auftraggebern in der Praxis in aller Regel sinnvoller sein dürfte.

23. Vgl. BGE 141 IV 108 E. 6.2.

könnte je nach Rechtslage in den Vertragsstaaten auch eine Straftat (vgl. Art. 305 StGB [Begünstigung]) darstellen.

- 14 Wie besehen (N. 9 f.), knüpft Art. 18 Abs. 1 lit. a CCC nicht direkt an den Speicherort von Daten an. Eine inländische Herausgabeverfügung kann jedoch Daten, die in der Schweiz gespeichert sind, unabhängig davon erfassen, ob sich die datenberechtigten Personen im Ausland befinden (etwa, wenn eine im Ausland ansässige Person Daten in der Schweiz lagert oder ein Datenzentrum betreibt). Befinden sich nur die Daten in der Schweiz, nicht aber die datenberechtigten Personen, so stellt sich einzig die Frage, wie die Herausgabeaufforderung an die im Ausland ansässige Person übermittelt werden kann – eine Fragestellung, die auch unter lit. b aktuell wird (vgl. N. 20 f.).

III. ANORDNUNG ZUR HERAUSGABE VON BESTANDESDATEN BEI PROVIDERN (ABS. 1 LIT. B)

- 15 Art. 18 Abs. 1 lit. b CCC bezieht sich auf die Herausgabe von **Bestandesdaten** durch **Dienstanbieter bzw. «service provider»** i.S.v. Art. 1 lit. c CCC,²⁴ die ihre **Dienste im Hoheitsgebiet des Vertragsstaats anbieten**. Der Artikel ist somit sowohl enger als auch weiter als lit. a gefasst, indem er auf Dienstanbieter und die Vorlage von Bestandesdaten («subscriber information») – z.B. die Identität des Kunden oder Angaben zum Zahlungsverkehr²⁵ (vgl. N. 24 ff.) – limitiert ist, andererseits aber nicht nur schweizerische, sondern auch ausländische Provider erfasst (vgl. dazu N. 17 f.). Die erforderliche Binnenbeziehung zur Schweiz wird hier, ähnlich der kartellrechtlichen Konzeption, im Sinne des **Auswirkungsprinzips** verstanden, weshalb auch ausländische Dienstanbieter erfasst werden, wenn sie auf dem schweizerischen Markt aktiv sind. Voraussetzung bleibt auch hier, dass sich die Daten **im Besitz oder unter der Kontrolle** des Verfügungsadressaten befinden (vgl. dazu N. 11 ff.).
- 16 Im Gegensatz zu Art. 32 CCC, der auf Freiwilligkeit beruht und für eine rechtskonforme Datenlieferung durch Provider u.a. eine Ermächtigung in den Allgemeinen Vertragsbedingungen o.Ä. voraussetzt,²⁶ ist eine Herausgabeaufforderung **verbindlich** und muss von den adressierten Dienstanbietern umgesetzt werden, sofern sie den innerstaatlichen Anforderungen des Vertragsstaates entspricht, in dem die Dienste angeboten werden und der die Verfügung erlassen hat. Der erleichterte und effizientere Zugang zu Bestandesdaten erscheint sachgerecht, da 80–90 % der international benötigten Daten Bestandesdaten sind; Art. 18 Abs. 1 lit. b CCC trägt somit zur Entlastung des Systems der internationalen Rechtshilfe bei.²⁷
- 17 Zur Frage, wann ein Dienst **in einem Vertragsstaat «angeboten»** wird, existiert in europäischen Staaten bereits Rechtsprechung in anderen Kontexten: Erforderlich ist, dass die Aktivitäten des Dienstanbieters auf Nutzerinnen und Nutzer des Staates ausgerichtet sind,²⁸ also der Dienstanbieter

24. Unter den Begriff des Dienstanbieters («service provider») fallen nach Art. 1 lit. c CCC alle öffentlichen oder privaten Stellen, die es Nutzern ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren, sowie jede andere Stelle, die für einen solchen Kommunikationsdienst oder für seine Nutzer Computerdaten verarbeitet oder speichert. Er umfasst sowohl Internet Access Provider wie auch Internet Service Provider. Es ist unerheblich, ob die Nutzer eine geschlossene Gruppe bilden oder ob der Anbieter seine Dienste der Öffentlichkeit anbietet, sei es kostenlos oder gegen Entgelt. Erfasst sich auch Dienste, die Hosting- und Caching-Dienste bereitstellen, als auch Dienste, die eine Verbindung zu einem Netzwerk ermöglichen. Ein blosser Anbieter von Inhalten (wie eine Person, die einen Vertrag mit einem Webhosting-Unternehmen abschliesst, um ihre Webseite zu hosten) ist jedoch nicht von dieser Definition erfasst, wenn dieser Inhaltsanbieter keine Kommunikations- oder verwandten Datenverarbeitungsdienste anbietet, Explanatory Report, Rz. 27.

25. Nicht jedoch Verbindungs- oder Inhaltsdaten, BBl 2010 4720.

26. OK-Graf, Art. 32 CCC N. 48; BGE 141 IV 108 E. 5.10.

27. Seger, S. 80.

beabsichtigt, dass Nutzerinnen und Nutzer dieses Staats seine Services anwenden. Die blosser Zugänglichkeit einer Webseite oder Möglichkeit, sich von einem anderen Land aus anzumelden, reicht hierfür nicht aus.²⁹ Als Indizien für das «Anbieten» eines Dienstes können etwa die Verwendung anderer Sprachen oder Währungen, als im Sitzstaat üblich sind, die Nutzung von Top-Level-Domains oder einer Telefonvorwahl eines Staats dienen.³⁰ So stellte beispielsweise das höchste belgische Gericht fest, dass Yahoo! Inc. unter Strafandrohung zur Herausgabe von Bestandesdaten verpflichtet werden konnte, weil Yahoo! Inc. als Anbieter eines kostenlosen Webmail-Dienstes aktiv am belgischen Wirtschaftsleben teilnahm. Dies zeigte sich unter anderem durch die Nutzung der Domain «www.yahoo.be», die Verwendung der Landessprache, die Schaltung von Werbung basierend auf dem Standort der Nutzer und die Einrichtung eines Beschwerdeformulars sowie eines FAQ-Bereichs für belgische Nutzer.³¹ Schliesslich verlangt der neue Art. 3 Ziff. 4 der 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. Juli 2023 («e-Evidence-Verordnung») für das Kriterium des «Anbietens von Diensten in der EU» kumulativ (a) die Schaffung einer Möglichkeit für natürliche oder juristische Personen in einem Mitgliedstaat, die Dienste in Anspruch zu nehmen, und (b) eine wesentliche Verbindung zu diesem Mitgliedstaat, die etwa dann als unterhalten gilt, wenn der Diensteanbieter eine Niederlassung oder eine erhebliche Zahl von Nutzerinnen und Nutzern in diesem oder mehreren Mitgliedstaaten hat oder seine Tätigkeit auf diese ausgerichtet ist. Solcherlei Kriterien können auch für Art. 18 CCC fruchtbar gemacht werden.

- 18 Sind ausländische Provider mit einem Dienst im Markt eines Vertragsstaates aktiv, so sind sie verpflichtet, die Bestandesdaten herauszugeben, die auf die Nutzerinnen und Nutzer dieses konkreten Dienstes im jeweiligen Vertragsstaat bezogen sind.³² Dies ist beispielsweise der Fall, wenn sich jemand über die «.ch»-Adresse des Diensteanbieters registriert, die Schweiz als seinen Wohnsitz oder Sitz angegeben oder im Registrierungszeitpunkt oder zu einem späteren Zeitpunkt eine schweizerische IP-Adresse verwendet hat.
- 19 Auch innerhalb der Gremien des Europarats herrscht die Auffassung vor, dass sowohl von einem **inländischen Provider** Bestandesdaten, die auf einer Datenverarbeitungsanlage **im Ausland gespeichert** sind, herausverlangt werden dürfen (sofern sie unter seiner Kontrolle stehen, vgl. auch N. 11 ff.), als auch, dass Anordnungen direkt an einen **ausländischen Provider** adressiert werden können.³³ Beides steht auch im Einklang mit dem Wortlaut von Art. 18 CCC.
- 20 Auch das Bundesgericht hat sich bereits mit diesen zwei Fragen auseinandergesetzt und differenziert geurteilt: In einem Urteil vom 16. November 2016 hielt es fest, dass Art. 18 CCC bzw. Art. 265 StPO die Edition sämtlicher Daten erlaubt, sofern der Verfügungsadressat faktisch und rechtlich darauf zugreifen kann («avoir un pouvoir de disposition, en fait et en droit, sur ces données»),³⁴ mithin auch solcher, die im Ausland gespeichert sind. Mit Urteil vom 14. Januar 2015 erklärte es dagegen, dass auf Grundlage von Art. 18 CCC nicht direkt mittels einer Editionsverfügung an einen ausländischen Provider herangetreten werden darf, selbst wenn dieser seine Dienste in der Schweiz anbietet – Art.

28. EuGH, Google Spain SL und Google Inc. v Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, C-131/12, 13.5.2014, Ziff. 60.

29. Ein «Geofencing» ist also nicht notwendig. Weitergehend T-CY Guidance Note # 10, S. 8.

30. Vgl. EuGH, Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG und Hotel Alpenhof GesmbH gegen Oliver Heller, C-585/08 und C-144/09, 7.12.2010, Ziff. 83.

31. Kassationshof Belgien, ECLI:BE:CASS:2015:ARR.20151201.1, 1.12.2015, Ziff. 9.

32. Vgl. Explanatory Report, Rz. 173; s.a. T-CY Guidance Note # 10, S. 9.

33. Siehe T-CY Guidance Note # 10, S. 6; T-CY, Benefits, S. 22; Seger, S. 80. T-CY, Cloud, Rz. 38, nennt dies «a logical interpretation».

34. BGer 1B_142/2016 vom 16.11.2016 E. 3.6.

32 CCC regelt demnach den direkten grenzüberschreitenden Zugriff abschliessend, und Art. 25 Abs. 4 Satz 1 CCC legt fest, dass die internationale Rechtshilfe den gängigen Instrumentarien zu folgen hat, sofern nicht «ausdrücklich» eine abweichende Regelung in der CCC vorgesehen ist.³⁵ Immerhin konstatierte das Bundesgericht, dass in der Schweiz ansässige Tochter- oder Partnergesellschaften ausländischer Provider, die in der Schweiz Daten speichern (wie etwa Serverfarmen), dem schweizerischen Recht unterliegen.³⁶ Es setzte sich jedoch weder mit dem Wortlaut von Art. 18 CCC noch mit dem Explanatory Report oder der Botschaft auseinander, nach welcher der Gesetzgeber ja gerade davon ausging, dass das inländische Recht den Anforderungen des Art. 18 CCC entspreche.³⁷ Es ist nicht Aufgabe des Bundesgerichts, den klaren Willen des Gesetzgebers zu übersteuern. Zudem ist keine Souveränitätsverletzung erkennbar, wenn Dienste in der Schweiz angeboten werden, da in diesem Fall eine hinreichende Binnenbeziehung zur Schweiz doch gerade vorliegt.³⁸ Eine Beschränkung auf in der Schweiz ansässige Diensteanbieter würde Art. 18 Abs. 1 lit. b CCC denn auch obsolet machen, da Provider mit Sitz in der Schweiz bereits von Art. 18 Abs. 1 lit. a CCC erfasst werden (vgl. N. 9) und entsprechend nicht nur Bestandes-, sondern auch Inhalts- und Verbindungsdaten herausgeben müssen. Daher kann bei Lichte betrachtet auch Art. 18 Abs. 1 lit. b CCC als Grundlage für die gängige, in der Schweiz primär auf Art. 32 CCC abgestützte Praxis herangezogen werden, nach welcher die Strafverfolgungsbehörden **direkte Anfragen an ausländische Provider** («Information Requests») richten.³⁹ Das gilt auch im umgekehrten Sinne – schweizerische Provider, die ihre Dienste in ausländischen Märkten anbieten, dürfen von jenen Behörden direkt zur Herausgabe aufgefordert werden, und da sie grundsätzlich einer Herausgabepflicht unterliegen, machen sie sich im Falle der Datenlieferung auch nicht wegen Art. 271 StGB («Verbotene Handlung für einen fremden Staat») strafbar.

- 21 Was die **Zustellung** der Editionsverfügungen betrifft, so stellen grössere Provider sog. «Law Enforcement Portals» zur Verfügung, über die sich auch schweizerische Strafverfolgungsbehörden registrieren und ihre Anfragen direkt eingeben können. Bei kleineren Diensteanbietern können die Herausgabeaufforderungen über den Polizeiweg (via Interpol) oder, sofern akzeptiert, auch direkt (bspw. per E-Mail) zugestellt werden. Art. 18 Abs. 1 lit. b CCC ermöglicht insoweit den Verzicht auf den förmlichen Rechtshilfeweg und erlaubt es den Vertragsstaaten, solche Editionsverfügungen direkt an Provider in anderen Vertragsstaaten zuzustellen.⁴⁰ Dies ist zulässig und sachgerecht, da das Erfordernis einer rechtshilfeweisen Zustellung der Editionsverfügung die Erleichterungen zunichte machen würde, die Art. 18 Abs. 1 lit. b CCC gerade ermöglichen möchte. Nur durch die direkte Zustellung ist sichergestellt, dass die Strafverfolgungsbehörden effizient und schnell auf die notwendigen Bestandesdaten zugreifen können, ohne den oft langwierigen und bürokratischeren Rechtshilfeweg beschreiten zu müssen. Fakt ist jedoch, dass die mangelnde Kooperation nicht direkt, sondern nur auf dem formellen Rechtshilfeweg mittels über Art. 18 CCC hinausgehenden Zwangsmassnahmen **durchgesetzt** werden kann.
- 22 Da es sich bei der Herausgabeaufforderung um eine **innerstaatliche Beweiserhebungsmassnahme** handelt,⁴¹ ist nicht das Recht des Vertragsstaats massgeblich, in dem der Provider seinen Sitz hat, sondern das Recht des Vertragsstaats, in dem der Provider seine Dienste anbietet.

35. BGE 141 IV 108 E. 6.4; zustimmend Forster, S. 619 f.; Roth, Rz. 50 ff.; a.M. Schweingruber, Rz. 21 ff.

36. BGE 141 IV 108 E. 6.2.

37. BBl 2010 4721.

38. Ähnlich Kassationshof Belgien, ECLI:BE:CASS:2015:ARR.20151201.1, 1.12.2015, Ziff. 8.

39. Schweingruber, Rz. 28; Seger, S. 80.

40. Hinzu kommt, dass die direkte Zustellung ohnehin in verschiedenen Staatsverträgen geregelt ist, siehe etwa Art. 52 Abs. 1 des Schengener Durchführungsübereinkommens vom 19.6.1990 («SDÜ») oder Art. 16 Abs. 1 des Zweiten Zusatzprotokolls zum Europäischen Übereinkommen über die Rechtshilfe in Strafsachen vom 8.11.2001 («ZP II EuER»).

41. T-CY Guidance Note # 10, S. 7.

IV. VERWEIS AUF ART. 14–15 CCC (ABS. 2)

- 23 Staaten können im Rahmen von Art. 15 CCC **Bedingungen und Schutzvorkehrungen** festlegen und Daten vom Anwendungsbereich des Art. 18 CCC ausschliessen. So ist es bspw. gerechtfertigt, die Herausgabe von Verbindungsdaten auf bestimmte Delikte zu beschränken und dafür die Notwendigkeit der Einholung einer Genehmigung des Zwangsmassnahmengerichts zu verlangen (Art. 273 StPO).⁴² Weiter ist es zulässig, Herausgabeanordnungen mit Mitteilungsverboten zu verknüpfen,⁴³ wie dies im Schweizer Recht umgesetzt wurde (Art. 73 Abs. 2 StPO).

V. DEFINITION VON BESTANDESDATEN (ABS. 3)

- 24 Als **Bestandesdaten** kommen sämtliche Informationen – die nicht als Verbindungs- oder Inhaltsdaten qualifizieren – in Betracht, die von einem Diensteanbieter im Zusammenhang mit einem Nutzer oder Abonnenten seiner Dienste gespeichert werden. Zentrales Ziel der Bestandesdatenabfrage ist die Bestimmung der **Identität** des Abonnenten bzw. Nutzers sowie die Ermittlung der vom Nutzer verwendeten Services. Darüber hinaus können auch kommerzielle Informationen wie Abrechnungs- und Zahlungsdaten relevant sein, insbesondere im Zusammenhang mit Cyberbetrügen und anderen Vermögensdelikten.⁴⁴
- 25 Zu den Bestandesdaten zählen nach Art. 18 Abs. 3 CCC alle Informationen bezüglich (a) der Art des genutzten Kommunikationsdienstes, der dafür getroffenen technischen Massnahmen⁴⁵ und der Dauer des Dienstes; (b) der Identität des Teilnehmers, seiner Post- oder Hausanschrift, Telefon- und sonstigen Zugangsnummern sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen; sowie (c) anderer Informationen über den Standort der Kommunikationsanlage, die auf Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen. In der Schweiz werden die Informationen, die i.A.v. Art. 22 Abs. 1 BÜPF herausgegeben werden können, namentlich in den Art. 36–38 der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017 («VÜPF», SR 780.11) konkretisiert. Als Bestandesdaten gelten namentlich Adressierungselemente wie die Zuordnung von Namen, Telefonnummern und Adresse des Benutzers zu einer bekannten IP-Adresse,⁴⁶ alsdann auch Originalverträge und Kopien von bei Vertragsabschluss vorgelegten Ausweisen⁴⁷ sowie technische Auskünfte im Fernmeldeverkehr.⁴⁸
- 26 Abzugrenzen sind Bestandesdaten von **Inhaltsdaten**, die den Inhalt der Kommunikation oder gespeicherte Dateien umfassen, sowie von Verbindungs- bzw. **Verkehrsdaten**, die in Zusammenhang mit einer Kommunikation erzeugt werden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation hervorgeht (Art. 1 lit. d CCC). Das Bundesgericht differenziert Bestandes- und Randdaten anhand dem Abgrenzungskriterium, ob den Strafverfolgungsbehörden bereits ein Internetanschluss oder eine E-Mail-Adresse bekannt ist, die es lediglich noch einer konkreten Person zuzuordnen gilt, beziehungsweise es um eine Bestandesdatenabfrage geht. Falls den Strafverfolgungsbehörden dagegen allein strafbare Internet-

42. Vgl. auch Explanatory Report, Rz. 174.

43. Explanatory Report, Rz. 175.

44. Explanatory Report, Rz. 178.

45. Explanatory Report, Rz. 179: «The term «technical provisions» includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks)».

46. Vgl. BGE 133 IV 271 E. 2.4 f.

47. TPF 2006 255.

48. BSK-Jean-Richard-dit-Bressel, Art. 273 StPO N. 7.

Kommunikationsaktivitäten bekannt sind und über die Verbindungs-Randdaten der betreffenden Kommunikation die zugewiesenen IP-Adressen und registrierten Kunden erst ermittelt werden sollen, soll es sich um eine (genehmigungspflichtige) rückwirkende Randdatenerhebung i.S.v. Art. 273 StPO handeln.⁴⁹ Nach der Rechtsprechung soll dies pauschal auch für die Aufforderung zur Herausgabe einer IP-History gelten.⁵⁰ Richtigerweise ist die Abgrenzung danach zu vollziehen, ob es darum geht, wer wann mit wem kommuniziert hat (Verbindungsdaten i.S.v. Art. 273 StPO),⁵¹ oder vielmehr darum, wer einen bestimmten Dienst zu einem bekannten Zeitpunkt benutzt hat (Bestandesdaten i.S.v. Art. 22 Abs. 1 BÜPF).⁵² **Registrierungs-IP-Adressen** für einen bereits bekannten Account müssen demgemäss eindeutig als Bestandesdaten und nicht als Verkehrsdaten betrachtet werden, da sie ausschliesslich der Identifikation eines Teilnehmers dienen und keinen Bezug zur anschliessenden Kommunikation über den Account aufweisen. Auch sonstige «**access data**» (z.B. die IP-History von Logins auf einem nicht zur Kommunikation gedachten Service, wie etwa das Login auf einem Kryptowallet oder in einer Cloud) können richtigerweise nicht als Verbindungs-Randdaten in Betracht kommen. Diese Daten betreffen weder unmittelbar noch mittelbar die Kommunikation zwischen Menschen und deren Überwachung. Die IP-Adressen sind in solchen Fällen vielmehr mit am Tatort hinterlassenen Tatspuren vergleichbar, ähnlich einem Fingerabdruck oder einer DNA,⁵³ und stellen keine Randdaten im Kontext menschlicher Kommunikation, sondern vielmehr Bestandesdaten dar.⁵⁴ Das bundesgerichtliche Diktum zur Qualifikation von IP-Histories als Verkehrsdaten i.S.v. Art. 273 StPO ist insoweit zu wenig differenziert.

VI. VORAUSSETZUNGEN FÜR EINE ZULÄSSIGE DATENERHEBUNG NACH SCHWEIZERISCHEM STRAFPROZESSRECHT

- 27 Für **Bestandesdaten** i.S.v. Art. 18 Abs. 3 CCC – d.h. insb. (auch rückwirkende) Angaben darüber, wer als Inhaber bzw. Rechnungsadressat des Anschlusses bei dem schweizerischen Recht unterworfenen Diensteanbieterinnen registriert ist bzw. war (vgl. N. 24 ff.) – kann eine einfache Abfrage gemäss Art. 22 Abs. 1 BÜPF beim für die Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF) gestellt werden.⁵⁵ Solche Informationen können auch durch Edition (Art. 265 StPO) erlangt werden, insbesondere wenn der ausländische Provider, der seine Dienste i.S.v. Art. 18 Abs. 1 lit. b CCC in der Schweiz anbietet, nicht dem BÜPF unterstellt ist.⁵⁶ Die Informationsabfrage über den Dienst ÜPF stellt lediglich eine Ordnungsvorschrift dar; weder die StPO noch das BÜPF oder die dazugehörige Verordnung sehen vor, dass Auskünfte, die nicht über den Dienst ÜPF mitgeteilt werden, unverwertbar wären.⁵⁷ Eine Bestandesdatenabfrage setzt einen Tatverdacht, dass eine Straftat (Verbrechen, Vergehen oder Übertretung) über das Internet begangen worden ist (Art. 22 Abs. 1 BÜPF),

49. BGer 6B_656/2015 vom 16.12.2016 E. 1.3.2; BGer 6B_1353/2023 vom 6.11.2024 E. 4.4.1; Betschmann, S. 360 f.; a.M. Hansjakob, Überwachungsrecht, Rz. 1638.

50. BGer 6B_1353/2023 vom 6.11.2024 E. 4.4.3; BGer 6B_656/2015 vom 16.12.2016 E. 1.4.3; krit. OK-Graf, Art. 32 CCC N. 17, 56 und 60; Hansjakob, Erhebung, S. 252 ff.

51. Vgl. BGE 141 IV 108 E. 6.2; BGer 6B_656/2015 vom 16.12.2016 E. 1.3.2; BGE 144 I 126 E. 6.2.

52. SK-Hansjakob/Pajarola, Art. 273 StPO N. 47 ff.

53. So AppGer BS AG.2017.447 vom 24.2.2017 E. 3.3 (*in casu* ging es darum, anhand der IP-Adressen zu eruieren, wer sich für zwei verleumderische Blogs verantwortlich zeichnete).

54. Das Bundesgericht scheint den Begriff der genehmigungspflichtigen Verbindungs- bzw. Randdaten dessen ungeachtet wohl auch auf derartige Fallkonstellationen zu beziehen, siehe den Verweis in BGer 6B_1353/2023 vom 6.11.2024 E. 4.4.2 auf BBl 2013 2743 f.: «Dies korrespondiert mit den Ausführungen in der Botschaft BÜPF, gemäss denen es sich bei den Daten, aus welchen sich ergibt, «wie oft eine bestimmte Person eine bestimmte Website angesurft hat und «zu welchen Zeiten» dies der Fall war, um Randdaten handelt, deren Erhebung einer gerichtlichen Bewilligung bedarf».

55. BBl 2013 2736; s.a. BBl 2010 4720 (m.V.a. aArt. 14 Abs. 4 BÜPF).

56. S.a. BGE 141 IV 108 E. 6.2.

57. BGer, 1B_595/2022 v. 23.12.2022, E. 5.4.

⁵⁸ die potentielle Untersuchungsrelevanz bzw. Beweiserheblichkeit der erfragten Informationen sowie die Verhältnismässigkeit voraus. Gegen eine Bestandesdatenabfrage ist kein ordentliches Rechtsmittel zulässig; namentlich ist die Siegelung (Art. 248 StPO) nicht einschlägig, da von vornherein nicht erkennbar ist, inwieweit die angeforderten Bestandesdaten einem Beschlagnahmeverbot gemäss Art. 264 StPO unterliegen könnten. Die Provider unterliegen einer Auskunftspflicht;⁵⁹ weigern sie sich, so kann eine Ordnungsbusse oder Busse nach Art. 292 StGB verhängt werden (sofern sie vorher darauf hingewiesen wurden), oder es können Zwangsmassnahmen ergriffen werden (analog zu Art. 265 Abs. 3 und 4 StPO). Für ausländische Providern, die ihre Dienste in der Schweiz anbieten, dürfte die Androhung der Strafdrohung nach Art. 292 StGB zwar ebenfalls zulässig sein, jedoch müssten Zwangsmassnahmen zur Durchsetzung der Bestandesdatenabfrage rechtshilfweise beim betreffenden Staat beantragt werden.

- 28 Für Inhalts- und Verbindungsdaten, die beide nach Art. 18 Abs. 1 lit. a StPO herausverlangt werden dürfen, ist alsdann zu differenzieren: **Inhaltsdaten**, die für Beweiszwecke relevant sein können, sind nach Art. 265 StPO zu edieren, sofern sie im Zeitpunkt der Anordnung gespeichert («in storage») sind und sich nicht noch im Übermittlungsstadium («in traffic») befinden.⁶⁰ Praxisrelevant sind bspw. Inhaltsdaten von Webmail-Betreibern, bspw. der E-Mail-Account einer «@bluewin.ch»-Adresse bei der Swisscom.⁶¹ Voraussetzung für die Herausgabe von Inhaltsdaten ist ein hinreichender Tatverdacht für eine beliebige Straftat, die potentielle Beweiserheblichkeit bzw. mögliche Relevanz der edierten Aufzeichnungen für das Strafverfahren sowie die Einhaltung des Verhältnismässigkeitsgrundsatzes. Die Editionsverfügung kann mit einem Mitteilungsverbot gemäss Art. 73 Abs. 2 StPO verknüpft werden, was bewirkt, dass die Account-Inhaberin vom Diensteanbieter bis auf weiteres nicht benachrichtigt werden darf. Gegen eine Editionsverfügungen steht den Inhabern sowie weiteren berechtigten Personen der Rechtsbehelf der Siegelung (Art. 248 StPO) offen, jedenfalls soweit sie eigene Geheimnisinteressen geltend machen können. Dem Provider steht dabei zwar formell das Siegelungsrecht zu, allerdings kann er die Siegelung nicht stellvertretend für seine Kundinnen und Kunden verlangen⁶² und eigene Beschlagnahmeverbote gemäss Art. 264 StPO wird er kaum je geltend machen können. Für **Verbindungs- bzw. Randdaten** (vgl. N. 26) hat die Staatsanwaltschaft keine Edition, sondern eine Anordnung nach Art. 273 StPO zu erlassen, die strengerer Anforderungen unterliegt: (1) Es muss ein dringender Tatverdacht für ein Verbrechen oder Vergehen vorliegen; (2) die Schwere der Straftat muss die Überwachung rechtfertigen; (3) die bisherigen Untersuchungshandlungen müssen erfolglos geblieben sein oder die Ermittlungen wären sonst aussichtslos oder würden unverhältnismässig erschwert (Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 StPO). Die Anordnung muss zudem vom Zwangsmassnahmengericht genehmigt werden (Art. 274 StPO), andernfalls die erhobenen Beweise absolut unverwertbar sind (Art. 277 Abs. 2 StPO). Die

58. Wobei noch kein Verfahren eröffnet worden sein muss, die Polizei mithin auch im selbständigen Ermittlungsmassnahmen diese Informationen erheben kann, Hansjakob, Überwachungsrecht, Rz. 1642.

59. Hansjakob, Überwachungsrecht, Rz. 1643.

60. Bei einem E-Mail-Account sind sämtliche eingegangenen E-Mails seit dem letzten Zugriff auf das E-Mail-Konto durch die berechnigte Person «in traffic» (BGE 140 IV 181 E. 2.7). Derartige Daten können gemäss Bundesgericht nur durch eine geheime Überwachungsmassnahme nach Art. 269 ff. StPO erhältlich gemacht werden, und nicht etwa mittels einer Edition nach Art. 265 StPO. Da heutzutage «Push»-Nachrichten im Falle des Eingangs von E-Mails verbreitet sind, hat diese Rechtsprechung weitgehend an Bedeutung verloren.

61. Beispiel eines Verfügungstexts aus der Praxis: «Die Swisscom AG / Swisscom (Schweiz) AG wird aufgefordert, der Staatsanwaltschaft innert 10 Arbeitstagen die folgenden Daten herauszugeben: Den gesamten E-Mail-Verkehr des Kontos «[...]@bluewin.ch» für den Zeitraum ab Eröffnung bis heute oder zur Löschung des Kontos, soweit die E-Mails vor dem letzten Login bzw. Abrufen des E-Mail-Accounts eingetroffen sind. Sämtliche verlangten Daten sind in einer handelsüblichen elektronischen Form herauszugeben».

62. Siehe bspw. BGer 1B_243/2021 vom 20.12.2021 E. 3.6; Graf, Crypto-Leaks, *passim*.

Genehmigung des Zwangsmassnahmengerichts kann durch die überwachte Person, ggf. auch durch den Provider, mit Beschwerde nach Art. 393 ff. StPO angefochten werden (Art. 279 Abs. 3 StPO).

LITERATURVERZEICHNIS

Betschmann Simon, Randdatenerhebung im Fernmeldeverkehr gemäss Art. 273 StPO, AJP 2019, S. 358 ff.

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. ...).

Graf Damian K., Corona- und Crypto-Leaks – die Strafverfolgung bewegt sich nicht im rechtsfreien Raum, Gastkommentar, NZZ vom 17.2.2023, abrufbar unter <https://www.nzz.ch/meinung/was-darf-die-staatsanwaltschaft-die-corona-und-crypto-leaks-ld.1725348>, besucht am 31.3.2025 (zit. Crypto-Leaks).

Graf Damian K., Kommentierung zu Art. 32 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter <https://onlinekommentar.ch/de/kommentare/ccc32>, besucht am 31.3.2025 (zit. OK).

Forster Marc, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Festgabe Schweizerischer Juristentag 2015, Zürich 2015, S. 615 ff.

Hansjakob Thomas, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 vom 16.12.2016, forumpoenale 4 (2017), 252 ff. (zit. Erhebung).

Hansjakob Thomas, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich/Basel/Genf 2017 (zit. Überwachungsrecht).

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

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

Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10. November 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.

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

MATERIALIENVERZEICHNIS

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 31.3.2025.

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 31.3.2025.

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 31.3.2025 (zit. T-CY, Benefits).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 10, Production orders for subscriber information (Article 18 Budapest Convention), Strassburg, 28.2.2017, abrufbar unter <https://rm.coe.int/16806f943e>, besucht am 31.3.2025 (zit. T-CY Guidance Note # 10).

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 31.3.2025 (zit. T-CY, Cloud).

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter <https://rm.coe.int/16800cce5b>, besucht am 31.3.2025 (zit. Explanatory Report).