



ONLINEKOMMENTAR
DER FREI ZUGÄNLICHE
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

Art. 16 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Ugur Gürbüz
Herausgegeben von Damian K. Graf

Stand der Bearbeitung: 15.07.2025

PDF erstellt am: 06.10.2026

DOI: 10.17176/20250715-185545-0

ZITIERVORSCHLAG

Ugur Gürbüz, Kommentierung zu Art. 16 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Gürbüz, Art. 16 CCC N. XXX.

Titel 2: Umgehende Sicherung gespeicherter Computerdaten

Art. 16 Umgehende Sicherung gespeicherter Computerdaten

¹ Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, damit ihre zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten einschliesslich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.

² Führt eine Vertragspartei Absatz 1 so durch, dass eine Person im Wege einer Anordnung aufgefordert wird, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden, sicherzustellen, so trifft diese Vertragspartei die erforderlichen gesetzgeberischen und anderen Massnahmen, um diese Person zu verpflichten, die Unversehrtheit dieser Computerdaten so lange wie notwendig, längstens aber 90 Tage, zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschliessend verlängert werden kann.

³ Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um den Verwahrer oder eine andere Person, welche die Computerdaten zu sichern hat, zu verpflichten, die Durchführung dieser Verfahren für den nach ihrem innerstaatlichen Recht vorgesehenen Zeitraum vertraulich zu behandeln.

⁴ Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

GLIEDERUNG

I. Einleitung	4
II. Anwendungsbereich und Ziele	4
A. Absatz 1: Umgehende Sicherung von Computerdaten	4
B. Absatz 2: Sicherung von Daten mittels Anordnung auf Aufbewahrung	5
C. Absatz 3: Geheimhaltungspflicht.....	6
D. Absatz 4.....	6
III. Umsetzung in der Schweiz	6
A. Sicherung durch Strafverfolgungsbehörden	7
B. Sicherungsaufforderung an Personen.....	7
C. Fehlende Gesetzesbestimmung betreffend Anordnung auf Aufbewahrung.....	8
D. Durch das Bundesgericht ausgebremsste Sicherung bei gültigem Siegelungsantrag	9
Literaturverzeichnis.....	10
Materialienverzeichnis	10

I. EINLEITUNG

- 1 Dass professionell agierende und fachkundige Cyberkriminelle für ihre illegalen Zwecke zunehmend neueste Technologien und das Internet nutzen, stellt die Behörden vor zunehmende Herausforderungen. Die technischen Missbrauchsmöglichkeiten garantieren aber keine dauerhafte und absolute Sicherheit für Kriminelle, solange Behörden gezielt handeln. Denn **auf Datenträgern und im Internet werden Spuren hinterlassen**: Jede Aktion, die online ausgeführt wird, beispielsweise das Besuchen einer Webseite, das Posten in den sozialen Medien oder das Online-Einkaufen, erzeugt Daten, die gespeichert werden und nachverfolgt werden können. Durch die Erstellung von Images im Falle von sichergestellten Datenträgern können gelöschte und nicht überschriebene Daten wiederhergestellt werden. Solche auch nur kurzzeitig und vorübergehend gespeicherte Daten können für Strafverfolgungsbehörden zur Ermittlung der Täterschaft, Aufklärung von Straftaten oder Durchführung von Überwachungsmassnahmen nützlich sein, solange sie rechtzeitig gesichert werden.
- 2 Ob **Computerdaten gespeichert** wurden und zum Zeitpunkt der laufenden Ermittlungen noch **vorhanden sind**, hängt einerseits vom Löschverhalten des Dateninhabers und andererseits von den Datenschutzbestimmungen des jeweiligen Vertragsstaates ab.

II. ANWENDUNGSBEREICH UND ZIELE

- 3 Computerdaten sind wegen ihrer Flüchtigkeit einfach zu manipulieren, zu verändern und zu löschen. Das Risiko von Datenverlust oder Vernichtung von Daten ist in der Praxis folglich hoch. Um die Sicherung von solchen Computerdaten sowie von Verbindungsdaten in inländischen Strafverfahren nicht von langwierigen Beweiserhebungsprozessen abhängig zu machen, sondern durch rasche und effektive Massnahmen die Löschung und Veränderung von beweisrelevanten Daten rechtzeitig mittels einer Sicherungsanordnung zu verhindern und dadurch die Effektivität der Verfolgung der in der Cybercrime-Konvention näher umschriebenen Straftaten zu steigern, haben sich die Vertragsstaaten verpflichtet, innerstaatlich die notwendigen legislativen Massnahmen zu ergreifen. Das Verfahren, gespeicherte Computerdaten umgehend und rechtzeitig zu sichern, wird in der Praxis als «**Quick-Freeze-Verfahren**» bezeichnet. Nicht zu verwechseln ist das Quick-Freeze-Verfahren mit der unverzüglichen Sicherung von Daten im grenzüberschreitenden Kontext, dem sogenannten Preservation Request, der in Art. 29 CCC geregelt ist.
- 4 Art. 16 CCC regelt die **unverzügliche Sicherung von Daten**, berechtigt aber die Vertragsstaaten nicht per se, die Herausgabe der Daten anzuordnen oder deren Inhalt einzusehen, solange keine innerstaatliche Befugnisnorm dies ausdrücklich gestattet. Die Herausgabe der Daten wird in Art. 18 CCC geregelt, während die Durchsuchung und Beschlagnahme in Art. 19 CCC behandelt werden.

A. Absatz 1: Umgehende Sicherung von Computerdaten

- 5 Art. 16 Abs. 1 CCC gewährleistet die rasche Sicherung von Computerdaten innerhalb eines Vertragsstaates, um der Verdunklungsgefahr aufgrund der Flüchtigkeit von Computerdaten entgegenzuwirken. Daten sollen geschützt werden *«from anything that would cause its current quality or condition to change or deteriorate»*¹ und somit umfassend vor Veränderungen, Verschlechterungen oder Löschungen. Mit Sicherung wird die **vorläufige Aufbewahrung von Daten** bezeichnet und nicht die Verweigerung des Zugriffs auf die Daten. Rechtmässige Nutzer sollen die Daten resp. Kopien

1. Explanatory Report, Rz. 159.

davon weiterhin nutzen können,² solange sie nicht sinngemäss Art. 19 CCC beschlagnahmt werden müssen.

- 6 Art. 16 CCC verpflichtet die Vertragsstaaten weder dazu, das Angebot oder die Nutzung von Diensten einzuschränken, noch neue technische Möglichkeiten zur Aufbewahrung und Erhebung von Daten einzuführen. Die Bestimmung führt somit nicht zu einer Pflicht zur Vorratsdatenspeicherung. Sie soll lediglich sicherstellen, dass Vertragsstaaten auf nationaler Ebene eine **beschleunigte Sicherung** gespeicherter Computerdaten veranlassen können, um sich auf internationaler Ebene gegenseitig zu unterstützen.³
- 7 Die konkrete **Ausgestaltung** der Sicherungen wird den Vertragsparteien überlassen. In der Praxis kommen als Sicherungsmethoden zwei Optionen in Frage: die Sicherung der Originaldaten und die Erstellung identischer Datenkopien.
- 8 Gemäss dem Wortlaut von Art. 16 Abs. 1 CCC betrifft die Sicherung *«bestimmte Computerdaten einschliesslich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden»*. Erfasst werden alle Arten von Computerdaten, die bereits von den Dateneinhabern oder Diensteanbietern erhoben wurden⁴ und gespeichert sind, sogenannte **«stored computer data»**. Explizit genannt werden auch Verbindungs- und Verkehrsdaten, sog. *«traffic data»*.⁵ Der Verweis auf Verkehrsdaten dient dazu, eine Verbindung zwischen den Massnahmen in Art. 16 und Art. 17 CCC herzustellen.⁶ Für Verkehrsdaten sieht die letztgenannte Bestimmung gewisse Besonderheiten vor. Nicht erfasst sind zukunftsgerichtete Echtzeit-Erhebungen von Computerdaten sowie Vorratsdatenspeicherungen, sogenannte *«data retention»*. Diese sind in den Art. 20 und Art. 21 CCC geregelt.
- 9 Die Sicherung kann entweder angeordnet oder in ähnlicher Weise bewirkt werden.
 - a) Unter **«Anordnen»** fällt sowohl die gerichtliche oder behördliche Anordnung zur Sicherung von Daten als auch die Verpflichtung eines Anordnungsadressaten zur aktiven Mitwirkung. Letztere soll dadurch erfolgen, indem der Anordnungsadressat die Daten unverändert und verlustfrei sichert (vgl. dazu Art. 16 Abs. 2 CCC).
 - b) Die Formulierung **«oder in ähnlicher Weise bewirken»** ermöglicht es den Vertragsstaaten, die Sicherung von Daten entsprechend ihrem Verfahrensrecht flexibel und mit eigenen Mitteln zu gestalten.
- 10 Sicherungsmassnahmen sollten von den Vertragsstaaten insbesondere dann festgelegt werden, wenn es Grund zur Annahme gibt, dass Computerdaten besonders **anfällig für Verlust oder Veränderung** sind. Dies kann sich etwa auf Situationen beziehen, in denen die Daten gestützt auf die Geschäftspolitik einer kurzen Aufbewahrungsfrist unterliegen, in regelmässigen Abständen gelöscht oder auf unsichere Weise gespeichert werden.⁷

B. Absatz 2: Sicherung von Daten mittels Anordnung auf Aufbewahrung

- 11 Art. 16 Abs. 2 CCC legt fest, dass in Fällen, in denen Computerdaten gemäss Art. 16 Abs. 1 CCC durch Anordnung gegenüber einer anderen Person gesichert werden, die Vertragsstaaten Massnahmen ergreifen und **«Preservation Orders»** einführen können, um die Unversehrtheit dieser

2. Explanatory Report, Rz. 159.

3. Explanatory Report, Rz. 157.

4. Explanatory Report, Rz. 158.

5. Explanatory Report, Rz. 158.

6. Explanatory Report, Rz. 161.

7. Explanatory Report, Rz. 161.

Computerdaten für eine begrenzte Zeit sicherzustellen. Eine Verpflichtung zu solchen Massnahmen besteht für Vertragsstaaten jedoch nicht.⁸ Vertragsstaaten müssen sicherstellen, dass ihre Untersuchungsbehörden – unabhängig vom gewählten Verfahren – die umgehende/sofortige Sicherung anordnen oder bewirken können.

- 12 Als **Anordnungsadressaten** gelten Personen, die entweder im Besitz von gespeicherten Computerdaten sind oder die Verfügungsgewalt über die Daten haben.
- 13 Die Vertragsstaaten können im innerstaatlichen Recht als Massnahme im Sinne von Art. 16 Abs. 2 CCC die Anordnungsadressaten verpflichten, so lange wie erforderlich, jedoch höchstens für 90 Tage, die Unversehrtheit jener Computerdaten zu erhalten, die Gegenstand der Anordnung bilden. Sie können aber auch eine Verlängerung dieser **Aufbewahrungsfrist** vorsehen. Die Fristansetzung als Massnahme dient dazu, den zuständigen Behörden ausreichend Zeit für die Einholung der erforderlichen Berechtigungen sowie das Einleiten rechtlicher Schritte wie bspw. Durchsuchung, Beschlagnahme, Sicherstellung, Erlass einer Herausgabeeanordnung zu gewähren, damit sie anschliessend in einem zweiten Schritt Kenntnis vom Inhalt der Daten erhalten, insbesondere auch im Rahmen einer Rechtshilfe im Sinne von Art. 29 CCC.⁹

C. Absatz 3: Geheimhaltungspflicht

- 14 Art. 16 Abs. 3 CCC verlangt von den Vertragsstaaten, die erforderlichen gesetzgeberischen Massnahmen zu treffen, um bei einer Anordnung, die sich an den **Verwahrer oder an einen Dritten richtet**, diese für einen im innerstaatlichen Recht festgelegten Zeitraum zur vertraulichen Durchführung der Datensicherung zu verpflichten. Diese Massnahme berücksichtigt einerseits die Erfordernisse der Strafverfolgungsbehörde, dass Verdächtige und Dritte nicht von den Ermittlungen erfahren können, andererseits schützt sie die Privatsphäre betroffener Personen, insbesondere solcher, die in den Daten erwähnt werden oder identifizierbar sind.¹⁰

D. Absatz 4

- 15 Durch die **Verweise** in Art. 16 Abs. 4 CCC verpflichten sich die Vertragsstaaten dazu, sicherzustellen, dass die in den Art. 16 CCC genannten Befugnisse und Verfahren den in den Art. 14 und Art. 15 CCC festgelegten Bedingungen und Garantien unterliegen.

III. UMSETZUNG IN DER SCHWEIZ

- 16 Die Sicherung gespeicherter Computerdaten gemäss Art. 16 CCC stellt ein wichtiges **Ermittlungsinstrument** zur Bekämpfung von Computer- und IT-bezogenen Straftaten dar. Die Vertragsstaaten – einschliesslich der Schweiz – sind verpflichtet, die hierfür erforderlichen gesetzgeberischen und organisatorischen Rahmenbedingungen zu schaffen.
- 17 Die Schweiz hat das in Art. 16 CCC vorgesehene «Quick-Freeze-Verfahren» nicht als eigenständige Massnahme in die geltende Schweizerische Strafprozessordnung aufgenommen. Stattdessen kommt das **Schweizer Recht** den Vorgaben von Art. 16 CCC im Allgemeinen bereits dadurch nach, indem **Anbieter von Fernmeldediensten** verpflichtet sind, einerseits **gemäss Art. 21 Abs. 2 und Art. 22 Abs. 2 BÜPF** sicherzustellen, dass bei Aufnahme der Kundenbeziehung Identifikationsdaten erhoben werden und diese während der gesamten Kundenbeziehung sowie bis sechs Monate nach deren

8. Vgl. dazu BBl 2010 4718.

9. Explanatory Report, Rz. 162.

10. Explanatory Report, Rz. 163.

Beendigung abrufbar bleiben, und andererseits **gemäss Art. 26 Abs. 5 BÜPF** Randdaten für sechs Monate zu speichern.

- 18 Auch spezifisch betrachtet erfüllt das geltende Schweizer Recht die Anforderungen der Konventionsbestimmung gemäss Art. 16 CCC. Gemäss der Schweizerischen Strafprozessordnung können Computerdaten entweder durch einen schriftlichen Befehl der Staatsanwaltschaft im Rahmen einer Durchsuchung gemäss **Art. 246 ff. StPO** gesichert oder mittels Editionsverfügung nach **Art. 265 StPO** zu den Akten genommen werden. Die Sicherung gespeicherter Computerdaten lässt sich in der Schweiz in zwei Kategorien unterteilen: Die Sicherung durch Strafverfolgungsbehörden und die Sicherungsaufforderung an Personen. Beide Massnahmen können auch von der Polizei, ohne staatsanwaltschaftliche Anordnung, ergriffen werden, wenn Gefahr in Verzug ist,¹¹ wodurch eine beschleunigte und verhältnismässige Sicherung gespeicherter Computerdaten gesetzlich gewährleistet wird.¹²

A. Sicherung durch Strafverfolgungsbehörden

- 19 Eine vorübergehende Sicherung von Datenmaterial wird in der Schweiz gemäss Art. 198 i.V.m. Art. 241 Abs. 1 und **Art. 246 StPO** durch einen Befehl der Staatsanwaltschaft (oder gegebenenfalls des Sachgerichts) angeordnet, um Aufzeichnungen zu durchsuchen. Diese Anordnung stellt sicher, dass Daten hinsichtlich ihres Inhalts oder ihrer Beschaffenheit geprüft werden können, um ihre Beweiseignung festzustellen und gegebenenfalls zu beschlagnehmen. Solche Durchsuchungen sowie die Sicherung von Datenmaterial werden in der Praxis der Polizei gemäss Art. 312 StPO in Auftrag gegeben. Die Polizei führt daraufhin gemäss Anweisung der Staatsanwaltschaft (oder des Sachgerichts) eine Durchsuchung durch und nimmt entweder den Datenträger zur Sicherstellung mit oder erstellt eine forensische Kopie von Daten, die auf den angetroffenen, zu durchsuchenden Datenträgern vorhanden sind (sogenannte «Datenspiegelung»¹³).¹⁴ Durch die Spiegelung wird sichergestellt, dass Daten auf einen externen Datenträger kopiert werden und vor Manipulationen geschützt sind.¹⁵ Insbesondere in Wirtschaftsstrafverfahren wird dadurch gewährleistet, dass Daten im Sinne von Art. 16 Abs. 1 CCC umgehend gesichert werden können. Andererseits können dadurch die von der Durchsuchung betroffenen Personen ihre Geräte weiterhin nutzen, um – unter Berücksichtigung des Verhältnismässigkeitsgrundsatzes – ihre Geschäftstätigkeiten fortzusetzen, solange die Geräte nicht gemäss Art. 263 StPO i.V.m. Art. 69 Abs. 1 StGB zwecks Einziehung beschlagnahmt werden müssen.
- 20 Um die **Sicherung von Daten auf digitalen Servern oder in der Cloud** zu gewährleisten, ist es zwingend erforderlich, vor Ort unverzüglich eine Datenspiegelung zu erstellen, um zu verhindern, dass diese Daten durch alternative Zugangsmöglichkeiten verändert oder gelöscht werden.¹⁶ Die Rechtsgrundlage für die Erstellung von Kopien solcher Aufzeichnungen und Daten im Rahmen einer Durchsuchung bildet Art. 247 Abs. 3 StPO.¹⁷

B. Sicherungsaufforderung an Personen

- 21 Hinsichtlich der Durchsuchung und Beschlagnahme von Datenmaterial hat die Staatsanwaltschaft (gegebenenfalls auch das Sachgericht) weiter die Möglichkeit, im Sinne von Art. 263 und Art. 265 StPO

11. Vgl. Art. 241 Abs. 3 und Art. 263 Abs. 3 StPO.

12. BBl 2010 4718.

13. Vgl. Graf, Rz. 52 und 235 ff.

14. Vgl. unten Rz. 26 f. betreffend Zuständigkeit und Zulässigkeit einer Anordnung zur Spiegelung nach verlangter Siegelung.

15. Graf, Rz. 237.

16. Graf, Rz. 238 f.

17. Graf, Rz. 237.

durch Verfügung die Herausgabe und Beschlagnahme von Daten anzuordnen, nämlich konkret den Inhaber unter Strafandrohung von Art. 292 StGB sowie unter Fristansetzung zu verpflichten, die elektronischen Datenträger und Daten im Original oder in Kopie als Beweismittel herauszugeben. Dieser Vorgang wird als **Edition** und **Edieren** bezeichnet. Die Anordnung einer solchen Herausgabe ist jedoch nur möglich, sofern es sich beim Inhaber weder um die beschuldigte Person noch um eine Person mit Aussage- oder Zeugnisverweigerungsrecht oder um ein Unternehmen handelt, das sich bei einer Herausgabe strafrechtlich oder zivilrechtlich verantwortlich machen könnte (Art. 265 Abs. 2 StPO). Weitere Voraussetzung für den Erlass eines Editionsbefehls ist, dass sich der Befehl an den tatsächlichen Inhaber der Daten mit einem schweizerischen Domizil richtet, anderenfalls der Weg der internationalen Rechtshilfe in Strafsachen beschritten werden muss.¹⁸

- 22 Wird eine Person nach Art. 2 BÜPF als Dateninhaberin verpflichtet, die ihr verfügbaren Randdaten einer überwachten Person zu übermitteln, finden die Art. 269 ff. StPO Anwendung. Soweit die Voraussetzungen gemäss Art. 269 Abs. 1 lit. b und c StPO erfüllt sind und eine Genehmigung des Zwangsmassnahmengerichts vorliegt, kommt eine Beschlagnahme gestützt auf Art. 263 StPO zwar nicht in Betracht,¹⁹ jedoch können in der Schweiz ansässige **Fernmeldedienstanbieter** als Inhaber der Randdaten dazu angehalten werden, eine Datensicherung gemäss Art. 273 StPO vorzunehmen.²⁰ Die Beschaffung von Bestandesdaten ist keine Zwangsmassnahme und erfordert keine Genehmigung des Zwangsmassnahmengerichts.²¹

C. Fehlende Gesetzesbestimmung betreffend Anordnung auf Aufbewahrung

- 23 In der Schweiz werden lediglich Fernmeldedienstanbieter gemäss Art. 2 BÜPF gesetzlich verpflichtet, Identifikations- und Randdaten für die Dauer von sechs Monaten aufzubewahren.²² Im Zusammenhang mit diesen aufbewahrten Daten wird verschiedenen Behörden des Bundes und der Kantone gemäss **Art. 15 BÜPF** das Recht eingeräumt, Auskünfte zu Angaben über Fernmeldedienste nach Art. 21 BÜPF sowie zur Identifikation der Täterschaft nach Art. 22 BÜPF einzuholen. Eine solche Auskunftserteilung ist einer Herausgabepflicht gemäss Art. 265 StPO gleichzusetzen. Ein «Preservation Order» im Sinne von Art. 16 Abs. 2 CCC liegt hierbei nicht vor.
- 24 Die Schweiz hat sich mit der Ratifizierung der Cybercrime-Konvention nicht in die Pflicht gestellt, «Preservation Orders» im innerstaatlichen Recht einzuführen. Derzeit bietet die Schweizerische Strafprozessordnung auch **keine Rechtsgrundlage** dafür, dass Dateninhaber und Dienstanbieter per Anordnung verpflichtet werden können, Daten vor Verlust oder Veränderung zu schützen und für Strafverfolgungsbehörden bereitzuhalten, ohne sie sogleich herausgeben zu müssen. Die Botschaft geht davon aus, die Möglichkeit, jedermann mittels Verfügung zur Aufbewahrung von Daten zu verpflichten, ginge zu weit und wäre kaum mit dem Grundsatz der Verhältnismässigkeit vereinbar.²³ Diese Einschätzung erweist sich nicht mehr als zeitkonform: Aufgrund der sich stetig weiterentwickelnden Digitalisierung verfügen heutzutage selbst Privatpersonen über erhebliche Speicherkapazitäten auf ihren Datenträgern. Zahlreiche, vertrauenswürdige und kooperationsbereite Unternehmen verfügen freiwillig und im Sinne der Schweizerischen Datenschutzbestimmungen (DSG) über zu Beweis Zwecken relevante Daten wie beispielsweise Kundendaten sowie technische (nicht unter das BÜPF fallende) Daten, ohne hierfür an eine Aufbewahrungsfrist gebunden zu sein. Eine Anordnung an Inhaber solcher Daten, die Aufbewahrungsfrist höchstens für 90 Tage zu verlängern,

18. Vgl. BGE 143 IV 21.

19. Vgl. auch BGer 6B_1353/2023 vom 6. November 2024.

20. BBl 2010 4718 f.

21. Hansjakob, Rz. 1615.

22. Vgl. Art. 21 Abs. 2, Art. 22 Abs. 2 und Art. 26 Abs. 5 BÜPF.

23. BBl 2010 4718 f.

stellt eine wesentlich mildere Massnahme dar, als die Durchsuchung von Aufzeichnungen bei entsprechenden Dateninhaber anzuordnen (vgl. oben N. 19 f.) oder sie sofort zur Herausgabe der vollständigen Daten zu verpflichten (vgl. oben N. 21 f.). Bei einer Verlängerung der Aufbewahrungsfrist werden Verfügungsadressaten angesichts der heutzutage bestehenden technischen Möglichkeiten nicht zu einem unverhältnismässigen Aufwand verpflichtet und es besteht ein öffentliches Interesse daran, sicherzustellen, dass die von Privatpersonen freiwillig gesammelten Daten zur Wahrheitsfindung als Beweismittel gesichert werden können, bevor sie gelöscht werden.

- 25 Unter der geltenden Schweizerischen Strafprozessordnung kann die Aufbewahrung von Daten in Besitz von Personen, die nicht unter das BÜPF fallen, gemäss dem Rechtsgrundsatz **argumentum a maiore ad minus** auch durch eine gestufte Verfügung sichergestellt werden: Es kann eine Verfügung im Sinne von Art. 263 ff. StPO erlassen werden, womit der Dateninhaber zunächst unter Androhung der Ungehorsamsstrafe nach Art. 292 StGB zur Auskunft, Aufbewahrung der Daten sowie zur Geheimhaltung verpflichtet wird, um in einem zweiten Schritt die für die Untersuchung relevanten Daten zuhänden der Untersuchungsakten zu erheben. Eine solche schrittweise Verpflichtung widerspricht nicht dem Grundsatz des numerus clausus bei Zwangsmassnahmen (Art. 197 Abs. 1 lit. a StPO), weil bereits die erste Verpflichtung zur Aufbewahrung der Daten zum Zweck erfolgt, die beweisrelevanten Daten später gemäss Art. 263 StPO herauszuverlangen. Eine solche schrittweise Verpflichtung greift weniger in die Rechte des Dateninhabers ein als die Anordnung zur Durchsuchung gemäss Art. 246 ff. StPO oder ein Editionsbefehl nach Art. 265 StPO. Die in Art. 16 Abs. 2 CCC vorgesehene Aufbewahrungsfrist von längstens 90 Tagen muss eingehalten werden, damit die Massnahme nicht über den Konventionstext hinausgeht.

D. Durch das Bundesgericht ausgebremsste Sicherung bei gültigem Siegelungsantrag

- 26 Das Bundesgericht musste in den letzten Jahren mehrmals über die Konstellation entscheiden, dass nach der Sicherstellung elektronischer Geräte trotz Siegelung eine forensische Sicherungskopie (Spiegelung) der darauf befindenden Daten durch die Untersuchungsbehörden bzw. durch eine beauftragte Fachstelle erstellt wurden. Das Bundesgericht hält es für unzulässig, dass nach einem Siegelungsgesuch eine Untersuchungsbehörde die Spiegelung der Daten veranlasst bzw. an eine von ihr beauftragte und weisungsgebundene Person oder Behörde überträgt.²⁴ Vielmehr müsse die Untersuchungsbehörde nach der Siegelung der Datenträger beim **Zwangsmassnahmengericht ein Spiegelungsgesuch stellen, und zwar auch dann, wenn eine Spiegelung zum Schutz vor Datenverlust dringlich erforderlich ist**. Das Gesuch könne zusammen mit dem Entsiegelungsantrag²⁵ oder bei dringlicher Notwendigkeit superprovisorisch gestellt werden.²⁶ Die Anordnung einer Spiegelung oblige nach der Siegelung ausschliesslich dem Zwangsmassnahmengericht.
- 27 Diese Rechtsprechung hat zu Recht erhebliche **Kritik** erfahren.²⁷ Sie erweist sich auch im Hinblick auf die Cybercrime-Konvention als völkerrechtswidrig. So ignoriert das Bundesgericht,²⁸ dass sich die Schweiz verpflichtet hat, in inländischen Verfahren eine sofortige Sicherung von beweisrelevanten Computerdaten sicherzustellen, um Beweisverluste zu verhindern. Mit seiner Rechtsprechung führt das Bundesgericht nicht nur ein bisher unbekanntes superprovisorisches Verfahren beim

24. BGE 148 IV 221, E. 2.6.

25. BGE 148 IV 221, E. 2.6.

26. BGer 7B_59/2023 vom 12.10.2023 E. 2.1.

27. Vgl. Graf, Rz. 241 ff; Graf/Günal Rüttsche, S. 615 ff.; Geschäftsbericht der Staatsanwaltschaft St.Gallen, abrufbar unter <https://www.berichte.sg.ch/geschaeftsbericht-der-staatsanwaltschaft-st-gallen-2023/rueckblick/rechtsprechung.html>, besucht am 4.5.2025.

28. Vgl. Graf, Rz. 246.

Zwangsmassnahmengericht ein, sondern auch ein Verfahren, bei dem selbst im Falle einer zwangsrichterlichen Anordnung innert weniger Stunden die Erhebungen beweisrelevanter Daten erheblich gefährdet sein können: Solange die Untersuchungsbehörde bei einer Durchsuchung vor Ort keine Kopie der Daten erstellen resp. erstellen lassen kann und stattdessen sich an das Zwangsmassnahmengericht wenden und auf dessen Entscheidung warten muss, kann in der heutigen Praxis der erheblichen Gefahr, dass zugriffs- und zugangsberechtigte Personen die in den digitalen Servern oder Clouds gehaltenen Daten bis zum Spiegelungsentscheid des Zwangsmassnahmengerichts verändern oder löschen, nicht begegnet werden. Neue Entwicklungen bieten auch vermehrt Schutz vor behördlichen Zugriffen, sofern nicht unverzüglich reagiert wird. Erst kürzlich hat eines der grössten Technologieunternehmen auf seinen (Mobil-)Geräten eine Sicherheitsfunktion eingeführt, die den USB-Anschluss nach 60 Minuten seit dem letzten Entsperren des Geräts blockiert, mit der Folge, dass Daten ab diesem Zeitpunkt weder ausgelesen werden können noch eine Software auf das Gerät gespielt werden kann, die das spätere Auslesen ermöglicht. Es ist davon auszugehen, dass andere Unternehmen diesem Beispiel folgen werden. Folglich können bestimmte Gefahrenkonstellationen – sowohl neue als auch jene, die im Explanatory Report berücksichtigt sind²⁹ – nur durch sofortiges Eingreifen der Untersuchungsbehörde, resp. der vor ihr beauftragten Polizei oder Person bei der Durchsuchung vor Ort verhindert werden.³⁰ Durch den vom Bundesgericht festgelegten Ablauf, nach einer Siegelung einen superprovisorischen Spiegelungsantrag beim Zwangsmassnahmengericht zu stellen, wird die Gefahr von Beweisverlusten erheblich erhöht. Von einer von der Cybercrime-Konvention bezweckten effektiveren Strafverfolgung kann hierbei nicht die Rede sein.

LITERATURVERZEICHNIS

Burgermeister Daniel, Beweiserhebung in der Cloud, Master of Advanced Studies in Forensics (MAS Forensics), August 2015.

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

Graf Damian K./Günel Rütche Serdar, Datensicherung von Mobiltelefonen und Tablets – technische und (siegelungs-)rechtliche Herausforderungen im Strafverfahren, SJZ 121 (2025), S. 604 ff.

Hansjakob Thomas, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich 2018.

MATERIALIENVERZEICHNIS

Bundesamt für Justiz, Vernehmlassungsentwurf, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Vorentwurf und Erläuternder Bericht, Bern, März 2009, abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html>, besucht am 4.5.2025.

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 4.5.2025.

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz

29. Explanatory Report, Rz. 161.

über das Jugendstrafrecht vom 21.9.1998, BBl 1999 II 1779 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_1779_1787_1669/de, besucht am 4.5.2025.

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter <https://rm.coe.int/16800cce5b>, besucht am 4.5.2025 (zit. Explanatory Report).

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), abrufbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679>, besucht am 4.5.2025.