



ONLINEKOMMENTAR
DER FREI ZUGÄNGLICHE
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

Art. 29 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Simon Bächtold
Herausgegeben von Damian K. Graf

Stand der Bearbeitung: 26.07.2024
PDF erstellt am: 06.10.2026
DOI: 10.17176/20240726-082428-0

ZITIERVORSCHLAG

Simon Bächtold, Kommentierung zu Art. 29 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Bächtold, Art. 29 CCC N. XXX.

Abschnitt 2: Besondere Bestimmungen

Titel 1: Rechtshilfe bei vorläufigen Massnahmen

Art. 29 Umgehende Sicherung gespeicherter Computerdaten

¹ Eine Vertragspartei kann eine andere Vertragspartei um Anordnung oder anderweitige Bewirkung der umgehenden Sicherung von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der anderen Vertragspartei befindet, und derentwegen die ersuchende Vertragspartei beabsichtigt, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu stellen.

² Ein Ersuchen um Sicherung nach Absatz 1 hat Folgendes genau zu bezeichnen:

- a. die Behörde, die um die Sicherung ersucht;
- b. die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung;
- c. die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat;

d. alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standorts des Computersystems;

e. die Notwendigkeit der Sicherung; und

f. die Absicht der Vertragspartei, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der gespeicherten Computerdaten zu stellen.

³ Nach Eingang des von einer anderen Vertragspartei gestellten Ersuchens trifft die ersuchte Vertragspartei alle geeigneten Massnahmen zur umgehenden Sicherung der bezeichneten Daten in Übereinstimmung mit ihrem innerstaatlichen Recht. Für die Zwecke der Erledigung eines Ersuchens wird die beiderseitige Strafbarkeit als Voraussetzung für die Vornahme dieser Sicherung nicht verlangt.

⁴ Eine Vertragspartei, welche die beiderseitige Strafbarkeit als Voraussetzung für die Erledigung eines Rechtshilfeersuchens um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe gespeicherter Daten verlangt, kann sich in Bezug auf andere als die nach den Artikeln 2–11 umschriebenen Straftaten das Recht vorbehalten, Ersuchen um Sicherung nach diesem Artikel abzulehnen, wenn sie Grund zu der Annahme hat, dass im Zeitpunkt der Weitergabe die Voraussetzung der beiderseitigen Strafbarkeit nicht erfüllt werden kann.

⁵ Darüber hinaus kann ein Ersuchen um Sicherung nur abgelehnt werden, wenn:

a. das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder

b. die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (ordre public) oder andere wesentliche Interessen zu beeinträchtigen.

⁶ Ist durch die Sicherung nach Ansicht der ersuchten Vertragspartei die künftige Verfügbarkeit der Daten nicht gewährleistet oder die Vertraulichkeit der Ermittlungen der ersuchenden Vertragspartei gefährdet oder in anderer Weise beeinträchtigt, so setzt sie die ersuchende Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.

⁷ Jede Sicherung, die in Erledigung des in Absatz 1 bezeichneten Ersuchens vorgenommen wird, erfolgt für mindestens 60 Tage, damit die ersuchende Vertragspartei ein Ersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten stellen kann. Nach Eingang eines solchen Ersuchens werden die Daten weiterhin gesichert, bis über das Ersuchen entschieden worden ist.

GLIEDERUNG

I. Einleitung	4
A. Multinational-arbeitsteilige Strafverfolgung bei Cyberkriminalität	4
B. Praktische Bedeutung und verwandte Artikel.....	4
II. Voraussetzung der doppelten Strafbarkeit (Art. 29 Abs. 3 und 4 CCC), Ausschluss politischer Strafverfolgung (Art. 29 Abs. 5 lit. a CCC) und Verstoss gegen den Ordre public (Art. 29 Abs. 5 lit. b CCC)	5
III. Sicherung und Erhebung von Daten im Ausland	6
A. Einen Preservation Request stellen	6
1. Die ersuchende Behörde (lit. a.)	6
2. Die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung (lit. b.).....	7
3. Die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat (lit. c.)	7
4. Alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standorts des Computersystems (lit. d.)	7
5. Die Notwendigkeit der Sicherung (lit. e.) und die Absicht der Vertragspartei, ein Rechtshilfeersuchen zu stellen (lit. f.)	7
B. Weiterleitung und Verarbeitung des Preservation Requests	8
C. Abgrenzung zum Information Request	8
D. Prosequierung mittels Rechtshilfeersuchen	9
E. Best Practices für Rechtshilfeersuchen an die USA.....	9
IV. Ausführen von Preservation Requests durch Schweizer Behörden.....	11
A. Verfahrensablauf und Zuständigkeiten.....	11
B. Umsetzung mittels Schweizer Recht.....	11
Literaturverzeichnis.....	14
Materialienverzeichnis	14

I. EINLEITUNG

A. Multinational-arbeitsteilige Strafverfolgung bei Cyberkriminalität

- 1 Kriminelle verwenden das **Internet** zur Begehung von Straftaten vor allem aus zwei Gründen. Einerseits, um anonym zu bleiben. Andererseits, um ihr kriminelles Geschäftsmodell kostengünstig zu skalieren, also um eine Vielzahl potentieller Opfer zu erreichen (insb. Cyber-Betrug). Hinzu kommen jene Computer-Straftaten im engeren Sinn, die in der analogen Welt gar nicht denkbar sind (z.B. Hacking, DDOS-Attacken etc.).
- 2 Entsprechend der Natur des Internets als weltweites Kommunikationsnetz, findet Internetkriminalität stets **international** statt. Organisierte Täterschaften agieren in der Regel weltweit, zumindest aber – aus Schweizer Perspektive betrachtet – europaweit, vereinzelt auch nur sprachregional (z.B. deutschsprachiger Raum). Daraus folgt, dass kein Staat alleine die Internetkriminalität bekämpfen kann. Cyber-Ermittlungen müssen fast immer international geführt werden bzw. weisen grenzüberschreitende Aspekte auf. Bei grossen und aufwändigen Ermittlungen spricht man von international-arbeitsteiliger Strafverfolgung. Der Kontrast dazu bei der (Schweizer) Strafverfolgung könnte nicht deutlicher sein. Aufgrund der primären Zuständigkeit der Kantone für die Strafverfolgung gehen hierzulande noch immer sehr viele Ressourcen für die Klärung der innerstaatlichen Zuständigkeit verloren. Ein nationales Lagebild zu Cybercrime-Phänomenen existiert bestenfalls in Ansätzen.
- 3 Wer im Cyber-Bereich ermittelt, kommt ausserhalb des Bagatellbereichs in der Regel am Art. 29 CCC (Preservation Request / umgehende Sicherstellung von Daten) nicht vorbei.

B. Praktische Bedeutung und verwandte Artikel

- 4 Art. 29 CCC zählt zusammen mit Art. 32 lit. b CCC zu den praktisch relevantesten Bestimmungen der Cybercrime Convention, zumindest aus Sicht der Strafverfolgungsbehörden.
- 5 Der Preservation Request soll das Problem lösen, dass elektronische Daten flüchtig sind und häufig im Ausland¹ gespeichert sind, Rechtshilfeverfahren jedoch regelmässig sehr langwierig sind.² Aus Sicht der Strafverfolgung kommt erschwerend hinzu, dass viele Länder keine sogenannte «Voratsdatenspeicherung» kennen, was dazu führen kann, dass ermittlungsrelevante Daten verloren sind, bevor überhaupt ein Rechtshilfeersuchen anhängig gemacht werden kann. Mittels Preservation Requests sollen also Daten im Ausland, die für die Strafverfolgung relevant sind, einfach und schnell einstweilen **sichergestellt** werden können, damit der ersuchende Staat Zeit hat, die Daten auf dem Rechtshilfeweg erhältlich zu machen.³
- 6 Im Gegensatz zum Information Request gemäss Art. 32 lit. b CCC, welcher niederschwellig und für den ersuchenden Staat ohne Nachteile und Kosten gestellt werden kann, verpflichtet sich der ersuchende Staat, welcher sich auf Art. 29 CCC beruft, dazu, später die im Ausland gesicherten Daten tatsächlich auch mittels **Rechtshilfeersuchen** anzufragen. Ein Rechtshilfeersuchen ist für die

1. In den allermeisten Fällen in den Vereinigten Staaten von Amerika.

2. Zu langwierige und komplexe Rechtshilfeverfahren gelten allgemein als eines der grössten Hindernisse bei der Bekämpfung der Internetkriminalität (vgl. T-CY, Assessment Report, S. 3). Die typische Bearbeitungsdauer für internationale Rechtshilfeersuchen im Cyber-Bereich liegt zwischen 6 und 24 Monaten (vgl. T-CY, Assessment Report, S. 38). Die USA erhalten hunderte von Rechtshilfeersuchen jedes Jahr und geben an, überlastet zu sein – ebenso Zypern (T-CY, Assessment Report, S. 6 und 39).

3. Vgl. dazu auch BGE 141 IV 108 E. 5.5.

ersuchende Staatsanwaltschaft mit einem gewissen Aufwand verbunden, sodass die Staatsanwaltschaft Preservation Requests nicht leichtfertig stellen wird.

- 7 Immer wieder stellt sich die Frage nach der **Rechtsnatur** eines Preservation Requests. Dies zum Beispiel, wenn nach Einreichung einer Strafanzeige noch unklar ist, ob ein hinreichender Anfangsverdacht zur Eröffnung eines Strafverfahrens gegeben ist (Art. 309 Abs. 1 lit. a StPO). Nur dann sind staatsanwaltliche Zwangsmassnahmen möglich und gerechtfertigt. Handelte es sich beim Preservation Request nicht um eine Zwangsmassnahme, wäre es möglich, dass auch die Polizei von sich aus einen Preservation Request stellt, was von der Intention her zu begrüssen wäre, weil eine Datensicherung umso erfolgreicher sein dürfte, je rascher sie erfolgt. Die Frage nach der Rechtsnatur wird von der Cybercrime Convention selbst nicht beantwortet, sondern richtet sich nach dem Recht des angefragten Staates (Art. 25 Abs. 4 CCC).⁴ Die Antwort kann somit unterschiedlich ausfallen. Für die Schweiz wird hier vertreten, dass die Polizei ohne das Einverständnis der Staatsanwaltschaft grundsätzlich keinen Preservation Request stellen darf, weil letztere sich damit verpflichtet, später ein internationales Rechtshilfeersuchen zu stellen (was nur bei eröffnetem Strafverfahren möglich ist). Ebenfalls bewirkt das Ersuchen um umgehende Datensicherung eine vorübergehende Sicherstellung von Aufzeichnungen, die im inländischen Verhältnis eine Zwangsmassnahme darstellen würde.⁵ Faktisch muss ein Preservation Request daher analog einer **strafprozessualen Zwangsmassnahme** behandelt werden.⁶ In der Konsequenz muss ein Preservation Request damit grundsätzlich durch die Staatsanwaltschaft angeordnet werden, wobei der Vollzug der Polizei delegiert werden kann. In inländischen Sachverhalten ist eine vorübergehende Sicherstellung durch die Polizei indes ausnahmsweise dann zulässig, wenn «Gefahr im Verzug» ist und die Staatsanwaltschaft nicht rechtzeitig (auch nicht mündlich) informiert werden kann (Art. 263 Abs. 3 StPO).⁷ In solchen Ausnahmefällen darf die Polizei Ersuchen nach Art. 29 CCC auch autonom stellen.
- 8 Zu erwähnen ist auch Art. 16 CCC, welcher von den Mitgliedsstaaten verlangt, die nötigen gesetzgeberischen und organisatorischen Voraussetzungen zu schaffen, damit Preservation Requests ausländischer Staaten gemäss Art. 29 CCC nachgekommen werden kann. Die Schweiz entschied sich im Zuge der Umsetzung des Übereinkommens, diesbezüglich kein neues Strafprozessrecht zu erlassen (vgl. nachstehend, N. 32).

II. VORAUSSETZUNG DER DOPPELTEN STRAFBARKEIT (ART. 29 ABS. 3 UND 4 CCC), AUSSCHLUSS POLITISCHER STRAFVERFOLGUNG (ART. 29 ABS. 5 LIT. A CCC) UND VERSTOSS GEGEN DEN ORDRE PUBLIC (ART. 29 ABS. 5 LIT. B CCC)

- 9 Die Cybercrime Convention ist bestrebt, die internationale Zusammenarbeit bei der Strafverfolgung von Computerdelikten bestmöglich zu fördern. Aus diesem Grund enthält die Konvention selbst kein Erfordernis der beiderseitigen Strafbarkeit, sondern stellt es Vertragsstaaten frei, Unterstützung zu

4. BGE 141 IV 108 E. 4.3.8-4.3.9.

5. Vgl. zur vorübergehenden Sicherstellung bzw. provisorischen Beschlagnahme nach Art. 263 StPO BGer 1B_65/2014 vom 22.8.2014, E. 2.4.

6. Dies im Gegensatz zum Information Request gemäss Art. 32 lit. b CCC, der zumindest dann keine Zwangsmassnahme darstellt, wenn lediglich Registrierungsdaten («Subscriber Data») erhoben werden sollen. Solche Abklärungen («Auskünfte») sind nicht mit Überwachungen zu verwechseln, stellen nach Schweizer Recht keine Zwangsmassnahmen dar und liegen daher auch im Kompetenzbereich der Polizeien. Vgl. Art. 15 Abs. 1 lit. b BÜPF, Art. 26 VÜPF, Art. 35 ff. VÜPF. Ein Preservation Request wird in der Schweiz meist mittels Editionsverfügung (Art. 265 StPO) umgesetzt werden. Auch dies spricht für die Qualifikation als Zwangsmassnahme. Editionsverfügungen sind als Zwangsmassnahmen zu betrachten (BSK-StPO-Bommer/Goldschmid, Art. 265 StPO, N 1a; anders indes BGer 1S.4/2006 vom 16.5.2006 E. 1.3-1.4). Dies leuchtet ein, weil damit das Grundrecht der informationellen Selbstbestimmung tangiert wird (Art. 13 BV i.V.m. Art. 196 StPO).

7. Vgl. bspw. BGer 6B_307/2012 vom 14.2.2013 E. 1.5; E. 1.5; BGer 1B_519/2017 vom 27.3.2018 E. 3.7.

leisten, wenn auch nur der ersuchende Staat eine entsprechende Straftat unter Strafe stellt (Art. 29 Abs. 3 CCC). Den Vertragsstaaten steht es frei, bei der Ratifizierung einen Vorbehalt anzubringen, wonach die doppelte Strafbarkeit eine Voraussetzung sei. In diesem Fall darf der ersuchte Staat einen Preservation Request ablehnen, wenn bereits in diesem Zeitpunkt feststeht, dass die zur Sicherung angefragten Daten auf dem Wege der Rechtshilfe nicht werden herausgegeben werden können (Art. 29 Abs. 4 CCC). Von den 70 Staaten, welche die Konvention ratifizierten, haben 23 einen entsprechenden Vorbehalt angebracht, darunter die Schweiz und die Vereinigten Staaten von Amerika.⁸ Weil die USA bzw. deren Bundesstaaten keinen strafrechtlichen Tatbestand analog unserer **Ehrverletzungsdelikte** kennen, ist Rechtshilfe diesbezüglich stets ausgeschlossen und folglich wird auch kein Preservation Request akzeptiert.

- 10 Unabhängig von der Frage der doppelten Strafbarkeit, schliesst die Cybercrime Convention den Preservation Request für die politisch motivierte Strafverfolgung (Persecution) aus (Art. 29 Abs. 5 lit. a CCC), was aus Schweizer Sicht eine Selbstverständlichkeit sein dürfte. Dasselbe gilt dann, wenn die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (Ordre public) oder andere wesentliche Interessen zu beeinträchtigen (Art. 29 Abs. 5 lit. b CCC).

III. SICHERUNG UND ERHEBUNG VON DATEN IM AUSLAND

- 11 Aus Schweizer Sicht ist Art. 29 CCC vor allem für die Erhebung von Computerdaten im Ausland relevant (vgl. sogleich, N. 12 ff.). Der Artikel kommt aber ebenso bei Anfragen ausländischer Staaten an die Schweiz zur Anwendung (vgl. nachstehend, N. 31 ff.).

A. Einen Preservation Request stellen

- 12 Der Konventionstext selbst gibt eine recht detaillierte Anleitung, wie ein Preservation Request zu formulieren sei. Ausdrücklich genannt werden die folgenden Anforderungen:

1. Die ersuchende Behörde (lit. a.)

- 13 Hierbei wird es sich in der Praxis regelmässig um eine **Staatsanwaltschaft** handeln (vgl. auch vorstehend, N. 7). Aus Sicht der Konvention spricht jedoch nichts dagegen, dass – in enger Absprache mit der staatsanwaltschaftlichen Verfahrensleitung (welche später das Rechtshilfeersuchen stellen muss) – auch bereits die Polizei einen Preservation Request stellen kann.⁹ Da es um die rechtzeitige Sicherstellung volatiler Daten geht, kann dies sogar sinnvoll sein. Die Umsetzung des Preservation Requests respektive seine rechtliche Qualifikation richtet sich nach dem nationalen Recht des ersuchten Staates (Art. 25 Abs. 4 CCC¹⁰). In vielen ersuchten Staaten wird die Umsetzung des Preservation Requests (Sicherstellung von Daten am Speicherort) als Zwangsmassnahme qualifiziert werden, sodass nicht selten ein Ersuchen – oder zumindest eine (Mit-)Unterschrift – eines Staatsanwaltes verlangt wird. Die Handhabung ist insgesamt sehr uneinheitlich.

8. Die Schweiz und 22 weitere Vertragsstaaten haben einen expliziten Vorbehalt nach Art. 29 Abs. 4 (doppelte Strafbarkeit) angebracht. Die USA machten einen Vorbehalt gemäss Art. 41 (Bundesstaatsklausel), wonach die Rechtsbehelfe der Konvention nur insoweit Anwendung finden, wie es das Recht der Bundesstaaten zulässt. Vgl. Reservations and Declarations.

9. Das Cybercrime Convention Committee (T-CY) stellte bereits 2017 explizit klar, dass aus Sicht der Konvention nichts dagegen spricht, dass auch Polizeibehörden (und nicht nur justizielle Behörden wie Staatsanwaltschaften und Gerichte) Preservation Requests stellen (T-CY, Competent Authority).

10. BGE 141 IV 108 E. 4.3.8-4.3.9.

2. Die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung (lit. b.)

- 14 Hier geht es darum, dass der ersuchte Staat erkennen kann, ob die **doppelte Strafbarkeit** erfüllt ist (vgl. vorstehend, N. 9) und ob das Ersuchen, das durchaus mit erheblichem Aufwand verbunden sein kann, verhältnismässig ist (Zweck-/Mittel-Relation). Bei gängigen Phänomenen reicht aber dennoch eine Beschreibung aus zwei, drei Sätzen aus, um das Erfordernis zu erfüllen.

3. Die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat (lit. c.)

- 15 Es muss substantiiert werden, welche Daten konkret zu sichern sind (z.B. Registrierungsdaten, Logfiles/Randdaten oder gar Inhaltsdaten, falls möglich und sinnvoll auch unter Angabe der Dateiformate). Insbesondere aber soll begründet werden, *weshalb* diese Daten auch tatsächlich einen **Zusammenhang zum Tatverdacht** begründenden Sachverhalt haben. Dieses Kriterium ähnelt der sogenannten potentiellen Beweiserheblichkeit im Kontext einer inländischen Durchsuchung nach Art. 246 StPO (wonach «zu vermuten ist», dass sich in den betreffenden Aufzeichnungen Informationen befinden, die beschlagnahmt werden können); die Daten müssen hier nur, aber immerhin, «von Bedeutung sein können»¹¹ bzw. nicht «offensichtlich untauglich»¹² erscheinen. Beweisausforschungen (*Fishing Expeditions*) sind verpönt. Das Kriterium wird durchaus ernst genommen und eine sorgfältige Begründung ist angezeigt. Zu bedenken ist, dass in anderen Staaten die Kompetenz zur Sicherstellung und/oder Herausgabe von Daten nicht bei der Staatsanwaltschaft liegt, sondern durch ein Zwangsmassnahmengericht angeordnet werden muss. So muss etwa im praxisrelevanten Verkehr mit den USA das Department of Justice an ein Gericht gelangen, um die Herausgabe der Daten bei einem Dienstanbieter mittels Durchsuchungsbefehls verfügen zu lassen.¹³ Dies erfordert eine substantiierte und (je nach den Umständen) mit den wesentlichen Unterlagen (in Englisch) belegte Darstellung des Deliktsskonnexes. Die Begründungsdichte geht hier deutlich über das hinaus, was sich Schweizer Staatsanwaltschaften aus dem nationalen Strafprozessrecht gewohnt sind. Die US-amerikanischen Behörden nehmen immerhin praxisgemäss Rücksprache mit der ersuchenden Behörde, falls der Substantiierungsgrad des Ersuchens noch nicht ausreicht, und räumen die Gelegenheit ein, den Preservation Request näher zu begründen.

4. Alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standorts des Computersystems (lit. d.)

- 16 Hier dürfte in der Regel schlicht das **Unternehmen** bezeichnet werden, welchem das konkrete Adressierungselement zugeordnet ist. Also etwa Google für @gmail-Mailadressen, Meta (für Facebook, Instagram und WhatsApp) etc.¹⁴

5. Die Notwendigkeit der Sicherung (lit. e.) und die Absicht der Vertragspartei, ein Rechtshilfeersuchen zu stellen (lit. f.)

- 17 Im Ersuchen muss explizit erklärt werden, dass das Ersuchen **erforderlich** ist (im Sinne der Subsidiarität und der Verhältnismässigkeit) und es muss bekräftigt werden, dass die ersuchende Behörde willens ist, den Preservation Request mittels Rechtshilfeersuchen zu prosequieren.

11. BGE 101 IV 364 E. 2.

12. BGE 142 IV 207 E. 7.1.5.

13. T-CY, Assessment Report, S. 57.

14. Dies sind lediglich Beispiele. In der Praxis betreiben die grossen Anbieter eigene Law Enforcement Request (LERS)-Portale, auf denen die Behörden über entsprechende Masken ihre Ersuchen erfassen können.

B. Weiterleitung und Verarbeitung des Preservation Requests

- 18 Unabhängig vom Wortlaut der Cybercrime Convention, gibt es in der Praxis **zwei Wege**, auf denen ein Preservation Request gestellt werden kann beziehungsweise muss. Der typische Weg ist über das 24/7 Network gemäss Konventionstext (Art. 35 CCC). Jeder Signatarstaat hat sich verpflichtet, eine Anlaufstelle zu betreiben, welche rund um die Uhr, sieben Tage die Woche bereit ist, Preservation Requests entgegen zu nehmen. In der Schweiz übernimmt diese Rolle das Bundesamt für Justiz zusammen mit dem Bundesamt für Polizei (fedpol).
- 19 Aus Effizienzgründen (Vermeidung von Medienbrüchen, Automatisierung) sind aber viele grosse Anbieter von internetbasierten Kommunikationsdiensten dazu übergegangen, eigene Law Enforcement Request Systeme (LERS) zu betreiben, worüber die Strafverfolgungsbehörden ihre Anfragen auf standardisierte Weise direkt erfassen und den Fortschritt verfolgen können, ohne dass weitere staatliche Behörden (z.B. Bundesamt für Justiz / Departement of Justice) involviert werden müssen.¹⁵ Es ist sinnvoll und in einigen Kantonen so umgesetzt, dass eine zentrale Stelle bei der Polizei oder der Staatsanwaltschaft die Zugänge zu sämtlichen verfügbaren **LERS-Portalen** betreut, Preservation und Information Requests im Auftrag der Verfahrensleitungen stellt und administriert. So können die Erfahrungswerte im Umgang mit den verschiedenen Diensteanbietern zentral gesammelt und ausgewertet werden und Verfahrensleitungen haben kompetente Ansprechpartner, um die Erfolgsaussichten der entsprechenden Anfragen im Voraus besprechen zu können.
- 20 Alternativ haben die Strafverfolgungsbehörden die Möglichkeit, ihre Anfragen per E-Mail (verschlüsselt und authentifiziert) an das **Bundesamt für Polizei** (fedpol) zu senden. Dort werden die Ersuchen geprüft, falls nötig mittels Rückfragen ergänzt, übersetzt und an die zuständige Behörde im Ausland weitergeleitet. Allgemein wird Englisch als Sprache für Preservation Requests weltweit empfohlen.¹⁶ Die Koordinationsstelle des fedpol kann zudem angefragt werden, ob andere Schweizer Strafverfolgungsbehörden schon denselben Preservation Request gestellt haben,¹⁷ was wertvolle Rückschlüsse im Hinblick auf die Koordination laufender Ermittlungen ergeben kann (oder die Möglichkeit, ein Gerichtsstandsersuchen an den anderen Kanton zu stellen).

C. Abgrenzung zum Information Request

- 21 Was unterscheidet nun den Preservation Request vom Information Request gemäss Art. 32 lit. b CCC? Diesbezüglich sei zunächst auf die Kommentierung zu Art. 32 CCC verwiesen.¹⁸ Kurz gesagt geht es beim Information Request um die **freiwillige Herausgabe** von Daten an einen CCC-Partnerstaat direkt durch den Diensteanbieter. Die «Freiwilligkeit» bezieht sich dabei in der Praxis auf den Diensteanbieter und nur mittelbar auf den Benutzer/Kunden des Dienstes. Die Benutzer werden in ihren Nutzungsbedingungen regelmässig vorsehen, dass eine Weiterleitung von Daten an Strafverfolgungsbehörden möglich ist, im konkreten Fall werden die betroffenen Kunden nicht mehr

15. Die Möglichkeit, Preservation Requests (ebenso wie Information Requests gemäss Art. 32 lit. b CCC) direkt an die Diensteanbieter zu adressieren, ist in den USA allgemein anerkannt, weniger jedoch in europäischen Ländern (T-CY Cloud, S. 28); z.B. LERS-Google, abrufbar unter: https://lers.google.com/signup_v2/landing, zuletzt besucht am 24.1.2024; LERS-Facebook, abrufbar unter: <https://www.facebook.com/records/login/>, zuletzt besucht am 24.1.2024; LERS-WhatsApp, abrufbar unter: <https://www.whatsapp.com/records/login/>, zuletzt besucht am 24.1.2024; etc.

16. T-CY Cloud, S. 42. Die Verwendung von Englisch hilft, Verzögerungen durch Übersetzungen, Missverständnisse und unnötige Kosten zu vermeiden. Eine Verpflichtung, auf Englisch zu kommunizieren, besteht indes gemäss der Cybercrime Convention nicht.

17. Solche Abfragen mit dem Ziel, Verbindungen zu parallellaufenden Fällen zu finden, werden als «Cross Matching» bezeichnet. Deren Erkenntnisse sind umso wertvoller, da die Kantone keine Übersicht betreffend in anderen Kantonen laufende Strafverfahren haben.

18. OK-Graf, Art. 32 CCC N. 1 ff.

gefragt.¹⁹ Die Freiwilligkeit auf Seiten der Nutzer ist insofern relativ, dass ohne die Einwilligung in die Nutzungsbedingungen (und damit in die Weiterleitung von Daten an die Strafverfolgung) viele Dienste schlicht nicht nutzbar sind.

- 22 Wenngleich die Cybercrime Convention diese Einschränkung nicht kennt, kann ein Information Request gemäss dem nationalen Recht der relevanten Partnerstaaten in der Regel nur Registrierungsdaten (auch: «Bestandesdaten» oder «Subscriber Information») gemäss Art. 18 Abs. 3 lit. b CCC (z.B. Name, Geburtsdatum, Adresse, Benutzername, Rechnungsadresse, E-Mail-Adressen, IP-Adresse bei der Registrierung) umfassen und Randdaten («Traffic Data», z.B. die IP-History), aber in aller Regel **keine Inhaltsdaten** («Content Data»).20 Der Begriff Inhaltsdaten meint den Inhalt einer Kommunikation, also z.B. einer Nachricht, eines Posts, von Medien-Dateien etc. Registrierungsdaten werden mit Abstand am häufigsten abgeklärt.²¹ Oft werden Information und Preservation Requests auch zeitgleich gestellt, da unsicher ist, welche Daten die Dienstanbieter überhaupt freiwillig zur Verfügung stellen.
- 23 In der Praxis werden Information Requests sehr viel niederschwelliger gestellt, weil sich dadurch die Staatsanwaltschaft nicht zu einem Rechtshilfeersuchen verpflichtet. Ein solches ist auch nicht notwendig, weil die Herausgabe der Daten ja freiwillig erfolgt und direkt durch den Dienstanbieter beantwortet wird. Die **Kooperationsbereitschaft** der Dienstanbieter hängt stark von der Art des Delikts ab. Besonders kooperationsbereit sind die Dienste regelmässig bei Sexualdelikten, insbesondere zum Nachteil von Kindern. Problematischer sind Vermögensdelikte. Am unteren Ende der Skala finden sich die Ehrverletzungsdelikte, bei denen die Kooperation regelmässig schon am Erfordernis der doppelten Strafbarkeit scheitert (vgl. vorstehend, N. 9 und N. 14).

D. Prosequierung mittels Rechtshilfeersuchen

- 24 Wie bereits mehrfach erwähnt und auch im Konventionstext explizit festgehalten, verpflichtet sich die Staatsanwaltschaft mit dem Preservation Request dazu, die sichergestellten Daten auf dem Rechtshilfeweg anzufragen. Sicherlich gibt es Fälle, wo sich im Nachhinein herausstellt, dass zunächst gesicherte Daten unterdessen obsolet wurden. Auch hat der **Verzicht auf ein Rechtshilfeersuchen** keine direkten Konsequenzen (es entstehen z.B. keine Kostenfolgen). Es wird aber allgemein erwartet, dass Staatsanwaltschaften sich an diese konventionsrechtliche Verpflichtung halten, um die gute Zusammenarbeit unter Konventionsstaaten nicht zu gefährden.²²
- 25 Die Sicherstellung der Daten erfolgt für **mindestens 60 Tage** (vgl. Art. 29 Abs. 7 CCC). Die konkrete Dauer wird in der schriftlichen Bestätigung des Preservation Request angegeben und ist in der Regel länger. Die ersuchende Behörde kann meist auch ein Ersuchen um Fristerstreckung stellen. Innert der Frist muss das Rechtshilfeersuchen formell gestellt werden.

E. Best Practices für Rechtshilfeersuchen an die USA

- 26 Aufgrund der grossen praktischen Bedeutung wird nachfolgend auf die Best Practices für Rechtshilfeersuchen an die USA eingegangen. Die folgenden Ausführungen beruhen auf dem

19. Ohne die Einwilligung des Nutzers läge eine rechtswidrige, weil datenschutzwidrige, Beweiserhebung vor, die aber bei schweren Delikten gestützt auf Art. 141 Abs. 2 StPO bei entsprechender Güterabwägung dennoch verwertbar sein kann.

20. Eine Ausnahme bildet offenbar Armenien, das Verbindungsranddaten (keine Inhaltsdaten) ohne Rechtshilfeersuchen zur Verfügung stellen kann. Bis zu einem gewissen Grad offenbar auch Australien (Vgl. T-CY, Assessment Report, S. 8).

21. T-CY, Assessment Report, S. 5.

22. US-Dienstleister monieren, dass in zu vielen Fällen nach einem Preservation Request kein Rechtshilfeersuchen folge (T-CY, Cloud, S. 28).

«Practical Guide for Requesting Electronic Evidence Across Borders», herausgegeben von UNODC, CTED und IAP, sowie auf eigenen Erfahrungen.

- 27 An ausländische Behörden gerichtete Rechtshilfeersuchen in Cybercrime-Fällen müssen folgende Angaben enthalten:
- Sprache des Ersuchens: Rechtshilfeersuchen sind idealerweise direkt in Englisch zu erfassen, andernfalls übersetzen zu lassen;
 - Sachverhalt: ist unter Angabe des Tatortes (resp. Erfolgsortes), der genauen Tatzeit und der Art der Tatbegehung kurz aber in wesentlichen Zügen darzustellen;
 - Allfälliger Modus Operandi: ist detailliert zu schildern;
 - Rechtliche Bezeichnung der Tat, inkl. anwendbare Gesetzesartikel im Wortlaut;
 - Gründe des Ersuchens, wobei insbesondere der Zusammenhang zwischen dem geführten Verfahren und den verlangten Massnahmen aufzuzeigen ist;
 - Die gesuchten Beweise oder verlangten Handlungen sind genau zu bezeichnen (bspw. Herausgabe der Kontoauszüge betreffend Konto X für den Zeitraum A bis B, Einholung von Unterlagen beim Provider Y, woraus zum Remote ID 12345678 für die Zeit zwischen A und B die Registrierungsdaten sowie die Logfiles ersichtlich sind usw.);
 - Ausführungen zum allfällig bereits gestellten Preservation Request, wobei sämtliche im Anschluss an den Preservation Request mitgeteilten Referenznummern im Ersuchen auszuführen sind (CCIPS sowie Referenznummern des fedpol, der ersuchten ausländischen Polizeibehörde und der ersuchten ausländischen Staatsanwaltschaft).
- 28 Zur Erhältlichmachung von Inhaltsdaten von US-Diensteanbietern muss das Department of Justice einen Durchsuchungsbefehl nach US-Recht bei einem Gericht erwirken. Die Hürde des Beweismasses ist «*probable cause*». Dies bedeutet, dass das Gericht überzeugt werden muss, dass das betreffende Nutzerkonto wahrscheinlich immer noch deliktsrelevante Beweise enthält (es sei denn, die Daten seien gestützt auf einen Preservation Request bereits vorläufig sichergestellt worden). Erforderlich ist weiter ein belastbares Beweisfundament für die Annahme, dass eine Straftat begangen wurde oder wird und dass die Beweise für die Straftat sich im verlangten Benutzerkonto finden werden. Die Quellen der vorgelegten Indizien müssen vertrauenswürdig sein (z.B. Polizeirapporte, vertrauenswürdige private Quellen). Zentrale Indizien sollten vorgelegt werden. Falls Indizien vorgelegt werden, müssen sie auf Englisch übersetzt werden. Zusammengefasst muss erläutert werden, wieso der Kontoinhaber ein Ziel der Ermittlungen ist, weshalb man davon ausgeht, das fragliche Nutzerkonto gehöre dieser Person, und welche Beweismittel man sich von diesem Nutzerkonto erhofft.
- 29 Das Rechtshilfeersuchen ist entweder auf dem diplomatischen Weg über das Bundesamt für Justiz oder – wenn vereinbart und vorgesehen – auf direktem Übermittlungsweg an die Staatsanwaltschaft im Ausland zuzustellen. Der Rechtshilfeführer des Bundesamts für Justiz enthält nähere Angaben zu den konkreten Übermittlungswegen.
- 30 Merke:
- Bei Rechtshilfeersuchen in Cybercrime-Fällen ist als Rechtsgrundlage zusätzlich die CCC einzutragen (sofern das Zielland die Konvention ratifiziert hat).
 - Die Darstellung des Sachverhalts, die Subsumtion des Sachverhalts unter die Straftatbestände sowie das Aufzeigen der Gründe des Ersuchens sind das A und O eines Ersuchens um internationalen Rechtshilfe.

- Detaillierte Angaben zur Rechtshilfe sind im Rechtshilfeführer des Bundesamts für Justiz zu finden, mit Mustern in verschiedenen Sprachen und einem Länderindex.
- Ein Rechtshilfeersuchen nach einem gestellten Preservation Request hat sobald als möglich, spätestens innert der Prosequierungsfrist (Art. 29 Abs. 7 CCC), zu erfolgen.

IV. AUSFÜHREN VON PRESERVATION REQUESTS DURCH SCHWEIZER BEHÖRDEN

A. Verfahrensablauf und Zuständigkeiten

- 31 Alle Staaten, welche die Cybercrime Convention ratifiziert haben, gaben an, welche ihrer Behörden als zentrale Anlaufstelle für ersuchende Staaten fungiert («24/7 network»,²³ Art. 35 CCC). Gemäss Erklärung der Schweiz ist dies primär das Bundesamt für Justiz.²⁴ Für Belange der Cybercrime Convention, insbesondere für Preservation Requests, ist jedoch die Bundeskriminalpolizei (fedpol) zuständig (das Bundesamt für Justiz leitet diesbezügliche Anfragen an das fedpol weiter). Fedpol erhält pro Jahr gegen **200 Anfragen**²⁵ aus dem Ausland, die es wiederum zur Verarbeitung an die kantonalen Polizeikörpers weiterleitet.

B. Umsetzung mittels Schweizer Recht

- 32 Der Prozess, wie ein ausländischer Preservation Request in der Schweiz verarbeitet wird, ist **nicht gesetzlich geregelt**. Bemerkenswert ist, wie wenig die Botschaft zur Umsetzung der Cybercrime Convention sich mit verfahrensrechtlichen und praktischen Fragen auseinandersetzte.²⁶ Erwähnt wird lediglich, dass die Vertragsstaaten nicht verpflichtet sind, nebst der Beschlagnahme und Edition weitere rechtliche Instrumente zu schaffen.²⁷
- 33 Das Schweizer Strafprozessrecht kennt **keine «Preservation Orders»** im Sinne der Cybercrime Convention.²⁸ Ein Preservation Order wäre eine behördliche Verfügung an einen Dienstanbieter, Daten für einen gewissen Zeitraum zur Verfügung zu halten (typischerweise im Sinne eines Back Ups). Da dieses Instrument in der Strafprozessordnung nicht vorgesehen ist, muss die langfristige Verfügbarkeit der Daten anderweitig sichergestellt werden, was sinnvollerweise nur mittels Edition (Art. 265 StPO) geschehen kann. Da die Kantonspolizeien keine Kompetenzen haben, Daten zu edieren, müssen diese die entsprechenden Ersuchen, welche sie von fedpol erhalten, ihrerseits an die zuständige Staatsanwaltschaft weiterleiten, welche schliesslich eine Editionsverfügung erlässt. Während die Strafprozessordnung keine Grundlage für Preservation Orders kennt, wurde die gesetzlich vorgeschriebene Vorratsdatenspeicherung im Fernmeldebereich auf vergleichbare Weise umgesetzt. So sind es die Fernmeldedienstanbieter selbst, welche die Registrierungs- und

23. CoE 24/7 Network.

24. Erklärung zu Art. 27 Abs. 9: Die Schweiz erklärt, dass das Bundesamt für Justiz des Eidgenössischen Justiz- und Polizeidepartements, 3003 Bern, in dringenden Fällen im Sinne von Artikel 27 Absatz 9 die zentrale Behörde darstellt, an welche alle Rechtshilfeersuchen an die Schweiz zu richten sind.

25. Gemäss *ad hoc* Auskunft von fedpol auf Anfrage vom November 2023. Die Anfragen an die Schweiz nehmen ständig zu. Dies, weil mehrere Anbieter für verschlüsselte Kommunikation (z.B. Protonmail, Threema) ihren Sitz (und ihre Server) in der Schweiz haben (T-CY, Benefits, S. 18).

26. Vgl. BBl 2010 4718.

27. Damit ist die Schweiz in guter Gesellschaft: Rund 58% der Staaten haben kein spezifisches Cyber-Strafprozessrecht geschaffen (T-CY, Benefits, S. 6).

28. Auch wenn der Begriff «Preservation Request» aufgrund seiner Geläufigkeit in der IT-Branche mitunter auch in Editionsverfügungen zu lesen ist. Vgl. z.B. OGer NW BAS 21 3 vom 27.5.2021 E. A.

Kommunikationsranddaten ihrer Kunden für die Dauer von 6 Monaten für die Strafverfolgungsbehörden vorhalten müssen (Art. 21 Abs. 2, Art. 22 Abs. 2 und Art. 26 Abs. 5 BÜPF).²⁹

- 34 Diese schweizerische Ausgestaltung des Preservation Requests gemäss Art. 29 CCC ist relativ weit vom Geist der Konvention entfernt, die eine rasche, unkomplizierte und mit möglichst geringen Einschränkungen für alle Beteiligten verbundene Massnahme wollte. Der soeben dargelegte Prozess involviert mindestens drei Behörden und die adressierte Unternehmung, also zahlreiche Schnittstellen, was zu Verzögerungen führt und zwangsläufig die Fehleranfälligkeit erhöht. Eine Editionsverfügung, verbunden mit physischer oder digitaler Auslieferung und Aufbewahrung von – unter Umständen sehr erheblichen – Datenmengen bedeutet zudem einen **erheblichen Aufwand** für Dienstanbieter und die für die Datenvorhaltung verantwortlichen Behörden. International wird diskutiert, ob Staaten, welche keine Preservation Orders im Sinne der Konvention eingeführt haben und sich stattdessen mit Editionsverfügungen behelfen (wie die Schweiz), die Anforderungen der Konvention überhaupt erfüllen. Zwar wird dies offenbar mehrheitlich bejaht, dennoch bleiben Kritikpunkte, namentlich betreffend höhere juristische Hürden (nicht in der Schweiz), längere Verfahrensdauer und die möglicherweise erhöhte Gefahr, dass die betroffenen Personen von der Massnahme erfahren, was den Untersuchungszweck vereiteln kann.³⁰
- 35 Die Ausführung ausländischer Preservation Requests im Inland ist noch nicht Teil eines formellen Rechtshilfeverfahren und auch keine vorsorgliche Massnahme gemäss IRSG (oder anderer Grundlagen des Rechtshilfeverfahrens). Sie ist einem allfälligen Rechtshilfeverfahren vorgelagert. Faktisch dürfte längst nicht auf jeden Preservation Request auch ein formelles Rechtshilfeersuchen folgen. Der Preservation Request findet seine Grundlage in der Cybercrime Convention selbst (die, soweit hinreichend konkret, im monistischen System der Schweiz direkt anwendbar ist³¹). Die hiesige Ausführung des Preservation Requests ist nicht hinreichend bestimmt, weshalb – wie oben erwähnt – auf die Rechtsinstitute des nationalen Strafprozessrechts zurückgegriffen werden muss, also auf die Strafprozessordnung (z.B. Art. 265 StPO, Edition) sowie auf das BÜPF und dessen Verordnungen (z.B. Art. 38 VÜPF, IR_8_IP (NAT): Inhaber von IP-Adressen). Dies, immer mit dem Ziel, dem Geist der Cybercrime Convention (rasche, unkomplizierte, effektive Verhinderung des Beweisverlustes) so gut wie möglich nachzuleben. Dies bedeutet auch, dass Editionsverfügungen, die zur Ausführung eines Preservation Requests ergehen, mit einem **Mitteilungsverbot** an die Editionsadressatin zu versehen sind, um den Ermittlungserfolg nicht zu gefährden (Art. 29 Abs. 6 CCC; Art. 73 Abs. 2 StPO i.V.m. Art. 292 StGB; vgl. analog auch Art. 11b Abs. 2 lit. c IRSG und Art. 80b Abs. 2 lit. a IRSG). Die Konsequenz daraus ist, dass die Betroffenen gegen die Edition selbst im Zeitpunkt der Ausführung mangels Kenntnis noch kein Rechtsmittel ergreifen können. Sobald (falls) ein formelles Rechtshilfeverfahren eröffnet wird, sind die Dateninhaber (die betroffenen Kunden des Dienstes) über ihr Siegelungsrecht zu unterrichten (Art. 9 IRSG i.V.m. Art. 248 Abs. 2 StPO).³² Geht hingegen innert Frist von 60 Tagen gemäss Art. 29 Abs. 7 CCC und allfälliger Ermahnung/Nachfristansetzung kein Rechtshilfeersuchen ein, sind die Daten mangels Rechtsgrundlage für eine längere Aufbewahrung unwiderruflich zu löschen.
- 36 Der Dienstanbieter selbst hat gemäss der aktuellen Rechtslage bei der Edition als Gewahrsamsinhaber der Daten ein eigenes Siegelungsrecht (vgl. Art. 248 Abs. 1 StPO).³³ Eine Siegelung bereits durch den **Dienstanbieter** könnte jedoch zu sinnlosem Aufwand führen, nämlich dann, wenn ein aufwändiges Entsiegelungsverfahren durchgeführt werden muss und der ersuchende Staat anschliessend auf das

29. Vgl. dazu die Botschaft zur Umsetzung der Cybercrime Convention, BBl 2010 4718.

30. Vgl. T-CY, Preservation Assessment, S. 4.

31. BGE 138 II 42 E. 3.1.

32. Vgl. Graf, Rz. 142.

33. BGE 140 IV 28 E. 3.2.

Rechtshilfeverfahren verzichtet.³⁴ Hinzu kommt, dass durch die Edition oftmals keine eigenen Geheimnissinteressen des Dienstanbieters tangiert werden. Dies wäre aber Voraussetzung für einen gültigen Siegelungsantrag, denn es kann nicht stellvertretend für eine Drittperson (etwa die Account-Inhaberin) die Siegelung verlangt werden.³⁵ Werden Daten von Diensteanbietern erhoben, bei denen aufgrund der Natur ihres Dienstes regelmässig mit geheimnisgeschützten Daten zu rechnen ist, stellt sich andererseits die Frage, ob die Staatsanwaltschaft, welche den Preservation Request ausführt (die Editionsverfügung erlässt), nicht schon von Amtes wegen im Zeitpunkt der Edition eine Siegelung vornehmen müsste.³⁶ In beiden Fällen müsste die Staatsanwaltschaft aber, um den Preservation Request auszuführen, innert 20 Tagen ein Entsiegelungsersuchen stellen (Art. 248 Abs. 3 StPO), dies in einem Zeitpunkt, in dem der Dateninhaber noch nichts vom Preservation Request wissen sollte und folglich sinnvollerweise nicht in das Entsiegelungsverfahren einzubeziehen wäre (ganz abgesehen davon, dass er regelmässig in der Schweiz kein Zustelldomizil haben wird).

- 37 Um den Ermittlungserfolg nicht zu gefährden und unnötige Leerläufe zu verhindern, wäre daher die einzige für den Kontext der Cybercrime Convention stimmige Vorgehensweise, wenn die Siegelung/Entsiegelung erst im Rahmen des formellen Rechtshilfeverfahrens zur Anwendung käme.³⁷ In jedem Fall kann eine Siegelung erst möglich sein, wenn die Datenerhebung als solche abgeschlossen ist. Zu denken ist etwa an Datenerhebungen, die auf einen einzigen Preservation Request zurückgehen, aber im Inland mehrere aufeinander aufbauende Schritte erfordern, zum Beispiel mehrere Auskunftersuchen an den Dienst ÜPF (1. Ermittlung Adressierungselement anhand IP-Adresse, 2. Ermittlung Anschlussinhaber anhand Adressierungselement).
- 38 Es stellt sich die Frage, ob es nach Schweizer Recht zulässig wäre, Diensteanbieter auch ausserhalb des Anwendungsbereichs des BÜPF, anstelle der Herausgabe, zur blossen Vorhaltung bestimmter Daten zu verpflichten.³⁸ Dies würde viele der zuvor andiskutierten Probleme mit der Edition entschärfen und wäre daher zu befürworten. Eine echte **Effizienzsteigerung** liesse sich aber vor allem erreichen, wenn der Vollzug der ausländischen Preservation Requests auf Stufe Bund (fedpol) zentralisiert würde, wofür jedoch aktuell in der Strafprozessordnung keine Grundlage existiert (vgl. Art. 22 ff. StPO *e contrario*). Eine vergleichbare Rechtsgrundlage findet sich hingegen heute schon in Art. 18 Abs. 2 IRSG, wonach das Bundesamt für Justiz selbst vorsorgliche Sicherungsmassnahmen verfügen kann, wenn Gefahr im Verzug ist.

34. Angesichts der nach wie vor langen Dauer von Entsiegelungsverfahren und der relativ kurzen Frist an ausländische Staaten zur Stellung des Rechtshilfeersuchens (60 Tage) ist diese Gefahr aber zugegebenermassen gering.

35. BGer 1B_243/2021 vom 20.12.2021, E. 3.6.

36. Ähnlich BSK-StPO-Thormann/Brechbühl, Art. 248 StPO, N 14. Dies ist gerechtfertigt, zumal die Betroffenen sich regelmässig im Ausland befinden dürften, die hiesige Rechtsordnung nicht kennen, nicht anwaltlich vertreten sein dürften und somit Gefahr laufen, ihr Siegelungsrecht zu verwirken. Die Effizienz in der Strafverfolgung sollte aber nicht durch dadurch gefördert werden, dass gesetzlich vorgesehene Rechte verwirken, sondern durch die operative Straffung der Prozesse bei den beteiligten Akteuren.

37. Was von der Logik her der Regelung gemäss IRSG entspricht, welche dem internationalen Kontext Rechnung trägt (Vgl. Art. 80e IRSG [grundsätzlich nur Anfechtung der Schlussverfügung]; Art. 11b Abs. 2 lit. c IRSG und Art. 80b Abs. 2 lit. a IRSG [kein Einbezug der Betroffenen, falls dies den Untersuchungszweck gefährdet]). Diese Bestimmungen wären analog anzuwenden, respektive Art. 248 Abs. 1 StPO wäre im Kontext des Preservation Requests teleologisch zu reduzieren, um dem Sinn und Zweck der Cyber Crime Convention zu entsprechen.

38. Das Argument wäre, dass wenn ein Diensteanbieter zur Herausgabe aufgefordert werden kann, es *a maiore ad minus* auch möglich sein muss, ihn die Daten bloss vorhalten zu lassen (Backup) – was für den Diensteanbieter in aller Regel bedeutend einfacher sein dürfte, weil in den internen Prozessen schon etabliert und der Handwechsel (verbunden mit der Handhabung physischer Datenträger) an die Behörden wegfällt. Auch die Löschung ist einfacher.

LITERATURVERZEICHNIS

Bommer Felix/Goldschmid Peter, Kommentierung zu Art. 265 StPO, in: Niggli Heer/Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung, Strafprozessrecht I + II, 3. Aufl., Basel 2023.

Graf Damian K., Praxishandbuch zur Siegelung, StPO inkl. revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022.

Thormann Oliver/Brechbühl Beat, Kommentierung zu Art. 248 StPO, in: Niggli Heer/Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung, Strafprozessrecht I + II, 3. Aufl., Basel 2023.

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 24.1.2024.

Council of Europe, The 24/7 Network established under the Convention on Cybercrime (known as the Budapest Convention), What is the 24/7 Network?, abrufbar unter: <https://www.coe.int/en/web/cybercrime/24/7-network-new->, zuletzt besucht am 24.1.2024 (zit. CoE 24/7).

Cybercrime Convention Committee (T-CY), Assessment report, Implementation of the preservation provisions of the Budapest Convention on Cybercrime, Supplementary report, 15/16.06.2015, abrufbar unter: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b>, zuletzt besucht am 24.1.2024 (zit. T-CY, Preservation Assessment).

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, 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), 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).

Opinion of the T-CY on the competent authority for issuing a preservation request under Articles 29 and 35 Budapest Convention, 28.11.2017, abrufbar unter: <https://rm.coe.int/t-cy-2017-18-opinion-article29-/168076cf95>, zuletzt besucht am: 19.1.2024 (zit. T-CY, Competent Authority).

Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185), Status as of 09/03/2024, abrufbar unter: <https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0>, besucht am 9.3.2024 (zit. Reservations and Declarations).

United Nations Office on Drugs and Crime (UNDOC), Sharing Electronic Resources and Laws on Crime (SHERLOC), The Practical Guide for Requesting Electronic Evidence across Borders, für Strafbehörden abrufbar unter: <https://sherloc.unodc.org/cld/en/st/evidence/practical-guide.html>, besucht am 27.09.2023, zuletzt besucht am 24.01.2024 (zit. Practical Guide for Requesting Evidence).