

Letzte Änderung: 29.07.2026

PDF erstellt am: 05.10.2026



ONLINEKOMMENTAR
DER FREI ZUGÄNLICHE
RECHTSKOMMENTAR

INHALTSVERZEICHNIS

Art. 1 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	5
Art. 2 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	31
Art. 3 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	47
Art. 4 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	63
Art. 5 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	75
Art. 6 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	89
Art. 7 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	103
Art. 8 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	115
Art. 9 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	125
Art. 11 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	141
Art. 12 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	147
Art. 16 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	165
Art. 18 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	181
Art. 25 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	201
Art. 27 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	215
Art. 28 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	237

Art. 29 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	247
Art. 32 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	271
Art. 33 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	325
Art. 34 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention]).....	341

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 1 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 1 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 1 CCC N. XXX.

Kapitel I: Begriffsbestimmungen

Art. 1 Begriffsbestimmungen

Im Sinne dieses Übereinkommens bedeutet:

- a. «Computersystem» eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen;

b. «Computerdaten» 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;

c. «Diensteanbieter»

i. jede öffentliche oder private Stelle, die es Nutzern ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren,

ii. jede andere Stelle, die für einen solchen Kommunikationsdienst oder für seine Nutzer Computerdaten verarbeitet oder speichert;

d. «Verkehrsdaten» alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht.

GLIEDERUNG

I. Allgemeines.....	8
II. Computersystem (Buchst. A).....	8
A. Ein Gerät.....	9
B. Ein Programm	11
C. Automatische Datenverarbeitung	12
D. Perspektiven	13
1. Die Entmaterialisierung von Computersystemen	13
2. Das Internet der Dinge (IoT).....	14
3. Künstliche Intelligenz	15
III. Computerdaten (Buchstabe b).....	16
A. Die Form der Daten.....	16
B. Datentypen.....	17
C. Programme.....	19
D. Perspektiven	19
E. Exkurs: Die Unterscheidung zwischen Teilnehmerdaten, Verkehrsdaten und Inhaltsdaten im Schweizer Strafrecht	19
1. Teilnehmerdaten	20
2. Verkehrsdaten (oder Sekundärdaten)	20
3. Inhaltsdaten	21
IV. Diensteanbieter (Bst. c)	22
A. Zugangsanbieter.....	22
B. Speicher- oder Inhaltsanbieter	24
C. Perspektiven	26
V. Verkehrsdaten (Bst. d).....	26
Literaturverzeichnis	29
Materialienverzeichnis	29

I. ALLGEMEINES

- 1 Das Übereinkommen über Cyberkriminalität enthält zunächst in Artikel 1 vier Definitionen der zentralen Begriffe, auf die sich die nachfolgenden Artikel beziehen. Die Verfasser des Übereinkommens haben zwar in ihrem Erläuternden Bericht klargestellt, dass die Vertragsparteien nicht verpflichtet seien, die vier in Art. 1 des Übereinkommens definierten Begriffe wörtlich in ihre innerstaatlichen Rechtsvorschriften zu übernehmen. Sie haben jedoch klargestellt, dass die nationalen Gesetze diese Begriffe in einer Weise abdecken müssen, die mit den Grundsätzen des Übereinkommens vereinbar ist und einen gleichwertigen Rahmen für dessen Umsetzung bietet. Der Zweck dieser Definitionen liegt somit auf der Hand: alle Vertragsparteien auf eine gemeinsame Grundlage zu stellen, um sicherzustellen, dass sie sich auf dieselben Konzepte beziehen. Dies ermöglicht insbesondere die **Vermeidung von Rechtsstreitigkeiten**, beispielsweise dass eine Vertragspartei sich weigert, bestimmte Bestimmungen umzusetzen, mit der Begründung, dass sie einen Begriff anders auslegt als eine andere Vertragspartei.
- 2 Den Verfassern des Übereinkommens war offensichtlich **die rasante Entwicklung** der Informatik bewusst. Wahrscheinlich haben sie sich aus diesem Grund dafür entschieden, die Definitionen in Art. 1 StGB so technologieneutral wie möglich zu formulieren und sich dabei auf die funktionale Beschreibung jedes Begriffs zu beschränken. Diese Strategie hat sich bewährt, da diese Definitionen auch 25 Jahre später trotz der erheblichen technologischen Entwicklung, die in diesem Zeitraum stattgefunden hat, nach wie vor relevant sind.

II. COMPUTERSYSTEM (BUCHST. A)

- 3 Die von den Verfassern des Übereinkommens über Cyberkriminalität gewählte Definition umfasst **drei Aspekte**. Sie setzt zunächst das Vorhandensein einer Vorrichtung voraus. Diese kann isoliert oder vernetzt sein. Die Definition umfasst somit sowohl den Personalcomputer als auch miteinander verbundene IT-Umgebungen. Das zweite Element ist das Vorhandensein eines Programms. Das Gerät muss also auf der Grundlage vorab festgelegter Anweisungen funktionieren. Das Gerät darf nicht rein mechanisch sein. Eine Spieluhr oder eine Uhr sind daher keine

Computersysteme. Schließlich muss die Datenverarbeitung automatisch erfolgen. Es reicht nicht aus, dass sich das Gerät auf eine passive Speicherung von Daten beschränkt; es muss automatisch einen Prozess zur Verarbeitung dieser Daten ausführen. Eine Kamera, ein Diktiergerät oder ein USB-Stick sind daher keine Computersysteme.

In seinen Leitlinien hat der Ausschuss des Übereinkommens über 4 Cyberkriminalität klargestellt, dass die Definition des Begriffs „Computersystem“ beispielsweise **moderne Mobiltelefone** umfasst, die multifunktional sind und unter anderem die Fähigkeit besitzen, Daten zu erzeugen, zu verarbeiten und zu übertragen, wie beispielsweise den Zugriff auf das Internet, das Versenden von E-Mails, die Übertragung von Anhängen sowie das Herunterladen von Inhalten oder Dokumenten. Das Gleiche gilt für **Personal Digital Assistants** (PDAs) mit oder ohne drahtlose Funktionen, die ebenfalls Daten erzeugen, verarbeiten und übertragen.

Die gewählte Definition betrachtet das IT-System bewusst unter dem 5 Gesichtspunkt seiner **Funktionalität** und nicht seiner Form. Dieser Ansatz verleiht ihr genügend Flexibilität, um sich im Laufe der Zeit weiterzuentwickeln und Technologien einzubeziehen, die im Jahr 2001 noch nicht existierten, wie beispielsweise *Smartphones*, das Internet der Dinge (*IoT*) oder das *Cloud Computing*.

A. Ein Gerät

Die Informatik basiert im Wesentlichen auf der Datenverarbeitung. Dieser 6 Begriff wird im Folgenden unter Ziffer III näher erläutert. An dieser Stelle lassen sich Daten als immaterielle digitale Informationen definieren. Um verarbeitet werden zu können, benötigen diese Informationen jedoch eine **Reihe von Hardwarekomponenten**, die sowohl ihre Verarbeitung als auch ihre Speicherung ermöglichen.

Obwohl sie nicht das wichtigste Element des Computersystems darstellt, 7 bildet die **Hauptplatine** dennoch das Rückgrat. Es handelt sich um eine große elektronische Platine, die als Träger für alle Komponenten des Systems dient. Das eigentliche Herzstück des Computersystems ist der **Prozessor**. Er stellt das Herz des Systems dar, da er alle Befehle und Anfragen verarbeitet, die von den verschiedenen Komponenten an ihn gesendet werden. Sobald die Daten verarbeitet sind, muss der Prozessor sie vorübergehend irgendwo

speichern können, da er über keinen eigenen Speicher verfügt. Die Daten werden daher vorübergehend im **Arbeitsspeicher** gespeichert. Dieser Speicher kann Daten jedoch nur speichern, solange das Computersystem mit Strom versorgt wird. Wenn es ausgeschaltet wird, gehen alle in diesem Speicher enthaltenen Daten verloren. Es ist daher notwendig, eine dauerhafte Speicherung dieser Daten auf einem geeigneten Gerät vorzusehen, wie beispielsweise einer Festplatte, einer externen Festplatte, einem USB-Stick, einer DVD usw.

- 8 Die letzten Komponenten, die für den Betrieb des Computersystems unverzichtbar sind, sind die **Peripheriegeräte**. Eingabegeräte ermöglichen die Eingabe von Daten in das System, wie beispielsweise die Maus, die Tastatur oder der Scanner. Dem gegenüber stehen Ausgabegeräte, die die Wiedergabe der vom System verarbeiteten Daten gewährleisten, wie der Bildschirm, der Drucker oder der DVD-Brenner. All diese materiellen Elemente werden als *Hardware* bezeichnet und bilden ein System.
- 9 Es wäre jedoch zu kurz gegriffen anzunehmen, dass alle Komponenten, aus denen das System besteht, zwangsläufig kompakt an **einem einzigen Ort** untergebracht sein müssen, denn dies würde bedeuten, den Begriff des Systems auf einen PC oder ein *Smartphone* zu beschränken. So gibt es derzeit Supercomputer, von denen jeder eine ganze Halle einnimmt. Umgekehrt gibt es auch Systeme, deren Komponenten über den gesamten Globus verstreut sind.
- 10 Das System kann **isoliert** oder vernetzt funktionieren. Vor der Verbreitung des Internets Mitte der 90er Jahre funktionierten die meisten Systeme isoliert. Seitdem stellt diese Funktionsweise eher die Ausnahme dar und ist Situationen vorbehalten, die ein Höchstmaß an Sicherheit erfordern, insbesondere um jegliches Eindringen über externe Verbindungen zu verhindern.
- 11 Geräte sind **miteinander vernetzt**, wenn sie über eine kabelgebundene oder kabellose Verbindung – wie Funkwellen, Infrarotverbindungen, Glasfaser oder Satellitenverbindungen – miteinander verbunden sind und so ein Netzwerk bilden. Dieses kann auf einen bestimmten geografischen Bereich beschränkt sein, zum Beispiel ein Wohnhaus, ein Unternehmen oder eine Universität. In diesem Fall handelt es sich um ein lokales Netzwerk (*Local Area Network* oder LAN). Dieses Netzwerk kann sich jedoch auch über ein

viel größeres Gebiet erstrecken, zum Beispiel eine Stadt, ein Land oder einen Kontinent. Man spricht dann von einem Weitverkehrsnetz (*Wide Area Network* oder WAN). Das größte Weitverkehrsnetz ist das Internet, da es sich um ein Netzwerk handelt, das aus einer Vielzahl miteinander verbundener Netzwerke besteht und sich über die ganze Welt erstreckt.

Schließlich umfasst der Begriff „Gerät“ auch die **anderen Geräte**, die es den an Netzwerke angeschlossenen Computern ermöglichen, Daten auszutauschen. In diesem Sinne sind auch Server, Router, Switches, Modems und Gateways als Geräte zu bezeichnen. 12

B. Ein Programm

Den Hardware-Komponenten stehen die Software-Komponenten gegenüber, zu denen die Gesamtheit der Programme gehört, die **den Betrieb und die Nutzung** der verschiedenen Komponenten des Computersystems ermöglichen. 13

Ein Programm lässt sich als eine **Reihe von Befehlen** definieren, die, wenn sie von einem Computersystem ausgeführt werden, ein bestimmtes Ergebnis erzielen. 14

Genau wie bei den Hardwarekomponenten ist es angebracht, Programme nach der Aufgabe zu unterscheiden, die sie erfüllen. Das „Startprogramm“ jedes Computersystems ist das **BIOS** (*Basic Input and Output System*) oder **UEFI** (*Unified Extensible Firmware Interface*). Es ist in einem Chip enthalten, der mit der Hauptplatine verbunden ist, und stellt die für den Systemstart erforderlichen Elemente bereit. Darüber hinaus übernimmt es die grundlegende Verwaltung der verschiedenen Hardwarekomponenten des Computersystems und fungiert als Schnittstelle zwischen diesen Komponenten und dem Betriebssystem. 15

Das **Betriebssystem** bildet seinerseits das zentrale Programm des Computersystems. Es gewährleistet den umfassenden und kohärenten Betrieb des Systems, indem es die verschiedenen Anfragen, die der Benutzer an das Computersystem richtet, sowie die Interaktionen zwischen den Hardwarekomponenten und den anderen Programmen koordiniert. Mit anderen Worten: Das Betriebssystem fungiert als wesentliche Schnittstelle zwischen der Anwendungssoftware und den Hardwarekomponenten des Systems. 16

- 17 Schließlich erfüllt jedes Anwendungsprogramm eine spezifische **Funktion**. So ermöglicht beispielsweise Word® die Textverarbeitung, Photoshop® die Bildbearbeitung und Outlook® den Empfang und Versand von E-Mails. Diese Programme sind jedoch auf das Betriebssystem angewiesen, um auf die Hardware-Ressourcen zugreifen und die Aufgaben ausführen zu können, für die sie entwickelt wurden.

C. Automatische Datenverarbeitung

- 18 Die automatisierte Datenverarbeitung bezeichnet die Tatsache, dass Daten automatisch von einem Programm verarbeitet werden, **ohne** dass ein direkter **menschlicher Eingriff** erforderlich ist. Diese Verarbeitung kann sowohl die Erfassung als auch die Speicherung oder die Wiedergabe von Daten betreffen.
- 19 Wie weiter unten unter Ziffer III zu sehen sein wird, stellen Daten immaterielle digitale Informationen dar. Um von einem Computersystem verarbeitet werden zu können, müssen die aus der materiellen Welt stammenden Informationen in eine **Sprache umgewandelt werden, die vom Gerät** verstanden wird. So wird beispielsweise der Druck auf eine Tastaturtaste, eine Maustaste oder einen Touchscreen in Binärsprache übersetzt und in elektrische, logische oder optische Signale umgewandelt.
- 20 Sobald die materielle Information in elektrische, logische oder optische Signale umgewandelt ist, ist das Programm in der Lage, die Daten automatisch zu verarbeiten. Nach Abschluss der Verarbeitung werden die Daten wieder in eine **für den Benutzer verständliche Sprache** übersetzt. So kann das Programm beispielsweise Buchstaben auf einem Bildschirm anzeigen, wenn ein Benutzer Tasten auf einer Tastatur drückt, die auf dem Bildschirm angezeigten visuellen Informationen an einen Drucker übertragen, damit sie auf Papier ausgegeben werden, wenn der Nutzer auf das Symbol „Drucken“ klickt, oder eine Telefonverbindung herstellen, wenn der Nutzer auf das grüne Telefonsymbol auf dem Touchscreen seines *Smartphones* tippt. Jeder Befehl, den der Nutzer an das Computersystem erteilt, führt zur Erzeugung von Computerdaten, die von Programmen automatisiert verarbeitet und anschließend dem Nutzer in einer für ihn verständlichen Form wiedergegeben werden.

D. Perspektiven

1. Die Entmaterialisierung von Computersystemen

Bereits in den 1980er Jahren tauchte die Idee der verteilten Datenverarbeitung auf, insbesondere durch den von Sun Microsystems lancierten Slogan: „*The network is the computer!*“ („Das Netzwerk ist der Computer!“). Dieser Ansatz basiert auf der **B Bündelung von Rechenressourcen**, um größere Datenmengen verarbeiten zu können. In diesem Zusammenhang, wenn es sich bei dem betreffenden Netzwerk um das Internet handelt, besteht der „Computer“, den es darstellt, aus der Gesamtheit der damit verbundenen Computer, was eine besonders beträchtliche Rechenkapazität darstellt. In diesem Zusammenhang entstanden ab Ende der 90er Jahre und mit der Verbreitung des Internets Projekte zum verteilten Rechnen. Diese bestehen darin, Privatpersonen anzubieten, die Rechenleistung ihrer PCs über das Internet zur Verfügung zu stellen, wenn sie diese nicht nutzen, um Berechnungen durchzuführen, die sehr hohe Rechenkapazitäten erfordern.

Im Laufe der Zeit beschränkte sich dieser Ansatz der gemeinsamen Nutzung nicht mehr nur auf den Prozessor. Die gesamte IT-Architektur wurde nach und nach neu konzipiert und entwickelte sich zu einer **verteilten Architektur**, in dem Sinne, dass sich die verschiedenen verfügbaren Ressourcen nicht mehr unbedingt am selben Ort oder auf demselben Rechner befinden. Ein symbolträchtiges Beispiel für eine verteilte Architektur, die Anfang der 2000er Jahre einen rasanten Aufschwung erlebte, ist das sogenannte „Peer-to-Peer“ (*peer-to-peer*). Dieses Modell ermöglicht den Dateiaustausch innerhalb einer Architektur, in der jeder Computer sowohl die Rolle des Clients als auch die des Servers übernimmt.

Zwischen Ende der 2000er und Anfang der 2010er Jahre entstand das *Cloud Computing* („Cloud Computing“) auf, bei dem auf entfernte, mit dem Internet verbundene Server zurückgegriffen wird, um Daten zu speichern, zu verwalten und zu verarbeiten, anstatt sich auf einen lokalen Server oder einen PC zu stützen. Diese Technik ermöglicht es dem Nutzer insbesondere, ein virtuelles Computersystem zu erstellen, dort ein Betriebssystem und Anwendungen zu installieren sowie Daten zu generieren, zu verarbeiten und zu speichern. Dazu reicht es aus, über ein mit dem Internet verbundenes Endgerät zu verfügen, da alle anderen Ressourcen virtuell und dezentral

bereitgestellt werden – von verschiedenen Standorten und manchmal auch von unterschiedlichen Dienstleistern aus, die über die ganze Welt verteilt sind. In einer solchen Konfiguration ist es leicht nachvollziehbar, dass die Einstufung als „System“ problematisch werden kann, da keine physische Einheit der Komponenten mehr besteht.

2. Das Internet der Dinge (IoT)

- 24 Seit einigen Jahren ist eine regelrechte Explosion der Anzahl **vernetzter Objekte** zu beobachten. Ob Uhren, Backöfen, Fernseher oder Fahrzeuge – fast alle Alltagsgegenstände gibt es in einer Form, die mit dem Internet verbunden werden kann.
- 25 In den 90er Jahren stellte SCHMID unter Berufung auf die Botschaft des Bundesrats fest, dass Lebensmittel-, Benzin- und Geldautomaten, Kopierer oder Spielautomaten nicht als Informatiksysteme eingestuft werden könnten, da der Bundesgesetzgeber den Begriff des Informatiksystems auf Geräte beschränken wollte, die in der Lage sind, **sogenannte „höhere Funktionen“** auszuführen.
- 26 Diese Auffassung lässt sich heute nicht mehr vertreten. Vernetzte Objekte sind mittlerweile fester Bestandteil des Internets, können ferngesteuert werden und sind in der Lage, so viele Aufgaben auszuführen, dass sie alle Kriterien erfüllen, die es ermöglichen, sie als Informatiksysteme im Sinne von Art. 1 Bst. a ZGB zu qualifizieren. Dieser **Paradigmenwechsel** wirft jedoch ernsthafte Probleme auf. Denn vernetzte Geräte verfügen in der Regel nicht über Schutzmaßnahmen, die denen herkömmlicher Computer entsprechen. Cyberkriminelle können daher leichter unberechtigt auf eine vernetzte Uhr zugreifen, um die darin enthaltenen Zahlungsmittel darin gespeichert sind, eine mit einem Hausautomationssystem verbundene Tür entriegeln, um in eine Wohnung einzudringen, oder sogar auf ein Unternehmensnetzwerk zugreifen, indem sie sich unberechtigt mit der vernetzten Kaffeemaschine in der Kantine verbinden, als auf einen speziell gegen unbefugten Zugriff geschützten PC. Daraus folgt, dass der Anwendungsbereich von Art. 2 ZGB für Staaten, die nicht wie die Schweiz verlangen, dass die Straftat unter Umgehung von Sicherheitsmassnahmen begangen wird, besonders weitreichend ist und sich in den kommenden Jahren noch weiter ausdehnen dürfte.

3. Künstliche Intelligenz

Wie oben dargelegt (unter Ziffer II, Buchstabe B), setzt die Definition in Art. 1 Buchstabe a StGB voraus, dass ein Computersystem mit einem Programm ausgestattet ist. Dieses Programm führt grundsätzlich eine Reihe von Befehlen aus, die vom Menschen vordefiniert wurden. Mit dem Aufkommen der künstlichen Intelligenz ist die **Unveränderlichkeit der Programme** nicht mehr unbedingt selbstverständlich. Auf künstlicher Intelligenz basierende Systeme sind nämlich zum autonomen Lernen fähig und können unter bestimmten Konfigurationen ihren eigenen Quellcode ändern oder die Parameter der Umgebung, in der sie agieren, anzupassen. Es stellt sich daher die Frage, ob der Begriff des Computersystems in seiner derzeitigen Definition noch weit genug gefasst ist, um diese technologischen Entwicklungen zu erfassen, oder ob eine Neudefinition erforderlich ist, um künftigen Entwicklungen im Bereich der künstlichen Intelligenz Rechnung zu tragen. Unserer Ansicht nach ist die aktuelle Definition weit genug gefasst, um die bisher bekannten technologischen Entwicklungen einzubeziehen. Denn selbst wenn künstliche Intelligenz in der Lage ist, den Quellcode eines Programms umzuschreiben, um sich an ihre Umgebung anzupassen, funktioniert das Computersystem weiterhin auf der Grundlage eines Programms. 27

Zwei sich abzeichnende Problemstellungen könnten jedoch in den kommenden Jahren eine Neudefinition erforderlich machen. Die erste betrifft autonome und eingesetzte agentenbasierte künstliche Intelligenz, d.h. Agenten, die in der Lage sind, zu verhandeln, zwischen Umgebungen zu wechseln, weitere Agenten zu erstellen oder ihre eigene Infrastruktur ohne menschliches Eingreifen zu verändern. Dies wirft das Problem der Einheit des Computersystems auf, da sich nicht mehr eindeutig bestimmen ließe, ab wann ein Schwarm von Agenten noch ein Computersystem oder bereits mehrere darstellt. Zudem lässt das Übereinkommen den Begriff des kurzlebigen, verteilten und selbstorganisierten Computersystems außer Acht. Die zweite Problematik betrifft die neuromorphe künstliche Intelligenz, also solche ohne separate Programme. Dies zeigt sich beispielsweise bei den Loihi-Chips von Intel, die das menschliche Gehirn nachahmen. Im Gegensatz zu herkömmlichen Prozessoren verarbeiten diese Chips Informationen ereignisgesteuert und integrieren den Speicher in den Prozessor. Es gibt also kein „Programm“ mehr, das von der Hardware getrennt ist. Ausführung und 28

Lernen sind untrennbar miteinander verbunden, sodass die derzeitige Definition des Computersystems überholt wäre.

- 29 Mittelfristig wäre es daher notwendig, **die Definition** des Computersystems einerseits auf eingesetzte autonome Agenten und andererseits auf alle Hardware- oder Hybridgeräte, die eine Datenverarbeitung mittels maschinellen Lernens durchführen, auch wenn die Ausführung nicht auf einem eigenständigen Programm beruht.

III. COMPUTERDATEN (BUCHSTABE B)

- 30 Computerdaten werden definiert als *„jede Darstellung von Tatsachen, Informationen oder Konzepten in einer Form, die sich für die computergestützte Verarbeitung eignet, einschließlich eines Programms, das dazu dient, ein Computersystem zur Ausführung einer Funktion zu veranlassen“* (Art. 1 Buchstabe b ZGB). Diese Definition, die derjenigen der Internationalen Organisation für Normung (ISO) übernommen wurde, zeichnet sich durch ihre **technologische Neutralität** aus. Dies verleiht ihr den Vorteil, dass sie der rasanten technologischen Entwicklung seit der Verabschiedung des Übereinkommens im Jahr 2001 bemerkenswert gut standgehalten hat.

A. Die Form der Daten

- 31 Computersysteme verwenden eine **Sprache**, die sich grundlegend von der menschlichen unterscheidet. Ein Text, ein Bild oder ein vom Menschen geschaffenes Musikwerk hat als solches für einen Computer keinerlei Bedeutung. Um verstanden und verarbeitet werden zu können, muss diese Information in eine für die Maschine verständliche Sprache umgewandelt werden. Vor diesem Hintergrund verwendet die im Übereinkommen festgelegte Definition von „Computerdaten“ den Ausdruck „die sich einer Verarbeitung eignen“. Dies bedeutet, dass die Darstellung von Tatsachen, Informationen oder Konzepten direkt von einem Computersystem verarbeitet werden können muss, ohne dass eine vorherige Umwandlung erforderlich ist, um deren Erkennung durch das System zu ermöglichen. Computerdaten sind somit Informationen, die von einem Computer direkt verstanden und verarbeitet werden können.

Die Informatik basiert auf einem **binären System**, was bedeutet, dass sie 32 ausschließlich die Ziffern 0 und 1 verwendet. Diese elementare Informationseinheit wird als *Bit* bezeichnet. Eine Folge von acht Bits bildet ein Byte (z. B. 10011101), mit dem sich 2^8 , also 256 verschiedene Werte darstellen lassen. Dieses System ermöglicht die Übersetzung von Informationen aus der menschlichen Sprache in für die Maschine verständliche Anweisungen. Je nach verwendetem Programm kann ein Byte eine Ziffer, einen Buchstaben, eine Farbe oder sogar einen Ton darstellen. Wenn ein Benutzer beispielsweise in einem Textverarbeitungsprogramm die Taste „a“ auf seiner Computertastatur drückt, wird diese Aktion in die Binärsprache in der Form „01100001“ umgewandelt. Dieses Byte stellt eine Information dar, die der Computer verarbeiten kann, indem er ein „a“ auf dem Bildschirm anzeigt. Ebenso werden Farben in Werte umgewandelt, die sich auf drei Achsen verteilen: Rot, Grün und Blau. Der Wert 0 bedeutet, dass die Farbe nicht vorhanden ist, und der Wert 255, dass die Farbe ihre maximale Intensität aufweist. So wird ein aprikosenfarbiges Pixel in einem Zeichenprogramm durch die Werte 230 auf der roten Skala, 126 auf der grünen Skala und 48 auf der blauen Skala dargestellt, was in Binärsprache „11100110111111011000000“. Diese 24-Bit-Daten ermöglichen es dem Zeichenprogramm, ein aprikosenfarbenes Pixel auf der weißen Seite anzuzeigen.

Die vorstehenden Beispiele veranschaulichen, dass in der Informatik die 33 Daten die elementare Einheit sind, die eine Information enthält. Umgekehrt spricht man von einer **Datei**, wenn eine Reihe von Daten zu einem zusammenhängenden Ganzen zusammengefasst wird. Dabei kann es sich um einen Text, ein Bild, ein Video oder eine Tonaufnahme handeln.

B. Datentypen

Die Definition in Art. 1 Bst. b ZGB wird **keine Unterscheidung** zwischen den 34 verschiedenen Arten von Daten getroffen. Alle Daten sind davon betroffen, unabhängig davon, ob sie personenbezogen sind oder nicht, privat oder öffentlich, für Menschen verständlich oder nur für Maschinen lesbar. Auch der Inhalt der Daten spielt keine Rolle, sei es bei Sachdaten (Daten, Uhrzeiten, Messwerte usw.), bei Informationen (Berichte, Analysen, usw.) oder um abstrakte Konzepte (Modelle, Algorithmen, Codes usw.). Als Daten im Sinne von Art. 1 Buchst. b ZGB gelten somit auf Speichermedien

gespeicherte Daten, temporäre Daten, Daten im Transit, Metadaten und sogar verschlüsselte Daten.

- 35 Zu den vom Menschen geschaffenen Daten sind unserer Ansicht nach jene hinzuzurechnen, die automatisch von einem Computersystem aus bereits vorhandenen Daten erzeugt werden und als **abgeleitete oder abgeleitete Daten** bezeichnet werden, insbesondere durch Transformationsverfahren, Kombinations- oder algorithmischen Analyseverfahren. Als Beispiele seien hier Nutzerprofile, Bewertungen, Vorhersagen oder Klassifizierungen genannt, die ohne direkten menschlichen Eingriff generiert werden. Obwohl es sich dabei nicht um Daten handelt, die ursprünglich von einem Nutzer bereitgestellt wurden, müssen sie unserer Ansicht nach ebenfalls in die Definition von Art. 1 Bst. b ZGB einbezogen werden, sofern sie sich für eine computergestützte Verarbeitung eignen und von einem Computersystem verwertbar sind.
- 36 Die Definition von Computerdaten erstreckt sich unserer Meinung nach auch auf **flüchtige** (oder kurzlebige) Daten, insbesondere solche, die vorübergehend im Arbeitsspeicher eines Systems gespeichert sind, bei der Ausführung eines Programms dynamisch erzeugt werden oder dazu bestimmt sind, nach sehr kurzer Zeit automatisch zu verschwinden. Obwohl ihre Lebensdauer kurz ist, sind sie im Rahmen von Strafverfahren von besonderer Bedeutung, insbesondere bei unrechtmäßigem Zugriff (Art. 2 StGB) oder einer Beeinträchtigung der Systemintegrität (Art. 5 StGB) mittels eines Distributed-Denial-of-Service-Angriffs.
- 37 Angesichts der ausschließlich funktionsorientierten Definition von Computerdaten spielt es keine Rolle, ob die Daten für einen Menschen verständlich sind. Daten bleiben auch dann Computerdaten, wenn sie **verschlüsselt, komprimiert, fragmentiert** oder in einer Form gespeichert sind, die kein unmittelbares Lesen zulässt. Die Verschlüsselung von Daten ist rechtlich irrelevant, da sie lediglich eine technische Maßnahme zur Datenverarbeitung darstellt, die darauf abzielt, den Zugriff auf die Daten einzuschränken. Daher ändert sich der rechtliche Status der Daten nicht dadurch, dass sie verschlüsselt oder von Cyberkriminellen vorübergehend unbrauchbar gemacht werden.

C. Programme

Die von den Verfassern des Übereinkommens beabsichtigte Präzisierung 38 „einschließlich eines Programms“ zielt darauf ab, jegliche Unklarheit hinsichtlich der Einbeziehung von **Programmen** in die Definition von Art. 1 Buchstabe b ZGB. Dieser Ansatz ist in zweierlei Hinsicht vollkommen schlüssig. Aus informatiktechnischer Sicht ist ein Programm eine Reihe von Anweisungen, die in einem Quellcode enthalten sind, der wiederum aus einer Vielzahl von Zeichen – also Daten – besteht, welche bestimmen, wie die ihm zugeführten Daten verarbeitet werden sollen. Aus systematischer Sicht entspricht die Einbeziehung von Programmen in die Definition von Daten dem klar zum Ausdruck gebrachten Willen der Verfasser des Übereinkommens, keine Unterscheidung zwischen den verschiedenen Arten von Daten zu treffen.

D. Perspektiven

Obwohl es zum Zeitpunkt der Ausarbeitung des Übereinkommens unmöglich 39 war, die zukünftigen Entwicklungen der Informatik vorherzusehen, ermöglichte die Wahl einer **technologieneutralen** Definition die Einbeziehung aller neuen Datenarten, die seit 2001 entstanden sind. Dies gilt insbesondere für Krypto-Assets, von vernetzten Geräten generierte Daten sowie *Datensätze*, d. h. strukturierte Datensammlungen, die für das Training von Modellen des maschinellen Lernens bestimmt sind.

E. Exkurs: Die Unterscheidung zwischen Teilnehmerdaten, Verkehrsdaten und Inhaltsdaten im Schweizer Strafrecht

Die rasante technologische Entwicklung in den letzten dreißig Jahren 40 erforderte **erhebliche gesetzliche Anpassungen**, um zu klären, welche Arten von Daten unter welchen Bedingungen erhoben werden dürfen. Das erste Gesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) wurde am 6. Oktober 2000 verabschiedet und trat am 1. Januar 2002 in Kraft. Es wurde 2016 vollständig revidiert und erfuhr anschließend mehrere Teilrevisionen, darunter insbesondere eine umfassende Revision im Jahr 2024.

Der Gesetzgeber ging davon aus, dass nicht alle Daten die gleiche Bedeutung 41 haben. Er legte die Prämisse zugrunde, dass je größer der Eingriff in die durch

Art. 13 BV garantierte Privatsphäre sei, desto strenger die Voraussetzungen für die Erhebung dieser Daten sein müssten. Das Gesetz unterscheidet somit zwischen **drei Arten von Daten**: den Teilnehmerdaten (*Bestandesdaten*), Verkehrsdaten (*Randdaten*) und Inhaltsdaten (*Inhaltsdaten*).

- 42 Das Übereinkommen über Cyberkriminalität nimmt in Artikel 18 dieselbe Unterscheidung vor.

1. Teilnehmerdaten

- 43 Die Teilnehmerdaten umfassen die **Identifikationsangaben des Inhabers** eines Anschlusses. Dabei handelt es sich insbesondere um den Namen, den Vornamen, das Geburtsdatum, die Adresse und, sofern bekannt, den Beruf des Nutzers (Art. 21 Abs. 1 Bst. a BÜPF) sowie die Adressierungsressourcen (Art. 21 Abs. 1 Bst. b BÜPF) und die Art der genutzten Dienste (Art. 21 Abs. 1 Bst. c BÜPF).
- 44 Diese Daten entsprechen den in **Art. 18 Abs. 3 ZGB** aufgeführten, nämlich: die Art des genutzten Kommunikationsdienstes, die diesbezüglich getroffenen technischen Vorkehrungen und die Dienstdauer (Bst. a); die Identität, die Post- oder geografische Adresse und die Telefonnummer des Teilnehmers sowie jede andere Zugangsnummer, die Daten zur Rechnungsstellung und Zahlung, die auf der Grundlage eines Vertrags oder einer Dienstleistungsvereinbarung verfügbar sind (Bst. b); alle weiteren Informationen über den Standort der Kommunikationsgeräte, die auf der Grundlage eines Vertrags oder einer Dienstleistungsvereinbarung verfügbar sind (Bst. c).
- 45 Es handelt sich hierbei um die **am wenigsten sensiblen Daten**. Ihre Erhebung stellt nur einen minimalen Eingriff in die Privatsphäre dar. Nach schweizerischem Recht unterliegt ihre Erhebung daher lediglich den Voraussetzungen von Art. 197 Abs. 1 StPO und erfordert keine Genehmigung durch das Zwangsmassnahmengericht.

2. Verkehrsdaten (oder Sekundärdaten)

- 46 Verkehrsdaten sind Daten, aus denen hervorgeht, mit **wem, wann, wie lange und von wo aus** die überwachte Person kommuniziert hat oder kommuniziert, sowie die technischen Merkmale der betreffenden Kommunikation (Art. 8 Bst. b BÜPF).

In einem Grundsatzurteil hat das Bundesgericht insbesondere festgestellt, 47
dass **der Verlauf der IP-Adressen** von Mitgliedern, die sich in ein soziales
Netzwerk eingeloggt haben, zu den Verkehrsdaten und nicht zu den
Teilnehmerdaten gehört. Dieses Urteil, das in der Rechtslehre stark kritisiert
wurde, wurde kürzlich in einem unveröffentlichten Urteil bestätigt.

Das Übereinkommen über Cyberkriminalität definiert sie in Art. 1 Buchst. d 48
CCC. Sie werden im nachstehenden Kapitel V ausführlich behandelt.

Diese **Daten** sind **sensibler** als Teilnehmerdaten. Der Schweizer Gesetzgeber 49
hat daher beschlossen, strengere Anforderungen an deren Beschaffung zu
stellen. Es müssen daher die Voraussetzungen von Art. 197 Abs. 1 und Art. 273
Abs. 1 StPO kumulativ erfüllt sein. Die Beschaffung dieser Daten ist daher nur
möglich, wenn ein schwerwiegender Verdacht besteht, der darauf hindeutet,
dass ein Verbrechen oder Vergehen begangen wurde. Bloße Vermutungen
oder vage Verdachtsmomente reichen nicht aus. Die Beschaffung dieser Daten
ist auch im Falle einer Ordnungswidrigkeit nicht möglich. Hinzu kommt, dass
die Beschaffung im Hinblick auf die Schwere der Straftat gerechtfertigt sein
muss (Verhältnismäßigkeitsprinzip) und dass die bisher im Rahmen der
Untersuchung getroffenen Massnahmen erfolglos geblieben sind oder die
Ermittlungen ohne Überwachung keine Aussicht auf Erfolg hätten oder
übermässig erschwert wären (Subsidiaritätsprinzip).

Die Beschaffung dieser Daten ist zudem nur mit der **Genehmigung** des 50
Zwangsmassnahmengerichts möglich (Art. 274 StPO).

3. Inhaltsdaten

Inhaltsdaten entsprechen dem eigentlichen **Inhalt der Kommunikation** 51
(Art. 8 Bst. a BÜPF). Es handelt sich um den schriftlichen oder mündlichen
Ausdruck menschlichen Denkens, insbesondere um den vom Verfasser einer
E-Mail oder einer Nachricht verfassten Text oder um die von einem
Gesprächspartner während eines Telefongesprächs geäußerten Worte.

Die Überwachung von Inhaltsdaten ist **die eingreifendste Form der** 52
Überwachung und stellt den schwerwiegendsten Eingriff in das
Fernmeldegeheimnis und die Privatsphäre dar. Es versteht sich daher von
selbst, dass die vom Schweizer Gesetzgeber gestellten Anforderungen bei
dieser Datenart die höchsten unter den drei Datenarten sind.

- 53 Inhaltsdaten sind in Art. 21 ZGB erwähnt. Die Verfasser des Übereinkommens waren ebenfalls der Ansicht, dass diese Daten nicht zur Verfolgung beliebiger Straftaten erhoben werden dürfen. Sie haben daher den **Grundsatz der Verhältnismäßigkeit** verankert, indem sie vorsahen, dass diese Daten nur zur Verfolgung bestimmter schwerer Straftaten erhoben werden dürfen, die im innerstaatlichen Recht definiert sein müssen.
- 54 Die Erhebung von Inhaltsdaten ist in **Art. 269 StPO** geregelt. Sie setzt das Vorliegen eines schwerwiegenden Verdachts voraus, der die Begehung eines Verbrechens oder Vergehens vermuten lässt, die in Art. 269 Abs. 2 StPO abschließend aufgeführt sind. Auch in diesem Fall reichen bloße Vermutungen oder vage Verdachtsmomente nicht aus. Die Erhebung dieser Daten muss zudem im Hinblick auf die Schwere der Straftat gerechtfertigt sein (Grundsatz der Verhältnismäßigkeit). Es reicht also nicht aus, dass die verfolgte Straftat in der Aufzählung des Art. 269 Abs. 2 StPO aufgeführt ist; vielmehr muss zudem die konkrete Schwere der Straftat im Einzelfall die Überwachungsmaßnahme rechtfertigen. Schliesslich müssen die bisher im Rahmen der Untersuchung getroffenen Massnahmen erfolglos geblieben sein oder die Ermittlungen hätten ohne Überwachung keine Aussicht auf Erfolg oder wären übermässig erschwert (Subsidiaritätsprinzip).
- 55 Genau wie bei den Verkehrsdaten ist die Beschaffung von Inhaltsdaten nur mit der **Genehmigung** des Zwangsmassnahmengerichts möglich (Art. 274 StPO).

IV. DIENSTEANBIETER (BST. C)

- 56 Gemäß Art. 1 Bst. c ZGB bezeichnet „*der Begriff ‚Dienstanbieter‘ jede öffentliche oder private Einrichtung, die den Nutzern ihrer Dienste die Möglichkeit bietet, mittels eines Informationssystems zu kommunizieren, sowie jede andere Einrichtung, die für diesen Kommunikationsdienst oder dessen Nutzer Daten verarbeitet oder speichert*“. Diese Definition unterscheidet zwischen **zwei Arten** von Anbietern: Zugangsanbieter und Speicher- oder Inhaltsanbieter.

A. Zugangsanbieter

- 57 Bei den in Art. 1 Bst. c Ziff. 1 ZGB genannten Diensteanbietern handelt es sich um Zugangsanbieter (*access provider*), d. h. um diejenigen, die es den Nutzern

ermöglichen, **sich mit einem Netzwerk zu verbinden** und **miteinander zu kommunizieren**, und zwar mittels eines Informationssystems.

Dabei handelt es sich in erster Linie um Telekommunikationsbetreiber (z. B. 58 Swisscom, SFR, Deutsche Telekom, Vodafone, TIM), die Privatpersonen den Zugang zum Internet ermöglichen. Diese Definition ist unserer Ansicht nach weitaus weiter zu fassen und muss sich auf alle **Einrichtungen erstrecken, die den Zugang zu einem Netzwerk** über ein Computersystem bereitstellen. Betroffen sind somit private Unternehmen oder öffentliche Körperschaften, die den Nutzern Internetzugangspunkte zur Verfügung stellen (z. B. Eisenbahnunternehmen, Hotels, Gemeinden usw.), private Unternehmen oder öffentliche Einrichtungen, die ein privates Netzwerk betreiben und ihren Nutzern Zugang zu diesem Netzwerk gewähren, sowie Privatpersonen, die über einen Internetzugang oder einen Zugang zu einem Heimnetzwerk verfügen, insbesondere in Form eines WLAN-Hotspots, und Dritten die Möglichkeit bieten, sich damit zu verbinden.

Diese **ausgeweitete Auslegung** wird von den Verfassern des 59 Übereinkommens bestätigt, die in ihrem Erläuternden Bericht betonen, dass es unerheblich ist, ob die Nutzer eine geschlossene Gruppe bilden oder ob der Anbieter seine Dienste der Öffentlichkeit anbietet oder nicht, sei es kostenlos oder gegen Zahlung von Gebühren. Die geschlossene Gruppe kann aus den Mitarbeitern eines privaten Unternehmens bestehen, denen die Dienste über ein Unternehmensnetzwerk bereitgestellt werden.

Unserer Ansicht nach umfasst die Formulierung „die den Nutzern ihrer 60 Dienste die Möglichkeit zur Kommunikation bietet“ nicht nur öffentliche oder private Einrichtungen, die den Zugang zum Netz bereitstellen, sondern auch alle diejenigen, die **die Kommunikation materiell ermöglichen**. Der Begriff „Zugangsanbieter“ erstreckt sich somit auf alle Einrichtungen, die eine Infrastruktur oder einen Dienst zur Verfügung stellen, der die Übertragung, das Routing oder die Weiterleitung von Daten über das Netz ermöglicht, sofern sie den Nutzern eine funktionale Kommunikationsdienstleistung anbieten. Nicht erfasst sind hingegen rein technische oder industrielle Akteure, die sich auf die Herstellung, Lieferung oder Wartung von Geräten beschränken, ohne selbst einen Kommunikationsdienst anzubieten.

Aus rein funktionaler Sicht betrifft die Definition von Art. 1 Bst. c Ziff. 1 ZGB 61 betrifft auch bestimmte Kategorien von **Vermittlern im Netz**, die zwar

keinen klassischen Internetzugang bereitstellen, aber eine entscheidende Rolle dabei spielen, dass die Kommunikation mittels eines Informatiksystems tatsächlich möglich ist. Dies gilt insbesondere für Anbieter von Diensten für virtuelle private Netzwerke (*Virtual Private Network* oder VPN), die ihren Nutzern einen sicheren und anonymen Zugang zu über das Netz erreichbaren Ressourcen gewährleisten, indem sie Funktionen des Routings, der Übertragung und der Verschlüsselung der Kommunikation kombinieren.

- 62 Ebenfalls aus funktionaler Sicht können von Art. 1 Bst. c Ziff. 1 ZGB die **Betreiber von Infrastrukturdiensten** erfasst werden, die für die Kommunikation im Internet unerlässlich sind, wie beispielsweise Anbieter von öffentlich zugänglichen Domain-Name-System-Diensten (DNS) oder Betreiber von Internet-Knotenpunkten (*Internet Exchange Points* oder IXP), sofern sie eine Dienstleistung anbieten, die die Weiterleitung oder die Zusammenschaltung von Kommunikationen zwischen Nutzern oder Netzbetreibern ermöglicht.

B. Speicher- oder Inhaltsanbieter

- 63 Die in Art. 1 Buchst. c Ziff. 2 ZGB genannten **Dienstleister** sind solche, die unentgeltlich oder gegen Entgelt Speicherplatz (*Hosting-Anbieter*) oder Inhalte für Websites (*Content-Anbieter*) zur Verfügung stellen.
- 64 Die **Speicheranbieter** (*Hosting-Anbieter*) sind Unternehmen, die Internetnutzern Server zur Speicherung oder Verarbeitung von Daten zur Verfügung stellen. Sie lassen sich in **zwei Kategorien** unterteilen: diejenigen, die Daten im Auftrag der unter Punkt (i) genannten Unternehmen speichern oder verarbeiten, und diejenigen, die Daten im Auftrag der Nutzer der von den unter Punkt (ii) genannten Personen angebotenen Dienste speichern oder verarbeiten:
- 65 Die erste Kategorie umfasst Speicheranbieter, die die Daten der **Zugangsanbieter** verarbeiten oder speichern. Dabei handelt es sich insbesondere um Verkehrsdaten (siehe Abschnitt V unten), um Daten des Domain-Name-Systems (*Domain Name System* oder DNS), das Domainnamen mit der IP-Adresse der Server verknüpft, auf denen sie gehostet werden, sowie um Daten zu den verschiedenen Servern, über die E-Mails weitergeleitet werden.

Die zweite Kategorie betrifft Anbieter, die die Daten der **Nutzer** der 66
Zugangsanbieter speichern oder verarbeiten. Dies betrifft insbesondere
Unternehmen, die Websites hosten, Speicherplätze für die Bereitstellung
virtueller IT-Systeme anbieten oder Umgebungen bereitstellen, in denen
Daten aus der Ferne gespeichert, verwaltet oder verarbeitet werden können
(*Cloud Computing*).

Im Zusammenhang mit dem *Cloud Computing* gilt die Einstufung als 67
Dienstleister im Sinne von Art. 1 Bst. c Ziff. 2 ZGB unterschiedslos für die
verschiedenen üblicherweise unterschiedenen Dienstleistungsmodelle,
nämlich Infrastructure as a Service (*IaaS*), Platform as a Service (*PaaS*) und
Software as a Service (*Software as a Service* oder *SaaS*). Unabhängig von der
gewählten Form beinhalten alle diese Modelle die Speicherung, Verarbeitung
oder Bereitstellung von Computerdaten im Auftrag Dritter, was ihre
Einbeziehung in die Definition der Dienstleister gemäß Art. 1 Bst. c Ziff. 2 OR
rechtfertigt.

Zu den Dienstleistern zählen auch Unternehmen, die **Content-Delivery-** 68
Netzwerke

(*Content Delivery Networks* oder CDN) betreiben. Diese Akteure sorgen
mittels geografisch verteilter Server für das Caching, die vorübergehende
Speicherung und die optimierte Verteilung von Daten.

Die Definition in Art. 1 Bst. c Ziff. 2 OR ist jedoch nicht dazu bestimmt, auf 69
einen reinen Inhaltsanbieter (z. B. eine Person, die mit einem Hosting-
Anbieter einen Vertrag über das Hosting ihrer Website abschließt) Anwendung
zu finden, sofern dieser nicht zusätzlich Kommunikationsdienste oder andere
Datenverarbeitungsdienste anbietet. Dagegen fallen unserer Ansicht nach
Websites in den Anwendungsbereich der Definition von Art. 1 Bst. c Ziff. 2
ZGB, die über die Bereitstellung von Inhalten hinaus
Kommunikationsdienste anbieten, wie beispielsweise Websites, die E-
Mail-Postfächer, Instant-Messaging-Dienste oder Diskussionsforen zur
Verfügung stellen. Das Gleiche gilt für Websites, die
Datenverarbeitungsdienste anbieten, insbesondere Datenverschlüsselung,
Textübersetzung, finanzielle Datenanalyse oder auch die automatisierte
Erfassung unstrukturierter Daten und deren Umwandlung in strukturierte
Daten (*Web Scraping*).

- 70 Diese Analyse gilt auch für **Online-Plattformen** und **soziale Netzwerke**, die über die Verbreitung von Inhalten hinaus strukturierte Funktionen für die Kommunikation und Interaktion zwischen Nutzern anbieten. Diese Dienste beinhalten in der Regel die Einrichtung von Konten, den Austausch von Nachrichten, die Veröffentlichung von Inhalten sowie die automatisierte Datenverarbeitung zum Zwecke der Klassifizierung, gezielter Werbung oder Moderation.

C. Perspektiven

- 71 Schließlich ist die Definition des Begriffs „Dienstleister“ – ebenso wie die für Computerdaten gewählte Definition – technologieneutral gehalten. Dieser Ansatz ermöglichte es, die seit 2001 entstandenen **neuen Arten von Diensten** einzubeziehen, insbesondere Unternehmen, die auf künstlicher Intelligenz basierende Dienste zur Verarbeitung oder Generierung von Daten anbieten. Es ist jedoch zu präzisieren, dass nicht die künstliche Intelligenz an sich Gegenstand der Definition ist, sondern vielmehr die Funktionen der Speicherung, Verarbeitung oder Übermittlung von Computerdaten, die sie ermöglicht.

V. VERKEHRSDATEN (BST. D)

- 72 Die letzte im Übereinkommen enthaltene Definition findet sich in Art. 1 Bst. d ZGB, wonach Verkehrsdaten *„alle Daten bezeichnen, die sich auf eine über ein Informationssystem verlaufende Kommunikation beziehen, von diesem als Teil der Kommunikationskette erzeugt werden und die Herkunft, den Bestimmungsort, die Route, den Zeitpunkt, das Datum, die Größe und die Dauer der Kommunikation oder die Art des zugrunde liegenden Dienstes“*. Diese Daten haben einen **besonderen rechtlichen Status**, da sie in Strafverfahren als Anhaltspunkte oder sogar als Beweismittel dienen können. Sie werden von den verschiedenen IT-Systemen erzeugt, die in die Kommunikationskette eingebunden sind, um die Kommunikation von ihrem Ursprungsort zu ihrem Zielort zu leiten. Sie sind somit Hilfsmittel der Kommunikation selbst selbst.
- 73 Verkehrsdaten sind notwendig, um die **Quelle der Kommunikation** zu ermitteln; sie bilden einen Ausgangspunkt für die Erhebung weiterer Beweise oder sind ein Bestandteil des Beweises für die Straftat. Aufgrund des enormen Volumens der täglich ausgetauschten Kommunikationen haben die Daten zu

diesen Kommunikationen jedoch eine sehr begrenzte Aufbewahrungsdauer. Es ist daher unerlässlich, zügig zu handeln, um den Weg der verdächtigen Kommunikation zurückzuverfolgen, bevor die Spuren verschwinden. Angesichts der oft langen Dauer der üblichen Verfahren der internationalen Rechtshilfe in Strafsachen sieht das Übereinkommen die Möglichkeit vor, auf das in Art. 17 StGB vorgesehene Verfahren der raschen Offenlegung zurückzugreifen. Dieses ermöglicht es, unverzüglich Informationen über den Kommunikationsweg zu erhalten und weitere Beweise zu sichern, bevor diese gelöscht werden, oder einen Verdächtigen zu identifizieren. Dieses beschleunigte und weniger formelle Verfahren steht im Einklang mit dem Grundsatz der Verhältnismäßigkeit, da die Beschaffung von Verkehrsdaten einen deutlich geringeren Eingriff in die Persönlichkeitsrechte darstellt als die Beschaffung von Inhaltsdaten, da sie nicht den Inhalt der Kommunikation offenlegt, sondern lediglich deren Verlauf.

Art. 1 Buchst. d ZGB enthält eine **abschließende** Aufzählung der Kategorien 74 von Verkehrsdaten, die im Übereinkommen einer Sonderregelung unterliegen, nämlich: Herkunft, Ziel, Weg, Uhrzeit, Datum, Umfang und Dauer der Kommunikation oder die Art des zugrunde liegenden Dienstes.

Der **Ursprung** und das **Ziel** entsprechen den Punkten im Netz, von denen 75 aus eine Kommunikation gesendet und empfangen wird. Sie werden je nach verwendeter Kommunikationsart durch Telefonnummern oder, allgemeiner, durch IP-Adressen identifiziert, die den betreffenden IT-Systemen zu einem bestimmten Zeitpunkt zugewiesen sind. Diese Identifikatoren ermöglichen nicht unbedingt die direkte Identifizierung eines Endnutzers, insbesondere bei dynamischen, gemeinsam genutzten oder durch Verfahren wie Netzwerkadressübersetzung (NAT), Relaisdienste (z. B. das TOR-Netzwerk) oder virtuelle private Netzwerke (VPN). Sie sind für strafrechtliche Ermittlungen von besonderer Bedeutung, da sie es ermöglichen, das IT-System oder den Netzwerkzugangspunkt am Ursprung oder am Ziel der Kommunikation zu ermitteln.

Die **Route** beschreibt den Weg, den die Kommunikation durch die 76 verschiedenen Relaispunkte des Netzwerks nimmt, insbesondere durch Router, Zwischenserver oder andere Transitinfrastrukturen. Sie entspricht der Abfolge der IT-Systeme, über die die Daten von ihrem Ursprungsort bis zu ihrem Zielort weitergeleitet werden. In der Praxis lässt sich dieser Weg anhand der von diesen verschiedenen Systemen generierten Daten teilweise

oder vollständig rekonstruieren, vorbehaltlich technischer Einschränkungen, die insbesondere mit der Netzwerkarchitektur, der Nutzung von Zwischendiensten oder der Verschlüsselung der Kommunikation zusammenhängen.

- 77 Die **Uhrzeit** und das **Datum** werden in koordinierter Weltzeit (UTC) angegeben. Diese Informationen sind unerlässlich, wenn es sich um dynamische IP-Adressen handelt. Da diese Adressen je nach den Bedürfnissen der Nutzer ständig neu zugewiesen werden, ist es unerlässlich, über diese Informationen zu verfügen, um beim Internetdienstanbieter erfragen zu können, welchem IT-System er zu einem bestimmten Zeitpunkt eine IP-Adresse zugewiesen hat. Diese Auskünfte müssen so schnell wie möglich eingeholt werden, da sie je nach Staat nur für einen Zeitraum von sechs bis maximal vierundzwanzig Monaten aufbewahrt werden. Nach Ablauf dieser Frist werden die Daten vernichtet, und es ist nicht mehr möglich, den Nutzer zu identifizieren, dem eine IP-Adresse zugewiesen wurde. Diese Schwierigkeit besteht hingegen nicht bei statischen IP-Adressen, da diese dauerhaft denselben Nutzern zugewiesen sind.
- 78 Die **Größe** der Kommunikation wird in Bit oder Byte angegeben und entspricht dem ausgetauschten Datenvolumen. Sie kann für Ermittler einen Hinweis auf die Art der ausgetauschten Daten darstellen, da bestimmte Arten von Inhalten, wie Bilder, Tonaufnahmen oder audiovisuelle Inhalte, grundsätzlich größere Datenmengen erzeugen als einfache Textnachrichten. Dieser Indikator ist jedoch angesichts der heutigen Techniken zur Komprimierung, Fragmentierung und Verschlüsselung von Datenströmen mit Vorsicht zu interpretieren.
- 79 Die **Dauer** der Kommunikation wird in Stunden, Minuten und Sekunden gemessen. Sie entspricht dem Zeitraum, in dem eine Verbindung bestand oder ein Datenaustausch zwischen den betroffenen IT-Systemen stattfand. Diese Information kann für die Ermittlungen nützliche Kontextangaben liefern, insbesondere um einmalige Verbindungen von länger andauernden oder wiederholten Verbindungen zu unterscheiden, ohne jedoch den Inhalt des während dieses Zeitraums stattgefundenen Austauschs preiszugeben.
- 80 Schließlich bezieht sich die **Art des zugrunde liegenden Dienstes** auf die Kommunikationsart oder die funktionale Kategorie des Dienstes, der im Rahmen des Datenaustauschs genutzt wurde, wie beispielsweise E-Mail,

Instant-Messaging-Dienste, das Ansehen von audiovisuellen Inhalten im Internet oder das Herunterladen von Daten. Es handelt sich um eine allgemeine Einstufung des genutzten Dienstes, die sich als schwierig erweisen kann, genau zu bestimmen, wenn mehrere Dienste innerhalb desselben Kommunikationsflusses kombiniert werden oder wenn die Daten gekapselt oder verschlüsselt sind.

LITERATURVERZEICHNIS

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994.

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible sous <https://rm.coe.int/16800cce5b>, visité le 10.01.2026 (cité : Rapport explicatif de la Convention sur la cybercriminalité).

Comité de la Convention cybercriminalité (T-CY), Guidance Notes, disponible sous <https://www.coe.int/fr/web/cybercrime/guidance-notes>, visité le 10.01.2026 (cité : Note d'orientation).

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 2 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 2 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 2 CCC N. XXX.

Kapitel II: Innerstaatlich zu treffende Massnahmen

Abschnitt 1: Materielles Strafrecht

Titel 1:

Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen

Art. 2 Rechtswidriger Zugang

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmassnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

GLIEDERUNG

I. Allgemeines.....	34
II. Rechtlich geschütztes Gut	35
III. Grundlegende Tatbestandsmerkmale	35
A. Ein Computersystem.....	35
B. Ein Zugang zum Computersystem	36
C. Die Rechtswidrigkeit	38
D. Die Absicht.....	39
IV. Zusätzliche fakultative Tatbestandsmerkmale	40
A. Zugriff unter Verletzung von Sicherheitsmaßnahmen	40
B. Die Absicht, Computerdaten zu erlangen oder eine andere besondere Absicht. .	41
C. Ein Computersystem, das mit einem anderen Computersystem verbunden ist ..	43
V. Vergleich mit dem Schweizer Recht	43
Literaturverzeichnis	45
Materialienverzeichnis.....	45

I. ALLGEMEINES

- 1 Der illegale Zugang zu einem Computersystem ist das Grunddelikt im Bereich der Cyberkriminalität. Häufig handelt es sich dabei um die notwendige kriminelle Vorleistung für die Begehung einer anderen Computerstraftat, wie z. B. der Verletzung der Integrität von Daten (Art. 4 CCC), der Verletzung der Integrität des Systems (Art. 5 CCC), der Computerfälschung (Art. 7 CCC) oder des Computerbetrugs (Art. 8 CCC). Manche Cyberkriminelle begnügen sich jedoch damit, sich aus Trotz oder allein wegen der damit verbundenen technischen Herausforderung unberechtigten Zugang zu einem Computersystem zu verschaffen, ohne eine nachfolgende Straftat zu begehen. Daher ist es gerechtfertigt, dieses Verhalten als solches unter Strafe zu stellen, anstatt es in den Straftaten aufgehen zu lassen, die in den nachfolgenden Artikeln unter Strafe gestellt werden. So macht sich der Täter allein durch die Tatsache, dass er sich Zugang zu einem Computersystem verschafft, des illegalen Zugangs schuldig. Es ist nicht erforderlich, dass er Daten aus dem Computersystem stiehlt oder verändert.
- 2 Manche mögen Hacking für eine relativ harmlose, spielerische Aktivität halten, die ein paar Geeks auf der Suche nach neuen Herausforderungen betreiben. Die Realität sieht jedoch ganz anders aus. Dieses Verhalten ist viel weiter verbreitet, als man auf den ersten Blick meinen könnte, und die Täter verfolgen weitaus weniger ehrenwerte Ziele als bloße Unterhaltung.
- 3 Natürlich ist die Einführung starker Sicherheitsmaßnahmen das wirksamste Mittel, um ein Computersystem vor unberechtigtem Zugriff zu schützen. Angesichts der Bedrohung oder Verletzung der Sicherheit von Computersystemen und -daten, die Hacking darstellt, müssen technische Maßnahmen von gesetzgeberischen Maßnahmen begleitet werden, die Cyberkriminelle von der Tat abhalten oder sie im Falle der Begehung bössartiger Handlungen bestrafen sollen. Auf diese Weise wird das Interesse von Organisationen und Einzelpersonen, ihre Computersysteme ohne Störungen oder Behinderungen jeglicher Art steuern, betreiben und kontrollieren zu können, bestmöglich geschützt.

II. RECHTLICH GESCHÜTZTES GUT

Art. 2 CCC schützt die Unverletzlichkeit von Computersystemen. Dieser 4
Schutz durch das Strafrecht ist aus mindestens zwei Gründen geboten.

Zum einen kann der illegale Zugriff auf ein Computersystem beim 5
Rechteinhaber erhebliche Instandsetzungskosten verursachen. Die Täter
verändern nämlich häufig Daten, um in das Innere des Systems einzudringen.
Außerdem bemerken die Opfer den Einbruch oft erst einige Zeit nach dem
Geschehen. Daher ist es besonders schwierig, herauszufinden, was von den
Tätern verändert wurde und welche neuen Daten das Computersystem als
Folge dieser Veränderung erzeugt hat. Sobald diese Daten identifiziert sind,
müssen sie in ihren ursprünglichen Zustand zurückversetzt werden. Diese
Vorgänge können sehr zeitaufwendig und daher sehr kostspielig sein.

Andererseits ermöglicht der illegale Zugang den Tätern, Informationen 6
einzusehen, zu denen sie keinen Zugang haben sollten (z. B. vertrauliche
Berichte, Geschäftsgeheimnisse, Kundenlisten, Buchhaltungsunterlagen,
Kreditkartennummern, persönliche Daten, ...). Diese Informationen können
dann auf dem Schwarzmarkt weiterverkauft werden, was für den
Rechteinhaber einen noch viel größeren Schaden verursachen kann als nur
die Wiederherstellung des Systemschutzes.

III. GRUNDLEGENDE TATBESTANDSMERKMALE

A. Ein Computersystem

Nach Art. 1 lit. a CCC "bezeichnet der Ausdruck 'Computersystem' eine 7
einzelne Vorrichtung oder eine Gesamtheit miteinander verbundener oder
verwandter Vorrichtungen, die in Ausführung eines Programms eine
automatische Datenverarbeitung bewirkt oder von der ein oder mehrere
Elemente eine automatische Datenverarbeitung bewirken". Der Begriff
Computersystem umfasst somit die gesamte Hardware (Hauptplatine,
Prozessor, Festplatte, Bildschirm, Tastatur, Drucker, ...) und Software (BIOS,
Betriebssystem, Software, Updates, ...) sowie die Geräte, die die Verbindung
dieser verschiedenen Elemente untereinander ermöglichen (Kabel, Router,
WiFi-Anschluss, ...).

- 8 Für weitere Details zu diesem Begriff wird auf die Ausführungen in Art. 1 CCC verwiesen.

B. Ein Zugang zum Computersystem

- 9 Man könnte versucht sein, den illegalen Zugang zu einem Computersystem mit dem Straftatbestand des Hausfriedensbruchs zu vergleichen. Der Zugang zum Computersystem wäre somit das digitale Äquivalent zum Eindringen in die Wohnung. Diese Analogie hat etwas Beruhigendes an sich, denn man kann sich die Situation intellektuell sehr gut vorstellen. Die virtuelle Welt ist jedoch komplexer als dies und die Konturen der juristischen Begriffe notwendigerweise verschwommener.
- 10 Es ist kompliziert, eine Analogie zur realen Welt zu ziehen. Wenn man dennoch eine Analogie ziehen müsste, könnte man den Zugang zu einem Computersystem mit dem Betreten einer mittelalterlichen Burg vergleichen. Der Zugang zur Burg ist durch eine Mauer und einen Wassergraben begrenzt. Das Haupteingangstor wird in der Regel von Wachen bewacht. Diese kontrollieren, ob die Personen, die die Festung betreten, auch wirklich dazu berechtigt sind. Sobald sie sich im Inneren befinden, haben die Personen je nach ihrem Rang Zugang zu bestimmten Teilen der Burg und zu anderen nicht. Der Rang wird von dem Herrscher festgelegt, dem die Burg gehört. In jedem Teil des Schlosses befinden sich Gegenstände, die angeschaut, berührt, verändert oder sogar zerstört werden können. Auch bei diesen Gegenständen bestimmt der Burgherr, wer was mit welchem Gegenstand tun kann. Der Burgherr ist der Einzige, der Zugang zu allen Räumen der Burg hat und mit allen Gegenständen in der Burg nach Belieben verfahren kann.
- 11 In einem Computersystem funktioniert es ähnlich wie in einer Ritterburg. Um auf das Computersystem zugreifen zu können, muss der Nutzer in der Regel einen Benutzernamen und ein Passwort eingeben. Nach der Anmeldung kann der Nutzer je nach seiner Akkreditierungsstufe, die vom Administrator des Computersystems festgelegt wird, auf das gesamte oder einen Teil des Computersystems zugreifen. Diese Akkreditierungsstufe bestimmt auch, was der Nutzer in den Teilen des Computersystems, auf die er Zugriff hat, tun oder nicht tun kann, d. h. nur den Titel der in einem Ordner enthaltenen Dokumente sehen, sie zum Lesen öffnen, bearbeiten oder löschen. Der Administrator ist der einzige, der auf das gesamte Computersystem zugreifen

kann und über die Rechte verfügt, die es ihm ermöglichen, alle gewünschten Aktionen mit den darin enthaltenen Daten durchzuführen.

Die Analogie zur realen Welt endet hier jedoch. Der Begriff des "Zugriffs" in der virtuellen Welt kann nicht mit dem Begriff des "Eindringens" in der realen Welt verglichen werden. In der Informatik bedeutet "Zugang", dass es dem Täter gelingt, eine Verbindung zu einem ganzen oder einem Teil eines Computersystems herzustellen. Es gibt also streng genommen keine physische Bewegung des Täters von einem Ort zu einem anderen.

Bei der einfachen Form der Straftat ist es unerheblich, auf welche Weise der Täter eine Verbindung zum Computersystem herstellt. Der Täter kann also eine Verbindung mittels eines lokalen Zugangs oder eines Fernzugriffs herstellen. Wenn der Täter eine lokale Verbindung zu einem Computersystem herstellt, zu dem er physischen Zugang hat, wird er dies mithilfe einer - materiellen oder virtuellen - Tastatur und einer Maus tun, bei Tablets und Smartphones sogar einfach mit den Fingern. Er kann auch ein Terminal verwenden, um sich mit einem zentralen Computersystem zu verbinden. Entscheidet sich der Autor stattdessen, eine Fernverbindung herzustellen, kann er dies über jedes beliebige Telekommunikationsnetz tun. Die Art des Netzwerks (lokal, öffentlich, privat, ...) sowie die Art der Verbindung (drahtgebunden oder drahtlos) sind unerheblich.

Auch das Ausmaß des Zugriffs ist für die Verwirklichung der Straftat nicht entscheidend. Der Zugriff kann vollständig sein, in diesem Fall erstreckt er sich auf das gesamte Computersystem. Er kann auch nur partiell sein. In diesem Fall betrifft er nur einen Teil des Computersystems. Dies ist beispielsweise der Fall, wenn der Täter nur auf die Sitzung eines Nutzers oder auf einen Teil der auf einem Server gespeicherten Daten zugreift.

Die Straftat ist vollendet, sobald die Verbindung mit dem Computersystem hergestellt ist. Dann hindert den Täter nichts mehr daran, sich Kenntnis von den im Computersystem enthaltenen Computerdaten zu verschaffen. Für die Vollendung der Straftat ist es jedoch nicht erforderlich, dass der Täter von den Daten Kenntnis erlangt. In der Praxis fallen diese beiden Ereignisse jedoch meist zusammen, da zu dem Zeitpunkt, an dem der Zugriff festgestellt wird, die Daten auf dem Bildschirm angezeigt werden.

Der Begriff des Zugriffs im Sinne von Art. 2 CCC ist klar von der Verletzung der Integrität der Daten in Art. 4 CCC zu unterscheiden. Um die Straftat zu

verwirklichen, reicht es aus, dass sich der Täter Zugang zu einem Computersystem verschafft. Auch wenn die Einrichtung eines illegalen Zugangs in der Praxis regelmäßig zur Veränderung von Daten führt, sind solche Beeinträchtigungen für die Begehung der Straftat nicht erforderlich.

- 17 Schließlich ist nur die Herstellung eines illegalen Zugangs strafbar. Die Aufrechterhaltung eines rechtmäßig eingerichteten Zugangs, nachdem der Rechteinhaber des Computersystems dem Nutzer mitgeteilt hat, dass er nicht mehr berechtigt ist, auf das System zuzugreifen, ist nicht strafbar. Zu denken ist hier insbesondere an einen Arbeitnehmer, der während seiner beruflichen Tätigkeit seinen privaten Computer nutzt, um sich mit dem Firmennetzwerk zu verbinden, und der nach seiner Entlassung weiterhin Dateien des Unternehmens aufruft. Die fehlende Strafbarkeit dauert jedoch nur so lange, wie die Verbindung besteht. Wenn er die Verbindung unterbricht und eine neue herstellt, macht er sich der Straftat schuldig. Diese Straffreiheit stellt unserer Meinung nach eindeutig eine unzutreffende Lücke dar, da die Parteien diese Möglichkeit bei der Ausarbeitung des Textes wahrscheinlich einfach nicht in Betracht gezogen haben.

C. Die Rechtswidrigkeit

- 18 Um strafbar zu sein, muss der Täter unrechtmäßig gehandelt haben. Dies bedeutet, dass zunächst festgestellt werden muss, ob das Computersystem öffentlich - d. h. für jedermann zugänglich - oder nur beschränkt zugänglich ist, oder ob es sich um eine Kombination aus beidem handelt. Wenn das Computersystem öffentlich ist, kann der Zugang keinesfalls unrechtmäßig sein und eine Straftat ist ausgeschlossen. Ist der Zugang zum gesamten oder einem Teil des Computersystems hingegen beschränkt, macht sich derjenige strafbar, der unbefugt darauf zugreift.
- 19 Wer auf welchen Teil des Computersystems zugreifen darf, bestimmt der Berechtigte des Computersystems. Strafbar sind somit nicht nur Personen, denen der Zugriff auf das Computersystem nicht gestattet wurde, sondern auch Personen, denen der Zugriff auf einen Teil des Computersystems gestattet wurde, die aber auf einen anderen Teil des Computersystems zugreifen, zu dem ihnen der Zugriff nicht gestattet wurde. Nicht strafbar sind hingegen Personen, denen der Zugriff auf das Computersystem von seinem Rechteinhaber gestattet wurde und die sich an die Beschränkungen dieses Zugriffs halten.

Der Berechtigte des Computersystems ist nicht immer auch der Administrator. Dies ist insbesondere bei mittleren und großen Computersystemen der Fall. In diesen Situationen wird die Verwaltung des Computersystems von seinem Rechtsinhaber an einen Drittverwalter delegiert. Dieser Administrator kann entweder eine natürliche Person oder eine juristische Person sein. In beiden Fällen ermächtigt der Rechtsinhaber des Computersystems den Administrator, zur Erfüllung seiner Aufgaben auf das System zuzugreifen. Der Administrator greift also nicht unberechtigt auf das Computersystem zu, solange er dies zum Zweck der Erfüllung seiner Aufgabe tut. Unberechtigt ist der Zugriff hingegen, wenn er zu einem anderen Zweck erfolgt, z. B. um private oder vertrauliche Informationen abzurufen, die nicht für ihn bestimmt sind. 20

Wenn die Verwaltung des Computersystems an ein Unternehmen delegiert wird, sind alle natürlichen Personen, die in diesem Unternehmen mit dieser Aufgabe betraut sind, zum Zugriff auf das System berechtigt. Dies ist hingegen nicht der Fall für natürliche Personen innerhalb dieser juristischen Person, denen diese Aufgabe nicht zugewiesen wurde. Wenn diese Personen auf das Computersystem zugreifen, tun sie dies unrechtmäßig, da sie dies nicht tun, um die Aufgabe zu erfüllen, die der juristischen Person übertragen wurde. 21

Eine Person, die speziell beauftragt wurde, die Sicherheit des Computersystems zu testen, und der es gelingt, sich Zugang zum Computersystem zu verschaffen, indem sie die eingerichteten Schutzmaßnahmen umgeht, handelt nicht unrechtmäßig, da sie von ihrem Rechtsinhaber dazu ermächtigt wurde. 22

D. Die Absicht

Der illegale Zugriff muss vorsätzlich erfolgen. Der Vorsatz muss sich auf alle objektiven Elemente der Straftat beziehen. Der Täter muss sich also bewusst sein, dass er sich unrechtmäßig Zugang zu einem Computersystem verschafft, und er muss den Willen dazu haben. Eventualvorsatz reicht aus. Wenn der Täter ahnt, dass er auf ein Computersystem, auf das er keinen Zugriff haben sollte, ganz oder teilweise zugreift, aber trotzdem eine Verbindung herstellt, macht er sich des unrechtmäßigen Zugriffs schuldig. Begeht der Täter hingegen einen Bedienungsfehler und stellt wider besseres Wissen eine nicht autorisierte Verbindung her, fehlt es an Vorsatz und der Straftatbestand ist nicht erfüllt. 23

- 24 Die Norm stellt nur die Herstellung des illegalen Zugangs unter Strafe, nicht aber die Aufrechterhaltung des Zugangs gegen den Willen des Rechteinhabers. Wer sich also versehentlich Zugang zu einem Computersystem verschafft, aber nach dem Einloggen den Inhalt des Systems erforscht, ist nicht strafbar.
- 25 Wenn der Täter irrtümlich annimmt, dass das Computersystem, auf das er zugreift, öffentlich ist, oder wenn er irrtümlich annimmt, dass er aus einem anderen Grund berechtigt ist, auf das System zuzugreifen, begeht er einen Tatsachenirrtum.

IV. ZUSÄTZLICHE FAKULTATIVE TATBESTANDSMERKMALE

- 26 Zum Zeitpunkt der Ausarbeitung des Übereinkommens über Computerkriminalität wollte eine Mehrheit der Vertragsparteien das reine Hacken unter Strafe stellen. Andere hingegen waren gegen eine generelle Strafbarkeit des Hackens mit der Begründung, dass das bloße Eindringen nicht unbedingt Schaden anrichtet und dass durch Hackinghandlungen in manchen Fällen sogar Sicherheitslücken entdeckt und geschlossen werden können. Um diesen Überlegungen Rechnung zu tragen und da die nationalen Gesetze vieler Länder bereits Bestimmungen enthielten, die das Hacken in verschiedenen Formen unter Strafe stellten, wurde den Vertragsparteien die Möglichkeit eingeräumt, die Strafbarkeit des illegalen Zugangs einzuschränken, indem sie die Erfüllung eines oder mehrerer zusätzlicher Tatbestandsmerkmale verlangten.

A. Zugriff unter Verletzung von Sicherheitsmaßnahmen

- 27 Die Cybercrime-Konvention gibt den Vertragsparteien zunächst die Möglichkeit, den illegalen Zugriff nur dann zu bestrafen, wenn er unter Verletzung von Sicherheitsmaßnahmen erfolgt. Deutschland, Finnland, Japan, Litauen, Peru, die Slowakische Republik, die Tschechische Republik und die Schweiz haben von dieser Möglichkeit Gebrauch gemacht.
- 28 Diese zusätzliche Anforderung bedeutet, dass das Computersystem vor unberechtigtem Zugriff geschützt werden muss. Mit anderen Worten: Wenn sich der Täter unberechtigt Zugang zu einem Computersystem verschafft, das nicht geschützt ist, ist er nicht strafbar.

Der Begriff der Sicherheitsmaßnahmen ist weit zu verstehen. Er umfasst 29 sowohl physische als auch virtuelle Sicherheitsmaßnahmen. Was die physischen Sicherheitsmaßnahmen betrifft, kann sich das Computersystem beispielsweise in einem abgeschlossenen Raum befinden, zu dem man nur mit einem Schlüssel, einer Magnetkarte, einem Fingerabdruck, einem Retina- oder Stimmabdruck Zugang hat. Auf virtueller Ebene können die Sicherheitsmaßnahmen insbesondere in einem Schutz durch Firewall, PIN-Code, Passwort oder auch in einer doppelten oder sogar dreifachen Authentifizierung bestehen.

Wenn es dem Täter nicht gelingt, die Sicherheitsmaßnahmen zu überwinden, 30 oder wenn er spontan beschließt, seine Aktivität zu beenden, bevor er die Sicherheitsmaßnahmen überwunden hat, ist nur ein Versuch denkbar. Dies ist jedoch problematisch, da man bei der Lektüre von Art. 11 Abs. 2 CCC feststellt, dass von den Vertragsparteien nicht verlangt wird, den Versuch des illegalen Zugangs unter Strafe zu stellen. Es steht also jedem Staat frei, diesen Aspekt so zu behandeln, wie er es für richtig hält, so dass dieses Verhalten nach dem nationalen Recht der Vertragsstaaten möglicherweise überhaupt nicht strafbar ist.

B. Die Absicht, Computerdaten zu erlangen oder eine andere besondere Absicht.

Eine weitere Möglichkeit für die Vertragsparteien besteht darin, zu verlangen, 31 dass der Täter in einer besonderen Absicht gehandelt hat. Mehrere Staaten haben von dieser Möglichkeit Gebrauch gemacht.

Die Vereinigten Staaten von Amerika haben beschlossen, zu verlangen, dass 32 der Täter in der Absicht gehandelt hat, Daten zu erlangen. Obwohl diese Möglichkeit den Vertragsparteien eingeräumt wurde, ist ihre Nutzung bedauerlich, da sie die Norm weitgehend ihrer Substanz beraubt. Die Bestimmung wurde nämlich speziell entwickelt, um die Handlungen von Hackern zu bestrafen, die sich aus Mutwillen Zugang zu Computersystemen verschaffen, ohne sich jedoch für die darin enthaltenen Daten zu interessieren. Die Forderung nach dieser speziellen Absicht scheint daher dem Geist der Norm zu widersprechen.

Belgien erklärte seinerseits, dass es den illegalen Zugang nur dann unter Strafe 33 stellt, wenn er in betrügerischer Absicht oder in der Absicht, Schaden

anzurichten, begangen wird. Die betrügerische Absicht scheint sich auf die Absicht zu beziehen, einen ungerechtfertigten Vorteil für sich selbst oder für andere zu erlangen. Was die Schädigungsabsicht betrifft, so handelt es sich wahrscheinlich um die Absicht, anderen in irgendeiner Form Schaden zuzufügen.

- 34 Das Fürstentum Andorra und die Slowakische Republik haben beschlossen, den unrechtmäßigen Zugang nur dann zu verfolgen, wenn er mit dem Ziel begangen wird, sich unrechtmäßig Daten zu verschaffen, diese zu beschädigen (nur im Fall des Fürstentums Andorra) oder in einer anderen strafbaren Absicht. Mit dieser Formulierung soll verhindert werden, dass Täter einer Verurteilung entgehen, weil sie einen anderen Zweck als die Beschaffung oder Beschädigung von Daten verfolgten. Unserer Ansicht nach muss sie jedoch im Lichte der in Art. 2 CCC aufgeführten besonderen Absichten interpretiert werden und diesen sowohl hinsichtlich des vom Täter verfolgten Zwecks als auch hinsichtlich ihrer deliktischen Intensität ähneln. Am 1. Januar 2021 wurde das slowakische Strafgesetzbuch geändert und der Vorbehalt der Slowakischen Republik angepasst. Der § 247 wurde neu gefasst. In seiner einfachen Form verlangt diese Bestimmung keinen besonderen Vorsatz mehr (§ 247 Abs. 1). In § 247 Abs. 2 ist hingegen eine qualifizierte Form vorgesehen, wenn der Täter einen erheblichen Schaden verursacht.
- 35 Schließlich hat Kanada angegeben, dass es den illegalen Zugang nur dann verfolgen würde, wenn er mit krimineller Absicht begangen wird. Der letztgenannte Begriff ist besonders unpräzise und führt daher zu erheblicher Rechtsunsicherheit. Darüber hinaus scheint er sich mit dem Begriff des Vorsatzes zu überschneiden. Er sollte daher unserer Ansicht nach restriktiv ausgelegt werden.
- 36 Chile hatte ursprünglich einen Vorbehalt eingelegt, der mit dem Kanadas identisch war. Es änderte jedoch seine Gesetzgebung im Jahr 2022. Nach der neuen Fassung ist der acceso ilícito strafbar, wenn er vorsätzlich begangen wird. Eine besondere Absicht ist nicht mehr erforderlich. Wenn der illegale Zugang jedoch mit dem Ziel begangen wird, die im Computersystem enthaltenen Daten zu erlangen oder zu nutzen, wird das Strafmaß erhöht.

C. Ein Computersystem, das mit einem anderen Computersystem verbunden ist

Die Cybercrime-Konvention ermöglicht es den Vertragsparteien schließlich, die Strafbarkeit des illegalen Zugangs auf Verbindungen zu beschränken, die unrechtmäßig über ein anderes Computersystem mit einem Computersystem hergestellt werden. Indem sie von dieser Möglichkeit Gebrauch machen, können die Vertragsparteien Fälle ausschließen, in denen sich der Täter physischen Zugang zu dem Computersystem verschafft, gegen das er sich richtet, ohne über ein Netzwerk zu gehen. 37

Die einzigen Staaten, die von dieser Möglichkeit Gebrauch gemacht haben, sind die Slowakische Republik und Japan. Das slowakische Strafgesetzbuch wurde inzwischen geändert. Die Neufassung des § 247, die am 1. Januar 2021 in Kraft trat, sieht dieses Erfordernis in der aktuellen Fassung nicht mehr vor, sodass der Vorbehalt der Slowakischen Republik angepasst wurde. 38

V. VERGLEICH MIT DEM SCHWEIZER RECHT

Im Schweizer Recht wird Hacking durch Art. 143^{bis} StGB unter Strafe gestellt. Diese Bestimmung stellt den unberechtigten Zugriff auf ein fremdes, besonders gegen Zugriff geschütztes Computersystem mittels einer Datenübertragungsvorrichtung unter Strafe. Diese Norm entspricht jedoch in dreierlei Hinsicht nicht den Anforderungen von Art. 2 CCC. 39

Erstens unterscheidet die Konvention nicht zwischen Computersystemen. Es schützt die Integrität aller Computersysteme, unabhängig von ihrer Zugehörigkeit. Art. 143^{bis} Abs. 1 StGB hingegen stellt nur den unberechtigten Zugang zu einem Computersystem, das "einem anderen gehört", unter Strafe. Angesichts der Tatsache, dass sich diese Bestimmung im zweiten Titel des Strafgesetzbuches, d. h. Straftaten gegen das Vermögen, befindet, muss diese Formulierung im Hinblick auf die dinglichen Rechte ausgelegt werden. Das Computersystem muss also einer anderen Person als dem Urheber gehören. Wenn der Täter der Eigentümer oder Miteigentümer des Computersystems ist, ist dieser Tatbestand nicht erfüllt, da es nicht einer anderen Person gehört. Wenn also mehrere Sitzungen in demselben Computersystem eröffnet wurden, ist der Täter, der (Mit-)Eigentümer des Computersystems ist und auf eine andere Sitzung als seine eigene zugreift, nicht strafbar. Die Mehrheitsmeinung in der Lehre ist dagegen der Ansicht, dass unter 40

"fremdbesitzend" zu verstehen ist, dass eine andere Person als der Urheber berechtigt ist, auf das Computersystem oder ein Computeruntersystem zuzugreifen und darüber zu verfügen. Eine solche Auslegung würde jedoch dazu führen, dass der Begriff "einem anderen gehörend" redundant mit dem Tatbestandsmerkmal der Rechtswidrigkeit des Zugangs ist. Wenn der Gesetzgeber diese beiden Elemente getrennt erwähnt hat, so deshalb, weil es sich um zwei Begriffe handelt, die unabhängig voneinander analysiert werden müssen. Um der Konvention zu entsprechen, sollte daher der Begriff "andere" in Art. 143^{bis} Abs. 1 StGB gestrichen werden.

- 41 Art. 143^{bis} Abs. 1 StGB verlangt, dass sich der Täter mit Hilfe einer Datenübertragungsvorrichtung Zugang zum Computersystem verschafft hat. Dies hat beispielsweise zur Folge, dass ein Täter, der die Abwesenheit seines Opfers nutzt, um in dessen Büro einzudringen und sich direkt mit dessen Computer zu verbinden, sich nicht des unberechtigten Zugriffs auf ein Computersystem schuldig macht, da er keine Datenübertragungsvorrichtung verwendet. Art. 2 Abs. 2 CCC erlaubt es den Vertragsparteien, die Strafverfolgung auf den unrechtmässigen Zugang zu beschränken, der mittels eines Computersystems begangen wird, das mit einem anderen Computersystem verbunden ist. Die Schweiz hat jedoch nicht erklärt, von dieser Möglichkeit Gebrauch zu machen. Folglich sollte das Tatbestandsmerkmal des Zugriffs mittels einer Datenübertragungsvorrichtung gestrichen werden.
- 42 Schliesslich ist in Art. 143^{bis} StGB eine Straftat verankert, die nur auf Antrag verfolgt wird. Wenn eine Straftat nur auf Antrag verfolgt wird, kann eine Strafbehörde nicht selbst tätig werden. Da ein Lehrstreit darüber besteht, ob ein im ersuchenden Staat gestellter Strafantrag ausreicht, um die internationale Zusammenarbeit in Gang zu setzen, wäre es klug, den unberechtigten Zugriff auf ein Computersystem von Amts wegen zu verfolgen.
- 43 Angesichts der vorstehenden Ausführungen muss festgestellt werden, dass das Schweizer Recht nicht mit Art. 2 CCC übereinstimmt. Art. 143^{bis} StGB sollte daher geändert werden.

Die in diesem Beitrag enthaltenen Fachbegriffe der Informatik wurden mit Hilfe von Herrn Yannick Jacquy, eidgenössisch diplomierter ICT-Manager, verfasst. Ihm sei an dieser Stelle herzlich gedankt.

LITERATURVERZEICHNIS

Dupuis Michel / Geller Bernard / Monnier Gilles / Moreillon Laurent / Piguet Christophe / Bettex Christian / Stoll Daniel (éditeurs), Code pénal - Petit commentaire, 2. éd., Bâle 2017

Pfister Christa, Hacking in der Schweiz, Diss., Zürich, 2008

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Stratenwerth Günter / Bommer Felix, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8. éd., Berne, 2022

Trechsel Stefan / Cramer Dean, in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in : Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible sous <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible sous https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 3 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 3 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 3 CCC N. XXX.

Art. 3 Rechtswidriges Abfangen

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschliesslich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei

kann als Voraussetzung vorsehen, dass die Straftat in unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

GLIEDERUNG

I. Allgemeines.....	50
II. Geschütztes Rechtsgut	50
III. Grundlegende konstitutive Elemente	50
A. Computerdaten	50
B. Eine nicht-öffentliche Übermittlung	51
1. Der Begriff der Übertragung	51
2. Der nicht-öffentliche Charakter.....	52
C. Der Sonderfall der elektromagnetischen Emissionen.....	53
D. Das Abfangen mit technischen Mitteln.....	54
E. Die Rechtswidrigkeit	55
F. Absicht	57
IV. Zusätzliche fakultative Tatbestandsmerkmale	57
A. Die Absicht, Computerdaten zu erhalten oder eine andere besondere Absicht..	57
B. Ein Computersystem, das mit einem anderen Computersystem verbunden ist...	58
V. Vergleich mit dem Schweizer Recht	58
Literaturverzeichnis	60
Materialienverzeichnis.....	60

I. ALLGEMEINES

- 1 Um einen umfassenden Rechtsschutz zu gewährleisten, musste der illegale Zugang um das illegale Abfangen ergänzt werden. Wie bereits erwähnt (vgl. Art. 2 N. 9 ff.), stellt der illegale Zugang das rechtswidrige Eindringen in das Computersystem und die Einsichtnahme in die darin gespeicherten Daten durch Unbefugte unter Strafe. Das rechtswidrige Abfangen wiederum sanktioniert die Verletzung der Vertraulichkeit von Daten, die innerhalb des Computersystems zirkulieren, sowie von Daten, die zwischen dem Computersystem und der Außenwelt ausgetauscht werden.

II. GESCHÜTZTES RECHTSGUT

- 2 Diese Bestimmung schützt das Recht auf Vertraulichkeit der übertragenen Daten. Der Verstoß stellt die gleiche Verletzung des Rechts auf Kommunikationsgeheimnis dar wie das klassische Abhören und Aufzeichnen von Telefongesprächen zwischen Personen. Art. 3 CCC übernimmt die Garantie des Rechts auf Achtung des Briefverkehrs aus Art. 8 EMRK und wendet sie auf alle Formen der elektronischen Datenübertragung an, unabhängig davon, ob die Übertragung per Telefon, Fax, E-Mail oder Datei erfolgt.

III. GRUNDLEGENDE KONSTITUTIVE ELEMENTE

A. Computerdaten

- 3 Nach Art. 1 lit. b CCC bedeutet "Computerdaten" jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Datenverarbeitung geeigneten Form, einschließlich eines Programms, das ein Computersystem veranlassen kann, eine Funktion auszuführen". Der Begriff Computerdaten ist also sehr weit gefasst, da er unter anderem alle Buchstaben, Symbole oder Programmcodes umfasst, die von einem Computersystem eingegeben, verarbeitet und gespeichert werden können.
- 4 Für weitere Einzelheiten zu diesem Begriff wird auf die Ausführungen zu Art. 1 CCC verwiesen.

B. Eine nicht-öffentliche Übermittlung

1. Der Begriff der Übertragung

Anders als die Etymologie des Begriffs "Übertragung" vermuten lassen könnte, ⁵ bezieht sich der Begriff der Übertragung in Art. 3 in initio CCC nicht nur auf den Fernaustausch zwischen zwei Geräten. Wie die Präpositionen "nach", "aus" oder "innerhalb" eines Computersystems nahelegen, bezieht er sich auf alle Daten, die im Umlauf sind. Die einzigen Daten, die nicht unter diesen Begriff fallen, sind diejenigen, die fest auf einem Datenträger gespeichert sind, z. B. auf einer Festplatte, einem USB-Stick oder einer DVD.

Die Datenübertragung "innerhalb" eines Computersystems betrifft Daten, die ⁶ insbesondere in und zwischen dem Motherboard, dem Prozessor, der Grafikkarte, dem Computerbildschirm oder dem Drucker zirkulieren. Sie erstreckt sich sogar auf Daten, die im Arbeitsspeicher des Computersystems gespeichert sind, da diese Daten nicht dauerhaft in diesem Speicher abgelegt werden, sondern dort nur für einige Augenblicke aufbewahrt werden, bevor sie innerhalb des Computersystems weiterfließen.

Datenübertragungen "an" oder "von" einem Computersystem setzen voraus, ⁷ dass der Empfänger oder der Absender der Daten ein Computersystem ist, wobei der andere ein Mensch oder ein Computersystem sein kann.

Bei der Übertragung von Daten von einem Menschen "an" ein ⁸ Computersystem geht es um die Eingabe von Daten durch den Menschen in das Computersystem, z. B. mithilfe einer Tastatur, einer Maus oder eines Joysticks. Umgekehrt ist mit der Übertragung von Daten an den Menschen "aus" dem Computersystem die Wiedergabe von Daten aus dem Computersystem an den Menschen gemeint, indem die Daten auf einem Bildschirm angezeigt werden oder ein Dokument von einem Drucker ausgedruckt wird.

Wenn schließlich die Datenübertragung zwischen zwei Computersystemen ⁹ erfolgt, findet sie sowohl "zu" als auch "von" einem Computersystem statt. Dies ist insbesondere bei einem Austausch zwischen einem Computer und einem Server, zwischen zwei Computern oder auch zwischen einem Computer und einem Smartphone der Fall. Dabei spielt es keine Rolle, ob die beiden Computersysteme derselben Person oder verschiedenen Personen gehören. Ebenso ist es unerheblich, wie die Daten übertragen werden. Daten

können über eine drahtgebundene oder drahtlose Verbindung ausgetauscht werden (Wifi, NFC, Bluetooth, Radiowelle, ...).

- 10 Die vorstehenden Ausführungen zeigen, dass der Begriff der Übertragung sehr weit gefasst ist. Um den Anwendungsbereich dieser Bestimmung einzuschränken, erlaubt Art. 3 in fine CCC den Vertragsparteien, die Strafverfolgung allein auf das rechtswidrige Abfangen von Daten zu beschränken, die zwischen zwei über eine Fernverbindung verbundenen Computersystemen übertragen werden.

2. Der nicht-öffentliche Charakter

- 11 Art. 3 CCC bezieht sich nur auf nicht-öffentliche Übertragungen. Die Nichtöffentlichkeit bezieht sich auf die Übermittlung und nicht auf die übermittelten Daten. Es ist daher unerheblich, ob die übermittelten Daten öffentlich oder privat sind. Ausschlaggebend ist allein die Art der Übermittlung.
- 12 Unserer Ansicht nach ist eine Übermittlung nicht öffentlich, wenn sie auf eine bestimmte Anzahl von Personen oder auf bestimmte Personen beschränkt ist. Dies ist insbesondere der Fall bei der Übertragung einer Präsentation mittels Videokonferenz, die nur von einer begrenzten Anzahl von Teilnehmern verfolgt werden kann, oder bei Filmen, die von einem "Streaming"-Unternehmen nur seinen Abonnenten zur Verfügung gestellt werden.
- 13 Der Begriff der nicht-öffentlichen Übertragung bedeutet jedoch nicht, dass die Übertragung über ein Netz erfolgen muss, das nicht öffentlich ist. Die Übertragung kann unter Verwendung eines öffentlichen Netzwerks erfolgen; die Übertragung muss lediglich auf eine bestimmte Anzahl von Personen beschränkt sein.
- 14 Um eine Übertragung auf eine bestimmte Anzahl von Personen zu beschränken, müssen notwendigerweise technische Maßnahmen ergriffen werden. Es wird jedoch nicht verlangt, dass diese Sicherheitsmaßnahmen besonders weitreichend sind. Ein System, mit dem kontrolliert werden kann, ob die Person, die auf die Übertragung zugreifen möchte, zu den berechtigten Personen gehört, ist ausreichend. So ist es denkbar, dass man einem per E-Mail versandten Link folgen, einen zuvor bereitgestellten Code eingeben oder sich mit einem Benutzernamen und einem Passwort identifizieren muss.

C. Der Sonderfall der elektromagnetischen Emissionen

Als das Übereinkommen über Cyberkriminalität zwischen April 1997 und 15
Dezember 2000 ausgearbeitet wurde, wollten die Experten die
technologischen Entwicklungen vorwegnehmen. Das illegale Abfangen wurde
daher nicht nur auf die Datenübertragung beschränkt, sondern auch auf
elektromagnetische Emissionen ausgeweitet.

Um zu verstehen, wie das Abfangen von elektromagnetischen Emissionen 16
funktioniert, muss man sich vergegenwärtigen, dass Computerdaten in binärer
Sprache einer Folge von "0" und "1" entsprechen. In dieser Form werden die
Daten von den Computersystemen verarbeitet. Aus mikrotechnischer Sicht
müssen daher für eine "0" und für eine "1" unterschiedliche elektrische
Impulse erzeugt werden. Dafür sind Transistoren zuständig. Schematisch
betrachtet bestehen Computersysteme aus einer Vielzahl von Transistoren.
Diese sorgen dafür, dass die elektrische Spannung, die durch die
elektronischen Komponenten des Computersystems fließt, von niedrig bis
hoch variiert, je nachdem, ob das verarbeitete Bit eine "0" oder eine "1" ist.
Diese unzähligen Spannungsschwankungen erzeugen ein elektromagnetisches
Feld, das sich um das Computersystem herum ausbreitet. Dadurch kann eine
in der Nähe befindliche Person, die mit einem geeigneten Gerät ausgestattet
ist, diesen Strom auffangen, ihn wieder in "0" und "1" umwandeln und so die
vom Computersystem verarbeiteten Computerdaten rekonstruieren.

Nach Ansicht der Experten erschien das rechtliche Arsenal unvollständig, 17
wenn man sich darauf beschränkte, das Abfangen von Daten, die in, zu oder
von einem Computersystem übertragen werden, zu bestrafen, ohne
gleichzeitig das Abfangen der von einem Computersystem ausgestrahlten
elektromagnetischen Wellen unter Strafe zu stellen. Dies wäre in der realen
Welt gleichbedeutend damit gewesen, das Abhören einer Person in ihrer
Wohnung mithilfe eines Mikrofons zu bestrafen, während das Abhören der
Gespräche dieser Person von hinter der Wohnungstür aus straffrei bliebe.

Insbesondere ist daran zu erinnern, dass zur Zeit der Ausarbeitung des 18
Konventionstextes die Verwendung von Faxgeräten weit verbreitet war.
Dieses Gerät sendete unverschlüsselte Daten mit einer Frequenz und einer
Stromstärke, die es relativ leicht ermöglichten, sie zu empfangen und dann in
einer verständlichen Sprache zu rekonstruieren. Experten erkannten darin
sicherlich eine Sicherheitslücke, die von Cyberkriminellen ausgenutzt werden

könnte, und nahmen daher das Abfangen elektromagnetischer Wellen in die Liste der strafbaren Verhaltensweisen auf.

- 19 Im Laufe der Jahre ist das Faxgerät fast vollständig verschwunden. Heutzutage ist das Auffangen von elektromagnetischen Wellen aufgrund der technischen Schwierigkeiten, diese Signale zu empfangen, sehr marginal oder gar nicht mehr vorhanden. Die heute im Computerbereich verwendeten Stromkabel sind viel stärker isoliert als Ende der 1990er Jahre und die elektrischen Impulse sind viel schwächer. Gleichzeitig ist die Menge an Daten, die jede Sekunde ausgetauscht wird, explosionsartig angestiegen. Daher ist es heute nahezu unmöglich, die von einer einzigen Quelle ausgehenden Magnetwellen aufzufangen und sie zu verständlichen Daten zusammenzusetzen.
- 20 Bei der Ausarbeitung des Konventionstextes konnten die Experten jedoch nicht vorhersehen, in welche Richtung sich die Technologie entwickeln würde. Daher ist dieses Verhalten - auch wenn es mittlerweile anekdotisch ist - in der Liste der nach Art. 3 CCC unter Strafe gestellten Verhaltensweisen enthalten.

D. Das Abfangen mit technischen Mitteln

- 21 Art. 3 CCC gilt nur für das Abfangen von Daten, das mit technischen Mitteln durchgeführt wird. Die physische Entwendung von Daten, insbesondere der Diebstahl eines per Post versandten USB-Sticks oder der Diebstahl eines eingeschalteten und entsperrten Laptops an einem öffentlichen Ort, wird daher durch diese Bestimmung nicht unter Strafe gestellt.
- 22 Das in Art. 3 CCC erwähnte Abfangen kann entweder direkt oder indirekt erfolgen. Direkt fängt der Täter die Daten ab, wenn er sich Zugang zum Computersystem selbst verschafft. Die einfachste Form ist die Installation eines Trojaners im Computersystem, wodurch sich der Täter Zugang verschafft. Der Täter kann auch eine Hintertür (Backdoor) verwenden oder eine Sicherheitslücke ausnutzen. All diese Techniken ermöglichen es dem Täter, in Echtzeit Kenntnis von den Daten zu erlangen, die im Computersystem zirkulieren.
- 23 Das Abfangen wird als indirekt bezeichnet, wenn der Täter den Datenstrom abfängt, der zwischen zwei Geräten ausgetauscht wird. Dies ist beispielsweise der Fall, wenn der Datenstrom abgefangen wird, der zwischen einem Gerät und einem WLAN-Hotspot, mit dem es verbunden ist, fließt. Innerhalb eines

lokalen Netzwerks (LAN) kann der Täter auch die MAC-Adresse eines Computersystems zum Zeitpunkt des Broadcasts missbrauchen, um sich die Datenpakete senden zu lassen, die für das System bestimmt waren, dessen Adresse missbraucht wurde. Eine weitere Technik ist das sogenannte Port Mirroring. Ursprünglich dient dieses System dazu, die innerhalb eines Netzwerks ausgetauschten Daten zu kontrollieren. Dazu wird eine Kopie aller Daten, die über einen Netzwerkschalter (Switch) laufen, an ein Computerkontrollsystem gesendet. Indem er die Kontrolle über den Netzwerkschalter übernimmt, kann der Täter die kopierten Daten jedoch auf sein eigenes Computersystem umleiten, wodurch er Kenntnis von allen über das Netzwerk ausgetauschten Daten erhält.

Der von den Parteien verwendete Begriff der "technischen Mittel" ist sehr 24 weit gefasst und unpräzise. Er wird auch nicht von einer beispielhaften Liste begleitet. Diese Entscheidung soll wahrscheinlich bezwecken, dass sich der Standard leichter an technologische Neuerungen anpassen kann. Auf jeden Fall handelt es sich um Geräte, die das Abhören, Steuern oder Überwachen von Kommunikationsinhalten ermöglichen. Es handelt sich also um technische Geräte, die an Übertragungsleitungen angeschlossen sind, sowie um Geräte zum Sammeln und Aufzeichnen von drahtloser Kommunikation. Die technischen Mittel, von denen in Art. 3 CCC die Rede ist, sind jedoch nicht auf Hardwaresysteme beschränkt. Auch Software, Passwörter und andere Codes gehören dazu.

E. Die Rechtswidrigkeit

Um strafbar zu sein, muss der Täter unrechtmäßig gehandelt haben. Wer die 25 Daten zur Kenntnis nehmen darf, bestimmt der Rechteinhaber der Daten. Strafbar sind somit alle Personen, die nicht zur Einsichtnahme in die Daten berechtigt waren. Nicht strafbar sind hingegen Personen, die vom Berechtigten zur Kenntnisnahme der Daten ermächtigt wurden oder die aufgrund eines Gesetzes oder eines Vertrags dazu berechtigt sind.

Die nationalen Gesetze enthalten in der Tat Ausnahmen von der garantierten 26 Vertraulichkeit der Daten. Sie erlauben es insbesondere den Nachrichtendiensten, Kenntnis von Daten zu erlangen, die nicht für sie bestimmt sind. Sie ermöglichen es auch den Strafverfolgungsbehörden, im Rahmen einer strafrechtlichen Untersuchung einen Datenfluss in Echtzeit zu überwachen. Solche Abhörmaßnahmen sind nicht illegal, solange sie unter

striktter Einhaltung der geltenden gesetzlichen Bestimmungen durchgeführt werden. Eine Überwachung darf jedoch nur in schwerwiegenden Fällen eingerichtet werden und muss einer nachträglichen gerichtlichen Kontrolle unterliegen.

- 27 Das Abfangen von Daten gilt auch dann nicht als rechtswidrig, wenn es vertraglich erlaubt ist. Dies ist insbesondere der Fall, wenn der Administrator des Computersystems mit der Wartung beauftragt ist. In diesem Fall macht er sich nicht strafbar, wenn er die Daten abfängt, die er für seine Arbeit benötigt, da er vom Rechteinhaber dazu ermächtigt wurde. Ebenso macht sich die Person, die für die Überwachung eines Netzwerks zuständig ist, nicht strafbar, wenn sie Daten abfängt, die sie durch die bestimmungsgemäße Nutzung, insbesondere durch Port Mirroring, erhalten hat. Wenn diese Personen jedoch die ihnen zur Verfügung stehenden technischen Möglichkeiten nutzen, um Daten abzufangen, die für die Ausführung ihrer Arbeit nicht erforderlich sind, handeln sie unrechtmäßig.
- 28 Im Zusammenhang mit Arbeitsverhältnissen ist ein rechtmäßiges Abfangen von Daten denkbar, allerdings unter restriktiven Bedingungen. Im Allgemeinen hat der Europäische Gerichtshof für Menschenrechte festgestellt, dass die private Kommunikation von Arbeitnehmern durch Art. 8 EMRK geschützt ist. Eine Überwachung durch den Arbeitgeber ist daher nur dann denkbar, wenn der Arbeitnehmer über die Überwachung seiner Kommunikation, die Art und den Umfang dieser Überwachung sowie den Grad des Eingriffs in sein Privatleben und seine Korrespondenz informiert wurde. Wenn der Arbeitgeber diese Bedingungen erfüllt, ist das Abfangen von Daten seiner Angestellten rechtmäßig.
- 29 Ursprünglich war Art. 3 CCC nicht dazu gedacht, gängige Geschäftspraktiken zu bestrafen, die darauf abzielen, Informationen über Nutzer zu erhalten. Seit dem Inkrafttreten des Übereinkommens über Computerkriminalität haben sich die Geschäftspraktiken erheblich verändert, und die Informationen, die kommerzielle Unternehmen zur gezielten Ausrichtung ihrer Werbung zu erhalten suchen, werden immer wichtiger. Infolgedessen haben die nationalen Gesetze den Daten- und Verbraucherschutz erheblich gestärkt. Es ist daher sehr häufig geworden, dass Websites die Zustimmung von Internetnutzern einholen müssen, bevor sie Daten über sie sammeln, insbesondere mithilfe von "Cookies". Ohne die Zustimmung des Rechteinhabers könnte das Sammeln solcher Daten ein illegales Abfangen darstellen.

F. Absicht

Das rechtswidrige Abfangen muss vorsätzlich erfolgen. Der Vorsatz muss sich 30 auf alle objektiven Elemente der Straftat beziehen. Der Täter muss sich also bewusst sein, dass er sich Daten in unzulässiger Weise verschafft, und er muss den Willen dazu haben. Eventualvorsatz reicht aus. In der einfachen Form ist es unerheblich, welchen Zweck der Täter verfolgt.

IV. ZUSÄTZLICHE FAKULTATIVE TATBESTANDSMERKMALE

Art. 3 CCC ermöglicht es den Vertragsparteien, die Strafbarkeit auf bestimmte 31 besondere Handlungen zu beschränken, indem sie ein oder zwei Tatbestandsmerkmale hinzufügen, die am Ende dieser Bestimmung aufgeführt sind.

Je nachdem, wie das illegale Abfangen in nationales Recht umgeschrieben 32 wird, kann dieser Straftatbestand eng mit dem illegalen Zugang (Art. 2 CCC) verbunden sein. Angesichts der Tatsache, dass sich einige Staaten dafür entschieden haben, die Strafbarkeit des illegalen Zugangs auf Fälle zu beschränken, die mit besonderer Absicht oder mittels eines Computersystems, das mit einem anderen Computersystem verbunden ist, begangen werden, war es notwendig, diesen Staaten zu ermöglichen, das illegale Abfangen auf eben diese Fälle zu beschränken.

A. Die Absicht, Computerdaten zu erhalten oder eine andere besondere Absicht.

Die erste Möglichkeit, die den Vertragsparteien zur Verfügung steht, besteht 33 darin, zu verlangen, dass der Täter in einer besonderen Absicht gehandelt hat. Mehrere Staaten haben von dieser Möglichkeit Gebrauch gemacht.

Kanada, Japan und Peru haben angegeben, dass sie das rechtswidrige 34 Abfangen nur dann verfolgen würden, wenn es in krimineller Absicht begangen wurde. Der letztgenannte Begriff ist besonders unpräzise und führt daher zu erheblicher Rechtsunsicherheit. Darüber hinaus scheint er sich mit dem Begriff des Vorsatzes zu überschneiden. Er sollte daher unserer Ansicht nach restriktiv ausgelegt werden.

- 35 Chile hatte ursprünglich denselben Vorbehalt wie Kanada, Japan und Peru eingelegt. Es änderte jedoch seine Gesetzgebung im Jahr 2022. In der neuen Fassung ist für die interceptación ilícita kein besonderer Zweck mehr erforderlich.
- 36 Die Schweiz erklärte ihrerseits, dass sie das illegale Abfangen nur dann verfolgen würde, wenn der Täter in der Absicht der unrechtmäßiger Bereicherung gehandelt habe.
- 37 Während sie erklärt hatten, den rechtswidrigen Zugang nur unter der Bedingung zu verfolgen, dass der Täter von einer besonderen Absicht geleitet wird, verzichteten das Fürstentum Andorra, Belgien, die Vereinigten Staaten von Amerika und die Slowakische Republik darauf, diese gleiche Anforderung für das rechtswidrige Abfangen zu stellen.

B. Ein Computersystem, das mit einem anderen Computersystem verbunden ist.

- 38 Die Cybercrime-Konvention erlaubt den Vertragsparteien auch, die Strafbarkeit des illegalen Abfangens nur auf Daten zu beschränken, die zwischen zwei miteinander verbundenen Computersystemen übertragen werden. Die einzigen Staaten, die von dieser Möglichkeit Gebrauch gemacht haben, sind Japan und Peru.
- 39 Auch in diesem Fall ist es überraschend, dass die Slowakische Republik auf die Nutzung dieser Möglichkeit verzichtet hat, obwohl sie ausdrücklich erklärt hatte, dass sie den illegalen Zugriff nur dann verfolgen würde, wenn er mittels eines Computersystems begangen wird, das mit einem anderen Computersystem verbunden ist.

V. VERGLEICH MIT DEM SCHWEIZER RECHT

- 40 Der Bundesrat räumte in seiner Botschaft über die Genehmigung und Umsetzung des Übereinkommens des Europarats über die Cyberkriminalität ein, dass "das schweizerische Strafrecht keine Art. 3 des Übereinkommens entsprechende Regelung kennt, mehrere Strafnormen jedoch einen teilweisen Schutz gewährleisten". Dabei handelte es sich seiner Meinung nach um eine Kombination der Art. 143, 143bis und 321^{ter} StGB. In Wirklichkeit ist dies absolut nicht der Fall.

Art. 143^{bis} StGB stellt nur das Eindringen in ein Computersystem unter Strafe 41
und nicht das Abfangen von Daten.

Was Art. 321^{ter} StGB betrifft, so stellt er ein reines Eigenvergehen unter Strafe, 42
da die Straftat nur von einem Angestellten eines Unternehmens begangen
werden kann, das den Post- oder Telekommunikationsdienst erbringt.

Was Art. 143 StGB betrifft, so ist dies die Norm, die Art. 3 CCC am nächsten 43
kommt. Um den Anforderungen des Übereinkommens zu entsprechen, müsste
diese Bestimmung jedoch in vier Punkten geändert werden.

Zunächst einmal sind die von diesen beiden Normen geschützten Rechtsgüter 44
unterschiedlich. Art. 3 CCC schützt die Vertraulichkeit der übermittelten
Daten, während Art. 143 StGB "das Recht des rechtmäßigen Empfängers der
Daten, frei und nach seinem Willen über sie zu verfügen", schützt. Das durch
Art. 143 StGB geschützte Rechtsgut sollte daher angepasst werden.

Zweitens stellt Art. 3 CCC das Abfangen nicht öffentlicher Übertragungen 45
unter Strafe, wobei es keine Rolle spielt, ob die übertragenen Daten öffentlich
sind oder nicht. Art. 143 StGB stellt jedoch nur die Entwendung von Daten
unter Strafe, die gegen jeden Zugriff besonders geschützt sind. Die
Entwendung öffentlicher Daten, die nicht öffentlich übermittelt werden, fällt
daher nicht unter Art. 143 StGB. In der Praxis ist dies jedoch der häufigste Fall,
da elektronisch übermittelte Daten in der Regel nicht besonders vor dem
Zugriff geschützt sind.

Zweitens schützt Art. 143 StGB nur das Verfügungsrecht über Daten. 46
Computerdaten haben jedoch nicht immer einen intrinsischen Wert. Die
Forderung nach einer unrechtmäßigen Bereicherungsabsicht bedeutet daher,
dass der strafrechtliche Schutz in allen Fällen, in denen der Täter wertlose
Daten entwendet, ausgeschlossen ist. In Anbetracht des geschützten
Rechtsguts sollte dieses Tatbestandsmerkmal gestrichen werden.

Schließlich beschränkt sich Art. 3 CCC nicht nur auf nicht-öffentliche 47
Übertragungen, sondern schließt auch elektromagnetische Emissionen ein.
Diese sind jedoch nicht durch Art. 143 StGB geschützt. Sie sollten daher dort
hinzugefügt werden.

Aus all diesen Gründen muss festgestellt werden, dass das Schweizer Recht 48
nicht mit Art. 3 CCC übereinstimmt und daher angepasst werden sollte.

Die in diesem Beitrag enthaltenen Fachbegriffe der Informatik wurden mit Hilfe von Herrn Yannick Jacquey, eidgenössisch diplomierter ICT Manager, verfasst. Ihm sei an dieser Stelle herzlich gedankt.

LITERATURVERZEICHNIS

Oberholzer Niklaus, in: Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Treccani Jean, Interceptions électroniques, in : Plus de sécurité, moins de liberté, les techniques d'investigation et de preuve en question, Zurich et Coire 2003

Trechsel Stefan / Cramer Dean, in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Trechsel Stefan / Lehmkuhl Marianne Johanna , in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in: Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible sous <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible sous https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, FF 2010 4275, disponible sous <https://www.fedlex.admin.ch/eli/fga/2010/813/fr>, visité le 21.1.2024

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 4 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 4 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 4 CCC N. XXX.

Art. 4 Eingriff in Daten

¹ Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

² Eine Vertragspartei kann sich das Recht vorbehalten, als Voraussetzung vorzusehen, dass das in Absatz 1 beschriebene Verhalten zu einem schweren Schaden geführt haben muss.

GLIEDERUNG

I. Allgemeines.....	66
II. Rechtlich geschütztes Gut	66
III. Grundlegende konstituierende Elemente	66
A. Computerdaten	66
B. Ein strafbares Verhalten	67
1. Das Entfernen und Löschen von Daten	67
2. Beschädigung, Verstümmelung und Veränderung von Daten.	68
3. Die Art der Kommissionierung	69
C. Die Rechtswidrigkeit	69
D. Der Vorsatz.....	71
IV. Zusätzliches fakultatives Tatbestandsmerkmal.....	71
V. Vergleich mit dem Schweizer Recht	72
Literaturverzeichnis	73
Materialienverzeichnis.....	73

I. ALLGEMEINES

- 1 In den letzten zwanzig Jahren hat die Gesellschaft als Ganzes den Übergang in die digitale Welt vollzogen. Ein Großteil des Handels wird online abgewickelt, Finanztransaktionen werden über E-Banking abgewickelt, Behörden, Unternehmen und Privatpersonen speichern große Mengen an Informationen auf Personalcomputern, Servern oder sogar in Clouds. Trotz des Ausmaßes der bereits vollzogenen Veränderungen scheint diese Entwicklung noch lange nicht abgeschlossen zu sein. Es ist nämlich sehr wahrscheinlich, dass sich die Gesellschaft in den kommenden Jahrzehnten noch weiter digitalisieren wird.
- 2 Digitale Dokumente ersetzen nach und nach Papierdokumente. Diesem Trend folgend werden auch immer mehr Dokumente in elektronischer Form als verbindlich anerkannt.
- 3 Angesichts der wachsenden Bedeutung von Computerdaten in der digitalen Welt war es gerechtfertigt, diese vor böswilligen Handlungen zu schützen. Während die Art. 2 und 3 CCC die Vertraulichkeit der Daten schützen, soll Art. 4 CCC den Schutz der Integrität und Verfügbarkeit der Daten gewährleisten.

II. RECHTLICH GESCHÜTZTES GUT

- 4 Art. 4 CCC soll für Daten und Computerprogramme einen ähnlichen Schutz wie für körperliche Güter gegen vorsätzlich verursachte Schäden gewährleisten. Die durch diese Bestimmung geschützten Rechtsgüter sind zum einen die Integrität von Daten und Computerprogrammen und zum anderen das ordnungsgemäße Funktionieren oder die ordnungsgemäße Verwendung von Daten und Computerprogrammen.

III. GRUNDLEGENDE KONSTITUIERENDE ELEMENTE

A. Computerdaten

- 5 Gemäß Art. 1 lit. b CCC bedeutet "Computerdaten" jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die elektronische Verarbeitung geeigneten Form, einschließlich eines Programms, das ein Computersystem dazu veranlassen kann, eine Funktion auszuführen". Der

Begriff Computerdaten ist also sehr weit gefasst, da er unter anderem alle Buchstaben, Symbole oder Programmcodes umfasst, die von einem Computersystem eingegeben, verarbeitet und gespeichert werden können.

Für weitere Einzelheiten zu diesem Begriff wird auf die Ausführungen zu Art. 1 CCC verwiesen.

B. Ein strafbares Verhalten

Damit ein Computersystem ordnungsgemäß funktionieren kann, müssen die von ihm verarbeiteten Daten verfügbar und integer sein. Um diese beiden Aspekte zu gewährleisten, werden in Art. 4 ZKK fünf strafbare Verhaltensweisen aufgeführt. Die Strafbarkeit der Löschung und Unterdrückung von Daten soll die Verfügbarkeit der Daten schützen. Die Kriminalisierung von Beschädigung, Verstümmelung und Manipulation wiederum soll den Schutz der Datenintegrität gewährleisten. Diese Liste von Verhaltensweisen ist erschöpfend. Sie deckt jedoch alle möglichen schädlichen Verhaltensweisen ab.

1. Das Entfernen und Löschen von Daten

In der Informatik werden Daten in binärer Sprache als eine Folge von "0" und "1" dargestellt. In dieser Form werden die Daten verarbeitet und gespeichert. Wenn der Benutzer Daten speichert, speichert das Computersystem die Reihe von "0" und "1", die diesen Daten entsprechen, in einem noch leeren Bereich des Speichermediums (z. B. Festplatte, DVD, USB-Stick, ...). Um diese Daten wiederzufinden, wenn der Nutzer sie erneut benötigt, verfügt das Computersystem über eine Art Plan, der ihm zeigt, wo sich welche Daten auf dem Datenträger befinden.

Beim Löschen von Daten wird das Mittel zum Auffinden des Ortes, an dem sich die Daten befinden, zerstört. Die Daten sind zwar noch vorhanden, aber der Nutzer kann nicht mehr feststellen, wo sie sich auf dem Datenträger befinden, und kann daher nicht mehr auf sie zugreifen. Das Computersystem geht davon aus, dass der Platz auf dem Datenträger frei ist und speichert daher die neuen Daten über die gelöschten Daten. Die einzige Möglichkeit, die gelöschten Daten wiederherzustellen, besteht darin, so schnell wie möglich ein Datenrettungsprogramm zu verwenden. Dieses Programm liest den gesamten Datenträger und stellt eine Karte des Speichermediums wieder

her, um die Daten zu lokalisieren. So können die Daten wiederhergestellt werden, bevor andere darüber gespeichert werden.

- 10 Im Gegensatz zum Löschen ist das Löschen von Daten eine endgültige Vernichtung von Daten. Die Daten existieren nicht mehr auf dem Speichermedium. Sie sind in der Regel nicht mehr wiederherstellbar.

2. Beschädigung, Verstümmelung und Veränderung von Daten.

- 11 Die Datenintegrität ist für das reibungslose Funktionieren von Informationssystemen ebenso entscheidend wie die Verfügbarkeit von Daten. Ihre Bedeutung ist so groß, dass sie sogar Gegenstand einer ISO-Norm ist. Der Begriff der Datenintegrität bezieht sich auf die Zuverlässigkeit, Genauigkeit und Vollständigkeit der Daten. Mit anderen Worten: Daten, deren Integrität gewährleistet ist, sind Daten, die nach ihrer ursprünglichen Speicherung nicht verändert wurden. Der Begriff der Datenintegrität bezieht sich sowohl auf den Inhalt der Daten als auch auf ihre Form.
- 12 In der realen Welt kann der Begriff der garantierten Datenintegrität mit dem Versand eines Pakets per Post verglichen werden, bei dem bescheinigt wird, dass es tatsächlich von dem auf dem Paket angegebenen Absender stammt, dass der Versand an dem auf dem Poststempel angegebenen Datum und Ort stattgefunden hat, dass das Paket nicht geöffnet wurde, dass sein Inhalt dem vom Absender gesendeten Inhalt entspricht und dass nach dem Versand nichts aus dem Paket entfernt oder hinzugefügt wurde.
- 13 In diesem Zusammenhang sind "Beschädigung" und "Verschlechterung" von Daten überlappende Begriffe. Sie beschreiben negative Beeinträchtigungen der Form oder des Inhalts von Daten oder Programmen. Beschädigte oder verschlechterte Daten sind daher nicht mehr zuverlässig, genau und vollständig. Man kann also nicht mehr sicher sein, dass sie von dem Absender stammen, von dem sie zu stammen scheinen, dass es sich tatsächlich um die Daten handelt, die vom Absender gesendet wurden, und dass keine Daten gelöscht, hinzugefügt oder verändert wurden.
- 14 Was die "Veränderung" betrifft, so bezieht sie sich auf eine Änderung bestehender Daten. Diese Änderung kann sich sowohl auf die Form als auch auf den Inhalt der Daten beziehen. Es handelt sich um einen sehr weit gefassten Begriff, der alle Aktionen an Daten umfasst, durch die ein oder mehrere Elemente hinzugefügt, ersetzt oder gelöscht werden.

3. Die Art der Kommissionierung

Die verschiedenen Verhaltensweisen, die soeben untersucht wurden, können 15
direkt vom Täter begangen werden. Es ist jedoch auch möglich, einen Bot zu
benutzen, um diese Handlungen zu begehen. Dies hat den Vorteil, dass der
Täter seine Anweisungen nur einmal an das Programm geben muss, das dann
automatisch die geforderten Handlungen so oft wie nötig wiederholt.
Außerdem ist zu befürchten, dass die Entwicklung der künstlichen Intelligenz
diese Arbeit in Zukunft noch viel einfacher und effizienter machen wird.
WormGPT ist zweifellos der Vorläufer einer neuen Form der Begehung von
Straftaten, da es die Möglichkeit bietet, von künstlicher Intelligenz erzeugte
Inhalte in andere Computersysteme zu implementieren, während die
künstliche Intelligenz bislang auf eine Computersandbox beschränkt war.

Aber auch ohne Bot bietet die künstliche Intelligenz bereits heute unzählige 16
Möglichkeiten, Daten zu verändern. So kann man sie zum Beispiel ganz
einfach bitten, einen Text umzuschreiben, indem man eine Idee durch eine
andere ersetzt, oder ein Bild zu bearbeiten, indem man ein Element durch ein
anderes ersetzt. In Zukunft wird es also immer schwieriger werden,
authentische Daten von veränderten Daten zu unterscheiden.

In der überwiegenden Mehrheit der Fälle werden 17
Datenintegritätsverletzungen durch die Begehung eines strafbaren Verhaltens
verwirklicht. Datenintegritätsverletzungen können jedoch auch aufgrund
eines unzureichenden Schutzes des Computersystems entstehen. Unserer
Ansicht nach kann in solchen Fällen eine Begehung durch Unterlassen seitens
des Administrators des Computersystems vorliegen, da er aufgrund seiner
Funktion eine rechtliche Pflicht zum Handeln hat und somit eine
Garantenstellung gegenüber dem Datenberechtigten einnimmt.

C. Die Rechtswidrigkeit

Um strafbar zu sein, muss der Täter unrechtmäßig gehandelt haben. Wer 18
berechtigt ist, die Daten zu verändern, bestimmt der Rechteinhaber der
Daten. Strafbar sind somit alle Personen, die nicht berechtigt waren, diese
Daten zu verändern. Nicht strafbar sind hingegen Personen, die vom
Berechtigten ausdrücklich oder durch schlüssiges Handeln dazu ermächtigt
wurden, die Daten zu ändern, oder die durch Gesetz oder Vertrag dazu
berechtigt sind.

- 19 Heutzutage ist es üblich, dass Datenänderungen durch schlüssiges Handeln vorgenommen werden. Dies ist z. B. immer dann der Fall, wenn Nachrichten über Instant Messenger wie WhatsApp, Telegraph oder Threema ausgetauscht werden. Alle diese Anwendungen verschlüsseln die Daten vor dem Versender und entschlüsseln sie beim Empfang. Dabei handelt es sich um eine Datenveränderung. Diese ist jedoch rechtmäßig, weil sie zum einen von den Nutzern durch schlüssiges Handeln akzeptiert wird und zum anderen die Vertraulichkeit der Daten gewährleistet wird.
- 20 Ein weiterer Fall, in dem Daten durch schlüssiges Handeln verändert werden, ist die Aktualisierung von Anwendungen. Bei einem Update wird eine neue Version des Programms anstelle der alten installiert. Die vorhandenen Daten werden also gelöscht und neue Daten werden geschrieben und auf dem Speichermedium aufgezeichnet. Dieser Vorgang ist rechtmäßig, solange der Nutzer die Wahl hat, das Update zu installieren oder nicht zu installieren. Unserer Ansicht nach macht sich der Herausgeber der Anwendung, der den Nutzer dazu zwingt, eine neue Version der Anwendung zu installieren, weil die Anwendung sonst unbrauchbar wird oder die Daten unlesbar werden, strafbar.
- 21 Was die gesetzlich erlaubten Handlungen betrifft, so enthalten einige nationale Gesetze Ausnahmen von der Garantie der Datenintegrität. Sie erlauben insbesondere den Strafverfolgungsbehörden oder Nachrichtendiensten, Govware in Computersystemen zu installieren, um die Aktivitäten der Personen zu überwachen, die diese Systeme nutzen, z. B. um den Urheber einer Straftat zu ermitteln oder Informationen zu erhalten, die für den Staatsschutz relevant sind. Die Installation von Spyware ist nicht illegal, solange sie innerhalb des engen gesetzlichen Rahmens erfolgt. Eine Überwachung darf jedoch nur in schwerwiegenden Fällen durchgeführt werden und muss einer nachträglichen gerichtlichen Überprüfung unterzogen werden.
- 22 Die Veränderung von Daten ist auch dann nicht rechtswidrig, wenn sie vertraglich erlaubt wurde. Hier ist insbesondere an den Administrator des Computersystems zu denken, der für die Wartung zuständig ist. Er macht sich nicht strafbar, wenn er die Updates der im Computersystem installierten Programme vornimmt. Er macht sich hingegen strafbar, wenn er seinen Status ausnutzt, um die Daten eines Nutzers ohne dessen Zustimmung zu löschen oder zu verändern.

Ebenso macht sich ein Informatiker, der beauftragt wurde, Penetrationstests in einem Computersystem durchzuführen, nicht strafbar, wenn er Daten verändert, um eine Lücke in der Verteidigung zu schaffen, die eingerichtet wurde, um den Zugang zum Computersystem zu schützen. Dagegen ist ein Hacker, der ohne Genehmigung auf dieselbe Weise vorgeht, strafbar. 23

D. Der Vorsatz

Die Verletzung der Integrität von Daten muss vorsätzlich erfolgen. Der Vorsatz muss sich auf alle objektiven Elemente der Straftat beziehen. Der Täter muss sich also bewusst sein, dass er Daten in unzulässiger Weise verschlechtert, und er muss den Willen dazu haben. Eventualvorsatz reicht aus. 24

IV. ZUSÄTZLICHES FAKULTATIVES TATBESTANDSMERKMAL

Art. 4 Abs. 2 CCC erlaubt es den Vertragsstaaten, einen Vorbehalt anzubringen und nur Verhaltensweisen zu verfolgen, die zu einem schweren Schaden geführt haben. 25

Der Text definiert den Begriff des "schweren Schadens" nicht. Was den erläuternden Bericht betrifft, so heißt es dort lediglich, dass es jedem Staat freisteht, diesen Begriff nach eigenem Ermessen auszulegen. Die Vertragsparteien haben sich jedoch für den Begriff des Schadens ("harm") und nicht des Schadens ("damage") entschieden. Damit wird deutlich, dass sich der Schaden nicht nur auf den wirtschaftlichen Aspekt beschränkt. Der Schaden kann daher auch der Arbeitszeit entsprechen, die für die Wiederherstellung oder Neuerstellung der Daten erforderlich ist, sowie den Folgen des Verschwindens oder der Unmöglichkeit, die Daten zu nutzen. 26

Die Parteien haben auch klargestellt, dass der Schaden schwerwiegend sein muss. Dieses Adjektiv bedeutet in Verbindung mit dem Begriff des Schadens, dass er ein bestimmtes Ausmaß haben muss. Man kann sich also vorstellen, dass der Schaden einen erheblichen Geldbetrag oder eine große Anzahl von Arbeitsstunden darstellen oder schwerwiegende Folgen haben muss. 27

Aserbaidshan, Litauen, die Slowakische Republik, Chile und die Vereinigten Staaten von Amerika haben von der in Art. 4 Abs. 2 CCC gegebenen Möglichkeit Gebrauch gemacht. Aserbaidshan, Litauen, die Slowakische 28

Republik und die Vereinigten Staaten von Amerika haben klargestellt, dass in ihrem innerstaatlichen Recht der Begriff des schweren Schadens so auszulegen ist, dass er einen ernsthaften Schaden verursacht hat. Das slowakische Strafgesetzbuch wurde seitdem geändert. Der § 247 wurde durch § 247b ersetzt. In seiner einfachen Form ist das Eintreten eines ernsthaften Schadens nicht mehr erforderlich (§ 247b Abs. 1). Stattdessen wurde das Eintreten eines schweren Schadens zu einer qualifizierten Form der Straftat (§ 247b Abs. 2 lit. a). Chile sprach seinerseits von schweren Schäden. Es lässt sich also feststellen, dass, obwohl der Wortlaut des Übereinkommens eine sehr weite Auslegung zuließ, alle Staaten, die von der Möglichkeit des Art. 4 Abs. 2 CCC Gebrauch gemacht haben, den Begriff des Schadens auf den wirtschaftlichen Aspekt beschränkt haben.

- 29 An dieser Stelle ist es interessant, auf die originelle Art und Weise hinzuweisen, wie das Schweizer Recht die Frage des schweren Schadens behandelt hat. Anstatt die Strafverfolgung auf Verhaltensweisen zu beschränken, die einen schweren Schaden verursacht haben, sieht Art. 144^{bis} Ziff. 1 Abs. 2 StGB stattdessen eine qualifizierte Form vor, wenn der vom Täter verursachte Schaden erheblich ist.

V. VERGLEICH MIT DEM SCHWEIZER RECHT

- 30 Im Schweizer Recht findet die Verletzung der Integrität von Daten (Art. 4 CCC) ihr Pendant in Art. 144^{bis} Ziff. 1 StGB. Die durch diese beiden Normen geschützten Rechtsgüter sind jedoch nicht strikt identisch, da Art. 4 CCC die Integrität und das ordnungsgemäße Funktionieren oder den ordnungsgemäßen Gebrauch von gespeicherten Daten oder Computerprogrammen schützt, während Art. 144^{bis} Ziff. 1 StGB das Recht schützt, über intakte Daten zu verfügen. Sie sind jedoch sehr ähnlich und decken sich in ihrer Zielsetzung.
- 31 Was die von Art. 4 CCC unter Strafe gestellten Verhaltensweisen betrifft, so finden sich diese alle in Art. 144^{bis} Ziff. 1 StGB wieder. Die in Art. 4 CCC enthaltenen Begriffe "Beschädigung", "Verschlechterung" und "Veränderung" werden durch den Begriff "modifizieren" abgedeckt, der alle Formen der Umwandlung umfasst. Der im Übereinkommen erwähnte Begriff der "Löschung", d. h. die endgültige Vernichtung von Daten, ist im Schweizer Recht identisch. Schließlich wird die "Löschung" von Daten in Art. 4 CCC durch den Begriff "unbrauchbar machen" abgedeckt, der alle

Verhaltensweisen umfasst, durch die der Berechtigte an der ordnungsgemäßen Nutzung seiner Daten gehindert wird.

Schliesslich ist in Art. 144^{bis} Ziff. 1 StGB eine Straftat verankert, die nur auf 32 Antrag verfolgt wird. Wenn eine Straftat nur auf Antrag verfolgt wird, kann eine Strafbehörde nicht selbst tätig werden. Da es einen Lehrstreit darüber gibt, ob ein im ersuchenden Staat gestellter Strafantrag ausreicht, um die internationale Zusammenarbeit in Gang zu setzen, wäre es klug, die Datenbeschädigung in allen Fällen von Amts wegen zu verfolgen oder eine Erklärung abzugeben, die die Verfolgung auf Fälle beschränkt, in denen der entstandene Schaden erheblich ist.

Die in diesem Beitrag enthaltenen technischen Begriffe der Informatik wurden mit Hilfe von Herrn Yannick Jacquy, eidgenössisch diplomierter ICT-Manager, verfasst. Ihm sei an dieser Stelle herzlich gedankt.

LITERATURVERZEICHNIS

Corboz Bernard, Les infractions en droit suisse, vol. I, 3. éd., Berne 2010

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Trechsel Stefan / Cramer Dean, in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zürich, 2021

Weissenberg Philippe, in : Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 5 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 5 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 5 CCC N. XXX.

Art. 5 Eingriff in ein System

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um die unbefugte schwere Behinderung des Betriebs eines Computersystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

GLIEDERUNG

I. Allgemeines.....	77
II. Geschütztes Rechtsgut.....	78
III. Grundlegende Tatbestandsmerkmale	78
A. Ein Computersystem	78
B. Ein strafbares Verhalten	78
1. Die Eingabe von Daten	78
2. Die Übertragung von Daten	79
3. Beschädigung, Verstümmelung und Veränderung von Daten	80
4. Die Löschung und das Löschen von Daten	81
5. Die Art der Beauftragung	82
C. Eine schwere Beeinträchtigung des Funktionierens des Computersystems	82
D. Die Rechtswidrigkeit.....	84
E. Der Vorsatz	85
IV. Vergleich mit dem Schweizer Recht	85
Literaturverzeichnis	87
Materialienverzeichnis.....	87

I. ALLGEMEINES

In den letzten Jahrzehnten hat sich die Gesellschaft grundlegend verändert. 1
Viele Dienstleistungen haben sich digitalisiert. Smartphones", die es noch vor
zwanzig Jahren nicht gab, sind heute im Leben aller allgegenwärtig. Die
Unternehmen sind sich dieser Veränderung bewusst und haben ihre
Dienstleistungen an diese neuen Geräte angepasst und bieten in der
überwiegenden Mehrheit Online-Dienste an. Dieser Grundtrend wurde durch
die Coronavirus-Pandemie, die die Weltbevölkerung zwischen 2020 und
2022 heimsuchte, noch beschleunigt. Die von den Behörden eingeführten
Gesundheitsmaßnahmen schränkten die Kontakte zwischen den Menschen
deutlich ein. Der Handel musste daher neue Wege finden, um seine Geschäfte
weiterzuführen, um zu überleben.

Mehr als je zuvor in der Geschichte der Menschheit sind heute alle Akteure 2
der Gesellschaft miteinander vernetzt. Mit ihren Smartphones können die
Menschen von jedem Ort der Welt und zu jeder Zeit auf ihre "E-Banking"-
Konten zugreifen, online Handel treiben, Daten in den Clouds speichern oder
Videos "streamen".

Diese extreme Vernetzung schafft jedoch eine ebenso große gegenseitige 3
Abhängigkeit. Dies wird am besten durch die groß angelegte Cyberattacke
veranschaulicht, die Estland 2007 mehrere Tage lang heimsuchte. Eines der
am stärksten vernetzten Länder der Welt wurde dadurch vollständig
lahmgelegt. Die staatliche Verwaltung, das Bankensystem, der Handel: Nichts
funktionierte mehr, was der gesamten Gesellschaft erheblichen Schaden
zufügte. Heute ist es daher noch mehr als zu Beginn der 2000er Jahre
unerlässlich, dass Computersysteme ungehindert funktionieren können.

Angeichts der erheblichen Schäden, die eine Behinderung des 4
ordnungsgemäßen Funktionierens von Computersystemen verursachen kann,
war es unerlässlich, das ordnungsgemäße Funktionieren dieser Systeme
mithilfe einer Strafnorm zu schützen.

II. GESCHÜTZTES RECHTSGUT

- 5 Das durch Art. 5 CCC geschützte Rechtsgut ist das Recht des Betreibers und der Nutzer eines Computer- oder Telekommunikationssystems auf dessen ordnungsgemäßes Funktionieren.

III. GRUNDLEGENDE TATBESTANDSMERKMALE

A. Ein Computersystem

- 6 Nach Art. 1 lit. a CCC "bezeichnet der Ausdruck 'Computersystem' eine einzelne Vorrichtung oder eine Gesamtheit miteinander verbundener oder verwandter Vorrichtungen, die in Ausführung eines Programms eine automatisierte Datenverarbeitung bewirkt oder von der ein oder mehrere Elemente eine automatisierte Datenverarbeitung bewirken". Der Begriff des Computersystems umfasst somit die Gesamtheit der Hardware (Hauptplatine, Prozessor, Festplatte, Bildschirm, Tastatur, Drucker, ...) und der Software (BIOS, Betriebssystem, Software, Updates, ...) sowie die Geräte, die die Verbindung dieser verschiedenen Elemente untereinander ermöglichen (Kabel, Router, WLAN-Hotspot, ...).
- 7 Für weitere Details zu diesem Begriff wird auf die Ausführungen in Art. 1 CCC oben verwiesen.

B. Ein strafbares Verhalten

- 8 Art. 5 CCC zählt sieben strafbare Verhaltensweisen auf: das Eingeben, Übertragen, Beschädigen, Löschen, Verstümmeln, Verändern oder Unterdrücken von Computerdaten. Diese Liste ist erschöpfend. Verhaltensweisen, die das ordnungsgemäße Funktionieren des Computersystems beeinträchtigen, aber nicht in dieser Liste enthalten sind, sind daher nicht strafbar. Dies ist zum Beispiel der Fall, wenn Daten innerhalb des Computersystems verschoben werden, obwohl dies genauso schädlich ist wie die Beschädigung oder Beeinträchtigung von Daten.

1. Die Eingabe von Daten

- 9 Der Begriff der Einführung ist so zu verstehen, dass der Täter Daten, die von außerhalb des Zielsystems stammen, in das Zielsystem einführt. Manche Täter

tarnen diese Daten sogar, indem sie ihnen das Aussehen völlig harmloser Dateien geben, um zu verhindern, dass sie zu leicht entdeckt werden. Vom äußeren Erscheinungsbild her scheinen diese Daten also Originaldaten des Systems zu sein.

Art. 5 CCC erstreckt sich jedoch nicht auf alle Daten, die in das Computersystem eingegeben werden, sondern nur auf solche, die dazu bestimmt sind, das ordnungsgemäße Funktionieren des Systems zu beeinträchtigen. Es handelt sich also um bösartige Daten oder Programme, die das Funktionieren des Computersystems verlangsamen oder sogar vollständig blockieren. Dies kann entweder durch die Aktivierung einer Funktion erreicht werden, die den Datenverarbeitungsprozess verlangsamt oder blockiert, oder durch die Deaktivierung einer Funktion, die für das reibungslose Funktionieren des Computersystems erforderlich ist. Beispiele hierfür sind die Installation eines Trojanischen Pferdes, das es dem Täter ermöglicht, die Kontrolle über das gesamte oder einen Teil des Computersystems zu übernehmen, oder die Installation eines Virus, der den Prozessor lahmlegt oder einen Bootsektor zerstört, sodass der Computer nicht neu gestartet werden kann. 10

2. Die Übertragung von Daten

Unter "Datenübertragung" ist das Senden von Daten von einem Computersystem an ein anderes zu verstehen. Das hier gemeinte Verhalten ist das Versenden von Daten, die das reibungslose Funktionieren des Computersystems behindern. Die Parteien wollten insbesondere Denial-of-Service- und Distributed-Denial-of-Service-Angriffe unter Strafe stellen. Bei einem Denial-of-Service-Angriff wird eine so große Menge an Daten an ein Zielcomputersystem gesendet, dass dieses nicht mehr in der Lage ist, alle Daten zu verarbeiten und schließlich abstürzt. 11

Im Laufe der Zeit hat sich die Leistung von Computersystemen, insbesondere von Servern, erheblich gesteigert. Techniken zur Lastverteilung und Hochverfügbarkeit haben Denial-of-Service-Angriffe nahezu unmöglich gemacht. Cyberkriminelle haben daher den Denial-of-Service-Angriff zum Distributed-Denial-of-Service-Angriff weiterentwickelt. Dieser Angriff ist dem vorherigen ähnlich, mit dem Unterschied, dass der Täter eine Vielzahl von Computersystemen unter seiner Kontrolle hat, denen er den Befehl gibt, gleichzeitig sehr große Datenmengen an das Zielcomputersystem zu senden. 12

Aufgrund der großen Menge an Daten, die von allen Seiten kommen, kann das Zielcomputersystem nicht mehr alle Daten verarbeiten und stürzt schließlich ab. Diese Art von Angriffen ist derzeit relativ weit verbreitet. Sie ist fast immer mit Lösegeldforderungen als Gegenleistung für die Einstellung des Angriffs oder mit einem anderen Betrug wie Datendiebstahl verbunden. Auch heute noch gibt es keine Lösung, um sich wirksam gegen Distributed-Denial-of-Service-Angriffe zu verteidigen. Darüber hinaus ist der Schaden für die Opfer besonders groß, da sie entweder ihr Computersystem nicht mehr nutzen können oder durch die Zahlung des Lösegelds verarmt sind.

3. Beschädigung, Verstümmelung und Veränderung von Daten

- 13 Die Integrität von Daten ist für das reibungslose Funktionieren von Informationssystemen von entscheidender Bedeutung. Ihre Bedeutung ist so groß, dass sie sogar Gegenstand einer ISO-Norm ist.
- 14 Der Begriff der Datenintegrität bezieht sich auf die Zuverlässigkeit, Genauigkeit und Vollständigkeit von Daten. Daten, deren Integrität gewährleistet ist, sind Daten, die nach ihrer ursprünglichen Aufzeichnung nicht mehr verändert wurden. Zur Veranschaulichung könnte man den Begriff der garantierten Datenintegrität mit dem Versand eines Pakets per Post vergleichen, bei dem bestätigt wird, dass es tatsächlich von dem auf dem Paket angegebenen Absender versandt wurde, dass der Versand an dem auf dem Poststempel angegebenen Datum und Ort stattgefunden hat, dass das Paket während des Transports nicht geöffnet wurde und dass der Inhalt des Pakets nach dem Versand nicht verändert wurde.
- 15 Selbstverständlich ist der Inhalt der Daten, d. h. die Informationen, die die Daten enthalten (z. B. ein Text, ein Code, ein Bild usw.), ebenso wichtig wie die formale Integrität der Daten. Neben der Gewährleistung der formalen Datenintegrität ist es daher unerlässlich, auch zu gewährleisten, dass der Inhalt der Daten nicht beschädigt wurde. Im Beispiel des oben erwähnten Pakets wird die formale Integrität der Daten durch die Verpackung repräsentiert, während die Integrität des Dateninhalts dem Objekt entspricht, das sich im Paket befindet.
- 16 Die in Art. 5 CCC erwähnte Beschädigung und Verschlechterung von Daten sind Verhaltensweisen, die sich im Bereich der Informatik überschneiden. In beiden Fällen handelt es sich um negative Beeinträchtigungen der Integrität

oder des Inhalts von Daten oder Programmen. Die beschädigten oder verschlechterten Daten sind nicht mehr zuverlässig, genau und vollständig. Der Täter verändert die Daten des Zielcomputersystems so, dass sie bei der Datenverarbeitung nicht mehr korrekt verwendet werden können. Es genügt beispielsweise, einen Ordner umzubenennen, der Dateien enthält, die für das reibungslose Funktionieren des Betriebssystems unerlässlich sind, um das gesamte Computersystem zum Absturz zu bringen. Auch durch die Änderung des Programmiercodes einer Software kann deren ordnungsgemäße Funktion blockiert werden. In jüngerer Zeit verschlüsseln Cyberkriminelle Daten und machen den Verschlüsselungsschlüssel anschließend zu Geld.

Die Manipulation bezieht sich auf die Veränderung bestehender Daten im Computersystem als Folge einer anderen vom Täter vorgenommenen Handlung. Es handelt sich um einen sehr weit gefassten Oberbegriff, der alle Veränderungen an Daten umfasst, d. h. das Hinzufügen, Ersetzen oder Löschen von Daten. Diese Änderungen können sich sowohl auf die formale als auch auf die inhaltliche Integrität der Daten beziehen. Dies gilt insbesondere für Daten, die nach der Einführung eines Trojanischen Pferdes oder der Installation eines Virus verändert wurden. 17

4. Die Löschung und das Löschen von Daten

Computerdaten werden auf Speichermedien (z. B. Festplatte, DVD, USB-Stick, ...) in der Reihenfolge gespeichert, in der sie erstellt wurden. Um bestimmte Daten wiederfinden zu können, wenn der Nutzer sie erneut benötigt, erstellt das Computersystem eine Art Index, aus dem es ersehen kann, wo sich welche Daten auf dem Datenträger befinden. 18

Beim Löschen von Daten wird dieser Index, der es ermöglicht, den Speicherort der Daten zu finden, ganz oder teilweise zerstört. Die Daten sind zwar noch vorhanden, aber das Computersystem weiß nicht mehr, wo sie sich auf dem Datenträger befinden, und kann daher nicht mehr auf sie zugreifen. 19

Im Gegensatz zum Löschen handelt es sich bei der Datenlöschung um eine endgültige Zerstörung der Daten. Die Daten existieren nicht mehr auf dem Speichermedium. 20

Wenn der Urheber Daten löscht oder unterdrückt, die für das ordnungsgemäße Funktionieren des Computersystems unerlässlich sind, wie 21

z. B. die Daten, die das Betriebssystem ausmachen, wird das Computersystem unbrauchbar und funktioniert nicht mehr.

5. Die Art der Beauftragung

- 22 Die verschiedenen Verhaltensweisen, die gerade untersucht wurden, können natürlich auch direkt von einer natürlichen Person begangen werden. Dies wäre jedoch sehr zeitaufwändig. In der Praxis verwenden Cyberkriminelle daher eher Malware oder Bots, um diese Handlungen automatisiert auszuführen. Die sehr schnelle Entwicklung der künstlichen Intelligenz wird diese Art von Handlungen sicherlich noch viel einfacher machen. WormGPT gibt uns bereits einen Einblick in die Möglichkeiten, die künstliche Intelligenz bietet, da es die Implementierung von Inhalten, die von künstlicher Intelligenz generiert wurden, in andere Computersysteme ermöglicht, die bislang auf eine Computersandbox beschränkt waren.
- 23 Es stellt sich auch die Frage der Begehungsweise durch Unterlassen. Meistens handelt es sich bei strafbarem Verhalten um Handlungen von Cyberkriminellen, die das reibungslose Funktionieren des Computersystems behindern wollen, um im Gegenzug etwas zu erhalten. Es ist jedoch auch denkbar, dass das Computersystem irgendwann nicht mehr richtig funktioniert, weil sein Administrator sich nicht um die notwendigen Aktualisierungen kümmert. Unserer Meinung nach ist der Administrator des Computersystems in diesem Fall strafbar, da er aufgrund seiner Funktion eine rechtliche Pflicht zum Handeln hat und somit eine Garantenstellung gegenüber dem Rechteinhaber und den Nutzern des Computersystems einnimmt.
- 24 Unserer Ansicht nach ist die Lösung im Fall des Administrators des Computersystems, der keine Firewall und/oder kein Antivirenprogramm zum Schutz des Systems installiert und damit unzählige Möglichkeiten für Dritte offen lässt, das System anzugreifen, identisch.

C. Eine schwere Beeinträchtigung des Funktionierens des Computersystems

- 25 Um sich der Verletzung der Systemintegrität schuldig zu machen, reicht es nicht aus, dass der Täter die Integrität der im Computersystem enthaltenen Daten angreift, da es sich in diesem Fall um eine Verletzung der

Datenintegrität im Sinne von Art. 4 CCC handeln würde. Es ist erforderlich, dass die Handlung das Funktionieren des Computersystems ernsthaft beeinträchtigt.

Eine Funktionsbeeinträchtigung liegt vor, wenn das Computersystem nicht mehr optimal funktioniert. Der Wortlaut von Art. 5 CCC wurde so neutral formuliert, dass er den Schutz vielfältiger Funktionen ermöglicht. Es ist somit unerheblich, welche Funktionen beeinträchtigt werden. Es ist auch unerheblich, ob das gesamte Computersystem behindert wird oder ob nur bestimmte Funktionen behindert werden.

Das Computersystem wird in seiner ordnungsgemäßen Funktion beeinträchtigt, wenn es außer Betrieb gesetzt wird. Es ist auch dann beeinträchtigt, wenn eine Anwendung nicht mehr genutzt werden kann. Dies kann unter anderem dadurch geschehen, dass der Computercode des Programms beschädigt oder zerstört wurde oder dass die Daten, die der Nutzer gespeichert hatte, gelöscht, entfernt oder verschlüsselt wurden. Die Beeinträchtigung des Computersystems kann auch durch eine verminderte Leistung des Systems verursacht werden. Dies ist beispielsweise der Fall, wenn ein Cyberkrimineller die Fernsteuerung eines Computersystems übernimmt und es ohne das Wissen des Rechteinhabers als Zombie-Maschine verwendet. Dabei nutzt er einen Teil der Leistung des Computersystems ohne die Zustimmung des Rechteinhabers, meist zu bösartigen Zwecken. Schließlich kann das reibungslose Funktionieren eines Computersystems auch durch zu starke Beanspruchung beeinträchtigt werden. Dies ist bei Denial-of-Service- oder Distributed-Denial-of-Service-Angriffen der Fall. An sich funktioniert das Computersystem normal, aber es wird mit so vielen Anfragen gleichzeitig belagert, dass es diese nicht schnell genug bearbeiten kann und schließlich abstürzt.

Angesichts des Wortlauts der Norm muss sich die Behinderung aus dem strafbaren Verhalten ergeben. Da die Aufzählung in Art. 5 CCC abschliessend ist, muss sich die Behinderung notwendigerweise aus einem der aufgeführten Verhaltensweisen ergeben, um strafbar zu sein. Eine Behinderung, die aus einem anderen Verhalten resultiert, wie z. B. das Verschieben von Daten innerhalb des Computersystems, ist nicht strafbar.

Was das Attribut "schwerwiegend" betrifft, so wurde es absichtlich nicht definiert, um jedem Staat die Möglichkeit zu geben, es frei zu definieren. Für

die einen kann sich eine schwerwiegende Behinderung auf einen minimalen Schaden beziehen, der durch diese Behinderung verursacht wird. Für die anderen wird es sich um das Ausmaß der Behinderung handeln, wie z. B. die Blockierung jeglicher Verbindung eines Computersystems nach außen. Die Autoren des Entwurfs "stuften es als "schwerwiegend" ein, wenn an ein Computersystem Daten gesendet werden, deren Form, Umfang oder Häufigkeit die Fähigkeit des Eigentümers oder Betreibers, das betreffende System zu nutzen oder mit anderen Systemen zu kommunizieren, erheblich beeinträchtigt (dies ist der Fall bei Programmen, die Systeme in Form einer "Denial of Service"-Behinderung beeinträchtigen, bösartige Codes wie Viren, die den Betrieb des Systems unterbinden oder erheblich verlangsamen, oder Programme, die eine riesige Menge an E-Mails an einen Empfänger senden, um die Kommunikationsfunktionen des Systems lahmzulegen)".

D. Die Rechtswidrigkeit

- 30 Um strafbar zu sein, muss der Täter unrechtmäßig gehandelt haben. Wer das Recht hat, das Computersystem zu verwalten und zu nutzen, bestimmt der Rechteinhaber des Computersystems. Somit sind alle Personen strafbar, die nicht berechtigt sind, Änderungen an der Funktionsweise des Computersystems vorzunehmen. Nicht strafbar sind hingegen Personen, die vom Berechtigten ausdrücklich oder durch schlüssiges Handeln dazu ermächtigt wurden, die Funktionsweise des Computersystems zu verändern, sowie Personen, die gesetzlich oder vertraglich dazu berechtigt sind.
- 31 Bis Anfang der 2000er Jahre war es selten, dass das Betriebssystem oder eine Anwendung ein Update erforderte. In den letzten zwei Jahrzehnten sind Updates jedoch immer häufiger geworden. Heute sind sie sogar die Regel. Bei einer Aktualisierung wird eine neue Version des Programms anstelle der alten installiert. Die vorhandenen Daten werden also gelöscht und neue Daten werden geschrieben und auf dem Speichermedium aufgezeichnet. Im Wesentlichen enthalten Updates Programmkorrekturen, Fehlerbeseitigungen oder neue Funktionen. Es gibt also a priori keine Form der Beeinträchtigung des ordnungsgemäßen Funktionierens des Computersystems. Es kann jedoch vorkommen, dass bestimmte Updates mehr Speicherplatz auf der Festplatte benötigen oder einen größeren Teil des Arbeitsspeichers oder der Prozessorkapazität beanspruchen. Dies führt dazu, dass das Computersystem langsamer wird. Es wird also in seiner ordnungsgemäßen Funktion behindert.

In den meisten Fällen stellt dies kein Problem dar, da die Verlangsamung des Computersystems sehr gering oder sogar unbedeutend ist. In Ausnahmefällen kann es vorkommen, dass Updates den Betrieb des Computersystems blockieren, insbesondere weil die vorherige Version der Anwendung bereits das Maximum der verfügbaren Ressourcen beanspruchte und das Update mehr Ressourcen erfordert, als verfügbar sind. In jedem Fall sollte der Nutzer die Wahl haben, das Update zu installieren oder nicht zu installieren. Unserer Ansicht nach macht sich der Herausgeber der Anwendung strafbar, wenn er den Nutzer zwingt, eine neue Version der Anwendung zu installieren, da andernfalls das Computersystem in seiner ordnungsgemäßen Funktion beeinträchtigt wird oder die Anwendung sogar unbrauchbar gemacht wird.

Auch die in Art. 5 CCC aufgeführten Verhaltensweisen sind nicht³² rechtswidrig, wenn sie vertraglich erlaubt wurden. Hier ist insbesondere an den Administrator des Computersystems zu denken, dessen Aufgabe es ist, die Wartung zu gewährleisten. Er macht sich nicht strafbar, wenn er die Updates der im Computersystem installierten Programme durchführt. Er macht sich hingegen strafbar, wenn er seinen Status ausnutzt, um das ordnungsgemäße Funktionieren des Computersystems zu beeinträchtigen, z. B. durch die Deinstallation von Programmen oder das Löschen von Daten.

E. Der Vorsatz

Die Verletzung der Systemintegrität muss vorsätzlich erfolgen. Der Vorsatz³³ muss sich auf alle objektiven Elemente der Straftat beziehen. Der Täter muss also das Bewusstsein und den Willen haben, das ordnungsgemäße Funktionieren eines Computersystems zu stören, ohne dazu berechtigt zu sein.

IV. VERGLEICH MIT DEM SCHWEIZER RECHT

Es gibt kein Äquivalent zu Art. 5 CCC im Schweizer Recht. Die verschiedenen³⁴ Verhaltensweisen könnten zwar den Eindruck erwecken, dass eine Ähnlichkeit mit der Datenbeschädigung (Art. 144^{bis} Ziff. 1 StGB) besteht. Dies ist jedoch aus drei Gründen nicht der Fall.

Zunächst sind die durch Art. 5 CCC und Art. 144^{bis} Ziff. 1 StGB rechtlich³⁵ geschützten Güter völlig unterschiedlich. Wie oben erläutert, schützt Art. 5 CCC das Interesse des Betreibers und der Nutzer eines Computer- oder

Telekommunikationssystemen daran, dass dieses System ordnungsgemäß funktionieren kann, während Art. 144^{bis} Ziff. 1 StGB ein Verfügungsrecht über Daten sicherstellt. Mit anderen Worten: Ersteres garantiert das ordnungsgemäße Funktionieren eines Datenverarbeitungsmittels, während letzteres ein bestimmtes dingliches Recht schützt.

- 36 Angesichts der Tatsache, dass die rechtlich geschützten Güter nicht dieselben sind, sind auch die Personen, die durch diese beiden Straftaten geschädigt werden, nicht identisch. Die durch die Datenbeschädigung (Art. 144^{bis} Ziff. 1 StGB) geschädigte Person ist der Inhaber der beschädigten Daten. Dagegen verletzt die Verletzung der Systemintegrität (Art. 5 CCC) den Rechtsinhaber des Computersystems.
- 37 Zweitens: Obwohl die beiden Straftaten viele Gemeinsamkeiten aufweisen, können sie nicht gleichgesetzt werden. Denn die Verletzung der Systemintegrität (Art. 5 CCC) ist gewissermaßen als eine Sonderform der Datenbeschädigung (Art. 144^{bis} Ziff. 1 StGB) zu sehen, da sie verlangt, dass die Verletzung der Datenintegrität eine schwere Beeinträchtigung des Funktionierens des Computersystems verursacht. Dabei handelt es sich um ein zusätzliches Tatbestandsmerkmal, das im schweizerischen Recht nicht verlangt wird.
- 38 Schliesslich fallen gewisse Verhaltensweisen unter Art. 5 CCC, obwohl sie nach Art. 144^{bis} Ziff. 1 StGB nicht strafbar sind. Dies gilt insbesondere für Sendungen "an ein Computersystem von Daten, die aufgrund ihrer Form, ihres Umfangs oder ihrer Häufigkeit die Fähigkeit des Eigentümers oder Betreibers, das betreffende System zu nutzen oder mit anderen Systemen zu kommunizieren, erheblich beeinträchtigen". Diese Handlungen werden aus drei Gründen auch nicht angemessen durch Art. 179septies StGB (Missbrauch einer Telekommunikationsanlage) geahndet. Erstens, weil Art. 179septies StGB neben der Absicht einen besonderen Vorsatz - nämlich Bosheit oder Schelmerei - verlangt, was bei Art. 5 CCC nicht der Fall ist. Zweitens aufgrund der Tatsache, dass der Missbrauch einer Telekommunikationsanlage nur eine Übertretung darstellt und daher nur mit einer Geldstrafe geahndet wird. In Art. 13 Abs. 1 CCC heisst es jedoch ausdrücklich, dass die in den Art. 2 bis 11 CCC unter Strafe gestellten Straftaten mit Sanktionen geahndet werden müssen, die auch Freiheitsstrafen umfassen. Drittens, weil die Mittäterschaft und der Versuch der Verletzung der Systemintegrität nach Art. 11 CCC strafbar sind, während die Mittäterschaft und der Versuch der missbräuchlichen

Verwendung einer Fernmeldeanlage nicht strafbar sind, da es sich um eine Übertretung handelt (vgl. Art. 105 Abs. 2 StGB).

Aufgrund der vorstehenden Ausführungen ist festzustellen, dass das Schweizer Recht nicht mit Art. 5 CCC übereinstimmt. Es sollte daher angepasst werden. 39

Die in diesem Beitrag enthaltenen Fachbegriffe der Informatik wurden mit Hilfe von Herrn Yannick Jacquey, eidgenössisch diplomierter ICT-Manager, verfasst. Ihm sei an dieser Stelle herzlich dafür gedankt.

LITERATURVERZEICHNIS

Ottis Rain, Analysis of the 2007 Cyber Attacks against Estonia from the information warfare perspective, in : Proceedings of the 7th European Conference on information warfare and security, Plymouth, 2008, pp 163-168, disponible à <https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/> visité le 02.11.2023

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in : Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd.-, Bâle 2018

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.01.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 6 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 6 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 6 CCC N. XXX.

Art. 6 Missbrauch von Vorrichtungen

¹ Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

a. das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen:

i. einer Vorrichtung einschliesslich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2–5 umschriebene Straftat zu begehen,

ii. eines Computerpassworts, eines Zugangscode oder ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen, mit dem Vorsatz, sie zur Begehung einer nach den Artikeln 2–5 umschriebenen Straftat zu verwenden; und

b. den Besitz eines unter Buchstabe a Ziffer i oder ii bezeichneten Mittels mit dem Vorsatz, es zur Begehung einer nach den Artikeln 2–5 umschriebenen Straftat zu verwenden. Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst mit Besitz einer bestimmten Anzahl dieser Mittel eintritt.

² Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2–5 umschriebenen Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.

³ Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, sofern der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Verfügbarmachen der in Absatz 1 Buchstabe a Ziffer ii bezeichneten Mittel betrifft.

GLIEDERUNG

I. Allgemeines.....	92
II. Rechtlich geschütztes Gut	92
III. Grundlegende konstitutive Elemente	93
A. Ein rechtswidriger Gegenstand	93
1. Eine Vorrichtung, die die Begehung einer in den Artikeln 2 bis 5 CCC genannten Straftat ermöglicht.....	93
2. Daten, die den Zugriff auf ein Computersystem ermöglichen, um eine der in Art. 2 bis 5 CCC genannten Straftaten zu begehen.	94
B. Ein strafbares Verhalten	94
1. Die Herstellung, der Verkauf, die Beschaffung zum Gebrauch, die Einfuhr, die Verbreitung oder andere Formen der Bereitstellung.	95
2. Der Besitz.....	96
C. Die Rechtswidrigkeit	96
D. Absicht	97
E. Ein besonderer Vorsatz	97
IV. Die Vorbehalte	98
A. In Bezug auf strafbare Verhaltensweisen	98
B. In Bezug auf illegales Material	99
V. Vergleich mit dem Schweizer Recht	100
Literaturverzeichnis	101
Materialienverzeichnis.....	101

I. ALLGEMEINES

- 1 Die Begehung der in Art. 2 bis 5 CCC unter Strafe gestellten Straftaten erfordert in der Regel die Verwendung von Computerwerkzeugen. Nicht alle Cyberkriminellen sind jedoch in der Lage, diese Werkzeuge selbst herzustellen. Daher versuchen sie, diese von Dritten zu erwerben. Im Laufe der Zeit hat diese Nachfrage zu einem regelrechten Schwarzmarkt geführt, insbesondere im Darknet. Heutzutage kann fast jeder Malware jeglicher Art erwerben, Bot-Nets mieten oder sogar Cyberkriminelle mit der Erfüllung bestimmter Aufgaben beauftragen. Angesichts der Gefahr, die dieser Schwarzmarkt für alle Computersysteme und ihre rechtmäßigen Nutzer darstellt, haben die Vertragsparteien beschlossen, bestimmte, potenziell gefährliche Handlungen bereits im Vorfeld der Begehung der in Art. 2 bis 5 CCC genannten Straftaten strafrechtlich zu sanktionieren. Art. 6 CCC stützt sich auf Instrumente, die vom Europarat (Europäisches Übereinkommen über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten - ETS Nr. 178) und der Europäischen Union (Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten) angenommen wurden, sowie auf die in einigen Ländern in diesem Bereich erlassenen Bestimmungen.

II. RECHTLICH GESCHÜTZTES GUT

- 2 Indem die Vertragsparteien alle Formen des Handels mit oder des Besitzes von Material, das zur Begehung einer der in den Artikeln 2 bis 5 CCC unter Strafe gestellten Straftaten bestimmt ist, unter Strafe stellen, machen sie auch die Vorbereitungshandlungen für die Begehung dieser Straftaten strafbar. Ziel ist es also, den Schutz der durch die Art. 2 bis 5 CCC geschützten Rechtsgüter, nämlich die Unverletzlichkeit und Funktionsfähigkeit von Computersystemen sowie die Integrität, Verfügbarkeit und Vertraulichkeit von Daten, zu verstärken.

III. GRUNDLEGENDE KONSTITUTIVE ELEMENTE

A. Ein rechtswidriger Gegenstand

1. Eine Vorrichtung, die die Begehung einer in den Artikeln 2 bis 5 CCC genannten Straftat ermöglicht.

Der Begriff der Vorrichtung ist weder im Text des Übereinkommens noch in seinem erläuternden Bericht definiert. Unserer Ansicht nach ist eine Vorrichtung im Sinne von Art. 6 CCC eine Gesamtheit von Teilen, Elementen oder Daten, die dazu bestimmt ist, eine oder mehrere bestimmte Funktionen zu erfüllen. Dies wird dadurch belegt, dass die Parteien ausdrücklich das Computerprogramm als Beispiel für eine Vorrichtung nennen. Wie aus dem Zusatz "einschließlich" deutlich hervorgeht, soll der Begriff viel weiter gefasst sein als nur Computerprogramme. Neben Viren, Würmern, Trojanern, logischen Bomben und anderer Malware, die unbestreitbar zu den Programmen gehören, die von dieser Bestimmung erfasst werden, gehören also auch materielle Vorrichtungen wie Mikrofone, Kameras oder Roboter dazu.

Der Anwendungsbereich der Norm beschränkt sich jedoch auf Vorrichtungen, die dazu bestimmt oder geeignet sind, eine der in den Art. 2 bis 5 CCC unter Strafe gestellten Straftaten zu begehen. Es handelt sich also um Vorrichtungen oder Programme, die beispielsweise dazu bestimmt sind, Daten zu verändern oder gar zu zerstören oder in den Betrieb von Systemen einzugreifen, wie z. B. Virenprogramme, oder um Programme, die dazu bestimmt oder geeignet sind, auf Computersysteme zuzugreifen. Vorrichtungen, die solche Handlungen nicht ermöglichen, fallen nicht unter Art. 6 § 1 lit. a Ziff. 1 CCC. Dasselbe gilt für Vorrichtungen, die es ermöglichen, eine andere Straftat zu begehen, insbesondere eine der in Art. 7 bis 10 CCC unter Strafe gestellten Straftaten.

Bei der Ausarbeitung des Übereinkommens wurde eingehend erörtert, ob nur Vorrichtungen erfasst werden sollten, die ausschließlich oder eigens dazu bestimmt sind, die Begehung von Straftaten zu ermöglichen, was Vorrichtungen mit doppeltem Verwendungszweck ausschließen würde, oder ob stattdessen auch letztere einbezogen werden sollten. Die Parteien kamen schließlich zu dem Schluss, dass die Strafverfolgung nicht auf Vorrichtungen beschränkt werden sollte, die ausschließlich zur Begehung von Straftaten

konzipiert sind, da dies die Zahl der Fälle, auf die die Norm Anwendung finden könnte, erheblich verringert hätte. Die Vertragsparteien schlossen jedoch auch die Möglichkeit aus, die Norm auf alle - auch legalen - Vorrichtungen auszudehnen, die die Begehung von Straftaten auf die eine oder andere Weise ermöglichen könnten, da die Verwirklichung der Straftat dann nur noch auf dem Vorsatz des Täters beruht hätte. Daher wurde eine Zwischenlösung gewählt.

- 6 Art. 6 Abs. 1 lit. a Ziff. 1 CCC erfasst demnach Vorrichtungen, die hauptsächlich dazu bestimmt oder geeignet sind, die Begehung einer der in den Art. 2 bis 5 CCC unter Strafe gestellten Straftaten zu ermöglichen. Diese Formulierung schließt Vorrichtungen mit doppeltem Verwendungszweck aus, es sei denn, der Hauptverwendungszweck besteht darin, eine Straftat zu begehen.

2. Daten, die den Zugriff auf ein Computersystem ermöglichen, um eine der in Art. 2 bis 5 CCC genannten Straftaten zu begehen.

- 7 Um alle Mittel abzudecken, die Cyberkriminelle einsetzen, um eine der in Art. 2 bis 5 CCC genannten Straftaten zu begehen, haben die Vertragsparteien auch Handlungen unter Strafe gestellt, die darauf abzielen, Passwörter, ZugangsCodes und ähnliche Computerdaten zur Verfügung zu stellen, die den Zugang zu einem Computersystem oder einem Teil davon ermöglichen (Art. 6 Abs. 1 lit. a Ziff. 2 CCC). Ziel ist es, alle Lücken zu beseitigen. Dieser Ansatz ist angesichts der großen Zahl von Passwörtern und anderen Zugangsdaten, die gestohlen wurden und im Darknet zum Verkauf angeboten werden, durchaus gerechtfertigt.

B. Ein strafbares Verhalten

- 8 Die Vertragsparteien wollten alle Formen des Bereitstellens von illegalen Gegenständen sowie deren Besitz unter Strafe stellen. Im Gegensatz dazu ist festzustellen, dass die bloße Bereitstellung von Anleitungen - z. B. in Form von Texten oder Videos - zur Herstellung illegaler Gegenstände nicht strafbar ist.

1. Die Herstellung, der Verkauf, die Beschaffung zum Gebrauch, die Einfuhr, die Verbreitung oder andere Formen der Bereitstellung.

Art. 6 § 1 lit. a CCC zählt mehrere strafbare Verhaltensweisen auf, die sich auf den Handel beziehen. Diese Liste ist erschöpfend. Um kein Verhalten zu vergessen, endet sie jedoch mit einer Generalklausel ("Auffangtatbestand"). 9

"Produktion" ist die Herstellung von illegalem Material, das zur Begehung einer der in den Artikeln 2 bis 5 CCC aufgeführten Straftaten verwendet werden soll. Der Begriff "Herstellung" umfasst alle Schritte, die zur Herstellung des Gegenstandes erforderlich sind. Es umfasst also auch das Schreiben des Codes der Schadsoftware - in Computersprache - oder auch das Entschlüsseln eines Passworts. 10

Art. 6 § 1 lit. a CCC stellt dann den "Verkauf" unter Strafe. Dieser Begriff bezeichnet die Übergabe eines in diesem Absatz genannten illegalen Gegenstandes gegen eine Geldsumme. Dabei ist es unerheblich, in welcher Währung der Betrag gezahlt wird. Der Betrag kann sogar in Kryptowährungen gezahlt werden. Die Übergabe muss jedoch teuer sein. Es darf sich nicht um eine Schenkung handeln. 11

Das "Beschaffen zur Nutzung" setzt ein aktives Verhalten desjenigen voraus, der versucht, sich verbotenes Material zu beschaffen. Man muss sich mit jemandem in Verbindung gesetzt haben, der das verbotene Material besitzt, und es kostenlos oder gegen Entgelt erworben haben. Die Art und Weise, wie das Material übergeben wird, ist unerheblich. Die Übergabe kann also auf elektronischem Weg, per Post oder sogar durch persönliche Übergabe erfolgen. Entscheidend ist, dass der Täter das illegale Material mit dem Ziel erlangt, es zur Begehung einer der in den Artikeln 2 bis 5 CCC unter Strafe gestellten Straftaten zu verwenden. Wenn das Ziel darin besteht, eine andere Straftat zu begehen oder einfach nur solches Material zu sammeln, ist der Täter nicht strafbar. 12

Das vierte in der Liste genannte Verhalten ist die "Einfuhr". Dieser Begriff bezeichnet das Verbringen eines illegalen Gegenstands in das Land, das diese Handlung unter Strafe stellt. Die Einfuhr von verbotenem Material birgt ein hohes Risiko, dass es später an Dritte weitergegeben wird. Um dieses Risiko zu verringern, ist die bloße Verbringung in das Land verboten, selbst wenn der Importeur nur ein Glied in der Kette zwischen dem Hersteller des Materials und dem Endverbraucher ist. 13

- 14 Art. 6 Abs. 1 stellt weiterhin die "Verbreitung" unter Strafe. Dabei handelt es sich um die Übermittlung von illegalem Material an eine unbestimmte Anzahl von Personen, die nicht unbedingt darum gebeten haben. Die Versendung des Materials kann auf jedem beliebigen Weg erfolgen, sei es per Computer, per Post oder durch persönliche Übergabe.
- 15 Um Lücken zu vermeiden, endet die Liste mit "andere Formen der Bereitstellung". Mit dieser Annahme werden alle Fälle erfasst, die nicht genau den oben erörterten Begriffen entsprechen, es dem Urheber aber dennoch ermöglichen, Dritten illegale Gegenstände zur Verfügung zu stellen. Dieser Begriff umfasst beispielsweise die Erstellung oder Zusammenstellung von Hyperlinks, die den Zugang zu illegalem Material erleichtern sollen.

2. Der Besitz

- 16 Art. 6 § 1 lit. b CCC stellt den Besitz eines der oben genannten Gegenstände unter Strafe. Wie bei den in Art. 6 § 1 lit. a CCC aufgeführten Verhaltensweisen muss der Täter das verbotene Material in der Absicht besitzen, eine der in den Art. 2-5 CCC unter Strafe gestellten Straftaten zu begehen. Besitzt der Täter das Material in der Absicht, eine andere Straftat zu begehen, oder lediglich zu Sammelzwecken, ist er nicht strafbar.
- 17 Die Vertragsparteien haben den einzelnen Staaten jedoch einen gewissen Spielraum bei der Entscheidung eingeräumt, ob der Besitz eines einzigen Elements zur Verwirklichung des Straftatbestands ausreicht oder ob eine bestimmte Anzahl von Elementen besessen werden muss. Es ist jedoch festzustellen, dass diese Möglichkeit vor allem zugunsten der Vereinigten Staaten von Amerika eingeführt worden zu sein scheint, die als einzige von ihr Gebrauch gemacht haben. Sie haben jedoch nicht festgelegt, wie viele Elemente man mindestens besitzen muss, um sich strafbar zu machen. Sie verwiesen lediglich auf die Anzahl, die im anwendbaren Bundesgesetz der Vereinigten Staaten vorgesehen ist.

C. Die Rechtswidrigkeit

- 18 Das Erfordernis, dass der Täter unrechtmäßig gehandelt haben muss, ermöglicht es den Vertragsparteien, Ausnahmen von der strafrechtlichen Verfolgung zu schaffen. Dies ermöglicht es ihnen insbesondere, Strafverfolgungsbehörden, die im Rahmen ihrer Ermittlungen rechtmäßig

illegales Material in Form von Beschlagnahmen aufbewahren, vom Anwendungsbereich des Art. 6 CCC auszunehmen.

Art. 6 Abs. 2 behält ausdrücklich den Fall vor, dass der Täter nicht¹⁹ unrechtmäßig handelt, d.h. die in Art. 6 Abs. 1 lit. a Ziff. 1 CCC aufgeführten Verhaltensweisen sind nicht strafbar, wenn sie nicht darauf abzielen, eine nach den Art. 2 bis 5 CCC unter Strafe gestellte Straftat zu begehen. So werden beispielsweise Testgeräte (auch "Cracking-Geräte" genannt) und Netzwerkanalysegeräte, die von Fachleuten entwickelt wurden, um die Zuverlässigkeit ihrer IT-Produkte zu bewerten oder die Sicherheit von Systemen zu überwachen, zu rechtmäßigen Zwecken hergestellt, und ihre Benutzer werden daher als "rechtmäßig" handelnd angesehen.

D. Absicht

Der Missbrauch von Vorrichtungen ist vorsätzlich. Der Vorsatz muss sich auf²⁰ alle objektiven Elemente der Straftat beziehen. Wenn der Täter ein gewöhnliches Computerprogramm besitzt oder einem Dritten zur Verfügung stellt, ohne zu ahnen, dass es auch zur Begehung einer der in den Artikeln 2 bis 5 CCC unter Strafe gestellten Straftaten verwendet werden könnte, ist er nicht strafbar.

E. Ein besonderer Vorsatz

Neben dem Vorsatz muss der Täter in der Absicht gehandelt haben, eine der²¹ in den Artikeln 2 bis 5 CCC genannten Straftaten zu begehen. Es reicht daher nicht aus, dass der Täter ein Schadprogramm nur wegen der damit verbundenen technischen Herausforderung oder zum Zwecke der Sammlung herstellen will. Ebenso wenig reicht es aus, dass der Täter das Schadprogramm oder das Passwort verwenden will, um eine andere als die in Art. 2 bis 5 CCC unter Strafe gestellten Straftaten zu begehen.

Das vom Täter verfolgte Ziel muss darin bestehen, dass er selbst oder ein²² Dritter, dem er das verbotene Material zur Verfügung stellt, eine der in Art. 2 bis 5 CCC unter Strafe gestellten Straftaten begeht. In Art. 6 CCC ist ein abstraktes Gefährdungsdelikt verankert. Es ist daher nicht erforderlich, dass das verbotene Material später tatsächlich zur Begehung einer dieser Straftaten verwendet wird. Es reicht aus, dass die strafbare Handlung mit dem Ziel

begangen wird, eine der in den Art. 2-5 ZKK unter Strafe gestellten Straftaten zu begehen.

IV. DIE VORBEHALTE

- 23 Die einzigen Verhaltensweisen, die die Vertragsparteien zwingend unter Strafe stellen müssen, sind der Verkauf, die Verbreitung oder die sonstige Bereitstellung eines Passworts, eines Zugangscode oder ähnlicher Computerdaten, die den Zugang zu einem Computersystem oder einem Teil davon ermöglichen. Sie haben hingegen die Möglichkeit, den Anwendungsbereich dieser Norm in Bezug auf andere strafbare Verhaltensweisen und/oder illegale Gegenstände einzuschränken.

A. In Bezug auf strafbare Verhaltensweisen

- 24 Das Übereinkommen ermöglicht es den Vertragsparteien, die Strafverfolgung einzuschränken, indem sie die Verfolgung der Herstellung, der Beschaffung zur Nutzung, der Einfuhr und des Besitzes von illegalem Material ablehnen.
- 25 Georgien, die Schweiz, Chile, Japan und Sri Lanka haben von dieser Möglichkeit Gebrauch gemacht, um strafbare Verhaltensweisen auf ein Minimum zu beschränken.
- 26 Das Fürstentum Andorra gab an, dass die Beschaffung von in Art. 6 Abs. 1 lit. a CCC genannten Vorrichtungen, die zum Gebrauch bestimmt sind, nach seinem innerstaatlichen Recht nicht strafbar ist.
- 27 Aserbaidshon erklärte, dass es die in Art. 6 § 1 CCC aufgeführten Verhaltensweisen nur dann verfolgen würde, wenn ein ernsthafter Schaden entstünde.
- 28 Die Ukraine erklärte, dass sie die Beschaffung zur Nutzung und andere Formen der Bereitstellung der in Art. 6 Abs. 1 lit. a Ziff. 1 CCC genannten Gegenstände sowie die Herstellung und Beschaffung zur Nutzung der in Art. 6 Abs. 1 lit. a Ziff. 2 CCC genannten Gegenstände nicht unter Strafe stellen werde.
- 29 Die Vereinigten Staaten von Amerika haben sich das Recht vorbehalten, die Herstellung, die Beschaffung zur Verwendung, die Einfuhr und den Besitz von illegalem Material, das dazu bestimmt oder geeignet ist, die Begehung der in

Art. 4 und 5 CCC unter Strafe gestellten Straftaten zu ermöglichen, nicht zu verfolgen.

Israel erklärte, dass es weder die Beschaffung zur Verwendung oder die 30
Einfuhr von illegalem Material noch den Besitz eines Passworts, eines
Zugangscode oder ähnlicher Computerdaten, die den Zugang zu einem
Computersystem oder einem Teil davon ermöglichen, verfolgen werde.

Deutschland, das Fürstentum Andorra, Argentinien und Peru haben sich 31
darauf beschränkt, die Verfolgung des Besitzes von illegalem Material
abzulehnen (Art. 6 § 1 lit. b CCC).

B. In Bezug auf illegales Material

Das Übereinkommen erlaubt es den Vertragsparteien auch, die 32
Strafverfolgung einzuschränken, indem sie es ablehnen, Vorrichtungen,
einschließlich Computerprogrammen, als rechtswidrig zu betrachten, die
hauptsächlich dazu bestimmt oder geeignet sind, die Begehung einer der in
den Art. 2 bis 5 CCC unter Strafe gestellten Straftaten zu ermöglichen.

Auch Georgien, Norwegen, die Schweiz, Japan und Sri Lanka haben von 33
dieser Möglichkeit Gebrauch gemacht, um das strafbare Material so weit wie
möglich einzuschränken.

Chile hatte ursprünglich einen Vorbehalt eingelegt, der mit dem von 34
Georgien, Norwegen, der Schweiz und Japan identisch war. Es änderte jedoch
2022 seine Gesetzgebung. In der neuen Fassung entspricht der "abuso de los
dispositivos" Art. 6 CCC. Der Vorbehalt ist daher nicht mehr erforderlich.

Die Vereinigten Staaten von Amerika haben sich das Recht vorbehalten, 35
Vorrichtungen, einschließlich Computerprogrammen, die dazu bestimmt oder
geeignet sind, die Begehung der in den Art. 4 und 5 CCC unter Strafe
gestellten Straftaten zu ermöglichen, nicht zu verfolgen.

Deutschland erklärte, dass eine Vorrichtung, einschließlich eines 36
Computerprogramms, die hauptsächlich dazu bestimmt oder geeignet ist, die
Begehung einer nach den Art. 2 bis 5 CCC unter Strafe gestellten Straftat zu
ermöglichen, nach deutschem Recht kein strafbares Material ist.

V. VERGLEICH MIT DEM SCHWEIZER RECHT

- 37 In seiner Botschaft zur Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität wies der Bundesrat darauf hin, dass Art. 6 CCC im Wesentlichen durch Art. 144^{bis} Ziff. 2 StGB sowie durch die Hinzufügung eines zweiten Absatzes in Art. 143^{bis} StGB abgedeckt ist.
- 38 Nun hat die Schweiz zwar alle von Art. 6 Abs. 3 CCC gegebenen Möglichkeiten genutzt, um die strafbaren Handlungen und das illegale Material auf ein Minimum zu beschränken, doch bleibt es dabei, dass das Schweizer Recht aus mehreren Gründen weit davon entfernt ist, die von Art. 6 CCC gestellten Mindestanforderungen zu erfüllen.
- 39 Erstens ist Art. 144^{bis} Ziff. 2 Abs. 1 StGB nur auf Software anwendbar. Er ist daher nicht auf andere Geräte, Passwörter, Zugangscodes oder ähnliche Computerdaten anwendbar. Hinzu kommt, dass die von Art. 144^{bis} Ziff. 2 Abs. 1 StGB erfasste Software geeignet oder bestimmt sein muss, eine Straftat zu begehen, die nach Art. 144^{bis} Ziff. 1 Abs. 1 StGB unter Strafe gestellt ist. Dies führt zu zwei Problemen. Zum einen erfüllt 144^{bis} Ziff. 1 Abs. 1 StGB die Mindestvoraussetzungen von Art. 4 CCC nicht vollständig. Zum anderen lässt Art. 144^{bis} Ziff. 2 Abs. 1 StGB Software völlig außer Acht, die geeignet oder bestimmt ist, eine Straftat zu begehen, die den in Art. 2, 3 oder 5 CCC unter Strafe gestellten Straftaten entspricht. Solche Software ist daher nach schweizerischem Recht nicht strafbar.
- 40 Mit der Ergänzung von Art. 143^{bis} Abs. 2 StGB kann nur ein kleiner Teil dieser sehr wichtigen Lücken geschlossen werden. Diese Bestimmung stellt nämlich nur das Inverkehrbringen oder Zugänglichmachen eines Passworts, eines Programms oder anderer Daten unter Strafe, die geeignet oder bestimmt sind, die in Art. 143^{bis} Abs. 1 StGB unter Strafe gestellte Straftat zu begehen. Diese Norm entspricht jedoch zum einen nicht den Mindestanforderungen von Art. 2 CCC. Andererseits stellt sie das Inverkehrbringen oder Zugänglichmachen eines Passworts, eines Programms oder anderer Daten, die geeignet oder bestimmt sind, eine andere als die in 143^{bis} Abs. 1 StGB unter Strafe gestellte Straftat zu begehen, nicht unter Strafe.
- 41 Selbst wenn man davon ausgeht, dass Art. 143^{bis} Abs. 1 StGB den Anforderungen von Art. 2 ZKK und Art. 144^{bis} Ziff. 1 Abs. 1 StGB den Mindestanforderungen von Art. 4 ZKK entspricht, wäre die Strafbarkeit nach schweizerischem Recht auf das Inverkehrbringen oder Zugänglichmachen

eines Passworts, eines Programms oder anderer Daten beschränkt, die zur Begehung der in Art. 143^{bis} Abs. 1 StGB unter Strafe gestellten Straftat geeignet oder bestimmt sind. 2 CCC sowie auf die Herstellung, die Einfuhr, das Inverkehrbringen, die Förderung, das Anbieten oder das sonstige Zugänglichmachen von Software, die geeignet oder dazu bestimmt ist, die in Art. 4 CCC unter Strafe gestellte Straftat zu begehen.

Um den Mindestanforderungen von Art. 6 CCC zu entsprechen, müssten 42 daher die Art. 143 Abs. 1, 143^{bis} Abs. 1 und 144^{bis} Ziff. 1 Abs. 1 StGB im oben genannten Sinne angepasst werden; das Äquivalent von Art. 5 CCC und jede dieser Bestimmungen um einen Absatz ergänzen, der den Verkauf, die Verbreitung oder jede andere Bereitstellung eines Passworts, eines Zugangscode oder ähnlicher Computerdaten, die den Zugang zu einem Computersystem oder einem Teil davon ermöglichen, zum Zweck der Begehung einer dieser vier Straftaten unter Strafe stellt.

LITERATURVERZEICHNIS

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in: Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, FF 2010 4275, disponible à <https://www.fedlex.admin.ch/eli/fga/2010/813/fr>, visité le 21.1.2024

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 7 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 7 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 7 CCC N. XXX.

Titel 2: Computerbezogene Straftaten

Art. 7 Computerbezogene Fälschung

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben: das zu unechten Daten führende Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten in der Absicht, dass diese Daten für rechtliche Zwecke so angesehen oder einer Handlung zugrunde gelegt werden, als wären sie echt, gleichviel, ob die Daten

unmittelbar lesbar und verständlich sind. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst in Verbindung mit einer betrügerischen oder ähnlichen unredlichen Absicht eintritt.

GLIEDERUNG

I. Allgemeines.....	106
II. Geschütztes Rechtsgut	106
III. Grundlegende konstitutive Elemente	106
A. Elektronische Daten.....	106
B. Daten, die in Rechtsbeziehungen relevant sind	107
C. Ein strafbares Verhalten.....	108
1. Die Eingabe von Daten	109
2. Änderung, Löschung und Unkenntlichmachung von Daten	109
D. Rechtswidrigkeit	110
E. Vorsatz	111
IV. Zusätzliche fakultative Tatbestandsmerkmale.....	111
V. Vergleich mit dem Schweizer Recht	112
Materialienverzeichnis.....	113

I. ALLGEMEINES

- 1 Angesichts der Allgegenwart von Computern in der Gesellschaft ist eine Computer-Urkundenfälschung genauso gefährlich wie eine Urkundenfälschung in Papierform. Mit dieser Bestimmung soll daher ein Straftatbestand eingeführt werden, der das Gegenstück zur Fälschung von Urkunden auf Papier darstellt. Sie soll die strafrechtlichen Lücken im Zusammenhang mit der klassischen Fälschung schließen, die die visuelle Lesbarkeit der in einem Dokument enthaltenen Aussagen erfordert und nicht auf elektronisch gespeicherte Daten anwendbar ist. Die Manipulation von aufgezeichneten Daten mit Beweiswert kann ebenso schwerwiegende Folgen haben wie herkömmliche Fälschungshandlungen, wenn sie einen Dritten in die Irre führt. Computerfälschung besteht darin, dass aufgezeichnete Daten unbefugt so erstellt oder verändert werden, dass sie eine andere Beweiskraft erlangen, so dass der Ablauf von Rechtsgeschäften, der auf der Echtheit der durch diese Daten gelieferten Informationen beruht, irreführend sein kann.

II. GESCHÜTZTES RECHTSGUT

- 2 Das durch diese Norm geschützte Rechtsgut ist die Sicherheit und Zuverlässigkeit elektronischer Daten, die sich auf Rechtsbeziehungen auswirken können.

III. GRUNDLEGENDE KONSTITUTIVE ELEMENTE

A. Elektronische Daten

- 3 Gemäß Art. 1 lit. b CCC bedeutet "Computerdaten" jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Datenverarbeitung geeigneten Form, einschließlich eines Programms, das ein Computersystem dazu veranlassen kann, eine Funktion auszuführen". Der Begriff Computerdaten ist also sehr weit gefasst, da er unter anderem alle Buchstaben, Symbole oder Programmcodes umfasst, die von einem Computersystem eingegeben, verarbeitet und gespeichert werden können.
- 4 Für weitere Einzelheiten zu diesem Begriff wird auf die Ausführungen in Art. 1 CCC verwiesen.

B. Daten, die in Rechtsbeziehungen relevant sind

Die Verwendung des Begriffs "für rechtliche Zwecke" bedeutet, dass Art. 7 5 CCC nicht alle Computerdaten betrifft, sondern nur solche Daten, die in Rechtsbeziehungen eine Rolle spielen. Sie müssen also geeignet sein, einen rechtlich relevanten Sachverhalt zu beweisen, d. h. einen Sachverhalt, von dem die Begründung, Änderung oder das Erlöschen eines Rechts abhängt. Alle Daten, die für die Rechtsbeziehung nicht relevant sind, sind daher vom Anwendungsbereich dieser Norm ausgeschlossen.

Um in den Genuss der Beweiskraft zu kommen, muss die Herkunft der Daten 6 nachgewiesen werden können. In der realen Welt bedeutet diese Anforderung, dass der Urheber einer Urkunde identifizierbar sein muss und dass diese Urkunde den Ausdruck eines menschlichen Gedankens enthält. Konkret bedeutet dies zum Beispiel, dass die Information eine Bedeutung hat und das Dokument vom Autor handschriftlich unterzeichnet ist. In der virtuellen Welt nimmt die Garantie der Herkunft der Daten eine ganz andere Form an. Natürlich gibt es das Äquivalent eines Papierendokuments, das von seinem Autor unterzeichnet ist. Es handelt sich dann um ein von einem Menschen verfasstes Computerdokument, bei dem die handschriftliche Unterschrift durch das Anbringen einer qualifizierten elektronischen Signatur ersetzt wird. Die virtuelle Welt bietet jedoch viele zusätzliche Möglichkeiten zur Erzeugung von Daten, die für Rechtsbeziehungen relevant sind.

Anders als bei Wertpapieren, die in der realen Welt ausgegeben werden, ist es 7 in der virtuellen Welt nicht zwingend erforderlich, dass der Urheber der Daten eine menschliche Person ist. Bestimmte Daten können automatisch von Computersystemen generiert werden, ohne dass sie ihre Beweiskraft verlieren. Als Beispiel kann man an eine von einer E-Banking-Anwendung erstellte Zahlungsbestätigung denken, an einen für die Steuerbehörde bestimmten Lohnausweis, der vom Computersystem eines Unternehmens für seine Angestellten am Jahresende automatisch generiert wird, oder an die von einer Behörde automatisch versandte Quittung, die die Einreichung eines Rechtsakts auf elektronischem Weg belegt.

Wie aus dem Wortlaut von Art. 7 CCC ausdrücklich hervorgeht, erstreckt sich 8 diese Bestimmung auf alle in Rechtsbeziehungen relevanten Daten, "unabhängig davon, ob sie direkt lesbar und verständlich sind oder nicht". Es ist also auch nicht unbedingt erforderlich, dass die Daten den Ausdruck eines

menschlichen Gedankens enthalten. Die Daten können durchaus von einem Computersystem generiert worden sein. Sie müssen lediglich von einem Menschen oder einer Maschine verstanden werden können. Daten können also durchaus die Form einer Folge von Zeichen annehmen, die einen Code, einen Strichcode oder einen QR-Code bilden. Das beste aktuelle Beispiel für diese Art von Daten ist das computergenerierte COVID-Zertifikat in Form eines QR-Codes, das bescheinigt, dass eine Person gegen COVID geimpft ist, und das dem Inhaber den Zugang zu bestimmten Orten ermöglicht.

- 9 Letztendlich reicht es in der virtuellen Welt für die Beweiskraft von Daten, die im Rechtsverkehr verwendet werden können, aus, dass ihr Ursprung mit Sicherheit festgestellt werden kann und dass sie von einem Menschen oder einer Maschine verstanden werden können.

C. Ein strafbares Verhalten

- 10 Die Definition der Urkundenfälschung ist von Land zu Land sehr unterschiedlich. Ein einfacher Vergleich der Definitionen in der Schweiz und ihren Nachbarländern reicht bereits aus, um dies zu verdeutlichen. Weltweit ist festzustellen, dass für einige Länder der Begriff der Fälschung auf der Authentizität hinsichtlich des Urhebers des Dokuments beruht, während für andere der Wahrheitsgehalt der im Dokument enthaltenen Informationen ausschlaggebend ist. Die Vertragsparteien haben sich daher darauf geeinigt, dass sich die Fälschung zumindest auf die Identität des Ausstellers der Daten beziehen muss, unabhängig von der Richtigkeit oder Wahrhaftigkeit des Inhalts der Daten. Es steht ihnen jedoch frei, den Anwendungsbereich ihrer nationalen Bestimmungen auszuweiten, um auch die Fälschung der in dem Dokument enthaltenen Informationen unter Strafe zu stellen.
- 11 Die Echtheit der Daten hinsichtlich ihres Urhebers bedeutet, dass sie tatsächlich von der Person stammen, von der sie zu stammen scheinen. In diesem Sinne besteht die Fälschung authentischer Daten darin, dass ein Urheber angegeben wird, der nicht derjenige ist, von dem die Daten tatsächlich stammen. Der tatsächliche Urheber ist also nicht mit dem scheinbaren Urheber identisch.
- 12 Was die inhaltliche Echtheit der Daten betrifft, so bedeutet sie, dass die Daten in ihrem ursprünglichen Zustand geblieben sind. Eine Fälschung liegt folglich vor, wenn sie nach ihrer Erstellung verändert wurden. Die von Art. 7 CCC

erfasste Änderung ist nicht nur die Korrektur eines Schreibfehlers, sondern die Änderung der Bedeutung der Daten.

Art. 7 CCC zählt also vier strafbare Verhaltensweisen auf: das Eingeben, 13
Verändern, Löschen oder Unterdrücken von Computerdaten. Diese
Aufzählung ist erschöpfend. Die Eingabe von Daten stellt die Schaffung einer
falschen Urkunde unter Strafe, während sich die Veränderung, Löschung und
Unterdrückung auf die Fälschung einer echten Urkunde beziehen.

1. Die Eingabe von Daten

Die Dateneingabe ist die Handlung, durch die der Täter Daten, die von 14
außerhalb des Systems stammen, in ein Computersystem eingibt. Dabei kann
es sich um die unbefugte Eingabe von richtigen Daten oder das Hinzufügen
von unrichtigen Daten handeln.

Art. 7 CCC stellt nur die Eingabe von Daten unter Strafe, die dazu führt, dass 15
nicht-authentische Daten erzeugt werden. Wenn die in das Computersystem
eingegebenen Daten dazu bestimmt sind, das ordnungsgemäße Funktionieren
des Systems zu beeinträchtigen, ist Art. 5 CCC anwendbar.

Ein Beispiel für die Eingabe nicht authentischer Daten ist der Buchhalter 16
eines Unternehmens, der eine Zahlung eines Schuldners in das
Buchhaltungsprogramm einträgt, obwohl der Schuldner in Wirklichkeit gar
nicht gezahlt hat. Man könnte auch an den Täter denken, der eine Bankkarte,
die er betrügerisch kopiert hat, benutzt, um seine Einkäufe mit der
kontaktlosen Funktion zu bezahlen, und so das Terminal des Verkäufers
glauben lässt, dass die Zahlung vom rechtmäßigen Inhaber der kopierten
Karte autorisiert und durchgeführt wurde.

2. Änderung, Löschung und Unkenntlichmachung von Daten

Die Veränderung von Daten besteht darin, die Integrität und/oder den Inhalt 17
der Daten zu beeinträchtigen. Die Integrität von Daten bezieht sich auf ihre
Zuverlässigkeit, Genauigkeit und Vollständigkeit. In der realen Welt könnte
man die Gewährleistung der Datenintegrität mit einem per Post versandten
Paket vergleichen, bei dem bestätigt wird, dass es tatsächlich von dem auf
dem Paket angegebenen Absender versandt wurde, dass der Versand an dem
auf dem Poststempel angegebenen Datum und Ort stattgefunden hat und dass
das Paket während des Transports nicht geöffnet wurde. Was die Garantie für

den Inhalt betrifft, so könnte man sie mit der Bescheinigung vergleichen, dass der Inhalt des Pakets nach dem Versand nicht verändert wurde. Bei einer Datenmanipulation verändert der Täter gewissermaßen den Inhalt des Pakets und/oder seine Verpackung, um den Empfänger zu täuschen. Die Veränderung des Dateninhalts besteht darin, dass die ursprünglichen Daten durch andere Daten ersetzt werden. Dies ist zum Beispiel der Fall, wenn der Täter einen Text ändert, eine Bankverbindung austauscht oder ein Bild durch ein anderes ersetzt. Der Autor verändert hingegen die Integrität der Daten, wenn er die Metadaten ändert. Dies ist beispielsweise der Fall, wenn jemand die E-Mail-Adresse des Absenders fälscht, um den Eindruck zu erwecken, dass eine Nachricht von einer bestimmten Person stammt, obwohl sie in Wirklichkeit von einer anderen Person stammt, oder wenn er eine qualifizierte elektronische Signatur fälscht, um den Eindruck zu erwecken, dass ein Dokument von einer bestimmten Person erstellt wurde, obwohl dies in Wirklichkeit nicht der Fall ist.

- 18 Datenunterdrückung ist das Zurückhalten und Verstecken von Daten. Der Täter entfernt also absichtlich einen Teil der Daten, damit der Empfänger keine Kenntnis von den gesamten Daten erhält. Dies ist beispielsweise der Fall, wenn der Täter einen Teil der in Vergleichsgesprächen ausgehandelten Klauseln entfernt, um einen für ihn günstigeren Vertrag abzuschließen.
- 19 Im Gegensatz zum Löschen von Daten ist das Löschen von Daten eine endgültige Vernichtung aller oder eines Teils der Daten. Die Daten existieren nicht mehr. Man kann hier an diejenigen denken, die Teile von E-Mail-Konversationen löscht, die für ihn ungünstig sind, und dann die bereinigte Version als Beweismittel in einem Prozess vorlegt, oder an diejenigen, die Daten in einer elektronischen Krankenakte löscht, um einen von ihm begangenen medizinischen Fehler zu vertuschen.

D. Rechtswidrigkeit

- 20 Der Täter muss unrechtmäßig handeln, d. h. ohne vom Rechteinhaber dazu ermächtigt worden zu sein. Um rechtmäßig zu handeln, muss eine Person die Zustimmung des Rechteinhabers des Computersystems zur Eingabe von Daten in das System oder des Rechteinhabers der Daten zur Änderung der Daten einholen.

In der heutigen Gesellschaft arbeiten viele Unternehmen und Behörden mit Computersystemen. Die meisten Mitarbeiter, die für diese Körperschaften arbeiten, sind berechtigt, Daten in diese Systeme einzugeben oder sie zu verändern. Alle diese Personen handeln rechtmäßig, solange sie die ihnen erteilten Anweisungen befolgen. Ihre Handlungen werden jedoch illegal, wenn sie Daten entgegen den Anweisungen eingeben oder ändern. Dies ist z. B. der Fall, wenn eine Person, die für die Kasse zuständig ist, Waren stiehlt und dann falsche Verkäufe in das Computersystem eingibt, um die Spuren ihrer Tat zu verwischen. 21

E. Vorsatz

Eine Computerfälschung muss vorsätzlich erfolgen. Der Vorsatz muss sich auf alle objektiven Elemente der Straftat beziehen. Der Täter muss also das Bewusstsein und den Willen haben, falsche Daten zu erzeugen oder echte Daten zu fälschen, damit diese im Rechtsverkehr verwendet werden. 22

IV. ZUSÄTZLICHE FAKULTATIVE TATBESTANDSMERKMALE

Der letzte Satz von Art. 7 CCC ermöglicht es den Vertragsparteien, zusätzlich zum Vorsatz eine besondere Absicht zu verlangen. Dieser besondere Vorsatz kann die Form einer betrügerischen Absicht oder einer ähnlich schädlichen Absicht annehmen. Der erläuternde Bericht enthält keinen Hinweis darauf, wie der Begriff der betrügerischen Absicht zu verstehen ist. Unserer Ansicht nach bezieht sich die betrügerische Absicht auf die Absicht des Täters, einen ungerechtfertigten Vorteil für sich selbst oder für andere zu erlangen. Dieser Vorteil muss nicht unbedingt finanzieller Natur sein. Es kann sich um jeden Vorteil handeln, der die eigene oder die Situation einer anderen Person verbessert. Der angestrebte Vorteil muss jedoch ungerechtfertigt sein, d. h. gegen das Recht verstoßen. 23

Die Vereinigten Staaten von Amerika haben von der Möglichkeit des Art. 7 in fine ZK-DVO Gebrauch gemacht und erklärt, dass sie Computerfälschungen nur dann verfolgen würden, wenn sie in betrügerischer Absicht begangen werden. 24

- 25 Deutschland und Peru übernahmen die beiden in Art. 7 in fine CCC genannten Absichten, nämlich dass die Computerfälschung in betrügerischer Absicht oder in ähnlicher deliktischer Absicht begangen werden muss.
- 26 Belgien erklärte seinerseits, dass es die Computerfälschung nur dann unter Strafe stellen würde, wenn sie in betrügerischer Absicht oder mit Schädigungsabsicht begangen wird.
- 27 Die Schweiz hatte beschlossen, dass sie Computerfälschung nur dann verfolgen würde, wenn sie in der Absicht begangen wird, sich oder einem Dritten einen Vorteil zu verschaffen oder einen Schaden zu verursachen.
- 28 Schließlich hatte Chile zunächst erklärt, dass es Computerfälschung nur dann verfolgen werde, wenn sie in betrügerischer Absicht begangen werde und Dritten Schaden zufüge. Unserer Meinung nach entsprach diese Erklärung nicht dem Wortlaut von Art. 7 CCC, da eine Partei nur eine zusätzliche besondere Absicht verlangen kann. Es ist jedoch nicht möglich, das Eintreten eines Schadens zu verlangen, während Art. 7 CCC ein Gefährdungsdelikt unter Strafe stellt. Im Jahr 2022 änderte Chile jedoch seine Gesetzgebung. In der neuen Fassung entspricht die falsificación informática Art. 7 CCC. Der Vorbehalt ist daher nicht mehr erforderlich.

V. VERGLEICH MIT DEM SCHWEIZER RECHT

- 29 Art. 7 CCC zielt darauf ab, die Fälschung von Computerurkunden zu bestrafen. Im Schweizer Recht wird dieses Rechtsgut durch die Urkundenfälschung (Art. 251 StGB) geschützt, die seit dem 1. Januar 1995 auf Computerurkunden ausgedehnt wurde (Art. 110 Abs. 4 StGB).
- 30 Die von Art. 7 CCC bestraften Verhaltensweisen bestehen in der Fälschung von Daten mit Beweiswert mit dem Ziel, andere zu täuschen. Die Eingabe von Daten entspricht der Schaffung der gefälschten Urkunde. Das Verändern, Löschen und Unterdrücken hingegen entspricht der Fälschung einer Urkunde im Rahmen des herkömmlichen Straftatbestands der Urkundenfälschung.
- 31 Das schweizerische Recht entspricht somit den Anforderungen von Art. 7 des Übereinkommens.

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible à https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 8 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 8 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 8 CCC N. XXX.

Art. 8 Computerbezogener Betrug

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um folgende Handlung, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben: die Beschädigung des Vermögens eines anderen durch:

- a. Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten;
- b. Eingreifen in den Betrieb eines Computersystems;

in der betrügerischen oder unredlichen Absicht, sich oder einem anderen unbefugt einen wirtschaftlichen Vorteil zu verschaffen.

GLIEDERUNG

I. Allgemeines.....	118
II. Rechtlich geschütztes Gut	118
III. Grundlegende Tatbestandsmerkmale	118
A. Ein Computersystem.....	118
B. Computerdaten	119
C. Strafbares Verhalten	119
1. Eine Manipulation von Daten.....	119
a. Die Eingabe von Daten.....	119
b. Veränderung, Löschung und Unkenntlichmachung von Daten	120
2. Eine Beeinträchtigung der Funktionsweise des Computersystems	120
D. Ein Vermögensschaden.....	121
E. Die Rechtswidrigkeit	121
F. Die Absicht.....	122
G. Eine besondere Zeichnung	122
IV. Vergleich mit dem Schweizer Recht	123
Literaturverzeichnis	124
Materialienverzeichnis.....	124

I. ALLGEMEINES

- 1 Die Entwicklung der Computertechnik und ihre Verbreitung in allen Bereichen, insbesondere im Bereich des Geldtransfers, haben diesen Sektor in ein wahres Paradies für Wirtschaftskriminalität verwandelt. Die Leichtigkeit, mit der Straftaten begangen werden können, und das praktisch nicht vorhandene Risiko, strafrechtlich verfolgt zu werden, haben die Verlagerung "traditioneller" Wirtschaftsstraftaten ins Internet begünstigt. Um diese Form der Kriminalität zu bekämpfen, stellt Art. 8 CCC "jede missbräuchliche Manipulation bei der Verarbeitung von Daten zum Zwecke der unrechtmäßigen Übertragung von Eigentum" unter Strafe.

II. RECHTLICH GESCHÜTZTES GUT

- 2 Diese Bestimmung schützt Computersysteme vor betrügerischen Manipulationen, die mit dem Ziel vorgenommen werden, einem anderen einen Vermögensschaden zuzufügen und daraus einen Gewinn zu ziehen.

III. GRUNDLEGENDE TATBESTANDSMERKMALE

A. Ein Computersystem

- 3 Gemäß Art. 1 lit. a CCC bedeutet "der Ausdruck 'Computersystem' jede einzelne Vorrichtung oder eine Gesamtheit miteinander verbundener oder verwandter Vorrichtungen, die in Ausführung eines Programms eine automatische Datenverarbeitung gewährleistet oder bei der ein oder mehrere Elemente eine automatische Datenverarbeitung gewährleisten". Der Begriff Computersystem umfasst somit die gesamte Hardware (Hauptplatine, Prozessor, Festplatte, Bildschirm, Tastatur, Drucker, ...) und Software (BIOS, Betriebssystem, Software, Updates, ...) sowie die Geräte, die die Verbindung dieser verschiedenen Elemente untereinander ermöglichen (Kabel, Router, WiFi-Anschluss, ...).
- 4 Für weitere Details zu diesem Begriff wird auf die Ausführungen in Art. 1 CCC verwiesen.

B. Computerdaten

Gemäß Art. 1 lit. b CCC bedeutet "Computerdaten" jede Darstellung von 5
Tatsachen, Informationen oder Konzepten in einer für die Datenverarbeitung
geeigneten Form, einschließlich eines Programms, das ein Computersystem
dazu veranlassen kann, eine Funktion auszuführen. Der Begriff
Computerdaten ist also sehr weit gefasst, da er unter anderem alle
Buchstaben, Symbole oder Programmcodes umfasst, die von einem
Computersystem eingegeben, verarbeitet und gespeichert werden können.

Für weitere Einzelheiten zu diesem Begriff wird auf die Ausführungen zu Art. 6
1 CCC verwiesen.

C. Strafbares Verhalten

Art. 8 CCC zählt mehrere strafbare Verhaltensweisen auf und unterteilt sie in 7
zwei Kategorien. Die erste bezieht sich auf die Manipulation von Daten,
während sich die zweite auf die Beeinträchtigung der Funktionsweise des
Computersystems bezieht.

1. Eine Manipulation von Daten

a. Die Eingabe von Daten

Die Eingabe von Daten hat die gleiche Bedeutung wie in Art. 4, 5 und 7 CCC. 8
Es handelt sich also um die Handlung, durch die der Täter Daten, die von
außerhalb des Systems stammen, in das Innere eines Computersystems
einführt. Art. 8 CCC stellt jedoch nicht die Eingabe beliebiger Daten unter
Strafe, sondern nur solche, die geeignet sind, einen Vermögensschaden zu
verursachen.

Eine Dateneingabe liegt insbesondere dann vor, wenn der Täter unbefugt eine 9
Debitkarte in einen Bancomaten einführt und die persönliche
Identifikationsnummer eingibt, um Geld abzuheben, oder wenn der Täter sich
anstelle eines Dritten mit einer gestohlenen Benutzerkennung und einem
Passwort in ein E-Banking-Portal einloggt und unberechtigt Geld
überweist.

b. Veränderung, Löschung und Unkenntlichmachung von Daten

- 10 Die Begriffe der Veränderung, Unterdrückung und Löschung von Daten sind identisch mit denen der Art. 4, 5 und 7 CCC.
- 11 Eine Veränderung von Daten liegt vor, wenn der Täter die Integrität der Daten, d. h. ihre Zuverlässigkeit, Richtigkeit und Vollständigkeit, beeinträchtigt. Dies ist beispielsweise der Fall, wenn der Täter die Metadaten einer Zahlung bei einer Online-Transaktion ändert, was dazu führt, dass das Computersystem der Bank die Gelder auf ein Konto des Täters umleitet und nicht auf das Konto des ursprünglichen Empfängers.
- 12 Daten werden auch dann manipuliert, wenn der Täter den Inhalt der Daten angreift. Zu denken ist beispielsweise an den Fall, dass der Täter im Hintergrund die Bankverbindung oder den Betrag eines Zahlungsauftrags auf einer "E-Banking"-Plattform ändert, ohne dass der Nutzer dies bemerkt, so dass die Zahlung höher ausfällt als erwartet und/oder nicht auf dem vorgesehenen Konto gutgeschrieben wird.
- 13 Der Autor löscht Daten, wenn er den freien Zugang zu ihnen behindert. Der Täter hindert das Computersystem daran, vollständigen Zugriff auf alle Daten zu haben, auf die es Zugriff haben sollte. Dies ist der Fall, wenn ein Täter, der bei einem Kreditkartenunternehmen über einen Kreditrahmen verfügt, die Daten zu diesem Rahmen im Computersystem des Kreditkartenunternehmens löscht, damit dieses weiterhin Zahlungen auf Kredit vornehmen kann, obwohl es weiß, dass es sich die Rückzahlung nicht leisten kann.
- 14 Das Löschen von Daten schließlich ist eine endgültige Vernichtung der Daten. Sie existieren also nicht mehr. Man könnte hier an den Täter denken, der sich Zugang zum Computersystem seines Gläubigers verschafft und alle Daten löscht, die mit dem Betrag, den er schuldet, in Zusammenhang stehen, oder an denjenigen, der bei Online-Auktionen die höchsten Gebote löscht und sie durch sein eigenes Gebot zu einem viel niedrigeren Preis ersetzt.

2. Eine Beeinträchtigung der Funktionsweise des Computersystems

- 15 Um sicherzustellen, dass kein betrügerisches Verhalten vergessen wird, sieht Art. 8 lit. b CCC auch allgemein "jede Form der Beeinträchtigung der Funktionsweise eines Computersystems" vor. Diese Formulierung bezieht

sich auf Handlungen wie die Manipulation von Hardware, das Verhindern von Druckerausgaben und Handlungen, die Datensätze oder Datenströme sowie die Reihenfolge, in der Programme ausgeführt werden, beeinflussen.

Im Gegensatz zu den in Art. 5 CCC unter Strafe gestellten Verhaltensweisen muss die Beeinträchtigung der Funktionsweise des Computersystems nicht unbedingt schwerwiegend sein. Sie muss vielmehr dazu bestimmt sein, einen Vermögensschaden zu verursachen. 16

Ein Beispiel hierfür wäre die Manipulation eines Bankkartenterminals, das eine Zahlung an den Verkäufer bestätigt, obwohl diese in Wirklichkeit gar nicht auf dem zu belastenden Konto eingegangen ist. 17

D. Ein Vermögensschaden

Die oben genannten Verhaltensweisen sind nur dann strafbar, wenn sie einem anderen einen Vermögensschaden zufügen. Dieser Schaden kann wirtschaftlicher oder materieller Art sein und ist daher ein sehr weit gefasster Begriff, der sowohl Bargeld als auch materielle oder immaterielle Vermögenswerte mit einem wirtschaftlichen Wert umfasst. Allgemeiner kann er definiert werden als jede Verletzung des Vermögens in Form einer Verminderung der Aktiva, einer Erhöhung der Passiva, einer Nicht-Erhöhung der Aktiva oder einer Nicht-Verminderung der Passiva. 18

Der Wortlaut von Art. 8 CCC legt keinen Mindestbetrag hinsichtlich des verursachten Vermögensschadens fest. Ein Schaden, auch wenn er noch so gering ist, reicht aus. 19

Es wird auch nicht verlangt, dass der Schaden endgültig sein muss. Ein vorübergehender oder vorläufiger Schaden kann ausreichen. Eine betrügerisch durchgeführte Banktransaktion, die dem Inhaber des Kontos, das belastet wurde, einen finanziellen Schaden zufügt, der jedoch später wieder korrigiert wird, wenn der Betrug aufgedeckt wird, erfüllt den Straftatbestand. 20

E. Die Rechtswidrigkeit

Der Täter muss unrechtmäßig handeln, d. h. ohne vom Berechtigten, durch Gesetz oder Vertrag dazu ermächtigt worden zu sein. 21

Die Person, der der Berechtigte seine Benutzerkennung und sein Passwort anvertraut, um eine Zahlung per "E-Banking" vorzunehmen, handelt nicht 22

unrechtmäßig, solange sie nur die Anweisungen, die sie erhalten hat, strikt ausführt. Wenn sie ihre Zugänge nutzt, um den Überweisungsbetrag zu erhöhen oder die Identität des Begünstigten zu ändern, handelt sie hingegen unrechtmäßig.

- 23 Der Administrator eines E-Banking-Portals oder eines Online-Shops, dessen Aufgabe es ist, das Portal zu warten, macht sich nicht strafbar, wenn er Daten ändert oder die Website zeitweise nicht funktioniert. Nutzt er jedoch seinen Zugang aus, um beispielsweise die Daten im Konto eines Kunden zu ändern, macht er sich des Computerbetrugs schuldig.

F. Die Absicht

- 24 Computerbetrug ist vorsätzlich. Der Vorsatz muss sich auf alle objektiven Tatbestandsmerkmale beziehen, d. h. sowohl auf das strafbare Verhalten als auch auf das Eintreten eines Vermögensschadens.

G. Eine besondere Zeichnung

- 25 Zusätzlich zum Vorsatz verlangt Art. 8 CCC, dass der Täter in einer Zeichnung handelt, um sich oder einem Dritten einen wirtschaftlichen Nutzen zu verschaffen. Der Begriff des wirtschaftlichen Gewinns darf unseres Erachtens nicht in dem engen Sinne verstanden werden, der ihm in der Buchhaltung gegeben wird. Er umfasst vielmehr alle wirtschaftlichen Vorteile, die eine Bereicherung ermöglichen. Mit anderen Worten: Es handelt sich um jede Verbesserung der Vermögenssituation.
- 26 Dabei ist in erster Linie an eine Erhöhung der Aktiva, eine Verringerung der Passiva, eine Nicht-Verringerung der Aktiva oder eine Nicht-Erhöhung der Passiva zu denken. In diesen Annahmen entspricht die Bereicherung z. B. dem Preis einer gelieferten, aber nicht bezahlten Ware, dem von einem Bankkonto veruntreuten Betrag oder dem Betrag einer auf Kosten anderer erhaltenen Leistung.
- 27 Der Begriff des wirtschaftlichen Vorteils ist unserer Ansicht nach noch weiter gefasst und erstreckt sich auch auf jeden Vermögensvorteil. Dies gilt für den Urheber, der eine kostenpflichtige "Streaming"-Plattform börsenfrei nutzen kann, für denjenigen, der bei einer Online-Buchung als Sicherheit die Kreditkartennummer eines Dritten angibt, um nicht selbst das Risiko tragen zu müssen, dass seine Kreditkarte bei einer verspäteten Stornierung belastet

wird, oder auch für die Person, die die Kontaktdaten eines Dritten, wie z. B. eines Studenten oder Rentners, nutzt, um - zu einem reduzierten Preis - Leistungen zu erhalten, für die er den vollen Preis hätte zahlen müssen.

Der vom Täter angestrebte wirtschaftliche Nutzen muss auch ohne Recht 28 erlangt werden. Wenn der Täter einen Vermögensanspruch hat oder zu haben glaubt, der der erzielten Bereicherung entspricht, handelt er nicht unbefugt und ist daher nicht strafbar. Ebenso stellen konkurrierende geschäftliche Aktivitäten, die einer Person wirtschaftlichen Schaden zufügen und einer anderen einen Gewinn bringen können, aber nicht in betrügerischer oder unredlicher Absicht ausgeübt werden, wie z. B. die Verwendung von Programmen zur Informationsbeschaffung, um den Wettbewerb im Internet auszuspielen, keinen Computerbetrug dar.

IV. VERGLEICH MIT DEM SCHWEIZER RECHT

Im Schweizer Recht ist die Norm, die Art. 8 CCC am nächsten kommt, Art. 29 147 StGB. Diese Bestimmung entspricht jedoch in mehreren Punkten nicht den Anforderungen von Art. 8 ZKK.

Zunächst einmal sind die von diesen beiden Normen geschützten Rechtsgüter 30 unterschiedlich. Art. 8 CCC schützt Computersysteme vor betrügerischen Manipulationen, die mit dem Ziel vorgenommen werden, einem anderen einen Vermögensschaden zuzufügen und daraus einen Gewinn zu ziehen. Art. 147 StGB schützt dagegen nur das Vermögen und schließt das Interesse des Betreibers eines Computersystems an der ordnungsgemäßen Nutzung des Systems aus.

Was die strafbaren Verhaltensweisen betrifft, stellt Art. 147 StGB die 31 unrichtige, unvollständige oder unzulässige Verwendung von Daten unter Strafe. Diese decken sich weitgehend mit den Begriffen der Eingabe, Veränderung, Löschung oder Unterdrückung von Computerdaten, die in Art. 8 ZK-DVO erwähnt werden. Art. 147 StGB lässt jedoch eine wichtige Lücke offen, da er die Löschung von Daten, die sich im Computersystem hätten befinden müssen, nicht unter Strafe stellt.

Schließlich stellt Art. 147 StGB nur Computerbetrug unter Strafe, der durch 32 Datenmanipulation verursacht wird. Das in Art. 8 lit. b CCC erwähnte Verhalten fällt somit nicht unter Art. 147 StGB. Dieser Punkt ist besonders

problematisch, da sich viele Handlungen der Strafverfolgung entziehen, obwohl sich die Schweiz zu deren Verfolgung verpflichtet hat.

- 33 Es muss festgestellt werden, dass das Schweizer Recht nicht mit Art. 8 CCC übereinstimmt und daher angepasst werden sollte.

LITERATURVERZEICHNIS

Corboz Bernard, Les infractions en droit suisse, vol. I, 3. éd., Berne 2010

Fiolka Gerhard, in: Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Stratenwerth Günter/Bommer Felix, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8. éd., Berne, 2022

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800ccea5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 9 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jérémie Müller

ZITIERVORSCHLAG

Jérémie Müller, Kommentierung zu Art. 9 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Müller, Art. 9 CCC N. XXX.

Titel 3: Inhaltsbezogene Straftaten

Art. 9 Straftaten mit Bezug zu Kinderpornographie

¹ Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

a. das Herstellen von Kinderpornographie zum Zweck ihrer Verbreitung über ein Computersystem;

- b. das Anbieten oder Verfügbarmachen von Kinderpornographie über ein Computersystem;
- c. das Verbreiten oder Übermitteln von Kinderpornographie über ein Computersystem;
- d. das Beschaffen von Kinderpornographie über ein Computersystem für sich selbst oder einen anderen;
- e. den Besitz von Kinderpornographie in einem Computersystem oder auf einem Computerdatenträger.

² Im Sinne des Absatzes 1 umfasst der Ausdruck «Kinderpornographie» pornographisches Material mit der visuellen Darstellung:

- a. einer minderjährigen Person bei eindeutig sexuellen Handlungen;
- b. einer Person mit dem Erscheinungsbild einer minderjährigen Person bei eindeutig sexuellen Handlungen;
- c. real erscheinender Bilder, die eine minderjährige Person bei eindeutig sexuellen Handlungen zeigen.

³ Im Sinne des Absatzes 2 umfasst der Ausdruck «minderjährige Person» alle Personen, die das 18. Lebensjahr noch nicht vollendet haben. Eine Vertragspartei kann jedoch eine niedrigere Altersgrenze vorsehen, wobei 16 Jahre nicht unterschritten werden dürfen.

⁴ Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 Buchstaben d und e sowie Absatz 2 Buchstaben b und c ganz oder teilweise nicht anzuwenden.

GLIEDERUNG

I. Allgemeines.....	128
II. Rechtlich geschütztes Gut	129
III. Grundlegende Tatbestandsmerkmale	129
A. Eine kinderpornografische Darstellung	129
1. Die Medien der Darstellung.....	129
2. Der pornografische Charakter	129
3. Der Begriff des Minderjährigen	131
4. Der Begriff der Kinderpornografie.....	131
B. Ein strafbares Verhalten	132
C. Die Rechtswidrigkeit	134
D. Vorsatz	135
IV. Die Vorbehalte	136
A. In Bezug auf das Alter der Minderjährigen, die Gegenstand der Darstellung sind	136
B. Zu den strafbaren Verhaltensweisen.....	137
C. Zu den Objekten der Darstellung.....	137
V. Vergleich mit dem Schweizer Recht	138
Literaturverzeichnis	138
Materialienverzeichnis.....	139

I. ALLGEMEINES

- 1 Das Aufkommen des Internets hat den weitesten, schnellsten und effizientesten Austausch ermöglicht, den die Menschheit je erlebt hat. Es hat jedoch auch Kriminellen, die zuvor oft isoliert waren, sehr leistungsfähige Kommunikationswerkzeuge zur Verfügung gestellt. So konnten beispielsweise Personen, die Kinderpornografie produzieren, mit Personen, die solche Medien konsumieren, auf der ganzen Welt in Kontakt treten. Der Austausch von Ideen, Fantasien und Ratschlägen zwischen Pädophilen hat dazu beigetragen, Sexualstraftaten an Kindern zu unterstützen, zu fördern oder zu erleichtern.
- 2 Die virtuelle Welt hat nicht nur den Austausch von kinderpornografischem Material erleichtert, sondern den Tätern auch eine gewisse Anonymität und damit eine Form der Straflosigkeit garantiert. Es ist daher nicht überraschend, dass sich diese Art der Kriminalität mit der Verbreitung des Internets rasch ausgebreitet hat.
- 3 Art. 9 CCC entspricht somit dem Anliegen, das die Mitglieder des Europarats auf ihrem 2. Gipfeltreffen 1997 geäußert haben, und spiegelt eine internationale Entwicklung zugunsten des Verbots von Kinderpornografie wider, wie die kürzliche Annahme des Fakultativprotokolls zum Übereinkommen der Vereinten Nationen über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornografie sowie die jüngste Initiative der Europäischen Kommission zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie (KOM2000/854) bestätigen.
- 4 Diese Bestimmung zielt darauf ab, die Schutzmaßnahmen zugunsten von Kindern, insbesondere vor sexueller Ausbeutung, zu verstärken, indem das Strafrecht modernisiert wird, um die Nutzung von Computersystemen zur Begehung von Sexualstraftaten gegen Kinder wirksamer einzuschränken.
- 5 In den Jahren nach der Verabschiedung der Cybercrime-Konvention blieben Kinderpornografie und im weiteren Sinne die sexuelle Ausbeutung von Kindern weiterhin ein sehr wichtiges Thema. Dies führte zur Ausarbeitung des Übereinkommens des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, das am 25. Oktober 2007 in

Lanzarote verabschiedet wurde. Art. 20 dieses Vertrags orientiert sich sehr stark an Art. 9 CCC.

II. RECHTLICH GESCHÜTZTES GUT

Art. 9 CCC schützt zwei verschiedene Rechtsgüter. Art. 9 § 2 lit. a CCC 6 schützt direkt die sexuelle Integrität von Kindern. Art. 9 Abs. 2 lit. b und c CCC schützen ihre sexuelle Integrität indirekt, indem sie Verhaltensweisen verbieten, die zwar nicht notwendigerweise dem in dem betreffenden Material dargestellten "Kind" schaden, aber dennoch Kinder ermutigen oder dazu verleiten könnten, an solchen Handlungen teilzunehmen. Diese Bestimmungen stehen somit im Kontext einer Subkultur, die den Missbrauch von Kindern befürwortet.

III. GRUNDLEGENDE TATBESTANDSMERKMALE

A. Eine kinderpornografische Darstellung

1. Die Medien der Darstellung

Art. 9 CCC bezieht sich - ebenso wie Art. 20 des Übereinkommens des 7 Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch - ausschließlich auf bildliche Darstellungen von Kinderpornografie. Dies umfasst alle Darstellungen, die mit den Augen wahrgenommen werden können, insbesondere Fotos, Zeichnungen, Skizzen, Gemälde, Stiche, Skulpturen, Videos und Filme. Tonaufnahmen sowie Texte sind nicht betroffen.

Im Rahmen der Cybercrime-Konvention beschränkt sich die Strafbarkeit auf 8 visuelle Darstellungen in digitaler Form. Es ist unerheblich, auf welchem Medium sie gespeichert sind. Es ist also unerheblich, ob sie auf einer Festplatte, einem USB-Stick, einer DVD oder sogar in der Cloud gespeichert sind.

2. Der pornografische Charakter

Der Begriff der Pornografie wird weder in der Cybercrime-Konvention noch 9 im erläuternden Bericht definiert. Letzterer besagt lediglich, dass dieser Begriff im Einklang mit den Normen des innerstaatlichen Rechts auszulegen

ist, die sich mit der Einstufung der Darstellung als obszön, mit den öffentlichen Sitten unvereinbar oder in anderer Weise perverser Wirkung befassen.

- 10 In der Schweiz gilt als pornografisch, was darauf abzielt, beim Konsumenten eine sexuelle Erregung hervorzurufen, während die Sexualität derart von ihren menschlichen und emotionalen Komponenten losgelöst ist, dass die Person auf ein reines Sexualobjekt reduziert wird, über das man nach Belieben verfügen kann. Das sexuelle Verhalten ist grob und wird übertrieben in den Vordergrund gestellt. Pornografie ist die eindringliche und wiederholte Darstellung von Handlungen wie Oralsex, Cunnilingus und Masturbation. Diese Definition scheint weder zügellos noch besonders keusch zu sein. Sie scheint vielmehr ausgewogen zu sein und kann daher leicht auf internationaler Ebene übernommen werden. Die Kernelemente dieser Definition finden sich übrigens auch in Art. 20 des Übereinkommens des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch - der sich weitgehend an Art. 9 CCC orientiert -, der in seinem Absatz 2 Kinderpornografie als jedes Material definiert, das ein Kind bei tatsächlichen oder simulierten sexuell eindeutigen Handlungen visuell darstellt, oder jede Darstellung der Geschlechtsorgane eines Kindes zu überwiegend sexuellen Zwecken. Daher kann man sich an diese Definition halten.
- 11 Obwohl der Text von Art. 9 CCC dies nicht ausdrücklich erwähnt, gilt Material, das von künstlerischem, medizinischem oder wissenschaftlichem Interesse ist, nicht als pornografisch.
- 12 Die Bestimmung, was künstlerisch ist und was nicht, ist kompliziert, insbesondere im Zusammenhang mit einem internationalen Abkommen, das zwischen Staaten mit sehr unterschiedlichen Kulturen geschlossen wurde. Unserer Meinung nach muss der künstlerische Charakter von Fall zu Fall beurteilt werden. Generell kann man jedoch sagen, dass Material als künstlerisch zu bezeichnen ist, wenn der Künstler eine Sache auf originelle Weise darstellt, eine Botschaft vermitteln soll und das Ergebnis echter Forschung ist. Dies steht im Gegensatz zu einer rohen, trivialen oder vulgären Darstellung der Realität.
- 13 Was medizinisches oder wissenschaftliches Material angeht, so handelt es sich um Material, das für Ausbildung oder Forschung notwendig ist.

3. Der Begriff des Minderjährigen

Obwohl die nationalen Rechte einiger Vertragsparteien des Übereinkommens 14 ein höheres Volljährigkeitsalter kennen (z. B. Kanada, USA, Japan), haben sich die Vertragsparteien darauf geeinigt, dass unter dem Begriff des Minderjährigen grundsätzlich jede Person unter 18 Jahren zu verstehen ist (Art. 9 Abs. 3 CCC). Wie in Ziffer IV unten erläutert, können die Vertragsparteien jedoch Vorbehalte anbringen, um eine niedrigere Altersgrenze zu verlangen. In jedem Fall muss diese Grenze jedoch mindestens 16 Jahre betragen.

4. Der Begriff der Kinderpornografie

Art. 9 Abs. 2 CCC definiert den Begriff der Kinderpornografie, indem er eine 15 Liste mit drei Arten von strafbaren Darstellungen bereitstellt. Diese Liste ist erschöpfend.

Zunächst geht es um Darstellungen, die einen Minderjährigen zeigen, der ein 16 sexuell eindeutiges Verhalten an den Tag legt. Der Begriff "sexuell explizites Verhalten" bezieht sich vor allem auf sexuelle Beziehungen, einschließlich genito-genitaler, oro-genitaler, ano-genitaler oder oro-analer Beziehungen. Um im Sinne von Art. 9 § 2 lit. a CCC strafbar zu sein, müssen sie mindestens eine minderjährige Person einbeziehen. Dagegen ist es unerheblich, ob sie nur zwischen Minderjährigen oder mit einem oder mehreren Volljährigen stattfinden. Auch das Geschlecht oder die sexuelle Orientierung der einzelnen Teilnehmer ist unerheblich.

Der Begriff "sexuell eindeutiges Verhalten" ist jedoch weiter gefasst als nur 17 sexuelle Beziehungen. Er umfasst auch Zoophilie, die mit einem Minderjährigen begangen wird, die Masturbation eines Minderjährigen, sadomasochistische Gewalt in einem sexuellen Kontext, die an einem Minderjährigen begangen wird, oder die laszive Zurschaustellung der Genitalien oder des Schambereichs eines Minderjährigen.

Bei all den oben genannten Annahmen ist es unerheblich, ob das dargestellte 18 Verhalten echt oder vorgetäuscht ist. Der Täter kann sich also nicht der Verurteilung entziehen, nur weil das sexuell eindeutige Verhalten nicht wirklich stattgefunden hat.

- 19 Die zweite Art von Darstellungen, auf die Art. 9 Abs. 2 CCC abzielt, betrifft pornografische Bilder, die eine Person, die als Minderjähriger erscheint, bei sexuell eindeutigen Handlungen zeigen (Art. 9 Abs. 2 lit. b CCC). Es handelt sich um Bilder, auf denen Personen zu sehen sind, die entweder gerade erst volljährig geworden sind, aber versucht wird, sie als noch minderjährig erscheinen zu lassen, oder die eindeutig volljährig sind, aber durch ihre Kleidung, ihr Make-up oder die Accessoires, die sie tragen, den Anschein einer minderjährigen Person erwecken.
- 20 Art. 9 § 2 lit. c CCC erwähnt schließlich realistische Bilder, die einen Minderjährigen bei sexuell eindeutigen Handlungen darstellen. Letzteres gilt insbesondere für Comics oder Mangas, Fotomontagen und sogar für Bilder, die von Computern aus dem Nichts geschaffen werden, wie es bei künstlicher Intelligenz der Fall sein kann.

B. Ein strafbares Verhalten

- 21 Art. 9 § 1 CCC zählt fünf strafbare Verhaltensweisen auf. Diese Liste ist abschließend.
- 22 Das erste genannte Verhalten ist die "Produktion", d. h. die Herstellung, einer kinderpornografischen Darstellung zum Zweck ihrer Verbreitung über Computer. Der Begriff "Herstellung" umfasst alle Handlungen, die für die Herstellung von kinderpornografischen Darstellungen erforderlich sind. Dabei ist natürlich in erster Linie an die Fixierung von Bildern auf einem Bildträger zu denken. Es geht jedoch auch um die Vorbereitung des Ortes und des Materials, das für die Herstellung der Bilder erforderlich ist, um die Bearbeitung der Bilder nach ihrer Fixierung auf einem Bildträger, um die Montage von Fotografien oder Filmen oder sogar um die Erstellung von computergenerierten Bildern. Mit anderen Worten: Dieses Verhalten zielt auf alle Formen der Erstellung oder Bearbeitung von Bildträgern ab. In jedem Fall muss dieses Material jedoch für die Verbreitung über Computer bestimmt sein. Die Herstellung von digitalen Bildern für den Eigenbedarf ist nicht als Produktion, sondern nur aufgrund des Besitzes strafbar (Art. 9 § 1 lit. e CCC).
- 23 Art. 9 § 1 lit. b CCC stellt dann das Anbieten oder Zugänglichmachen von Kinderpornografie über ein Computersystem unter Strafe. Der Begriff "anbieten" bezeichnet ein Geschäftsverhalten, bei dem der Täter seine Kunden darüber informiert, dass er über ein oder mehrere Produkte verfügt,

und ihnen anbietet, diese zu erwerben. Die Art des Vertrags (Verkauf, Tausch, Schenkung, ...) ist dabei unerheblich. Das "Zurverfügungstellen" ist ein weiter gefasster Begriff als das "Anbieten", da er nicht unbedingt bedeutet, dass der Urheber irgendwelche aktiven Schritte unternimmt, um seiner Kundschaft ein Produkt anzubieten. Es handelt sich vielmehr um jede Handlung, die den Zugang zu einer kinderpornografischen Darstellung über Computer ermöglicht oder erleichtert. Dazu gehört insbesondere das Einstellen von Kinderpornografie, z. B. durch das Erstellen von Webseiten, sowie das Erstellen oder Zusammenstellen von Hyperlinks zu Seiten mit Kinderpornografie.

Ein weiteres strafbares Verhalten ist das Verbreiten oder Übertragen von 24
Kinderpornografie über ein Computersystem. Beide Begriffe beziehen sich auf das Versenden von Daten. Bei der "Verbreitung" handelt es sich um die Verteilung von kinderpornografischem Material an eine unbestimmte Anzahl von Personen, die nicht unbedingt darum gebeten haben. Die "Übermittlung" hingegen ist eine Sendung an eine oder mehrere bestimmte Personen, die dies beantragt haben. Der Versand der kinderpornografischen Darstellung kann auf jedem beliebigen Computerweg erfolgen, also insbesondere per E-Mail, Instant Messaging oder Peer-to-Peer-Übertragung.

Art. 9 lit. d CCC erwähnt außerdem "das Verschaffen von Kinderpornografie 25
über ein Computersystem für sich selbst oder für andere". Dieses Verhalten besteht in der aktiven Beschaffung von Kinderpornografie, z. B. durch Herunterladen. Die Daten müssen also auf das Computersystem des Täters oder vom Täter auf das Computersystem eines Dritten übertragen worden sein. Es muss eine Übertragung des Besitzes vorliegen. Die Beschaffung muss auf dem Computerweg erfolgen. Eine persönliche Übergabe oder ein Versand per Post fallen daher nicht unter das Übereinkommen.

Die letzte strafbare Handlung ist schließlich der "Besitz von 26
Kinderpornografie in einem Computersystem oder einem Speichermedium für Computerdaten" (Art. 9 § 1 lit. e CCC). Der klassische Begriff des Besitzes setzt sowohl die physische Herrschaft über den Gegenstand als auch den Willen zur Ausübung dieser Herrschaft voraus. In der virtuellen Welt muss das objektive Erfordernis der physischen Herrschaft über den Gegenstand unserer Ansicht nach insofern gelockert werden, als es ausreicht, dass der Besitzer jederzeit und frei in der Lage ist, auf seine Daten zuzugreifen. Dies ist natürlich der Fall, wenn sich die Daten in einem Computersystem befinden,

das ihm gehört, auf einem Datenspeichermedium wie einer externen Festplatte, einem USB-Stick oder in der Speicherkarte einer Kamera. Der Urheber ist jedoch auch im Besitz der Daten, wenn er sie auf einem entfernten Server speichert, zu dem er Zugang hat, oder wenn er sie in der "Cloud" speichert.

- 27 Unverständlicherweise wurde die Tatsache, dass Kinderpornografie direkt online abgerufen wird, ohne sich diese anzueignen, nicht erwähnt und ist daher nicht strafbar. Die fehlende Erwähnung dieses Verhaltens in der Liste des Art. 9 Abs. 1 CCC erscheint besonders überraschend. Angesichts des erklärten Willens, Kinderpornografie zu bekämpfen, scheint die Bestrafung des Konsums nämlich ebenso wichtig zu sein wie die Kriminalisierung der Herstellung kinderpornografischer Darstellungen. Dieses Versäumnis wurde glücklicherweise in der Konvention des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch korrigiert. In seinem erläuternden Bericht wird übrigens erwähnt, dass das in Art. 20 Abs. 1 Buchst. f erwähnte Verhalten darauf abzielt, die Verfolgung derjenigen zu ermöglichen, die sich Bilder von Kindern auf kinderpornografischen Seiten ansehen, sich aber der strafrechtlichen Verfolgung entziehen, weil sie diese nicht herunterladen.

C. Die Rechtswidrigkeit

- 28 Der Täter muss unrechtmäßig handeln. Dieses Tatbestandsmerkmal ermöglicht es den Vertragsparteien, Ausnahmen von der strafrechtlichen Verfolgung für Täter zu schaffen, die in einem schutzwürdigen Interesse handeln, ähnlich dem künstlerischen, medizinischen oder wissenschaftlichen Interesse.
- 29 Dieser Ausdruck ermöglicht es auch, Strafverfolgungsbehörden, die Bilder von Kinderpornografie in Form von Beschlagnahmen in den von ihnen untersuchten und abgeurteilten Ermittlungen rechtmäßig aufbewahren, vom Anwendungsbereich des Art. 9 CCC auszuschließen.
- 30 Die Allgegenwart von "Smartphones", auch in den Händen von Minderjährigen, hat zu verschiedenen Fehlentwicklungen geführt. So ist es heutzutage nicht ungewöhnlich, dass sich Personen - vor allem in der jüngeren Generation - während der Verführungsphase gegenseitig Fotos ihres Intimbereichs schicken. Diese Praxis ist problematisch, wenn es sich bei dem

Absender um einen Minderjährigen handelt, da er durch das Fotografieren seines Genitalbereichs Kinderpornografie produziert, das Foto beim Versenden über ein Instant-Messaging-System weiterleitet und es sogar besitzt, wenn er eine Kopie davon auf seinem Smartphone aufbewahrt. In dieser Situation ist der Minderjährige paradoxerweise sowohl Täter als auch Opfer der Straftat, die nach Art. 9 CCC unter Strafe steht. Im Rahmen von Art. 9 Abs. 2 Buchst. a CCC könnten die Vertragsparteien unseres Erachtens vorsehen, dass ein Minderjähriger, der eine Fotografie mit sexuellem Inhalt von sich selbst macht, diese weiterleitet oder besitzt, nicht unrechtmäßig handelt. Der Empfänger einer Sendung, der in Kenntnis des Alters des Absenders um den Erhalt eines solchen Bildes bittet, handelt hingegen eindeutig unrechtmäßig.

In Bezug auf Art. 9 Abs. 2 lit. b CCC könnte der Ausdruck "unbefugt" einer Vertragspartei auch erlauben, beispielsweise vorzusehen, dass eine Person nicht strafbar ist, wenn feststeht, dass die abgebildete Person nicht "minderjährig" im Sinne dieser Bestimmung ist. 31

D. Vorsatz

Eine Straftat muss vorsätzlich begangen werden. Der Vorsatz muss sich auf alle objektiven Elemente der Straftat beziehen. Der Täter muss also das Bewusstsein und den Willen haben, Kinderpornografie herzustellen, anzubieten, zur Verfügung zu stellen, zu verbreiten, zu übertragen, sich oder einem Dritten zu verschaffen oder zu besitzen. 32

Die Vertragsparteien können jedoch einen spezifischeren Standard annehmen, wobei in diesem Fall der letztgenannte Standard gelten würde. So könnte beispielsweise eine Haftung auferlegt werden, wenn "Kenntnis und Kontrolle" über die übermittelten oder gespeicherten Informationen besteht. Es reicht beispielsweise nicht aus, dass ein Diensteanbieter die Übermittlung dieser Darstellung vermittelt, indem er unter anderem eine Website oder ein Chatroom betreibt, wenn die erforderliche Absicht fehlt. Darüber hinaus ist ein Diensteanbieter nicht verpflichtet, den Inhalt zu überwachen, um eine strafrechtliche Haftung zu vermeiden. 33

IV. DIE VORBEHALTE

- 34 Art. 9 Abs. 3 und 4 CCC erlauben den Vertragsparteien, die Strafbarkeit auf drei verschiedene Arten einzuschränken, nämlich in Bezug auf das Alter der Minderjährigen, die strafbaren Verhaltensweisen und die Gegenstände der Darstellung.

A. In Bezug auf das Alter der Minderjährigen, die Gegenstand der Darstellung sind

- 35 Bei der Ausarbeitung des Übereinkommens waren sich die Vertragsparteien einig, dass es wichtig ist, das Alter der Volljährigkeit einheitlich festzulegen. Sie haben daher beschlossen, dass der Begriff "Minderjähriger" jede Person unter 18 Jahren bezeichnet. Diese Grenze wurde im Hinblick auf die Definition des Begriffs "Kind" in Artikel 1 des Übereinkommens der Vereinten Nationen über die Rechte des Kindes festgelegt. Es muss hier jedoch betont werden, dass sich dieses Alter auf die Ausbeutung von Kindern als Sexualobjekte bezieht. Es muss daher von dem Alter unterschieden werden, das für die Zustimmung zu sexuellen Beziehungen erforderlich ist.
- 36 Da einige Staaten in ihren nationalen Gesetzen zu Kinderpornografie eine niedrigere Altersgrenze festgelegt haben, erlaubt der letzte Satz von Absatz 3 den Vertragsparteien, eine andere Altersgrenze festzulegen, die in jedem Fall nicht unter 16 Jahren liegen darf.
- 37 Der einzige Staat, der von dieser Möglichkeit Gebrauch gemacht hat, ist die Schweiz. Sie legte die Altersgrenze auf 16 Jahre fest, um dem Wortlaut des früheren Artikels 197 Abs. 3 und 3bis StGB zu entsprechen. Am 16. Juni 2010 hat die Schweiz jedoch das Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch unterzeichnet. Art. 20 dieses Übereinkommens stellt Straftaten im Zusammenhang mit Kinderpornografie unter Strafe. Der dort erwähnte Begriff "Kind" wird in Art. 3 lit. a als jede Person unter 18 Jahren definiert. Da in Bezug auf die Altersgrenze keine Vorbehalte geltend gemacht werden konnten, musste Art. 197 StGB angepasst werden. Die neue Fassung dieser Bestimmung trat am 1. Juli 2014 in Kraft. Sie entspricht nun der allgemeinen Definition in Art. 9 § 3 CCC. Der von der Schweiz bei der Ratifizierung des Übereinkommens angebrachte Vorbehalt ist daher nicht mehr relevant.

B. Zu den strafbaren Verhaltensweisen

Das Übereinkommen erlaubt es den Vertragsparteien auch, die 38
Strafverfolgung einzuschränken, indem sie die Verfolgung der Tatsache, sich
oder einem Dritten kinderpornografische Bilder zu verschaffen und/oder den
Besitz solcher Bilder abzulehnen.

Zum Zeitpunkt der Ratifizierung des Übereinkommens machten die Ukraine, 39
Japan und Sri Lanka von dieser Möglichkeit Gebrauch, um die Beschaffung
und den Besitz von Kinderpornografie nicht zu verfolgen. Japan änderte 2014
seine Gesetze und stellte den Besitz von Kinderpornografie sowie die
Beschaffung von Kinderpornografie für andere unter Strafe. Die Beschaffung
für sich selbst ist jedoch weiterhin nicht strafbar.

Israel stellte klar, dass es sich weigert, die Beschaffung von Kinderpornografie 40
zu verfolgen.

Argentinien gab an, dass der Besitz von Kinderpornografie in seinem 41
nationalen Recht nicht strafbar ist.

Andere Staaten äußerten Vorbehalte hinsichtlich der Strafbarkeit der 42
Beschaffung oder des Besitzes von Kinderpornografie unter besonderen
Bedingungen.

So erklärte Dänemark, dass es auf die Bestrafung des Besitzes von 43
pornografischen Bildern mit Kindern ab 15 Jahren verzichtet, wenn der
betreffende Minderjährige dem Besitz zugestimmt hat.

Zum Zeitpunkt der Ratifizierung des Übereinkommens stellte Montenegro 44
klar, dass die Beschaffung und der Besitz von Kinderpornografie nicht strafbar
sind, wenn die Person, die in diesem Material zu sehen ist, mindestens 14
Jahre alt ist und ihre Zustimmung gegeben hat. Seitdem wurde diese
Ausnahme abgeschafft.

C. Zu den Objekten der Darstellung

Das Übereinkommen erlaubt den Vertragsparteien schließlich, die 45
Strafverfolgung einzuschränken, indem sie es ablehnen, Bilder als
rechtswidrig zu betrachten, auf denen eine Person zu sehen ist, die als
Minderjähriger bei eindeutig sexuellen Handlungen auftritt, und/oder

realistische Bilder, auf denen ein Minderjähriger bei eindeutig sexuellen Handlungen dargestellt wird.

- 46 Das Fürstentum Andorra, Großbritannien, Argentinien, Chile, die Vereinigten Staaten von Amerika, Japan, Peru und Sri Lanka haben erklärt, dass sie die in Art. 9 § 2 lit. b und c CCC erwähnten Darstellungen nicht verfolgen werden. Zum Zeitpunkt der Ratifizierung des Übereinkommens hatte Island einen Vorbehalt in diesem Sinne eingelegt. Dieser Vorbehalt ist jedoch nicht mehr aktuell, da mit dem Gesetz vom 25. Juni 2012 ein neuer Art. 210a in das isländische Strafgesetzbuch eingeführt wurde, der auch die in Art. 9 § 2 Buchst. b und c CCC genannten Darstellungen unter Strafe stellt.
- 47 Dänemark, Ungarn, Montenegro, die Schweiz und Israel gaben an, dass sie darauf verzichten, visuelle Darstellungen einer Person zu bestrafen, die als Minderjährige erscheint, die sich sexuell eindeutig verhält (Art. 9 § 2 Buchst. b). Frankreich machte einen ähnlichen Vorbehalt und erklärte, dass es Bilder nicht verfolgen werde, auf denen eine Person abgebildet ist, die zum Zeitpunkt der Aufnahme volljährig ist, aber als Minderjähriger erscheint und sich sexuell eindeutig verhält.

V. VERGLEICH MIT DEM SCHWEIZER RECHT

- 48 Die Verhaltensweisen sowie die verschiedenen Darstellungen, die durch die Konvention unter Strafe gestellt werden, finden ihre Entsprechung im Schweizer Recht in Art. 197 Abs. 4 und 5 StGB. Das Schweizer Recht steht vollständig im Einklang mit Art. 9 CCC.

LITERATURVERZEICHNIS

Corboz Bernard, *Les infractions en droit suisse*, vol. I, 3^e éd., Berne 2010

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (éditeurs), *Schweizerisches Strafgesetzbuch, Praxiskommentar*, 4. éd., Zurich 2021

Isenring Bernhard/Kessler Martin A., in : Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), *Basler Kommentar, Strafrecht II*, 4. éd., Bâle 2018

MATERIALIENVERZEICHNIS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Conseil de l'Europe, Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote 25.10.2007, disponible à <https://rm.coe.int/16800d3832>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels)

KOMMENTIERUNG ZU

Art. 11 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Julian Mausbach

ZITIERVORSCHLAG

Julian Mausbach, Kommentierung zu Art. 11 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Mausbach, Art. 11 CCC N. XXX.

Titel 5: Weitere Formen der Verantwortlichkeit und Sanktionen

Art. 11 Versuch und Beihilfe oder Anstiftung

¹ Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um die vorsätzliche Beihilfe oder Anstiftung zur Begehung einer nach den Artikeln 2–10 umschriebenen Straftat mit dem Vorsatz, dass eine solche Straftat begangen werde, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

² Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um den Versuch der Begehung einer nach den Artikeln 3–5 sowie 7, 8 und 9 Absatz 1 Buchstaben a und c umschriebenen Straftat, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

³ Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 2 ganz oder teilweise nicht anzuwenden.

GLIEDERUNG

I. Anwendungsbereich.....	144
II. Teilnahmestrafbarkeit (Art. 11 Abs. 1).....	144
III. Versuchsstrafbarkeit (Art. 11 Abs. 2 und Abs. 3)	145
Materialienverzeichnis.....	146

I. ANWENDUNGSBEREICH

- 1 Art. 11 bezweckt, eine **Versuchs- und Teilnahmestrafbarkeit** in Bezug auf die in der Konvention definierten Tatbestände grundsätzlich zu verankern. Dabei geht Abs. 1 davon aus, dass die vorsätzliche Teilnahme an einer vorsätzlichen Straftat gemäss Art. 2–10 sowohl im Sinne einer Beihilfe wie einer Anstiftung straf- und sanktionswürdig ist.
- 2 Bereits Abs. 2 begrenzt dies für die **Versuchsstrafbarkeit** auf die Art. 3–5 sowie 7, 8 und 9 Abs. 1 lit. a und c der Konvention. Diese Begrenzung der Versuchsstrafbarkeit auf die aufgezählten Delikte kann durch die Vertragsparteien so umgesetzt werden, dass eine Versuchsstrafbarkeit als Ganzes oder teilweise abbedungen wird (Abs. 3).
- 3 Die Schweiz hat von der Begrenzungsmöglichkeit des **Abs. 3 keinen Gebrach** gemacht und sieht daher über eine Anknüpfung an den Allgemeinen Teil des Strafgesetzbuches eine Versuchsstrafbarkeit vor.

II. TEILNAHMESTRAFBARKEIT (ART. 11 ABS. 1)

- 4 Art. 11 Abs. 1 sieht eine Teilnahmestrafbarkeit für die Art. 2–10 vor. Anders als im Allgemeinen Teil des Strafgesetzbuches (dort Art. 24 und 25 StGB) wird keine Unterscheidung zwischen Anstiftung und Beihilfe getroffen. Da die Umsetzung von Abs. 1 unmittelbar über die Bestimmungen des Allgemeinen Teils des Strafgesetzbuches erfolgte, wirkt die dort getroffene Ausgestaltung, etwa in Bezug auf die Versuchsstrafbarkeit (Art. 24 Abs. 2 StGB), auch im Anwendungsbereich der Konvention bzw. auf die entsprechende Umsetzung. Objektive Voraussetzungen, die über die Art. 24 und 25 StGB hinausgehen, sind nicht gegeben und daher ist auch hier die Umsetzung über diese Artikel kongruent.
- 5 Der in Abs. 2 vorgesehene doppelte **Teilnehmervorsatz** in Bezug auf Teilnahmehandlung und Haupttat wird durch die Regelungen des Allgemeinen Teils ebenfalls gefordert, so dass hier keine Ergänzungen erforderlich waren.
- 6 Hinzuweisen ist auf die Ergänzung der Strafnorm des Art. 143^{bis} StGB. Zu den Details darf auf die entsprechende Kommentierung zu Art. 6 verwiesen werden. Mit Bezug auf die Frage der Teilnahme und des Versuchs ist

hervorzuheben, dass auch nach der Ergänzung von Art. 143^{bis} StGB eine versuchte Gehilfenschaft wie die Beihilfe zu einer (noch) nicht versuchten Haupttat entsprechend strafflos bleiben.¹

III. VERSUCHSSTRAFBARKEIT (ART. 11 ABS. 2 UND ABS. 3)

In Abs. 2 wurde die Verpflichtung vorgesehen, eine Versuchsstrafbarkeit auf 7 die benannten Bestimmungen zu erstrecken. Hierbei werden weder objektive Kriterien genannt, noch wurde eine allgemeine Versuchsstrafbarkeit vorgesehen. Insbesondere letzteres ist auf den Umstand zurückzuführen, dass in den Rechtsordnungen einiger Vertragsparteien keine generelle, sondern eine abgestufte Versuchsstrafbarkeit vorgegeben wird. Die getroffene Regelung verspricht daher eine Umsetzungsoption, die ohne grosse Verwerfungen in den grundlegenden Rechtskonzepten der Vertragsstaaten vollzogen werden kann (und wurde).²

Die Umsetzung der Versuchsstrafbarkeit erfolgte über Art. 22 i.V.m. Art. 10 8 Abs. 2 und Abs. 3 StGB. Sie erstreckt sich damit auf **alle in Abs. 2 benannten Tatbestände**. Dies ergibt sich daraus, dass deren Umsetzung wiederum über Straftatbestände des Besonderen Teils des StGB erfolgt, die ihrerseits mindestens als Vergehen im Sinne des Art. 10 Abs. 2 StGB ausgestaltet sind.

Wenngleich Abs. 2 keine Verpflichtung enthält, die Versuchsstrafbarkeit auf in 9 Abs. 2 nicht benannte Bestimmungen zu erstrecken, führt wiederum die Umsetzung über Artikel des Strafgesetzbuches dazu, dass auch in Bezug auf Art. 2, Art. 9 als Ganzes wie Art. 10 CCC in der Schweiz eine Versuchsstrafbarkeit gegeben ist. Insbesondere unter Einbezug der Urkundendelikte (Art. 251 ff. StGB), der Delikte zum Schutz des Post- und Fernmeldegeheimnisses (Art. 321^{ter} StGB) sowie des Pornografieartikels (Art. 197 StGB), die wiederum ihrerseits mindestens als Vergehen ausgestaltet sind, erfolgte eine Umsetzung, die eine **Versuchsstrafbarkeit für die Art. 2–10** nach sich zieht. Es ergibt sich daher **keine Dissonanz** zu der im Schweizerischen Strafrecht grundsätzlich vorgesehen Versuchsstrafbarkeit für Vergehen und Verbrechen.

Abs. 3 sieht die Möglichkeit der Vertragsparteien vor, auf eine 10 Versuchsstrafbarkeit gänzlich oder in Teilen zu verzichten. Mittels dieser

1. Siehe hierzu auch BBl 2010 4708 f.

Regelung sollte allfälligen Umsetzungsschwierigkeiten der Vertragsparteien begegnet werden. Der so eingeräumte Umsetzungsspielraum sollte nach Möglichkeit eine Ratifizierung gestatten, die ohne grundlegende Veränderungen in der jeweiligen Rechtsordnung erfolgen kann.³ In der Schweiz ist und musste von dieser Möglichkeit, auch nicht in Bezug auf einzelne Tatbestände oder Teile hiervon, kein Gebrach gemacht worden. Das ist inhaltlich überzeugend, da damit kein Bruch mit dem Verständnis der Versuchsstrafbarkeit in der Schweiz einhergeht. Die Regelung des Abs. 3, welche letztlich wohl als Konzession an die Umsetzungspraktikabilität in Bezug auf die Rechtsordnungen der Vertragsparteien zu verstehen ist, ist daher in der Schweiz ohne Folge geblieben.

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 17.10.2023

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

2. Siehe hierzu Explanatory Report, Rz. 120.

3. Siehe hierzu Explanatory Report, Rz. 122.

KOMMENTIERUNG ZU

Art. 12 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Ugur Gürbüz

ZITIERVORSCHLAG

Ugur Gürbüz, Kommentierung zu Art. 12 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Gürbüz, Art. 12 CCC N. XXX.

Art. 12 Verantwortlichkeit juristischer Personen

¹Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um sicherzustellen, dass juristische Personen für eine nach diesem Übereinkommen umschriebene Straftat verantwortlich gemacht werden können, die zu ihren Gunsten von einer natürlichen Person begangen wird, die entweder allein oder als Teil eines Organs der juristischen Person handelt und die eine Führungsposition innerhalb der juristischen Person innehat aufgrund:

- a. einer Vertretungsmacht für die juristische Person;
- b. einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen;
- c. einer Kontrollbefugnis innerhalb der juristischen Person.

² Neben den in Absatz 1 bereits vorgesehenen Fällen trifft jede Vertragspartei die erforderlichen Massnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch eine in Absatz 1 genannte natürliche Person die Begehung einer nach diesem Übereinkommen umschriebenen Straftat zugunsten der juristischen Person durch eine ihr unterstellte natürliche Person ermöglicht hat.

³ Vorbehaltlich der Rechtsgrundsätze der Vertragspartei kann die Verantwortlichkeit einer juristischen Person straf-, zivil- oder verwaltungsrechtlicher Art sein.

⁴ Diese Verantwortlichkeit berührt nicht die strafrechtliche Verantwortlichkeit der natürlichen Personen, welche die Straftat begangen haben.

GLIEDERUNG

I. Einleitung	150
II. Anwendungsbereich und Ziele	151
A. Absatz 1: Bei Handlungen von Personen mit Führungsposition	151
B. Absatz 2: Verletzung der Aufsichtspflicht	153
C. Absatz 3: Art der Verantwortlichkeit	154
D. Absatz 4: Individuelle Haftung	154
III. Vergleichbare strafrechtliche Normen in der Schweiz	154
A. Strafrechtliche Sanktionen und Massnahmen gemäss StGB	154
B. Art. 102 Abs. 1 StGB: Subsidiäre Haftung	155
C. Art. 102 Abs. 2 StGB: Primäre Haftung	157
D. Bestimmungen im Verwaltungsstrafrecht	158
1. Art. 6 VStrR: Geschäftsherrenhaftung	158
2. Art. 7 VStrR: Unternehmenshaftung	159
IV. Umsetzung des strafrechtlichen Aspekts in der Schweiz	159
V. Vergleichbare zivil- und verwaltungsrechtliche Normen in der Schweiz	161
VI. Umsetzung des zivil- und verwaltungsrechtlichen Aspekts in der Schweiz	162
Literaturverzeichnis	162
Materialienverzeichnis	163

I. EINLEITUNG

- 1 Der aus dem römischen Recht stammende Grundsatz «**societas delinquere non potest**» galt in Kontinentaleuropa über Jahrzehnte hinweg als unveränderliche Regel, um das Strafrecht auf das Individuum zu fokussieren und Unternehmen von strafrechtlicher Verantwortlichkeit freizustellen. Diese Vorstellung einer Rechtsordnung ohne unmittelbare Unternehmensstrafbarkeit wurde überholt, als die Wirtschaft vermehrt von komplexeren Betriebsstrukturen und globalen Arbeitsteilungen geprägt wurde und dadurch die Möglichkeiten von Missbrauch sowie die Gefahr und Schädlichkeit von allfälligen Fehlverhalten von Unternehmen grösser wurden. In Europa implementierten im Jahr 1976 die Niederlanden,⁴ im Jahr 1994 Frankreich⁵ und im Jahr 1996 Dänemark⁶ die Strafbarkeit von Unternehmen in ihren Strafgesetzbüchern. In der Schweiz besteht seit dem 1.10.2003 ein im Strafgesetzbuch geregeltes Unternehmensstrafrecht, dennoch gilt die Schweiz im internationalen Vergleich als eine der Vorreiterstaaten bei der Einführung der Strafbarkeit von juristischen Personen. Bereits vor der Einführung im Strafgesetzbuch konnten ab dem Jahr 1974 bei Widerhandlungen in Geschäftsbetrieben gemäss Art. 26 UWG (Bundesgesetz gegen unlauteren Wettbewerb) die Artikel 6 und 7 des Verwaltungsstrafrechtsgesetzes (VStrR) herangezogen werden. Diese Bestimmungen galten allerdings als Ausnahmen zum damals allgemein anerkannten Grundsatz, wonach juristische Personen nicht deliktfähig sind, und wurden nicht dem Strafrecht zugerechnet.⁷
- 2 Im Rahmen der mit der Einführung der Cybercrime-Konvention des Europarates beabsichtigten Effektivierung der Strafverfolgung⁸ wurden – dem **europäischen Trend folgend** – den Vertragsparteien in Art. 12 CCC wie schon in den weitgehend gleichlautenden strafrechtlichen Bestimmungen des Strafrechtsübereinkommens über Korruption⁹ identische Regelungen der

4. Art. 51 des niederländischen Strafgesetzbuches, abrufbar unter <https://wetten.overheid.nl/BWBR0001854>, besucht am 30.4.2024.

5. Art. 121 des französischen Strafgesetzbuches, abrufbar unter https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006149817, besucht am 30.4.2024.

6. § 25 ff. des dänischen Strafgesetzbuches, abrufbar unter <https://www.retsinformation.dk/eli/ta/2022/1360>, besucht am 30.4.2024.

7. Riklin, § 12 N. 14 ff.

8. Präambel des Übereinkommens über die Cyberkriminalität.

Verantwortlichkeit juristischer Personen vorgegeben, nämlich für Zuwiderhandlungen ihrer Organe und sonstigen Mitarbeiter eine Verantwortlichkeit vorzusehen. Die Vertragsstaaten wurden auch mit Art. 12 CCC verpflichtet, sicherzustellen, dass juristischen Personen angemessene Sanktionen oder Massnahmen, darunter Geldsanktionen, aufzuerlegen sind. Der Grundsatz, wonach sich Unternehmen nicht strafbar machen können, wurde auch durch die Cybercrime-Konvention weiterhin geschützt.¹⁰

II. ANWENDUNGSBEREICH UND ZIELE

Die **Verantwortlichkeit von juristischen Personen** gemäss Artikel 12 zielt 3 zum einen darauf ab, Unternehmen für strafbare Handlungen von Personen in leitender Stellung haftbar zu machen, sofern diese Handlungen zum Nutzen der juristischen Person vorgenommen werden (Absatz 1). Zum anderen sieht die Bestimmung eine Verantwortlichkeit für Personen in leitender Stellung vor, welche das Beaufsichtigen oder Kontrollieren von Angestellten oder Beauftragten versäumt haben und dieses Versäumnis eine nach der Konvention umschriebene Straftat durch Angestellte oder Beauftragte erleichtert (Absatz 2). Die Konvention überlässt den Vertragsparteien die Wahl, ob sie die Verantwortlichkeit der juristischen Person zivil-, verwaltungs- oder strafrechtlicher Natur regeln wollen (Absatz 3). Weiter hält es fest, dass die Verantwortlichkeit einer juristischen Person der allfälligen Strafbarkeit einer natürlichen Person, welche die Straftat begangen hat, nicht entgegenstehen soll (Absatz 4).

A. Absatz 1: Bei Handlungen von Personen mit Führungsposition

Art. 12 Abs. 1 CCC verpflichtet die Vertragsparteien, die Verantwortlichkeit 4 der juristischen Person für Straftaten zu begründen, die von Personen mit einer Führungsposition innerhalb des Unternehmens begangen werden oder als Anstifter oder Gehilfen daran teilnehmen. Die Bestimmung statuiert eine **Kausalhaftung** und umfasst **vier Tatbestandsmerkmale**¹¹:

a) Die Konvention verlangt eine **Zuwiderhandlung gegen die in den 5 Artikeln 2-10 der Konvention formulierten Strafnormen**, namentlich der

9. Art. 18 und Art. 19 Ziff. 2 des Strafrechtsübereinkommens über Korruption, SR 0.311.43.

10. Vgl. Ziff. 2.2.11 des Vernehmlassungsentwurfs; vgl. Art. 13 CCC.

11. Explanatory Report, Rz. 124.

rechtswidrige Zugang (Art. 2), das rechtswidrige Abfangen (Art. 3), der Eingriff in Daten (Art. 4), der Eingriff in ein System (Art. 5), der Missbrauch von Vorrichtungen (Art. 6), die computerbezogene Fälschung (Art. 7), der computerbezogene Betrug (Art. 8), Straftaten mit Bezug zu Kinderpornographie (Art. 9) sowie die Verletzung des Urheberrechts und verwandter Schutzrechte (Art. 10).

- 6 b) Die strafrechtliche Haftung gemäss Konventionstext beschränkt sich auf Straftaten, die **zu Gunsten der juristischen Person begangen** werden. Mit dem Kriterium «*zu Gunsten der juristischen Person*» wird eine Verknüpfung zwischen der Straftat und der juristischen Person vorgenommen.¹² Der Anwendungsbereich ist auf Straftaten begrenzt, die zum Vorteil einer juristischen Person begangen werden. Dieser Vorteil kann finanziell oder anderweitig sein. Unmittelbar finanzielle Vorteile sind u.a. Erträge, die aus Straftaten erlangt werden und sich die juristische Person entweder bereichert oder einen Aufwand erspart. Ein Vorteil anderer Art liegt vor, wenn der Nutzen der juristischen Person nicht (primär) finanziell ist, beispielsweise wenn infolge von Bestechungen Aufträge bei der juristischen Person eingehen. Eine Legaldefinition für den Begriff der juristischen Person enthält die Konvention keine. Herangezogen wurden bei der Festlegung von Artikel 12 die historische und europäische Interpretation des Begriffs der „juristischen Person“, wonach jedes Rechtssubjekt darunterfällt, das den Status der juristischen Person nach dem anwendbaren Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung hoheitlicher Rechte und von öffentlich-rechtlichen internationalen Organisationen.¹³
- 7 c) Den privatrechtlichen Grundsätzen entsprechend, dass juristische Personen nur durch ihre Organe handeln können, die Handlungen der Organe unmittelbar Handlungen der juristischen Person sind und die juristische Person für die Handlungen der Organe gegenüber geschädigten Dritten haftet, setzt die Konvention die **Begehung der Straftat durch eine natürliche**

12. Erläuternder Bericht zum Zweiten Protokoll zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften, Ziff. 3.2.

13. Vgl. Art. 2 lit. c) der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013L0040>, besucht am 30.4.2024.

Person voraus, die eine **Führungsposition** innerhalb der juristischen Person innehat. Darunter fallen gemäss Aufzählung in den lit. a bis c jene natürlichen Personen, die ihre Führungs- und Leitungsfunktion aus einer Vertretungs-, Entscheidungs- oder Kontrollbefugnis ableiten. Der Konventionstext verlangt somit die Ausgestaltung der Verantwortlichkeit juristischer Personen als Sonderdelikt, ohne dabei eine formelle Organfunktion beim Täter vorauszusetzen.¹⁴

d) Von den Vertragsstaaten verlangt die Konvention des Weiteren, dass die natürliche Person im Rahmen der ihr zustehenden Befugnis in **Ausübung einer geschäftlich befugten Verrichtung** agiert, d.h. im Rahmen der ihr bei der juristischen Person zustehenden Vertretungs-, Entscheidungs- oder Kontrollbefugnis handelt, um die Verantwortlichkeit der juristischen Person gemäss Art. 12 Abs. 1 CCC auszulösen.¹⁵

B. Absatz 2: Verletzung der Aufsichtspflicht

Art. 12 Abs. 2 CCC verpflichtet die Vertragsstaaten, Unternehmen zur Verantwortung zu ziehen,

a) wenn die in Abs. 1 lit. a bis c genannten natürlichen Personen **durch mangelnde Überwachung und Kontrolle ihre Aufsichtspflicht** über unterstellte Mitarbeiter **verletzen**,

b) die dann als kausale Folge dieser Verletzung im Sinne von **Art. 2-10 CCC** eine Straftat

c) zum **Vorteil der juristischen Person** begehen.

Der Absatz 2 erweitert somit die Verantwortlichkeit der juristischen Person auf Handlungen von Personen, die eine Straftat als Mitarbeiter **ohne Führungsposition** der juristischen Person begehen und die Straftat dadurch ermöglicht wurde, dass die leitende Person den untergestellten Mitarbeiter nicht ausreichend beaufsichtigt hat.

Von einer **unterlassenen Beaufsichtigung** ist dann auszugehen, wenn versäumt wurde, geeignete und angemessene Massnahmen zur Hinderung

14. Explanatory Report, Rz. 124.

15. Explanatory Report, Rz. 124.

krimineller Handlungen zu Gunsten der juristischen Person durch Angestellte oder Beauftragte zu ergreifen.¹⁶ Dabei sind die Art und Intensität der Aufsichtspflicht von der Unternehmensform, seiner Grösse, den Sicherheitsstandards sowie den Geschäftspraktiken abhängig. Aus der Aufsichtspflicht ist keine generelle Überwachungspflicht zu begründen.

C. Absatz 3: Art der Verantwortlichkeit

- 12 Art. 12 Abs. 3 CCC wurde in die Konvention aufgenommen, um die nationalen Rechtsgrundsätze der Vertragsstaaten so weit wie möglich zu berücksichtigen. Gemäss dieser Konventionsbestimmung kann die **Verantwortlichkeit der juristischen Personen straf-, zivil- oder verwaltungsrechtlich** sein. Die Vertragsstaaten haben bei entsprechender Regelung sicherzustellen, dass ihre strafrechtlichen oder nichtstrafrechtlichen Sanktionen oder Massnahmen gegen juristische Personen die Kriterien von Art. 13 Abs. 2 CCC erfüllen, wonach sie wirksam, verhältnismässig und abschreckend sein und Geldsanktionen umfassen müssen.¹⁷

D. Absatz 4: Individuelle Haftung

- 13 Art. 12 Abs. 4 CCC stellt klar, dass die Haftung von juristischen Personen die **individuelle Haftung einer natürlichen Person nicht ausschliesst**. Die Vertragsstaaten werden mit dieser Regelung nicht dazu verpflichtet, eine parallele strafrechtliche Haftung einzuführen.¹⁸

III. VERGLEICHBARE STRAFRECHTLICHE NORMEN IN DER SCHWEIZ

A. Strafrechtliche Sanktionen und Massnahmen gemäss StGB

- 14 Die strafrechtliche Unternehmenshaftung wurde am 1.10.2003 in das Schweizerische Strafgesetzbuch eingefügt. Motive hierfür waren die Angst vor der organisierten Kriminalität, die Furcht vor menschengeschaffenen Grossgefahren sowie die Unterzeichnung des «Übereinkommens über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen

16. Explanatory Report, Rz. 125.

17. Explanatory Report, Rz. 126.

18. BBl 2010 4697 (zu Art. 12 CCC).

Geschäftsverkehr».¹⁹ Mit der Ratifizierung dieser **OECD-Konvention** verpflichtete sich die Schweiz nach Art. 2, in Übereinstimmung mit ihren Rechtsgrundsätzen, die erforderlichen Massnahmen zu treffen, um die Verantwortlichkeit juristischer Personen für die Bestechung eines ausländischen Amtsträgers zu begründen.

B. Art. 102 Abs. 1 StGB: Subsidiäre Haftung

Gemäss Art. 102 Abs. 1 StGB werden Verbrechen oder Vergehen – nicht aber 15
Übertretungen²⁰ – einem Unternehmen dann zugerechnet, wenn im
«Unternehmen in Ausübung geschäftlicher Verrichtung im Rahmen des
Unternehmenszwecks ein Verbrechen oder Vergehen begangen» wird und
«diese Tat wegen mangelhafter Organisation des Unternehmens keiner
bestimmten natürlichen Person zugerechnet werden» kann. Das Unternehmen
macht sich demzufolge bei **mangelhafter Organisation** subsidiär strafbar.

Der sich gegen das Unternehmen richtende Vorwurf besteht darin, dass 16

a) ein **Verbrechen oder Vergehen** gemäss schweizerischer Rechtsordnung
im Sinne von Art. 10 StGB **als Anlasstat** begangen wurde

b) die Anlasstat **in einem Unternehmen** begangen wurde und der Anlasstäter
hierarchisch oder organisatorisch in das Unternehmen eingebunden sein
muss,²¹

c) die Anlasstat «**in Ausübung geschäftlicher Verrichtung**» begangen
wurde, wodurch ein funktionaler Zusammenhang zwischen der Anlasstat und
der geschäftlichen Betätigung verlangt wird, d.h. eine minimale
wirtschaftliche Tätigkeit, die mit den Aktivitäten des Unternehmens in Bezug
steht²² und somit das in Art. 12 CCC vorausgesetzte Handeln mit Vertretungs-,
Entscheidungs- oder Kontrollbefugnis miteinschliesst,

d) die Anlasstat **im Rahmen des Unternehmenszwecks** begangen wurde,
womit gemäss h.M. eine Einschränkung auf betriebstypische Gefahren
begründet wird,²³

19. Vgl. BSK-Niggli/Gfeller, Art. 102 StGB N. 13 f.

20. Vgl. BGer 6B_256/2007 vom 15.10.2007 E. 2.2.

21. Vgl. BGer 6B_442/2013 vom 26.8.2013 E. 4.

22. Vgl. Ackermann, Niggli/Maeder, § 8 N. 65 ff.

e) und das Unternehmen die Verantwortung dafür trägt, dass die Strafverfolgungsbehörden wegen mangelhafter Organisation **keine verantwortliche natürliche Person** ausfindig machen können.

17 Solange die Verantwortlichkeit von juristischen Personen

- einerseits gemäss Art. 12 Abs. 1 der Konvention darauf abzielt, Unternehmen für strafbare Handlungen von Personen in leitender Stellung haftbar zu machen, sofern diese Handlungen zum Nutzen der juristischen Person vorgenommen werden,
- und andererseits gemäss Art. 12 Abs. 2 CCC darauf, dass Personen in leitender Stellung, welche das Beaufsichtigen oder Kontrollieren von Angestellten oder Beauftragten versäumt haben und dieses Versäumnis eine nach der Konvention umschriebenen Straftaten durch Angestellte oder Beauftragte erleichtert,

finden beide Tatvarianten eine weitgehende Entsprechung in der strafrechtlich subsidiären Unternehmenshaftung gemäss Art. 102 Abs. 1 StGB. Die Bestimmung **deckt alle Delikte gemäss Cyberkonvention ab**, ohne diese explizit aufzuzählen.

18 Die Konvention beschränkt sich auf Straftaten gemäss Art. 2-10 CCC, die zum Vorteil der juristischen Person und durch deren Vertreter begangen werden. Die Haftung gemäss StGB hingegen greift bei jedem Verbrechen oder Vergehen, die im Rahmen des Unternehmungszwecks durch eine Person in Ausübung einer geschäftlichen Verrichtung begangen werden.²⁴ Im Vergleich zum Konventionstext reicht die Haftung gemäss StGB somit weiter, weil die StGB **keine zu Gunsten der juristischen Person begangene Straftat als Kriterium** für die Unternehmenshaftung voraussetzt.

19 Art. 102 Abs. 1 StGB, wonach die Bestrafung der juristischen Person nur dann möglich ist, wenn die Handlung keiner natürlichen Person zugerechnet werden kann, und Art. 12 Abs. 4 CCC, wonach die Strafbarkeit der juristischen Person nicht die Verantwortlichkeit des Täters berühren soll, stehen nicht im Widerspruch zueinander, weil eine **strafrechtliche Haftung der handelnden natürlichen Personen durch die subsidiäre**

23. Vgl. Ackermann, Niggli/Maeder, § 8 N. 70.

24. Vgl. Ziff. 2.2.11 des Vernehmlassungsentwurfs.

Unternehmenshaftung nicht ausgeschlossen ist.²⁵ In der Schweiz ist sogar eine Bestrafung der natürlichen als auch der juristischen Person möglich, wenn die mangelhafte Organisation des Unternehmens von einer natürlichen Person verschuldet ist und diese Person erst nach der Verurteilung des Unternehmens ermittelt werden kann.²⁶

Als Strafe sieht Art. 102 Abs. 1 StGB eine **Busse bis zu fünf Millionen Franken** vor, was dem Konventionstext von Art. 13 Abs. 2 entspricht, wonach Vertragsstaaten Geldsanktionen auferlegen müssen. 20

C. Art. 102 Abs. 2 StGB: Primäre Haftung

Unabhängig von der Strafbarkeit natürlicher Personen wird seit dem 1.10.2003 21 ein **Unternehmen primär zu Verantwortung** gezogen, wenn es sich um eine Straftat nach den Artikeln 260^{ter} StGB (Kriminelle Organisation), 260^{quinqies} StGB (Finanzierung des Terrorismus), 305^{bis} StGB (Geldwäscherei), 322^{ter} StGB (Bestechung schweizerischer Amtsträger), 322^{quinqies} StGB (Vorteilsgewährung), 322^{septies} Absatz 1 StGB (Bestechung fremder Amtsträger) oder 322^{octies} StGB (Bestechen) handelt und das Unternehmen nicht alle erforderlichen und zumutbaren organisatorischen Vorkehrungen getroffen hat, um eine solche Straftat zu verhindern. Die **Pflichtverletzung** liegt in der Missachtung von Organisationspflichten, welche die abschliessend aufgezählten Anlasstaten begünstigen.²⁷ Die Bestrafung erfolgt gemäss Art. 102 Abs. 2 StGB neben einer eventuellen Bestrafung einer natürlichen Person.²⁸

Keiner der Delikte gemäss Art. 2-10 CCC ist im Deliktskatalog von Art. 102 22 Abs. 2 StGB enthalten, weswegen die Verantwortlichkeit juristischer Personen gemäss Art. 12 CCC in Bezug zur primären strafrechtlichen Unternehmenshaftung bedeutungslos bleibt. Daraus folgt, dass den bestehenden gesetzlichen Bestimmungen entsprechend in Zusammenhang mit den in den Art. 2-10 CCC formulierten Strafnormen in der Schweiz **keine direkte Zurechnung fremden Verschuldens an ein Unternehmen möglich ist**.

25. BBl 2010 4715.

26. Vgl. BSK-Niggli/Gfeller, Art. 102 StGB N. 119.

27. Vgl. StGB/JStG Kommentar, Art. 102 StGB N. 14.

28. BGE 142 IV 333 E. 3.1.

D. Bestimmungen im Verwaltungsstrafrecht

- 23 Vor Einführung der strafrechtlichen Unternehmenshaftung und der Zurechnungsregelung (Art. 29 StGB) im Kernstrafrecht und auch vor Ratifizierung der Cybercrime-Konvention wurden in der Schweiz natürliche und juristische Personen für Widerhandlungen in Geschäftsbetrieben mit dem Bundesgesetz über das Verwaltungsstrafrecht in die Pflicht genommen. Entsprechende Bestimmungen im Verwaltungsstrafrecht **gelten weiterhin**: Art. 6 VStrR ahndet natürliche Personen, die zum Geschäftsbetrieb in einer besonderen Beziehung stehen. Art. 7 VStrR befasst sich mit der Strafbarkeit von juristischen Personen. Überschneidungen bezüglich der Bestimmungen im StGB und im VStrR sind möglich. Anwendbar sind Art. 6 und 7 VStrR solange Gesetze entweder explizit auf einer der Bestimmungen oder auf das Verwaltungsstrafrecht insgesamt verweisen.

1. Art. 6 VStrR: Geschäftsherrenhaftung

- 24 Gegenstand der strafrechtlichen Verantwortlichkeit gemäss Art. 6 VStrR ist stets eine **individuelle Person**. Werden beim Besorgen von Angelegenheiten einer juristischen Person, Kollektiv- oder Kommanditgesellschaft, Einzelfirma oder Personengesamtheit ohne Rechtspersönlichkeit oder sonst in Ausübung geschäftlicher oder dienstlicher Verrichtungen Widerhandlungen begangen, so ist gemäss Absatz 1 die Strafbestimmung auf diejenigen natürliche Person anwendbar, welche die Tat verübt hat. Absatz 2 und 3 konkretisieren, dass der Geschäftsherr, Arbeit- und Auftraggeber, Vertretene oder sogar das Organ und Organmitglied, der geschäftsführende Gesellschafter, Liquidator und die tatsächlich leitende Person zur Verantwortung zu ziehen sind, solange sie vorsätzlich oder fahrlässig es in Verletzung einer Rechtspflicht unterlassen haben, eine Widerhandlung des Untergebenen, Beauftragten oder Vertreters abzuwenden oder in ihren Wirkungen aufzuheben. Artikel 6 ist ein Unterlassungsdelikt in Verletzung einer Rechtspflicht. Die sich aus Artikel 6 ergebende verwaltungsstrafrechtliche Verantwortung des Geschäftsherrn schränkt den Anwendungsbereich der subsidiären Strafbarkeit der Unternehmung gemäss Art. 102 Abs. 1 StGB erheblich ein und führt zur Entlastung des Unternehmens, weil sie die Zurechnung zu einer natürlichen Person ermöglicht.²⁹

29. BSK-Schwob, Art. 6 VStrR N. 2 ff.

2. Art. 7 VStrR: Unternehmenshaftung

Eine subsidiäre Strafbarkeit der juristischen Person im Verwaltungsstrafrecht 25 sieht Art. 7 VStrR vor. Die Bestimmung zielt darauf ab, dem gemässigten Opportunitätsprinzip entsprechend den Ermittlungsaufwand der Strafverfolgungsbehörden **bei geringfügigen Delikten** zu vermindern. Gleichzeitig widerspricht sie dem Prinzip der Ermittlung der materiellen Wahrheit und dem Legalitätsprinzip. So kann nach Art. 7 VStrR von der Verfolgung einer natürlichen Personen Umgang genommen und an ihrer Stelle die juristische Person, die Kollektiv- oder Kommanditgesellschaft oder die Einzelfirma zur Bezahlung einer Busse verurteilt werden, wenn folgende Voraussetzungen gegeben sind:

- a) Die Widerhandlung erfolgt im Geschäftsbetrieb
- b) es kommt eine Busse von maximal CHF 5'000.00 in Frage und
- c) die Ermittlung des Einzeltäters würde einen unverhältnismässigen Untersuchungsaufwand nach sich ziehen.

Wird eine natürliche Person als Täter ermittelt, so ist die Anwendung von Art. 7 VStrR ausgeschlossen.³⁰ Die Bestimmung ersetzt im Verwaltungsstrafrecht auch nicht Art. 102 Abs. 1 StGB. Wegen ihres unterschiedlichen Regelungsgehalts können beide Normen angewendet werden.

IV. UMSETZUNG DES STRAFRECHTLICHEN ASPEKTS IN DER SCHWEIZ

Aufgrund der **weitgehenden Abdeckung des Konventionsinhalts** durch 26 Art. 102 Abs. 1 StGB hat der Gesetzgeber von einer primären strafrechtlichen Unternehmenshaftung in Zusammenhang mit Art. 12 CCC und einer damit verbundenen Ausweitung des Anwendungsbereichs zurecht abgesehen.³¹ Zwar verankert die Konvention eine parallele Verantwortung des Unternehmens, welche in der Schweiz auf strafrechtlicher Ebene nur durch die primäre strafrechtliche Unternehmenshaftung gemäss Art. 102 Abs. 2 StGB

30. Vgl. Ackermann, Niggli/Maeder, § 8 N. 16 f.

31. Vgl. BBl 2010 4716 (zu Art. 12 CCC).

sichergestellt werden kann, doch verlangt sie von den Vertragsstaaten keine Regelung einer strafrechtlichen Verantwortlichkeit von Unternehmen. Artikel 12 der Konvention erfordert nicht die Schaffung einer Strafnorm im engeren Sinne, vielmehr überlässt sie in Abs. 3 den Vertragsstaaten, die Verantwortlichkeit der juristischen Person auch alternativ zivil- oder verwaltungsrechtlich zu regeln. Nachdem die subsidiäre Haftung nach Art. 102 Abs. 1 StGB alle Straftaten gemäss Artikel 2-10 CCC abdeckt, zumal sie sicherstellt, dass zugunsten einer Unternehmung begangene Verbrechen und Vergehen nicht unbestraft bleiben, ging der Gesetzgeber korrekterweise davon aus,³² dass eine umfassendere Primärhaftung über das mindesterforderliche Mass in der Konvention hinausgehen würde.³³ Aufgrund von Art. 2 VStrR, wonach die Regelung des Unternehmensstrafrechts des StGB auch auf das Verwaltungsstrafrecht Anwendung findet, soweit das VStrR selber oder das einzelne Verwaltungsgesetz nichts anderes bestimmt aber auch aufgrund von Art. 7 VStrR, wonach Personalverbänden anstelle von schwer ermittelbaren Individualtättern bestraft werden können, ist die Verantwortlichkeit von juristischen Personen auch bei Straftaten wegen Widerhandlungen gegen Bundesgesetze wie beispielsweise gegen das Urheberrechtsgesetz sichergestellt.

- 27 **Abweichend** vom Wortlaut und Zweck von Art. 12 Abs. 1 CCC hat der schweizerische Gesetzgeber Art. 102 StGB nicht als eine Kausalhaftung ausgestattet.³⁴ Während nach Art. 12 Abs. 1 CCC eine juristische Person unabhängig von einem Verschulden das Risiko für die Haftung bei einer Deliktsausübung im Unternehmen tragen soll, setzt Art. 102 StGB für die strafrechtliche Verantwortlichkeit der juristischen Person ein Organisationsverschulden voraus. Trotz dieses Unterschiedes kommt die Schweiz den Anforderungen von Art. 12 CCC dennoch nach, weil eine «Verantwortlichkeit» im Sinne der Konvention nicht zwingend eine Strafbarkeit der juristischen Person bedeutet (vgl. Art. 12 Abs. 3 CCC).

32. Vgl. BBl 2010 4716.

33. Eine andere Meinung hat Jean-Richard-dit-Bressel, S. 575 f.

34. Vgl. BGE 142 IV 333.

V. VERGLEICHBARE ZIVIL- UND VERWALTUNGSRECHTLICHE NORMEN IN DER SCHWEIZ

Die Schweizer Rechtsordnung kennt in zivil- und verwaltungsrechtlicher Hinsicht verschiedene Instrumente der Schadenshaftung sowie Verhütung zukünftiger Schädigungen. Nebst den **haftungsrechtlichen Regelungen und organisatorischen Massnahmen** im Zivilrecht ist auch auf die **Aufsichtsinstrumente** von Behörden hinzuweisen. 28

Im Einzelnen handelt es sich bei diesen Instrumenten unter anderem um die Folgenden (nicht abschliessend): 29

- Auflösung des Vereins durch das Gericht gemäss Art. 78 ZGB, wenn der Zweck des Vereins widerrechtlich oder unsittlich ist;
- Aufhebung der Stiftung durch die zuständige Bundes- oder Kantonsbehörde gemäss Art. 88 ZGB, deren Zweck widerrechtlich oder unsittlich geworden ist;
- Haftung der Gesellschaft aus Geschäftsherrenhaftung gemäss Art. 55 OR;
- Haftung der Gesellschaft für Hilfspersonen gemäss Art. 101 OR;
- Haftung der Gesellschaft für den Schaden aus unerlaubter Handlung, den ein Gesellschafter oder eine Gesellschafterin in Ausübung der geschäftlichen Verrichtung begangen hat gemäss Art. 567 Abs. 3 OR;
- Haftung der Gesellschaft für Schaden aus unerlaubten Handlungen, die ein Liquidator oder eine Liquidatorin in Ausübung der geschäftlichen Verrichtungen begeht gemäss Art. 586 OR und Art. 743 OR;
- Haftung der Gesellschaft für Schaden aus unerlaubten Handlungen, die eine zur Geschäftsführung oder zur Vertretung befugte Person in Ausübung ihrer geschäftlichen Verrichtungen begeht gemäss Art. 722 OR und Art. 817 OR;
- Auflösung der Gesellschaft bei bestehenden Mängeln in der Organisation gemäss Art. 731b OR;
- Haftung der Genossenschaft für Schaden aus unerlaubten Handlungen, die eine zur Geschäftsführung oder zur Vertretung befugte Person in Ausübung ihrer geschäftlichen Verrichtungen begeht gemäss Art. 899 OR;

- Verwaltungsrechtliche Sanktionen der Eidgenössische Finanzmarktaufsicht gemäss Finanzmarktaufsichtsgesetz.

VI. UMSETZUNG DES ZIVIL- UND VERWALTUNGSRECHTLICHEN ASPEKTS IN DER SCHWEIZ

- 30 Das schweizerische Zivil- und Verwaltungsrecht sieht eine **Vielzahl von Sanktionen und Massnahmen** gegen Gesellschaften bei unerlaubten Handlungen in Ausübung einer geschäftlichen Verrichtung vor. Solange Gesellschaften zum Betrieb eines Gewerbes und nicht ausschliesslich zur Begehung von Straftaten geführt werden, reichen die zivil- und verwaltungsrechtlichen Sanktionen und Massnahmen grundsätzlich aus, um die in Art. 13 Abs. 2 CCC geforderte wirksame und abschreckende Sanktionierung sicherzustellen.

LITERATURVERZEICHNIS

Ackermann Jürg-Beat, Wirtschaftsstrafrecht der Schweiz, 2. Aufl., Bern 2021 (zit. Ackermann, Bearbeiter/in, § ... N ...).

Donatsch Andreas/Heimgartner Stefan/Isenring Bernhard/Maurer Hans/Riesen-Kupper Marcel/Weder Ulrich (Hrsg.), StGB/JStG Kommentar, Mit weiteren Erlassen und Kommentaren zu den Strafbestimmungen des SVG, BetmG, AIG und OBG, 21. Aufl., Zürich 2022 (zit. StGB/JStG Kommentar, Art. ... StGB N ...).

Forster Matthias, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB, Bern 2006.

Frank Friedrich/Eicker Andreas/Markwalder Nora/Achermann Jonas (Hrsg.), Basler Kommentar zum Verwaltungsstrafrecht, 1. Aufl., Basel 2020 (zit. BSK-Bearbeiter/in, Art. ... VStrR N ...).

Heine Günter, Europäische Entwicklung bei der strafrechtlichen Verantwortlichkeit von Wirtschaftsunternehmen und deren Führungskräften, ZStrR 119 (2001), S. 22 ff.

Jean-Richard-dit-Bressel Marc, Das Desorganisationsdelikt in Finanzdienstleistungsunternehmen, SZW 2022, S. 572-585.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar zum Strafrecht I, Art. 1-136 StGB, 4. Aufl., Basel 2019 (zit. BSK-Bearbeiter/in, Art. ... StGB N ...).

Riklin Franz, Schweizerisches Strafrecht – Allgemeiner Teil I – Verbrechenslehre, 3. Aufl., Zürich/Basel/Genf 2007.

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 30.4.2024.

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21.9.1998, BBl 1999 II 1979 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_1979_1787_1669/de, besucht am 30.4.2024.

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 30.4.2024.

Dänischen Strafgesetzbuch, abrufbar unter <https://www.retsinformation.dk/eli/lta/2022/1360>, besucht am 30.4.2024.

Erläuternder Bericht zu dem Zweiten Protokoll zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften (vom Rat angenommen am 12.3.1999), abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A51999XG0331>, besucht am 30.4.2024.

Französisches Strafgesetzbuch, abrufbar unter https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2024-01-19, besucht am 30.4.2024.

Niederländischen Strafgesetzbuch, abrufbar unter <https://wetten.overheid.nl/BWBR0001854>, besucht am 30.4.2024.

Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013L0040>, besucht am 30.4.2024.

KOMMENTIERUNG ZU

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

Eine Kommentierung von Ugur Gürbüz

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	168
II. Anwendungsbereich und Ziele	168
A. Absatz 1: Umgehende Sicherung von Computerdaten	169
B. Absatz 2: Sicherung von Daten mittels Anordnung auf Aufbewahrung	171
C. Absatz 3: Geheimhaltungspflicht.....	171
D. Absatz 4	172
III. Umsetzung in der Schweiz	172
A. Sicherung durch Strafverfolgungsbehörden	173
B. Sicherungsaufforderung an Personen	174
C. Fehlende Gesetzesbestimmung betreffend Anordnung auf Aufbewahrung.....	175
D. Durch das Bundesgericht ausgebremsste Sicherung bei gültigem Siegelungsantrag	176
Literaturverzeichnis	178
Materialienverzeichnis.....	178

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.

Art. 16 CCC regelt die **unverzügliche Sicherung von Daten**, berechtigt aber 4 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

Art. 16 Abs. 1 CCC gewährleistet die rasche Sicherung von Computerdaten 5 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*»³⁵ 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 davon weiterhin nutzen können,³⁶ solange sie nicht sinngemäss Art. 19 CCC beschlagnahmt werden müssen.

Art. 16 CCC verpflichtet die Vertragsstaaten weder dazu, das Angebot oder die 6 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.³⁷

Die konkrete **Ausgestaltung** der Sicherungen wird den Vertragsparteien 7 überlassen. In der Praxis kommen als Sicherungsmethoden zwei Optionen in

35. Explanatory Report, Rz. 159.

36. Explanatory Report, Rz. 159.

37. Explanatory Report, Rz. 157.

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 wurden³⁸ und gespeichert sind, sogenannte **«stored computer data»**. Explizit genannt werden auch Verbindungs- und Verkehrsdaten, sog. *«traffic data»*.³⁹ Der Verweis auf Verkehrsdaten dient dazu, eine Verbindung zwischen den Massnahmen in Art. 16 und Art. 17 CCC herzustellen.⁴⁰ 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.⁴¹

38. Explanatory Report, Rz. 158.

39. Explanatory Report, Rz. 158.

40. Explanatory Report, Rz. 161.

41. Explanatory Report, Rz. 161.

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

Art. 16 Abs. 2 CCC legt fest, dass in Fällen, in denen Computerdaten gemäss 11 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 Computerdaten für eine begrenzte Zeit sicherzustellen. Eine Verpflichtung zu solchen Massnahmen besteht für Vertragsstaaten jedoch nicht.⁴² Vertragsstaaten müssen sicherstellen, dass ihre Untersuchungsbehörden – unabhängig vom gewählten Verfahren – die umgehende/sofortige Sicherung anordnen oder bewirken können.

Als **Anordnungsadressaten** gelten Personen, die entweder im Besitz von 12 gespeicherten Computerdaten sind oder die Verfügungsgewalt über die Daten haben.

Die Vertragsstaaten können im innerstaatlichen Recht als Massnahme im 13 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 Herausgabeanordnung 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.⁴³

C. Absatz 3: Geheimhaltungspflicht

Art. 16 Abs. 3 CCC verlangt von den Vertragsstaaten, die erforderlichen 14 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

42. Vgl. dazu BBl 2010 4718.

43. Explanatory Report, Rz. 162.

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.⁴⁴

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 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

44. Explanatory Report, Rz. 163.

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,⁴⁵ wodurch eine beschleunigte und verhältnismässige Sicherung gespeicherter Computerdaten gesetzlich gewährleistet wird.⁴⁶

A. Sicherung durch Strafverfolgungsbehörden

Eine vorübergehende Sicherung von Datenmaterial wird in der Schweiz ¹⁹ 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 beschlagnahmen. 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»⁴⁷).⁴⁸ Durch die Spiegelung wird sichergestellt, dass Daten auf einen externen Datenträger kopiert werden und vor Manipulationen geschützt sind.⁴⁹ 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

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

46. BBl 2010 4718.

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

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

49. Graf, Rz. 237.

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.⁵⁰ Die Rechtsgrundlage für die Erstellung von Kopien solcher Aufzeichnungen und Daten im Rahmen einer Durchsuchung bildet Art. 247 Abs. 3 StPO.⁵¹

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 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.⁵²
- 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,⁵³ jedoch können in der Schweiz

50. Graf, Rz. 238 f.

51. Graf, Rz. 237.

52. Vgl. BGE 143 IV 21.

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

ansässige **Fernmeldediensteanbieter** als Inhaber der Randdaten dazu angehalten werden, eine Datensicherung gemäss Art. 273 StPO vorzunehmen.⁵⁴ Die Beschaffung von Bestandesdaten ist keine Zwangsmassnahme und erfordert keine Genehmigung des Zwangsmassnahmengerichts.⁵⁵

C. Fehlende Gesetzesbestimmung betreffend Anordnung auf Aufbewahrung

In der Schweiz werden lediglich Fernmeldediensteanbieter gemäss Art. 2 BÜPF²³ gesetzlich verpflichtet, Identifikations- und Randdaten für die Dauer von sechs Monaten aufzubewahren.⁵⁶ 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.

Die Schweiz hat sich mit der Ratifizierung der Cybercrime-Konvention nicht²⁴ in die Pflicht gestellt, «Preservation Orders» im innerstaatlichen Recht einzuführen. Derzeit bietet die Schweizerische Strafprozessordnung auch **keine Rechtsgrundlage** dafür, dass Dateninhaber und Diensteanbieter 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.⁵⁷ 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

54. BBl 2010 4718 f.

55. Hansjakob, Rz. 1615.

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

57. BBl 2010 4718 f.

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, 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 zuhanden 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 ausgebremste 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.⁵⁸ 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 Entsiegelungsantrag⁵⁹ oder bei dringlicher Notwendigkeit superprovisorisch gestellt werden.⁶⁰ Die Anordnung einer Spiegelung oblige nach der Siegelung ausschliesslich dem Zwangsmassnahmengericht.

Diese Rechtsprechung hat zu Recht erhebliche **Kritik** erfahren.⁶¹ Sie erweist sich auch im Hinblick auf die Cybercrime-Konvention als völkerrechtswidrig. So ignoriert das Bundesgericht,⁶² 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 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. 27

58. BGE 148 IV 221, E. 2.6.

59. BGE 148 IV 221, E. 2.6.

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

61. Vgl. Graf, Rz. 241 ff.; Graf/Günal Rütscbe, 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.

62. Vgl. Graf, Rz. 246.

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 über das Jugendstrafrecht vom 21.9.1998, BBl 1999 II 1979 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_1979_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.

KOMMENTIERUNG ZU

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

Eine Kommentierung von Damian K. Graf

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.....	184
II. Anordnung zur Herausgabe von Computerdaten (Abs. 1 lit. a)	186
III. Anordnung zur Herausgabe von Bestandesdaten bei Providern (Abs. 1 lit. b)	189
IV. Verweis auf Art. 14–15 CCC (Abs. 2)	193
V. Definition von Bestandesdaten (Abs. 3)	194
VI. Voraussetzungen für eine zulässige Datenerhebung nach schweizerischem Strafprozessrecht	196
Literaturverzeichnis	198
Materialienverzeichnis.....	200

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.⁶⁵ 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. gespeicherten**⁶⁶ **Daten im Rahmen eines Strafverfahrens** beschränkt.⁶⁷ 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).⁶⁸ Das bedeutet

65. Vgl. Explanatory Report, Rz. 171.

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

67. Vgl. Explanatory Report, Rz. 182.

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

zugleich, dass das ersuchte Beweismaterial zumindest **potentiell beweiserheblich** sein muss, also für die Strafuntersuchung von Bedeutung sein kann bzw. nicht offensichtlich untauglich erscheinen darf,⁶⁹ was sich bereits aus dem allgemeingültigen Verhältnismässigkeitsgrundsatz (Voraussetzung einer «geeigneten» staatlichen Massnahme) ergibt.

Aufgrund des Wortlauts der Konvention («jede Vertragspartei trifft die 4 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.⁷⁰ Art. 18 CCC kann daher – im Gegensatz zu Art. 32 CCC – nicht direkt als Grundlage für eine strafprozessuale Massnahme herangezogen werden.

Allerdings erklärte der Bundesrat in der Botschaft, **das schweizerische 5 Recht entspreche bereits den Anforderungen von Art. 18 CCC.**⁷¹ 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** 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.⁷²

Art. 18 CCC legt nicht fest, wie die Massnahmen im jeweiligen Binnenrecht 6 genau umzusetzen sind; vielmehr umreisst 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.

Ebenso wenig regelt Art. 18 CCC, ob und bejahendenfalls in welchem Umfang 7 Daten gespeichert werden müssen, noch bestimmt er Aufbewahrungsfristen.⁷³

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

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

71. BBl 2010 4721.

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.⁷⁴ Solche Pflichten können sich ggf. aus innerstaatlichen Regelungen auf Gesetzes- oder Verordnungsstufe ergeben.⁷⁵

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.).⁷⁶ 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**

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

74. Explanatory Report, Rz. 181.

75. 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).

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

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.

Der Speicherort der Daten ist in diesem Kontext m.a.W. irrelevant. Demnach 10 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 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»).⁷⁷

Das Begriffspaar «Besitz oder Kontrolle» bezieht sich zum einen auf den 11 **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).⁷⁸ Dies umfasst bspw. eine Person, die Daten bei einem Drittanbieter, etwa in einer Cloud, gespeichert hat⁷⁹ – 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.⁸⁰ 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.⁸¹ «Kontrolle» setzt damit kumulativ die Möglichkeit des Zugriffs als auch die Berechtigung

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

78. Explanatory Report, Rz. 173.

79. Explanatory Report, Rz. 173.

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

81. 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».

voraus, auf diese Daten zuzugreifen.⁸² 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.⁸³

- 12 In **Konzernstrukturen** kann nicht ohne Weiteres davon ausgegangen werden, dass eine Konzerntochtergesellschaft auf Daten der Mutter- oder von Schwesterngesellschaften zugreifen kann.⁸⁴ 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,⁸⁵ während das aufbewahrende Unternehmen die Daten «besitzt», da sie sich in ihrem Herrschaftsbereich befinden.⁸⁶ 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.⁸⁷
- 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 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

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

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

84. 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.

85. Vgl. auch Walder, Fn. 81.

86. 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.

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

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)

Art. 18 Abs. 1 lit. b CCC bezieht sich auf die Herausgabe von **Bestandesdaten** 15 durch **Diensteanbieter bzw. «service provider»** i.S.v. Art. 1 lit. c CCC,⁸⁸ die ihre **Dienste im Hoheitsgebiet des Vertragsstaats anbieten**. Der Artikel ist somit sowohl enger als auch weiter als lit. a gefasst, indem er auf Diensteanbieter und die Vorlage von Bestandesdaten («subscriber information») – z.B. die Identität des Kunden oder Angaben zum Zahlungsverkehr⁸⁹ (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 Diensteanbieter erfasst werden, wenn sie auf dem schweizerischen Markt aktiv sind. Voraussetzung bleibt auch hier,

88. Unter den Begriff des Diensteanbieters («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.

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

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,⁹⁰ ist eine Herausgabeaufforderung **verbindlich** und muss von den adressierten Diensteanbietern 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.⁹¹
- 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 Diensteanbieters auf Nutzerinnen und Nutzer des Staates ausgerichtet sind,⁹² also der Diensteanbieter beabsichtigt, dass Nutzerinnen und Nutzer dieses Staates seine Services anwenden. Die bloße Zugänglichkeit einer Webseite oder Möglichkeit, sich von einem anderen Land aus anzumelden, reicht hierfür nicht aus.⁹³ 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 Staates dienen.⁹⁴ 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.⁹⁵ Schliesslich verlangt der

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

91. Seger, S. 80.

92. 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.

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

94. 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.

neue Art. 3 Ziff. 4 der Verordnung (EU) 2023/1543 über Europäische Herausgabebeanordnungen 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.

Sind ausländische Provider mit einem Dienst im Markt eines Vertragsstaates 18 aktiv, so sind sie verpflichtet, die Bestandesdaten herauszugeben, die auf die Nutzerinnen und Nutzer dieses konkreten Dienstes im jeweiligen Vertragsstaat bezogen sind.⁹⁶ 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.

Auch innerhalb der Gremien des Europarats herrscht die Auffassung vor, dass 19 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.⁹⁷ Beides steht auch im Einklang mit dem Wortlaut von Art. 18 CCC.

Auch das Bundesgericht hat sich bereits mit diesen zwei Fragen 20 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

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

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

97. 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».

ces données»),⁹⁸ 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. 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.⁹⁹ 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.¹⁰⁰ 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.¹⁰¹ 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.¹⁰² 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.¹⁰³ 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,

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

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

100. BGE 141 IV 108 E. 6.2.

101. BBl 2010 4721.

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

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

machen sie sich im Falle der Datenlieferung auch nicht wegen Art. 271 StGB («Verbotene Handlung für einen fremden Staat») strafbar.

Was die **Zustellung** der Editionsverfügungen betrifft, so stellen grössere 21
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.¹⁰⁴ 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.

Da es sich bei der Herausgabeaufforderung um eine **innerstaatliche** 22
Beweiserhebungsmassnahme handelt,¹⁰⁵ 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.

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

Staaten können im Rahmen von Art. 15 CCC **Bedingungen und** 23
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

104. 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»).

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

Notwendigkeit der Einholung einer Genehmigung des Zwangsmassnahmengerichts zu verlangen (Art. 273 StPO).¹⁰⁶ Weiter ist es zulässig, Herausgabeeanordnungen mit Mitteilungsverboten zu verknüpfen,¹⁰⁷ 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.¹⁰⁸
- 25 Zu den Bestandesdaten zählen nach Art. 18 Abs. 3 CCC alle Informationen bezüglich (a) der Art des genutzten Kommunikationsdienstes, der dafür getroffenen technischen Massnahmen¹⁰⁹ 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

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

107. Explanatory Report, Rz. 175.

108. Explanatory Report, Rz. 178.

109. 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)».

wie die Zuordnung von Namen, Telefonnummern und Adresse des Benutzers zu einer bekannten IP-Adresse,¹¹⁰ alsdann auch Originalverträge und Kopien von bei Vertragsabschluss vorgelegten Ausweisen¹¹¹ sowie technische Auskünfte im Fernmeldeverkehr.¹¹²

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, bejahendenfalls es um eine Bestandesdatenabfrage geht. Falls den Strafverfolgungsbehörden dagegen allein strafbare Internet-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.¹¹³ Nach der Rechtsprechung soll dies pauschal auch für die Aufforderung zur Herausgabe einer IP-History gelten.¹¹⁴ Richtigerweise ist die Abgrenzung danach zu vollziehen, ob es darum geht, wer wann mit wem kommuniziert hat (Verbindungsdaten i.S.v. Art. 273 StPO),¹¹⁵ oder vielmehr darum, wer einen bestimmten Dienst zu einem bekannten Zeitpunkt benutzt hat (Bestandesdaten i.S.v. Art. 22 Abs. 1 BÜPF).¹¹⁶ **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

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

111. TPF 2006 255.

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

113. 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.

114. 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.

115. 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.

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

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,¹¹⁷ und stellen keine Randdaten im Kontext menschlicher Kommunikation, sondern vielmehr Bestandesdaten dar.¹¹⁸ 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.¹¹⁹ 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.¹²⁰ Die Informationsabfrage über den Dienst ÜPF stellt lediglich eine Ordnungsvorschrift dar; weder die StPO noch das BÜPF oder die

117. 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).

118. 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».

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

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

dazugehörige Verordnung sehen vor, dass Auskünfte, die nicht über den Dienst ÜPF mitgeteilt werden, unverwertbar wären.¹²¹ Eine Bestandesdatenabfrage setzt einen Tatverdacht, dass eine Straftat (Verbrechen, Vergehen oder Übertretung) über das Internet begangen worden ist (Art. 22 Abs. 1 BÜPF),¹²² 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;¹²³ 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 rechtshilfeweise beim betreffenden Staat beantragt werden.

Für Inhalts- und Verbindungsdaten, die beide nach Art. 18 Abs. 1 lit. a StPO ²⁸ herausverlangt werden dürfen, ist alsdann zu differenzieren: **Inhaltsdaten**, die für Beweis Zwecke 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.¹²⁴ Praxisrelevant sind bspw. Inhaltsdaten von Webmail-Betreibern, bspw. der E-Mail-Account einer «@bluewin.ch»-Adresse bei der Swisscom.¹²⁵

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

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

123. Hansjakob, Überwachungsrecht, Rz. 1643.

124. Bei einem E-Mail-Account sind sämtliche eingegangenen E-Mails seit dem letzten Zugriff auf das E-Mail-Konto durch die berechtigte 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.

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 verlangen¹²⁶ 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 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.

125. 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».

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

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.

Segeer 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).

KOMMENTIERUNG ZU

Art. 25 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Miro Dangubic

ZITIERVORSCHLAG

Miro Dangubic, Kommentierung zu Art. 25 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Dangubic, Art. 25 CCC N. XXX.

Titel 3: Allgemeine Grundsätze der Rechtshilfe

Art. 25 Allgemeine Grundsätze der Rechtshilfe

¹ Die Vertragsparteien leisten einander im grösstmöglichen Umfang Rechtshilfe für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat.

² Jede Vertragspartei trifft ferner die erforderlichen gesetzgeberischen und anderen Massnahmen, um den in den Artikeln 27–35 bezeichneten Verpflichtungen nachzukommen.

³ In dringenden Fällen kann jede Vertragspartei Rechtshilfeersuchen oder damit in Zusammenhang stehende Mitteilungen durch schnelle Kommunikationsmittel einschliesslich Telefax oder elektronischer Post

übersenden, soweit diese Mittel einen angemessenen Sicherheits- und Authentisierungsstandard bieten (erforderlichenfalls auch unter Einsatz einer Verschlüsselung) und eine förmliche Bestätigung folgt, wenn die ersuchte Vertragspartei dies verlangt. Die ersuchte Vertragspartei nimmt das Ersuchen entgegen und beantwortet es mit einem dieser schnellen Kommunikationsmittel.

⁴ Soweit in den Artikeln dieses Kapitels nicht ausdrücklich etwas anderes vorgesehen ist, unterliegt die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen einschliesslich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann. Die ersuchte Vertragspartei darf das Recht auf Verweigerung der Rechtshilfe in Bezug auf die in den Artikeln 2–11 bezeichneten Straftaten nicht allein mit der Begründung ausüben, dass das Ersuchen eine Straftat betrifft, die von ihr als fiskalische Straftat angesehen wird.

⁵ Darf die ersuchte Vertragspartei nach diesem Kapitel die Rechtshilfe von der Bedingung abhängig machen, dass die beiderseitige Strafbarkeit gegeben ist, so gilt, gleichviel, ob die Straftat nach ihrem Recht in dieselbe Kategorie von Straftaten fällt oder mit dem gleichen Begriff benannt ist wie nach dem Recht der ersuchenden Vertragspartei, diese Bedingung als erfüllt, wenn die Handlung, die der Straftat, derentwegen um Rechtshilfe ersucht wird, zugrunde liegt, nach ihrem Recht eine Straftat darstellt.

GLIEDERUNG

I. Einleitung	204
II. Sachlicher Anwendungsbereich des CCC bei der kleinen Rechtshilfe	205
A. Straftat als Anknüpfungspunkt	205
B. Beweise in elektronischer Form als Anknüpfungspunkt	205
III. Rechtsquellen im Rechtshilfeverkehr	206
A. Rechtshilfebestimmungen	206
B. Subsidiäres Verfahrensrecht in der Schweiz	206
IV. Verpflichtung, Rechtshilfe zu leisten	207
V. Prinzip des maximalen Entgegenkommens	207
VI. Übermittlungsformen im Rechtshilfeverkehr	208
VII. Ausgestaltung des Prinzips der doppelten Strafbarkeit	209
A. Prinzip der doppelten Strafbarkeit	209
B. Prinzip der doppelten Strafbarkeit im Anwendungsbereich des CCC	210
VIII. Durchbrechung des Fiskalvorbehaltes	210
IX. Gesetzgebungsauftrag an die Vertragsstaaten	211
A. Allgemein	211
B. Umsetzung in der Schweiz	212
Literaturverzeichnis	212
Materialienverzeichnis	213

I. EINLEITUNG

- 1 Art. 25 CCC fasst unter der Marginalie «Allgemeine Grundsätze der Rechtshilfe» verschiedene Regelungen betreffend die **kleine Rechtshilfe** im Anwendungsbereich des CCC zusammen.¹²⁷ Im Einzelnen enthält der Artikel Bestimmungen betreffend
 - den sachlichen Anwendungsbereich des CCC (Abs. 1),
 - die im Rechtshilfeverfahren einschlägigen Rechtsquellen (Abs. 4),
 - die Pflicht, kleine Rechtshilfe zu leisten (Abs. 1),
 - das Prinzip des maximalen Entgegenkommens (Abs. 1),
 - die möglichen Übermittlungsformen im Rechtshilfeverkehr (Abs. 3),
 - die Ausgestaltung des Prinzips der doppelten Strafbarkeit (Abs. 5) und
 - die Durchbrechung des Fiskalvorbehalts (Abs. 4).
- 2 Des Weiteren enthält Art. 25 Abs. 2 CCC einen Gesetzgebungsauftrag an die Vertragsstaaten.
- 3 Das CCC soll die zwischen den Vertragsparteien bestehenden zwei- oder mehrseitigen Verträge und Übereinkünfte (insbesondere auch das EUeR¹²⁸) ergänzen¹²⁹ und dadurch Rechtshilfeverfahren beschleunigen und vereinfachen.¹³⁰ Die Konzipierung als ergänzendes Übereinkommen wirkt sich stark auf den Regelungsinhalt und die Regelungsdichte betreffend die kleine Rechtshilfe aus.¹³¹

127. Explanatory Report, Rz. 253.

128. Europäisches Übereinkommen vom 20.4.1959 über die Rechtshilfe in Strafsachen (SR 0.351.1).

129. Vgl. Art. 39 Abs. 1 CCC. Auch der Staatsvertrag vom 25.5.1973 zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (mit Briefwechseln («RVUS», SR 0.351.933.6) wird bspw. durch das CCC ergänzt: Vgl. BGE 141 IV 108 E. 4.3 ff.

130. Botschaft 2010, S. 4701.

131. Vgl. bspw. Art. 27 Abs. 1 CCC.

II. SACHLICHER ANWENDUNGSBEREICH DES CCC BEI DER KLEINEN RECHTSHILFE

Der sachliche Anwendungsbereich des CCC für die kleine Rechtshilfe wird in Art. 25 Abs. 1 CCC geregelt und hat **zwei alternative Anknüpfungspunkte**: Einerseits kann an die untersuchte Straftat angeknüpft werden («Straftaten in Zusammenhang mit Computersystemen und -daten») und andererseits an die zu erhebenden Beweise («Beweismaterial in elektronischer Form»)¹³²

A. Straftat als Anknüpfungspunkt

Der sachliche Anwendungsbereich greift einerseits, falls der Verdacht besteht, dass eine in den Art. 2–11 CCC umschriebene Straftat begangen worden ist.¹³³ Andererseits greift der sachliche Anwendungsbereich in Bezug auf Straftaten, die mittels eines Computersystems begangen worden sind – unabhängig von der konkret verübten Straftat. Das Tatmittel «Computersysteme» wird in Art. 1 lit. a CCC wie folgt definiert: «eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen».

Bei der prima-facie-Prüfung dieses sachlichen Anwendungsbereichs durch die Rechtshilfebehörden ist insbesondere Folgendes zu beachten: Gewisse Elemente des sachlichen Anwendungsbereichs gehören grundsätzlich zum rechtlich relevanten Sachverhalt, den es im Rahmen der ausländischen Strafuntersuchung abzuklären gilt; unter Umständen sollen gerade mit den nachgesuchten Beweismassnahmen diese Punkte geklärt werden. Entsprechend sind keine hohen Anforderungen an die Umschreibung dieser Sachverhaltselemente zu stellen.¹³⁴

B. Beweise in elektronischer Form als Anknüpfungspunkt

Gilt es im Rahmen der Rechtshilfe in Strafsachen Beweise zu erheben, welche in elektronischer Form vermutet werden, so greift der sachliche

132. Vgl. Explanatory Report, Rz. 253; zu eng: Botschaft 2010, S. 4726, welche nur von einer Gruppe von Straftaten spricht.

133. Explanatory Report, Rz. 253.

134. Vgl. Dangubic/Clerc, S. 289.

Anwendungsbereich des CCC unabhängig vom zu untersuchenden Delikt.¹³⁵
Beweise in elektronischer Form können insbesondere Daten sein.¹³⁶

III. RECHTSQUELLEN IM RECHTSHILFEVERKEHR

A. Rechtshilfebestimmungen

- 8 Rechtshilfeverfahren im Geltungsbereich des CCC richten sich primär nach den einschlägigen Staatsverträgen und dem CCC.¹³⁷ Soweit diese Staatsverträge bestimmte Fragen weder ausdrücklich noch stillschweigend regeln, kommen die nationalen Bestimmungen zur Anwendung (Art. 25 Abs. 4 CCC). In der Schweiz sind für die Rechtshilfe in Strafsachen das IRSG¹³⁸ und die IRSV¹³⁹ massgebend (Art. 1 Abs. 1 IRSG).¹⁴⁰ Das – auch in Art. 25 Abs. 1 CCC verankerte – Günstigkeitsprinzip besagt, dass die nationalen Bestimmungen auch dann zur Anwendung gelangen, wenn sie geringere Anforderungen an die Rechtshilfe stellen.¹⁴¹ Mithin kommen die Bestimmungen des CCC in Rechtshilfeverfahren nur zur Anwendung, falls sie aus der Sicht des ersuchenden Staates die rechtshilfefreundlichste Norm darstellen.¹⁴²

B. Subsidiäres Verfahrensrecht in der Schweiz

- 9 Fehlt es den Rechtshilfebestimmungen an einschlägigen prozessualen Regelungen, so gelangen in hiesigen Rechtshilfeverfahren die StPO¹⁴³ und das VwVG¹⁴⁴ sinngemäss zur Anwendung.¹⁴⁵ Die StPO ist in Rechtshilfeverfahren massgebend, wenn das IRSG direkt darauf verweist oder im Zusammenhang

135. Explanatory Report, Rz. 253.

136. Zum Datenbegriff vgl. insbesondere Art. 1 lit. b CCC.

137. BStGer RR.2019.136 vom 28.10.2020 E. 1.1.

138. Bundesgesetz vom 20.3.1981 über internationale Rechtshilfe in Strafsachen (SR 351.1).

139. Verordnung vom 24.2.1982 über internationale Rechtshilfe in Strafsachen (SR 351.11).

140. Im Rechtshilfeverkehr mit den Vereinigten Staaten von Amerika ist zudem das Bundesgesetz zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen vom 3.10.1975 («BG-RVUS», SR 351.93) massgebend.

141. Vgl. hierzu BSK-Fiolka, Art. 1 IRSG N. 24.

142. Im Ergebnis: Explanatory Report, Rz. 311.

143. Die Verwaltungsstraßbehörden wenden zudem auch das VStrR an.

144. Bundesgesetz vom 20.12.1968 über das Verwaltungsverfahren (SR 172.021).

145. Vgl. Art. 12 Abs. 1 IRSG.

mit strafprozessualen Verfahrenshandlungen i.S.v. Art. 63 ff. IRSG. In den übrigen Fällen dient das VwVG als subsidiäres Verfahrensrecht.¹⁴⁶

IV. VERPFLICHTUNG, RECHTSHILFE ZU LEISTEN

Gestützt auf Art. 25 Abs. 1 CCC ist der ersuchte Staat verpflichtet, falls 10
sämtliche Rechtshilfenvoraussetzungen erfüllt sind, kleine Rechtshilfe zu
leisten, wenn er von einer Vertragspartei darum ersucht wird.¹⁴⁷ Diese
Verpflichtung hat jedoch nicht zur Folge, dass dem ersuchenden Staat im
Rahmen des Rechtshilfeverfahrens Parteistellung oder Rechtsmittel
zukommen.¹⁴⁸ Allfällige abweichende Standpunkte von Staaten in Bezug auf
die Frage, ob die Bedingungen der Rechtshilfe in Strafsachen erfüllt sind und
Rechtshilfe zu leisten ist, werden auf diplomatischer Ebene gelöst.¹⁴⁹

Bei der ausservertraglichen Rechtshilfe in Strafsachen besteht kein Anspruch 11
auf zwischenstaatliche Zusammenarbeit in Strafsachen (vgl. Art. 1 Abs. 4
IRSG).¹⁵⁰

V. PRINZIP DES MAXIMALEN ENTGEGENKOMMENS

Art. 25 Abs. 1 CCC verpflichtet den ersuchten Staat, Rechtshilfeersuchen im 12
Anwendungsbereich des CCC «im grösstmöglichen Umfang» zu entsprechen
(sog. Prinzip des maximalen Entgegenkommens¹⁵¹).

Das Prinzip des maximalen Entgegenkommens ist ein allgemein anerkannter 13
Grundsatz der Rechtshilfe in Strafsachen, der nicht nur programmatischen
Charakter hat. Der Grundsatz beinhaltet das oben erwähnte
Günstigkeitsprinzip.¹⁵² In der hiesigen Praxis gilt das Günstigkeitsprinzip in
sämtlichen Rechtshilfeverfahren – auch wenn keine diesbezügliche
staatsvertragliche Verpflichtung besteht.¹⁵³ Es besagt, dass das nationale Recht

146. Dangubic, S. 113.

147. Explanatory Report, Rz. 253; Botschaft 2010, S. 4726.

148. Vgl. BGE 125 II 411 E. 3a.

149. Vgl. auch Art. 45 CCC.

150. Das Nichtbestehen eines Anspruchs darf indes nicht darüber hinwegtäuschen, dass aus innerstaatlicher Sicht bei gegebenen Voraussetzungen Rechtshilfe grundsätzlich geleistet wird. Vgl. BGE 111 Ib 242 E. 4c.

151. Popp, S. 127.

152. Popp, S. 127 ff.

153. Donatsch/Heimgartner/Meyer/Simonek, S. 24.

die Rechtshilfe in Strafsachen gegenüber vorrangigem Staatsvertragsrecht nicht erschweren, wohl aber erleichtern darf.¹⁵⁴

- 14 Das Prinzip des maximalen Entgegenkommens bezieht sich zudem auf den **Umfang** der zu leistenden Rechtshilfe.¹⁵⁵ Es erlaubt, die in einem Rechtshilfeersuchen nachgesuchten Massnahmen grosszügig auszulegen und sämtliche für das ausländische Strafverfahren potentiell erheblichen Beweismittel an die ersuchende Behörde herauszugeben – auch wenn die ersuchende Behörde nicht explizit darum ersucht hat.¹⁵⁶

VI. ÜBERMITTLUNGSFORMEN IM RECHTSHILFEVERKEHR

- 15 Gemäss dem IRSG sind an die Schweiz gerichtete Rechtshilfeersuchen grundsätzlich in **schriftlicher Briefform** an das Bundesamt für Justiz zu richten.¹⁵⁷ Mehrere europäische Staatsverträge erlauben hingegen auch den direkten Verkehr zwischen den zuständigen Justizorganen¹⁵⁸ (in der Regel Staatsanwaltschaften¹⁵⁹) sowie Alternativen zur schriftlichen Briefform.¹⁶⁰
- 16 Im Anwendungsbereich des CCC erlaubt Art. 25 Abs. 3 CCC in dringenden Fällen, dass «schnelle Kommunikationsmittel einschliesslich Telefax oder elektronischer Post» genutzt werden. Dies gilt nicht nur für das Stellen von Rechtshilfeersuchen, sondern für den gesamten Rechtshilfeverkehr.¹⁶¹ Sinn und Zweck dieser Bestimmung ist es, das Rechtshilfeverfahren zu beschleunigen und insbesondere eine rasche Beweissicherung zu ermöglichen, um der Gefahr des Beweisverlustes entgegenzuwirken.¹⁶² Auf explizite Aufforderung des ersuchten Staates hin ist ein Rechtshilfeersuchen in Schriftform nachzureichen.¹⁶³

154. Vgl. BSK-Heimgartner/Niggli, Einführung IRSG N. 52.

155. Popp, S. 127.

156. Donatsch/Heimgartner/Meyer/Simonek, S. 93.

157. Vgl. Art. 27 Abs. 2, Art. 28 Abs. 1 sowie Art. 29 Abs. 1 IRSG.

158. Vgl. Art. 53 Abs. 1 SDÜ, Art. 4 Abs. 1 ZPII EUeR oder Art. 27 Abs. 1 BBA.

159. Vgl. Art. 55 Abs. 1 StPO.

160. Vgl. Art. 4 Abs. 9 ZPII EUeR.

161. Explanatory Report, Rz. 44. Botschaft 2010, S. 4726.

162. Damit soll insbesondere auch der Flüchtigkeit von elektronischen Daten und den kurzen Speicherzeiten Rechnung getragen werden. Vgl. Botschaft 2010, S. 4726.

163. Botschaft 2010, S. 4726.

Zeitliche Dringlichkeit ist gegeben, wenn mit der Übermittlung in 17
Schriftform ein Beweisverlust drohen könnte. Dies ist insbesondere der Fall,
falls es rechtshilfeweise Daten zu erheben gilt.¹⁶⁴

Es besteht kein **numerus clausus** in Bezug auf die Kommunikationsmittel, 18
die verwendet werden dürfen. In der Praxis werden insbesondere E-Mail,
Telefax sowie staatliche Filesharing-Plattformen genutzt. Rechtshilfeersuchen
können jedoch auch telefonisch gestellt werden.¹⁶⁵

Die massgebenden **Sicherheits- und Authentisierungsstandards** ergeben 19
sich aus den nationalen Rechtsordnungen bzw. den Richtlinien und der Praxis
der entsprechenden Behörden.

VII. AUSGESTALTUNG DES PRINZIPS DER DOPPELTEN STRAFBARKEIT

Art. 25 Abs. 5 CCC regelt die Ausgestaltung des Grundsatzes der beidseitigen 20
Strafbarkeit.

A. Prinzip der doppelten Strafbarkeit

Die doppelte Strafbarkeit ist ein klassisches Prinzip der internationalen 21
Zusammenarbeit.¹⁶⁶ Es besagt, dass Rechtshilfe in Strafsachen nur im Hinblick
auf Delikte gewährt wird, welche sowohl nach dem Recht des ersuchenden
als auch nach dem Recht des ersuchten Staates unter Strafe gestellt sind.¹⁶⁷
Der Grundsatz der beidseitigen Strafbarkeit gehört in der Schweiz zum *ordre*
public und wurde entsprechend in allen bilateralen Verträgen und (mittels
Vorbehalten) in multilateralen Rechtshilfeübereinkommen sichergestellt¹⁶⁸ –
so auch für den Anwendungsbereich des CCC.¹⁶⁹

164. Botschaft 2010, S. 4726.

165. Vgl. auch Art. VII des Vertrages vom 13.11.1969 zwischen der Schweizerischen
Eidgenossenschaft und der Bundesrepublik Deutschland über die Ergänzung des
Europäischen Übereinkommens über die Rechtshilfe in Strafsachen vom 20.4.1959 und die
Erleichterung seiner Anwendung (SR.0351.913.61).

166. BSK-Heimgartner, Art. 64 IRSG N. 1.

167. Popp, S. 134.

168. BSK-Heimgartner/Niggli, Einführung IRSG N. 47.

B. Prinzip der doppelten Strafbarkeit im Anwendungsbereich des CCC

- 22 Sind im Rahmen des Rechtshilfeverfahrens Massnahmen anzuwenden, welche **prozessualen Zwang** erfordern, so gilt im Anwendungsbereich des CCC das Prinzip der beidseitigen Strafbarkeit.¹⁷⁰ Es bestehen jedoch auch Ausnahmen von diesem Grundsatz.¹⁷¹
- 23 Nach den allgemeinen Grundsätzen ist die Strafbarkeit nach dem Recht des ersuchenden Staates – auch im Anwendungsbereich des CCC – im hiesigen Rechtshilfeverfahren grundsätzlich nicht zu prüfen, vorbehältlich Fälle offensichtlichen Missbrauchs.¹⁷²
- 24 Zur Frage der doppelten Strafbarkeit nach schweizerischem Recht prüft die ausführende Behörde, ob der im Rechtshilfeersuchen wiedergegebene Sachverhaltskomplex prima facie unter eine schweizerische Strafnorm subsumiert werden kann.¹⁷³ Art. 25 Abs. 5 CCC besagt einerseits, dass es genügt, wenn der im Rechtshilfeersuchen geschilderte Sachverhalt unter einen einzigen Straftatbestand des schweizerischen Rechts subsumierbar ist – es braucht nicht weiter geprüft zu werden, ob darüber hinaus auch noch weitere Tatbestände erfüllt sein könnten. Andererseits stipuliert er, dass beidseitige Strafbarkeit keine identischen Strafnormen im ersuchenden und ersuchten Staat voraussetzt. Mithin entspricht der Regelungsinhalt von Abs. 5 bereits der geltenden Praxis in der Schweiz.¹⁷⁴

VIII. DURCHBRECHUNG DES FISKALVORBEHALTES

- 25 Traditionellerweise enthalten zahlreiche – sowohl nationale als auch internationale – Rechtsquellen einen sog. **Fiskalvorbehalt**.¹⁷⁵ Bspw.

169. Vgl. Vorbehalt gemäss Art. 27 Abs. 4 der Schweiz zum CCC: «Die Schweiz behält sich das Recht vor, die Ausführung eines Rechtshilfeersuchens, welche die Anwendung einer Zwangsmassnahme erforderlich macht, der Voraussetzung gemäss Artikel 29 Absatz 4 zu unterstellen.»

170. Vgl. auch Art. 64 IRSG.

171. Vgl. Art. 29 Abs. 3 CCC betreffend die Vornahme der Sicherung. Auch der direkte Zugriff nach Art. 32 CCC setzt die doppelte Strafbarkeit nicht voraus: Vgl. OK-Graf, Art. 32 CCC N. 61.

172. Statt vieler: BStGer RR.2020.303 vom 9.9.2021 E. 3.3.

173. Vgl. zum Ganzen BSK-Garré, Art. 35 IRSG N. 7.

174. Vgl. BSK-Heimgartner, Art. 64 IRSG N. 1 ff.

stipuliert Art. 3 Abs. 3 IRSG, dass auch die akzessorische Rechtshilfe bei Verfahren wegen Verkürzung fiskalischer Abgaben grundsätzlich ausgeschlossen ist.¹⁷⁶

Satz zwei von Art. 25 Abs. 4 CCC soll sicherstellen, dass allfällige Fiskalvorbehalte der Rechtshilfe im Anwendungsbereich des CCC nicht im Wege stehen, falls Straftaten i.S.v. Art. 2–11 CCC untersucht werden. Da es sich bei den in den Art. 2–11 CCC beschriebenen Straftaten nicht um Fiskaldelikte handelt¹⁷⁷, dürfte die praktische Relevanz dieser Bestimmung eher gering ausfallen. Zu denken wäre allenfalls an Konstellationen der Idealkonkurrenz¹⁷⁸: Der Täter begeht durch eine einzige Handlung oder auch durch ein einheitliches, zusammengehörendes Tun sowohl ein nicht rechtshilfefähiges Fiskaldelikt als auch eine Straftat i.S.v. Art. 2–11 CCC. Diesfalls würde der Fiskalvorbehalt stets durchbrochen.¹⁷⁹

IX. GESETZGEBUNGSaufTRAG AN DIE VERTRAGSSTAATEN

A. Allgemein

Art. 25 Abs. 2 CCC verpflichtet die Vertragsstaaten, bei der Ausgestaltung ihrer nationalen Rechtsordnung sicherzustellen, dass ein innerstaatliches Instrumentarium zur Umsetzung der Bestimmungen von Art. 27–35 CCC besteht.¹⁸⁰ Mithin stellt diese Norm primär einen sog. **völkerrechtlichen Gesetzgebungsauftrag** dar.

Die Verpflichtung richtet sich grundsätzlich an die Legislative und setzt ein aktives Tätigwerden des Vertragsstaates voraus – falls das innerstaatliche Recht den Vorgaben (noch) nicht genügt. Vertragsstaaten, die bereits über die notwendigen rechtlichen Instrumente verfügen, müssen gesetzgeberisch nicht tätig werden.

175. Vgl. zum Fiskalvorbehalt BSK-Kocher, Art. 3 IRSG N. 64.

176. Vgl. Art. 2 lt. a EUeR.

177. So auch Botschaft 2010, S. 4727.

178. Donatsch/Gothenzi/Tag, S. 437.

179. Das Zusammentreffen von Ausschluss und Zulässigkeit der Zusammenarbeit wird im IRSG in Art. 6 geregelt.

180. Explanatory Report, Rz. 254 f.

B. Umsetzung in der Schweiz

- 29 Die Bestimmungen der Art. 27–35 CCC sind nach hiesigem Verständnis grundsätzlich als **self-executing** zu qualifizieren.¹⁸¹ Im Hinblick auf ihre innerstaatliche Anwendbarkeit und Durchsetzbarkeit sah der Gesetzgeber lediglich in Bezug auf Art. 30 und 33 CCC einen Handlungsbedarf.¹⁸²
- 30 Zur Umsetzung des Art. 30 CCC (Umgehende Weitergabe gesicherter Verkehrsdaten) sowie Art. 33 CCC (Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit) wurde mit Bundesbeschluss vom 18. März 2011 Art. 18b IRSG mit der Marginalie «Elektronische Daten» in das Gesetz eingefügt.¹⁸³

LITERATURVERZEICHNIS

Böhi Simon, Kommentierung zu Art. 18b IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Dangubic Miro, Parteistellung und Parteirechte bei der rechtshilfeweisen Herausgabe von Kontoinformationen, *forumpoenale* 2018, S. 112–117.

Dangubic Miro/Clerc Yves, Art. 80dbis – ein Überblick, *forumpoenale* 2022, S. 287–292.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2. Aufl., Zürich et al. 2015.

Donatsch Andreas/Godenzi Gunhild/Tag Brigitte, Strafrecht I, Verbrechenslehre, 10. Aufl., Zürich 2022.

Garré Roy, Kommentierung zu Art. 35 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Graf Damian K., in: Ackermann Jürg-Beat (Hrsg.), Wirtschaftsstrafrecht der Schweiz, Hand- und Studienbuch, 2. Aufl., Bern 2021.

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

181. Explanatory Report, Rz. 255; Donatsch/Heimgartner/Meyer/Simonek, S. 16 f.; Graf, S. 1078 betreffend Art. 32 CCC.

Convention), abrufbar unter <https://onlinekommentar.ch/de/kommentare/ccc32>, besucht am 21.11.2023.

Heimgartner Stefan, Kommentierung zu Art. 64 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Heimgartner Stefan/Niggli Marcel Alexander, Kommentierung zu Einführung IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Kocher Martin, Kommentierung zu Art. 3 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Popp Peter, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel et al. 2001.

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.admin.ch/opc/de/federal-gazette/2010/4697.pdf>, besucht am 21.10.2023 (zit. Botschaft 2010).

Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23.XI.2001, abrufbar unter <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>, besucht am 21.10.2023 (zit. Explanatory Report).

182. Botschaft 2010, S. 4733 ff.

183. BSK-Böhi, Art. 186 IRSG N. 1.

KOMMENTIERUNG ZU

Art. 27 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Jan Reinhardt

ZITIERVORSCHLAG

Jan Reinhardt, Kommentierung zu Art. 27 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Reinhardt, Art. 27 CCC N. XXX.

Titel 4: Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte

Art. 27 Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte

¹ Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so finden die Absätze 2–9 Anwendung. Liegen ein solcher Vertrag, eine solche Übereinkunft oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung, wenn die betreffenden Vertragsparteien übereinkommen, an Stelle des Vertrags, der Übereinkunft oder der Rechtsvorschriften die Absätze 2–9 ganz oder teilweise anzuwenden.

² a. Jede Vertragspartei bestimmt eine oder mehrere zentrale Behörden, welche die Aufgabe haben, Rechtshilfeersuchen abzusenden, zu beantworten, zu erledigen oder an die für die Erledigung zuständigen Behörden weiterzuleiten.

b. Die zentralen Behörden verkehren unmittelbar miteinander.

c. Jede Vertragspartei teilt dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde die Bezeichnung und Anschrift der nach diesem Absatz bestimmten Behörden mit.

d. Der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien so bestimmten zentralen Behörden. Jede Vertragspartei stellt sicher, dass die in dem Verzeichnis enthaltenen Angaben stets richtig sind.

³ Rechtshilfeersuchen nach diesem Artikel werden nach den von der ersuchenden Vertragspartei bezeichneten Verfahren erledigt, sofern dies mit dem Recht der ersuchten Vertragspartei nicht unvereinbar ist.

⁴ Zusätzlich zu den Ablehnungsgründen nach Artikel 25 Absatz 4 kann die ersuchte Vertragspartei die Rechtshilfe verweigern, 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. sie der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (*ordre public*) oder andere wesentliche Interessen zu beeinträchtigen.

⁵ Die ersuchte Vertragspartei kann die Durchführung der in einem Ersuchen genannten Massnahmen aufschieben, wenn die Gefahr besteht, dass sie die von ihren Behörden geführten strafrechtlichen Ermittlungen oder Verfahren beeinträchtigen.

⁶ Bevor die ersuchte Vertragspartei die Rechtshilfe verweigert oder aufschiebt, prüft sie, gegebenenfalls nach Konsultation der ersuchenden Vertragspartei, ob dem Ersuchen zum Teil oder vorbehaltlich der von ihr als erforderlich erachteten Bedingungen entsprochen werden kann.

⁷ Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei umgehend das Ergebnis der Erledigung eines Rechtshilfeersuchens mit. Jede Ablehnung und jeder Aufschub des Ersuchens ist zu begründen. Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei gegebenenfalls auch die Gründe mit, aus denen die Erledigung des Ersuchens unmöglich ist oder sich wahrscheinlich erheblich verzögern wird.

⁸ Die ersuchende Vertragspartei kann die ersuchte Vertragspartei bitten, das Vorliegen eines Ersuchens nach diesem Kapitel und dessen Inhalt vertraulich zu behandeln, soweit die Erledigung des Ersuchens nichts anderes gebietet. Kann die ersuchte Vertragspartei der erbetenen Vertraulichkeit nicht entsprechen, so teilt sie dies der ersuchenden Vertragspartei umgehend mit; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.

⁹ a. In dringenden Fällen können Rechtshilfeersuchen und damit in Zusammenhang stehende Mitteilungen unmittelbar von den Justizbehörden der ersuchenden Vertragspartei an die Justizbehörden der ersuchten Vertragspartei übermittelt werden. In diesen Fällen ist gleichzeitig über die zentrale Behörde der ersuchenden Vertragspartei eine Kopie an die zentrale Behörde der ersuchten Vertragspartei zu senden.

b. Jedes Ersuchen oder jede Mitteilung nach diesem Absatz kann über die Internationale Kriminalpolizeiliche Organisation (Interpol) übermittelt werden.

c. Wird ein Ersuchen nach Buchstabe a übermittelt und ist die befasste Behörde für die Erledigung nicht zuständig, so leitet sie das Ersuchen an die zuständige Behörde ihres Landes weiter und setzt die ersuchende Vertragspartei unmittelbar davon in Kenntnis.

d. Ersuchen oder Mitteilungen nach diesem Absatz, die keine Zwangsmassnahmen erfordern, können unmittelbar von den zuständigen Behörden der ersuchenden Vertragspartei den zuständigen Behörden der ersuchten Vertragspartei übermittelt werden.

e. Jede Vertragspartei kann dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-,

Annahme-, Genehmigungs- oder Beitrittsurkunde mitteilen, dass Ersuchen nach diesem Absatz aus Gründen der Effizienz an ihre zentrale Behörde zu richten sind.

GLIEDERUNG

I. Allgemeines.....	220
II. Verhältnis zu anderen Vorschriften.....	220
III. Vorgaben für die Rechtshilfe.....	223
A. Einrichtung von Behörden (Abs. 2).....	223
B. Vorgaben hinsichtlich Art und Weise der Durchführung (Abs. 3).....	224
C. Einwände gegen die Durchführung.....	226
1. Zusätzliche Ablehnungsgründe (Abs. 4).....	226
2. Aufschieben der Rechtshilfe (Abs. 5).....	227
3. Bedingung als Minus zur Ablehnung und Aufschieben (Abs. 6).....	228
D. Mitteilungspflichten (Abs. 7).....	229
E. Vertraulichkeit (Abs. 8).....	229
F. «Beschleunigtes Verfahren» (Abs. 9).....	232
IV. Rechtsschutz.....	233
Literaturverzeichnis	234
Materialienverzeichnis.....	235

I. ALLGEMEINES

- 1 Art. 27 CCC ergänzt das allgemeine Rechtshilfegebot des Art. 25 Abs. 1 CCC und garantiert für die kleine Rechtshilfe einen **institutionellen Mindeststrahmen**. Die Regelung verhindert, dass zwischen zwei Vertragsparteien auf die vertraglose Rechtshilfe zurückgegriffen werden muss, und dient so dem Effektivitätsgrundsatz gemäss Art. 25 Abs. 1 CCC.
- 2 Die Norm enthält neben der Pflicht zur Benennung bestimmter Behörden eine näher ausgestaltete **Verpflichtung zur Erledigung von Rechtshilfeersuchen**. Insoweit ist sie nach dem schweizerischen monistischen Verständnis self-executing.¹⁸⁴ Für die einzelnen ersuchensgegenständlichen Massnahmen muss jedoch – wie bei der vertraglosen Rechtshilfe nach dem IRSG – eine Ermächtigungsgrundlage im nationalen Verfahrensrecht bestehen.¹⁸⁵ Aus Art. 25 Abs. 2 CCC folgt zudem, dass die Vertragsstaaten ihre Rechtsordnung so anzupassen haben, dass sie dem Verfahren nach den Artikeln des Abschnitts nicht entgegensteht. Hierzu wurde im Hinblick auf Art. 27 CCC kein Bedarf gesehen.¹⁸⁶

II. VERHÄLTNIS ZU ANDEREN VORSCHRIFTEN

- 3 Art. 27 CCC bestimmt lediglich ein Verfahren für Rechtshilfeersuchen. Eingangsvoraussetzung ist die Eröffnung des in Art. 25 Abs. 1 bestimmten Anwendungsbereiches. Dieser umfasst alle Verfahren in Zusammenhang mit Computersystemen und -daten sowie die Erhebung von Beweismaterial in elektronischer Form auch für andere Straftaten.¹⁸⁷ Gerade letzteres schafft einen **weiten Anwendungsbereich**.¹⁸⁸ Mehrere partielle Verweisungen auf Art. 27 CCC enthält das Zweite Zusatzprotokoll zur CCC, nämlich in Art. 3 Abs. 2 lit. a, Art. 7 Abs. 5 lit. a, Art. 8 Abs. 8, Art. 10 Abs. 7 und Art. 11 Abs. 2 lit b. Die Schweiz hat dieses Zusatzprotokoll jedoch bislang weder unterschrieben noch ratifiziert.¹⁸⁹

184. OK-Dangubic, Art. 25 CCC N. 29; Explanatory Report, Rz. 255; Donatsch/Heimgartner/Meyer/Simonek, S. 16 f.; allgemein Ambos/König/Rackow-Meyer, 6. Teil Rz. 642.

185. Ambos/König/Rackow-Meyer, 6. Teil Rz. 642.

186. Botschaft 2010, S. 4733 ff.

187. Hierzu eingehend OK-Dangubic, Art. 25 CCC N. 4 ff.

188. Explanatory Report Rz. 253.

Art. 25 CCC regelt neben dem Anwendungsbereich die Grundsätze der 4
Rechtshilfe nach der CCC. In seinen Abs. 2 und 4 verweist er vorrangig auf die
Bestimmungen der CCC und subsidiär auf das nationale Recht, in der Schweiz
massgeblich auf das IRSG, nachrangig auf das VwVG und die StPO.¹⁹⁰ Art. 27
CCC ist in seinem Anwendungsbereich also – aus der Perspektive der CCC –
vorrangig gegenüber Normen des nationalen Rechts. Es ist eine Frage
des nationalen Rechts, inwieweit auch aus dessen Perspektive der Vorrang
besteht. Für die Schweiz kann von einem grundsätzlichen Vorrang Art. 27
CCC ausgegangen werden.¹⁹¹ Angesichts der sehr grundlegenden, primär
organisatorischen Regelungen in Art. 27 CCC ist mit Konflikten dieser
Bestimmung zum nationalen Recht ohnehin kaum zu rechnen.¹⁹² Vielmehr
schafft sie einen Mindeststandard, der einer detaillierten und weitergehenden
Regelung durch das nationale Recht nicht entgegensteht.¹⁹³

Art. 27 Abs. 1 S. 1 und 2 CCC bestimmen entsprechend der Überschrift des 5
vierten Titels – «Verfahren für Rechtshilfeersuchen **ohne anwendbare
völkerrechtliche Übereinkunft**» –, dass die Bestimmungen des Artikels für
jedes einzelne Rechtshilfeersuchen nur anwendbar sind, wenn im Verhältnis
des ersuchenden zum ersuchten Staat nicht entweder ein (bilateraler)
Rechtshilfevertrag oder eine (multilaterale) Übereinkunft in Kraft ist oder
wenn die Parteien trotz bestehender vertraglicher Rechtshilfe
übereinkommen, Art. 27 CCC ganz oder teilweise anzuwenden. Über den
Wortlaut hinausgehend dürfte ein anderes auf einen sachlichen Teilbereich
beschränktes Übereinkommen nicht genügen. Gemeint ist vielmehr ein
allgemeines Rechtshilfeübereinkommen, das auch im Anwendungsbereich des
Art. 25 Abs. 1 CCC die vertragliche (kleine) Rechtshilfe gewährleistet. Besteht
ein solcher Vertrag, ist Art. 27 CCC vorbehaltlich einer Vereinbarung zwischen
den Vertragsparteien auch nicht teilweise, etwa hinsichtlich der zusätzlichen
Ablehnungsgründe des Art. 27 Abs. 4 CCC, anwendbar. Dies verdeutlicht, dass
Art. 27 CCC lediglich einen Mindeststandard normiert, der einer
weitergehenden Bindung der Vertragsstaaten in anderen

189. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=224>.

190. Botschaft 2010, S. 4728 Fn. 171.

191. Botschaft 2010, S. 4728.

192. Grützner/Pötz/Kress/Gazeas/Brodowski-Gercke, Vorbemerkungen CCC Rz. 15; vgl. auch Explanatory Report, Rz. 262.

193. Schomburg/Lagodny-Trautmann, Art. 27 CCC Rz. 2.

Übereinkünften nicht entgegensteht.¹⁹⁴ Es handelt sich nicht um eine essenzielle Regelung der CCC wie etwa Art. 25 Abs. 4 S. 2 CCC oder Art. 29 CCC, welche nach der Systematik der Konvention nicht nachgiebig sind.

- 6 Der tatsächliche Anwendungsbereich des Art. 27 CCC ist für die Schweiz wie für viele andere Vertragsstaaten gering. Er wird zunächst durch das Europäische Übereinkommen vom 20. April 1959 über die Rechtshilfe in Strafsachen¹⁹⁵ erheblich eingeschränkt. Dieses bietet zwischen den unterzeichnenden Mitgliedstaaten des Europarates eine umfassende und verdrängende Regelung.¹⁹⁶ Hinzu treten bilaterale Rechtshilfeverträge der Schweiz, etwa mit den Vereinigten Staaten von Amerika¹⁹⁷, Kanada¹⁹⁸ oder Peru¹⁹⁹. Diese Verträge regeln umfassend die gegenseitige Rechtshilfe in Strafsachen und ordnen auch die ergänzende Geltung des Art. 27 CCC nicht an, sodass dieser keine Anwendung findet. Die Regelung ist für die Schweiz **primär im Verhältnis zu vielen afrikanischen und lateinamerikanischen Staaten sowie zwischen der Schweiz und Japan anwendbar**. Staaten ohne anwendbares Übereinkommen oder bilateralen Vertrag sind von den derzeitigen Unterzeichnerstaaten (Stand: 12.4.2025) im Einzelnen: Argentinien, Benin, Brasilien, Cabo Verde, Costa Rica, Côte d'Ivoire, die Dominikanische Republik, die Fidschi-Inseln, Ghana, Grenada, Japan, Kamerun, Kiribati, Kolumbien, Marokko, Mauritius, Nigeria, Panama, Senegal, Sierra Leone, Sri Lanka, Tonga und Tunesien. Schliesslich dürfte das Verfahren nach der CCC auch im Verhältnis zu Paraguay Anwendung finden. Insoweit besteht lediglich ein Auslieferungsvertrag,²⁰⁰ aber kein umfassender Vertrag hinsichtlich der kleinen Rechtshilfe. Hinsichtlich der Beweiserhebung und -sicherung enthalten allein die Art. 16 und Art. 17 des Vertrages Regelungen zur Zeugeneinvernahme. Zudem ist der Anwendungsbereich des

194. Vgl. Schomburg/Lagodny-Trautmann, Art. 27 CCC Rz. 1; Botschaft 2010, S. 4728 Fn. 17; Explanatory Report, Rz. 262 f.

195. SR 0.351.1.

196. Explanatory Report, Rz. 263.

197. Staatsvertrag zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen vom 25.5.1973 (SR 0.351.933.6).

198. Rechtshilfevertrag in Strafsachen zwischen der Schweiz und Kanada vom 7.10.1993 (SR 0.351.923.2).

199. Vertrag zwischen der Schweizerischen Eidgenossenschaft und der Republik Peru über Rechtshilfe in Strafsachen vom 20.4.1959 (SR 0.351.964.1).

200. Auslieferungsvertrag zwischen der Schweiz und der Republik Paraguay vom 30.6.1906 (SR 0.353.963.2).

Auslieferungsvertrages in Art. 2, auf den in den weiteren Artikeln Bezug genommen wird, auf bestimmte Katalogtaten beschränkt. Die Auflistung beinhaltet, etwa in Form des gemäss Art. 2 Nr. 18 des Vertrages erfassten Betruges, allenfalls einen geringen Anteil der nach den Art. 2 ff. CCC vorzusehenden Strafbarkeit, was schon angesichts des Abschlusses im Jahr 1906 nicht überrascht. Auch im Verhältnis der Schweiz zu Ruanda dürfte Art. 27 CCC Anwendung finden. Die insoweit nach wie vor anwendbaren Art. 13 und Art. 14 des zwischen der Schweiz und Belgien bestehenden Auslieferungsvertrages²⁰¹ enthalten nur rudimentäre Regelungen zur kleinen Rechtshilfe über diplomatische Kanäle. Der Zweck des Art. 27 CCC, in seinem Anwendungsbereich einen effektiven Mindeststandard zu gewährleisten, erfordert auch insoweit die Anwendung der weitergehenden Regelungen dieses Artikels.

Normkonflikte innerhalb der CCC wären nach den allgemeinen ⁷ Auslegungsgrundsätzen, insbesondere nach dem *lex-specialis*-Grundsatz, aufzulösen.

III. VORGABEN FÜR DIE RECHTSHILFE

A. Einrichtung von Behörden (Abs. 2)

Die im Bereich der Rechtshilfe übliche Kommunikation über zentrale ⁸ Behörden soll der ersuchenden Partei einen **zentralen Ansprechpartner** verschaffen und so der gerade hinsichtlich der Cyberkriminalität bedeutsamen Beschleunigung der internationalen Strafverfolgung dienen.²⁰² Zugleich soll die Gleichbehandlung ein- und ausgehender Anfragen sichergestellt werden. Die Kommunikation über zentrale Behörden erspart die ansonsten im Fall der vertraglosen Rechtshilfe potenziell nötige, ineffiziente Kommunikation über diplomatische Kanäle.²⁰³

Der Bundesrat hat das **Bundesamt für Justiz** als zuständige Behörde ⁹ benannt.²⁰⁴ Somit besteht für auf die CCC gestützte Rechtshilfeersuchen

201. Vertrag zwischen der Schweiz und Belgien über gegenseitige Auslieferung von Verbrechern vom 13.5.1874 (SR 0.353.917.2).

202. Grützner/Pötz/Kress/Gazeas/Brodowski-Gercke, Vorbemerkungen CCC Rz. 4; Explanatory Report, Rz. 263; vgl. auch Schomburg/Lagodny-Gless, § 73 Rz. 80; Donatsch/Heimgartner/Simonek, S. 164.

203. Explanatory Report, Rz. 263.

keine Abweichung gegenüber Art. 27 Abs. 2 IRSG. Die aktuelle Liste der zuständigen Behörden aller Vertragsstaaten kann auf der Internetseite des Europarates in englischer Sprache abgerufen werden.²⁰⁵

B. Vorgaben hinsichtlich Art und Weise der Durchführung (Abs. 3)

- 10 Abs. 3 entspricht weitgehend Art. 65 IRSG und Regelungen in bilateralen Rechtshilfeverträgen.²⁰⁶ Mit der Regelung soll sichergestellt werden, dass die im Wege der Rechtshilfe gewonnenen Beweismittel im Strafverfahren des ersuchenden Staates verwertet werden können.²⁰⁷ Das Strafprozessrecht der einzelnen Vertragsstaaten unterscheidet sich hinsichtlich der Anforderungen an die Beweiserhebung teilweise erheblich. Als Beispiel wird das generelle Erfordernis der Beeidigung von Zeugenaussagen genannt,²⁰⁸ vgl. auch Art. 65 Abs. 1 lit. a IRSG. Würde der ersuchte Staat, der ein solches Erfordernis nicht kennt, ausschliesslich sein eigenes Verfahrensrecht berücksichtigen, drohte die **Unverwertbarkeit im ersuchenden Staat** und die Rechtshilfe verfehlte ihren Zweck. Denn der ersuchte Staat wendet regelmässig sein eigenes Strafverfahrensrecht an, vgl. Art. 12 und Art. 63 Abs. 1 IRSG.
- 11 Der Grundsatz effektiver Rechtshilfe wird jedoch nicht absolut gewährleistet. Vielmehr steht die Erledigung in dem von dem ersuchenden Staat bezeichneten Verfahren unter dem Vorbehalt der **Vereinbarkeit mit dem Recht des ersuchten Staates**, vgl. auch Art. 65 Abs. 2 IRSG. Dieser kann also – unbeschadet der etwaigen Möglichkeit zur Ablehnung der Rechtshilfe insgesamt – sein eigenes Verfahrensrecht anwenden, soweit das von dem ersuchenden Staat vorgegebene Verfahren mit seinem nationalen Recht unvereinbar ist. Unter Berücksichtigung des Wortlautes der englischen («except where») und französischen («sauf lorsqu'elle») Sprachfassung sowie des bezeichneten Zwecks der Ausnahmeregelung dürfte diese sich stets nur auf einzelne Vorgaben beziehen. Der ersuchte Staat darf also nicht insgesamt sein nationales Verfahren zur Anwendung bringen, weil eine einzelne Vorgabe mit seinem Recht unvereinbar ist. Dem genannten Wortlaut, dem Grundsatz

204. Botschaft 2010, S. 4728 f.

205. Aktuell (Stand: 13.3.2024) gilt die Liste vom 16.6.2023, <https://rm.coe.int/0900001680abad5e>.

206. Botschaft 2010, S. 4729 Fn. 173, m.w.N.

207. Botschaft 2010, S. 4729; Explanatory Report, Rz. 267.

208. Explanatory Report, Rz. 267.

des Art. 25 Abs. 1 CCC und dem Rechtsgedanken des Art. 27 Abs. 6 CCC entspräche es sogar, die unvereinbare Vorgabe soweit möglich auf das noch vereinbare Mass zu reduzieren und die Wahrscheinlichkeit der Verwertbarkeit im ersuchenden Staat so zu maximieren. Eine praktische Lösung liegt in der Rücksprache über die nach Abs. 2 zuständigen Behörden.

Von grosser Bedeutung ist die Unterscheidung zwischen einer mit dem nationalen Recht **unvereinbaren** und einer in diesem **lediglich nicht vorgesehenen** Art und Weise der Durchführung, da die Ablehnung nicht allein auf letztere Tatsache gestützt werden kann.²⁰⁹ Zur Verweigerung berechtigen jedenfalls Bestimmungen von Verfassungsrang, etwa solche zur Säkularität im Verhältnis zu religiösen Beeidigungserfordernissen.²¹⁰ Umgekehrt genügt die bloss andersartige Regelung im nationalen einfachen Recht naturgemäss nicht. Hiervon müssen durch Auslegung im Einzelfall solche einfachgesetzlichen Normen unterschieden werden, die der konkreten Durchführungshandlung ausdrücklich entgegenstehen. Der entscheidende Faktor dürfte in der Frage liegen, ob in der geforderten Förmlichkeit ein zusätzlicher wesentlicher Eingriff in Individualrechte liegt, für den es an einer gesetzlichen Grundlage fehlt.

Der Intention der Vertragsstaaten dürfte eine gegenüber Art. 65 Abs. 2 IRSG engere Handhabung des Abs. 3 entsprechen.²¹¹ Dies kommt auch darin zum Ausdruck, dass das zusätzliche weite Kriterium des wesentlichen Nachteils in der CCC nicht enthalten ist. Zudem bestimmt insbesondere Art. 25 CCC auch im Übrigen ein strengeres Rechtshilferegime für den besonders stark internationalisierten Bereich der Cyberkriminalität.²¹²

Zugleich zeigt der Vergleich zu Abs. 4 lit. a, dass die Reduktion auf einen reinen *ordre-public*-Vorbehalt für die eingeschränkte Ablehnungsbefugnis nach Abs. 3 nicht gewollt ist. Der Vorbehalt ist insofern zwischen der weiten Regelung des Art. 65 Abs. 2 IRSG und einem reinen *ordre-public*-Prinzip einzuordnen, wie es etwa auch in § 73 S. 1 des deutschen IRG²¹³ enthalten ist. Dementsprechend kann und muss ein Ersuchen abgelehnt werden, wenn zu

209. Explanatory Report, Rz. 267; Schomburg/Lagodny-Trautmann, Art. 27 CCC Rz. 4.

210. Vgl. hierzu auch Art. 27 Verordnung über internationale Rechtshilfe mit Strafsachen vom 24.2.1982 (IRSV; SR 351.11).

211. Explanatory Report, Rz. 267.

212. Vgl. Grützner/Pötz/Kress/Gazeas/Brodowski-Gercke, Vorbemerkungen CCC Rz. 4.

213. Gesetz über die internationale Rechtshilfe in Strafsachen vom 23.12.1982.

seiner Erledigung **wesentliche Eingriffe in Individualrechte** ohne gesetzliche Grundlage und entgegen der gesetzgeberischen Güterabwägung erfolgen müssten.

- 15 Soweit das nationale Verfahrensrecht **weitergehende Anforderungen** an die durchzuführende Massnahme stellt, sind diese durch die ausführenden Behörden des ersuchten Staates grundsätzlich einzuhalten, vgl. auch Art. 12 Abs. 1 IRSG.

C. Einwände gegen die Durchführung

1. Zusätzliche Ablehnungsgründe (Abs. 4)

- 16 Im Verfahren nach Art. 27 CCC gilt zunächst Art. 25 Abs. 4 CCC. Auch insoweit greift also der Verweis auf die Ablehnungsgründe des nationalen Rechts oder eines anwendbaren Rechtshilfevertrages ein, wobei die Ablehnung *allein* aufgrund der Einordnung als fiskalische Straftat unzulässig ist.²¹⁴ Art. 27 Abs. 4 CCC nimmt auf Art. 25 Abs. 4 CCC Bezug und bestimmt zwei ergänzende Ablehnungsgründe: die Verfolgung **politischer Straftaten** und den *ordre-public-Grundsatz*. Auf diese Ablehnungsgründe kann sich der ersuchte Staat also auch dann berufen, wenn das nationale Recht sie nicht vorsieht. Im Fall einer anwendbaren völkerrechtlichen Übereinkunft gelangt Art. 27 CCC hingegen gemäss seinem Abs. 1 grundsätzlich nicht zur Anwendung.
- 17 Vor dem Hintergrund der Systematik der CCC, nach der im Fall des Art. 27 CCC regelmässig die Ablehnungsgründe des nationalen Rechts eingreifen, wird auf den ersten Blick nicht gänzlich klar, welchen praktischen Mehrwert die zusätzlichen Ablehnungsgründe bieten. Ein Staat, der in seinem nationalen Recht diese Schranken nicht vorsieht, wird sich regelmässig auch im Verfahren nach der CCC nicht darauf berufen, denn die Ablehnung nach Abs. 4 steht im Ermessen des ersuchten Staates. Die Bedeutung dürfte daraus folgen, dass sich die Staaten in Anwendung des Gebotes grösstmöglicher Rechtshilfe darauf verständigt haben, im Anwendungsbereich der CCC von den Ablehnungsgründen nach nationalem Recht, die in Abs. 4 nicht genannt werden, nur in Ausnahmefällen Gebrauch zu machen.²¹⁵ Abs. 4 entfaltet vor

214. Botschaft 2010, S. 4728 Fn. 171.

215. Explanatory Report, Rz. 269.

diesem Hintergrund **klarstellende und symbolische Wirkung**. Die Regelung zeigt auf, dass die genannten Ablehnungsgründe als Ausfluss der nationalen Weltanschauung jedenfalls valide bleiben. Die Verständigung auf die Nichtanwendung sonstiger Ablehnungsgründe im Regelfall dürfte jedoch primär politisch bindend sein, auch weil sie in den Text des Übereinkommens nicht aufgenommen wurde.

Für die Schweiz dürfte neben dem IRSG allenfalls ein **geringer Anwendungsbereich** für die zusätzlichen Ablehnungsgründe in unmittelbarer Anwendung des Abs. 4 bestehen. Bei politischen Straftaten greift der Ablehnungsgrund des Art. 3 Abs. 1 IRSG. Es ist davon auszugehen, dass auch Art. 27 Abs. 4 lit. a CCC sowohl absolute als auch relative politische Delikte umfasst.²¹⁶ Angesichts der zurückhaltenden und weiträumig auf das nationale Recht verweisenden Regelung in der CCC sowie der subjektiven und zwischen den Staaten abweichenden Einordnung einer Tat als politisch oder nicht politisch²¹⁷ sollte keine autonome Auslegung erfolgen. Vielmehr ist die Ausgestaltung des Ablehnungsgrundes – vorbehaltlich eines Rechtsmissbrauchs – dem jeweils ersuchten Staat zu überlassen. Im Fall eines Ausschlusses gemäss Art. 3 Abs. 2 IRSG ist auch mit der Verweigerung nach Art. 27 Abs. 4 lit. a CCC nicht zu rechnen.

Der *ordre-public*-Vorbehalt kommt in Art. 2 IRSG teilweise zum Ausdruck. Als allgemeiner völkerrechtlicher Grundsatz und in Ansehung der verfassungskonformen Auslegung des IRSG, insbesondere der Generalklausel des Art. 2 lit. d IRSG, ist auch im Übrigen von der Geltung bereits nach nationalem Recht auszugehen. Art. 27 Abs. 4 lit. b CCC vereinfacht insoweit allenfalls die Begründung der Ablehnung. Unter den *ordre-public*-Vorbehalt fällt auch die fehlende Gewährleistung elementarer Datenschutzstandards, wobei hohe Anforderungen zu stellen sind.²¹⁸ Vorrangig dürfte die Rechtshilfe unter die Bedingung einer entsprechenden Zusicherung zu stellen sein.²¹⁹

2. Aufschieben der Rechtshilfe (Abs. 5)

Abs. 5 erlaubt es dem ersuchten Staat, d.h. der zuständigen Behörde, die Erledigung des Rechtshilfeersuchens aufzuschieben und somit von dem

216. Hierzu Schomburg/Lagodny-Gless, § 73 Rz. 97.

217. Schomburg/Lagodny-Gless, § 73 Rz. 96.

218. Explanatory Report, Rz. 269; Schomburg/Lagodny-Trautmann, Art. 27 CCC Rz. 6.

219. Schomburg/Lagodny-Trautmann, Art. 27 CCC Rz. 6.

Gebot der zügigen Erledigung abzuweichen, welches in Art. 25 Abs. 1 CCC, der Präambel des Übereinkommens sowie der Möglichkeit eines Eilverfahrens nach Art. 27 Abs. 9 CCC zum Ausdruck kommt. Im Umkehrschluss folgt hieraus, dass bei Nichtvorliegen der Voraussetzungen des Abs. 5 das Ersuchen innert nützlicher Frist zu erledigen ist. Da es sich um ein milderes Mittel zur Ablehnung handelt,²²⁰ gibt es keine feste Höchstdauer. Vielmehr kann die Erledigung des Ersuchens so lange aufgeschoben werden, wie die Voraussetzungen des Abs. 5 vorliegen.

- 21 Voraussetzung für das Aufschieben ist die Gefahr, dass bei sofortiger Erledigung eigene strafrechtliche Ermittlungen oder Verfahren des ersuchten Staates beeinträchtigt würden. Als Beeinträchtigung wird nicht nur die Vereitelung der Ermittlung, etwa bei längerfristiger verdeckter Ermittlung durch den ersuchenden Staat, eingestuft. Zur Ablehnung berechtigt vielmehr bereits die anderenfalls zu erwartende **Verzögerung einer unmittelbar bevorstehenden Beweiserhebung** durch Herausgabe des Beweismittels an den ersuchenden Staat.²²¹ Dennoch ist im Interesse umfassender und zügiger Rechtshilfe von der Möglichkeit des Abs. 5 nur zurückhaltend Gebrauch zu machen.²²²
- 22 Nach der Systematik des Art. 27 CCC stehen **Ablehnung und Aufschieben** wegen ihrer unterschiedlichen Voraussetzungen und Rechtsfolgen selbständig nebeneinander, sodass die Entscheidung über eine Ablehnung bis zum Ende des Zeitraums nach Abs. 5 hinausgezögert werden könnte. Eine Gesamtbetrachtung muss jedoch jedenfalls bei der Entscheidung nach Abs. 6 erfolgen und dürfte auch im Übrigen dem Gebot effektiver Rechtshilfe entsprechen.²²³

3. Bedingung als Minus zur Ablehnung und Aufschieben (Abs. 6)

- 23 Abs. 6 verwirklicht den Grundsatz der effektiven und umfassenden Rechtshilfe gemäss Art. 25 Abs. 1 CCC. Der ersuchende Staat soll nicht gezwungen sein, detailliert Haupt- und Hilfsanträge auszuarbeiten. Vielmehr obliegt es dem ersuchten Staat, **dem Ersuchen so weit wie möglich zu entsprechen und bei Bedenken den ersuchenden Staat zu konsultieren.**

220. Explanatory Report, Rz. 270.

221. Botschaft 2010, S. 4729 Fn. 177; Explanatory Report, Rz. 270.

222. Schomburg/Lagodny-Trautmann, Art. 27 CCC Rz. 7.

223. Vgl. auch Explanatory Report, Rz. 270.

Hieraus folgt zunächst die Beschränkung der Einwände auf abtrennbare Teile des Ersuchens, soweit dies möglich ist. Der nicht betroffene Teil ist dann unverzüglich zu erledigen. Als zweite Möglichkeit, die zeitnahe Erledigung zu gewährleisten, nennt Abs. 6 die Erledigung unter Bedingungen. Diese Bedingungen betreffen primär die Verwendung der übergebenen Beweismittel im ersuchenden Staat. Vor der Herausgabe werden entsprechende Zusicherungen eingeholt.²²⁴ Häufig ist etwa die Bedingung, dass das Beweismittel nur für das vorliegende Verfahren und nicht darüber hinaus für weitere Verfahren verwendet werden darf.²²⁵ Soweit demgegenüber Bedenken gegen die Rechtmässigkeit der Erledigung im ersuchenden Staat bestehen, ist im Rahmen der Konsultation auf eine Anpassung des Ersuchens hinzuwirken. Erfolgt eine solche nicht, ist das Ersuchen ganz oder teilweise abzulehnen oder nach Abs. 3 zu verfahren. Auch von den Rechten des ersuchten Staates nach Abs. 6 soll im Interesse effektiver Rechtshilfe nur zurückhaltend Gebrauch gemacht werden.²²⁶

D. Mitteilungspflichten (Abs. 7)

Abs. 7 enthält Mitteilungspflichten hinsichtlich der Ergebnisse der Erledigung 24 und der Gründe einer Ablehnung oder eines Aufschiebens. Dies dient der Information des ersuchenden Staates, damit dieser **zukünftige Ersuchen** an denselben Staat zielführender gestalten kann.²²⁷ Eine separate Mitteilung über die Gründe für eine Bedingung ist nicht erforderlich. Offenbar wird davon ausgegangen, dass die Gründe entweder aus der Bedingung selbst hinreichend ersichtlich werden oder dass sie im Rahmen einer Konsultation nach Abs. 6 mit dem ersuchenden Staat erörtert werden.

E. Vertraulichkeit (Abs. 8)

Abs. 8 erlaubt über Abs. 3 hinausgehend eine Vorgabe für die Erledigung des 25 Ersuchens, die nicht der Verwertbarkeit im ersuchenden Staat, sondern sonstigen **ermittlungstaktischen oder politischen Interessen** dient. Der Wortlaut «soweit die Erledigung des Ersuchens nichts anderes gebietet» in der deutschen Übersetzung ist missverständlich: Aus der englischen («except to

224. Vgl. Ambos/König/Rackow-Meyer, 6. Teil Rz. 679.

225. Etwa BGer 1A.253/2002 vom 28.1.2003.

226. Explanatory Report, Rz. 271.

227. Explanatory Report, Rz. 272.

the extent necessary») und französischen («sauf dans la mesure nécessaire») Sprachfassung geht hervor, dass dieser Halbsatz den Begriff der Vertraulichkeit ausgestaltet und nicht die Möglichkeit eines Vorgehens nach Abs. 8 prinzipiell beschränkt. Vertraulich im Sinne des Abs. 8 ist insbesondere auch eine Massnahme, die dem Betroffenen, etwa der Bank des Beschuldigten, notwendig bekannt wird.

- 26 Angesichts des restriktiven Wortlautes und des Gebotes möglichst umfassender Rechtshilfe können jedenfalls strukturelle tatsächliche Defizite nicht zur Begründung des Unvermögens herangezogen werden, etwa Probleme mit Korruption innerhalb der zuständigen Behörden. Der Ausnahmetatbestand dürfte vielmehr entsprechend Abs. 3 Halbs. 2 auszulegen sein und somit **rechtliche Hindernisse** betreffen. Der Vertraulichkeit kann also dann nicht entsprochen werden, wenn die ersuchensgegenständlichen Massnahmen einschliesslich der Tatsache, dass ihnen ein Rechtshilfeersuchen zugrunde liegt, nach zwingendem nationalen Recht offengelegt werden müssen.²²⁸
- 27 Das Interesse des ersuchenden Staates ist meist darauf gerichtet, die Kenntnisnahme durch den **Beschuldigten** zu verhindern. Gleiches gilt für den von der Massnahme **Betroffenen**, sofern dieser dem Beschuldigten nahesteht und die Massnahme grundsätzlich heimlich erfolgen kann. Die Vertraulichkeit ist insofern jedenfalls dann nicht gewährleistet, wenn eine direkte Bekanntgabe an den Beschuldigten erfolgt oder wenn die Information durch den Betroffenen zu erwarten ist. Weiterhin ist die Vertraulichkeit naturgemäss dann nicht gewährleistet, wenn die Tatsache, dass ein Ersuchen gestellt wurde, oder der Inhalt dieses Ersuchens der Öffentlichkeit, d.h. einer unbestimmten Vielzahl von Personen, die nicht durch besondere Eigenschaften miteinander verbunden sind, bekannt wird.
- 28 Dies steht in einem Spannungsverhältnis zu dem Recht des von der Massnahme Betroffenen auf **effektiven Rechtsschutz**: Werden die Ergebnisse der Massnahme an einen ausländischen Staat übermittelt, der an das Schweizer Recht nicht gebunden ist, können die Folgen eines Verstosses gegen das IRSG nicht mehr beseitigt werden. Die Menschenrechte des Beschuldigten und des Betroffenen sind mit den legitimen Vertraulichkeitsinteressen des ersuchenden Staates in Einklang zu bringen.

228. Botschaft 2010, S. 4730 Fn. 178; Explanatory Report, Rz. 273.

Der Interessenausgleich durch das IRSG ist als tendenziell betroffenenfreundlich einzustufen.

Art. 80m IRSG regelt die Zustellung der Verfügungen der ausführenden 29 Behörde und setzt somit die **Eröffnung sowohl der Eintretens- als auch der Schlussverfügung** sowie etwaiger Zwischenverfügungen voraus. Der Zeitpunkt der Zustellung wird dabei nicht geregelt. Umgekehrt sieht Art. 63 Abs. 2 IRSG Massnahmen der kleinen Rechtshilfe vor, die durch eine vorherige Ankündigung vereitelt würden. Dies betrifft namentlich die Durchsuchung von Personen und Räumen. Zudem ist Gegenstand des Rechtsschutzes und somit vorrangiger Anknüpfungspunkt des rechtlichen Gehörs gemäss Art. 12 IRSG i.V.m. 29 VwVG²²⁹ nicht die Eintretens-, sondern gemäss Art. 80e Abs. 1 IRSG²³⁰ die Schlussverfügung.²³¹ Die Eröffnung der Eintretensverfügung an den Betroffenen erst zusammen mit der Schlussverfügung ist daher zulässig.²³²

Hierdurch wird für Massnahmen, die nicht ihrer Natur nach dem Betroffenen 30 bekannt werden – wie etwa die Einvernahme –, die Vertraulichkeit hinsichtlich Vorliegens und Inhalts des Ersuchens zeitweise gewährleistet. Vor der Übermittlung der Ergebnisse der Massnahme an den ersuchenden Staat ist jedoch gemäss Art. 80d i.V.m. 80l Abs. 1 IRSG die **Rechtskraft der Schlussverfügung** abzuwarten. Eine vorzeitige Übermittlung, welche die Vertraulichkeit gegenüber dem Betroffenen längerfristig wahrt, ist nur unter den überaus engen Voraussetzungen des Art. 80d^{bis} IRSG möglich, welcher insbesondere einen Fall der organisierten Kriminalität oder des Terrorismus voraussetzt. In diesem Fall wird die Mitteilung an die betroffene Person gemäss Art. 80d^{bis} Abs. 5 IRSG aufgeschoben, muss aber nachgängig erfolgen. Eine vollständige Vertraulichkeit gegenüber dem Betroffenen über das Bestehen eines Ersuchens kann somit in keinem Fall gewährleistet werden.

Erfährt der Betroffene – durch die Eröffnung einer Verfügung oder 31 anderweitig – von der Massnahme, stehen ihm²³³ die Rechte des Art. 80b

229. Zur menschen- und verfassungsrechtlichen Fundierung des Anspruchs auf rechtliches Gehör im Rechtshilfeverfahren Donatsch/Heimgartner/Simonek, S. 159.

230. Ausführlich zum Rechtsschutz Donatsch/Heimgartner/Simonek, S. 166 ff.

231. BStGer RR.2008.252 vom 16.2.2009; Popp, § 17 Rz. 461.

232. Vgl. nur BStGer RR.2021.43 vom 25.4.2022.

233. Und nicht dem abweichenden Beschuldigten, OK-Dangubic/Stelzer-Wieckowska, Art. 80b IRSG N. 9.

Abs. 1 IRSG zu, nämlich das **Akteneinsichtsrecht** und das Recht auf **Teilnahme an Durchführungshandlungen**.²³⁴ Dadurch wird die Vertraulichkeit hinsichtlich des Inhalts des Rechtshilfeersuchens gefährdet. Insoweit bieten Art. 80b Abs. 2 lit. a und b IRSG jedoch die weitgehende Möglichkeit, der Bitte um Vertraulichkeit hinsichtlich des Inhalts des Ersuchens zu entsprechen.²³⁵

- 32 Der Betroffene ist zudem gemäss Art. 80n Abs. 1 IRSG grundsätzlich berechtigt, seinen Mandanten oder Kunden, regelmässig den Beschuldigten, über die Rechtshilfemassnahme zu **informieren**. Die Vertraulichkeit kann dann auch diesem gegenüber nicht mehr gewährleistet werden. Art. 80n Abs. 1 Halbs. 2 IRSG erlaubt es der zuständigen Behörde jedoch, die Information des Mandanten oder Kunden strafbewehrt zu untersagen, was etwa bei Editionsverfügungen gegenüber Banken teilweise erfolgt (Art. 73 Abs. 2 StPO i.V.m. Art. 292 StGB).²³⁶ So wird die Vertraulichkeit zumindest aus rechtlicher Perspektive sichergestellt.
- 33 Die Vertraulichkeit kann insofern nach verschiedenen Einzelregelungen in Teilaspekten gewährleistet werden. Eine allgemeine Regelung, die die vertrauliche Erledigung von Rechtshilfeersuchen mit gleicher Effektivität wie bei inländischen Massnahmen erlaubt, existiert demgegenüber nicht. Ob dies dem **Anpassungsauftrag des Art. 25 Abs. 2 CCC** in jedem Fall genügt, ist fraglich.²³⁷
- 34 S. 2 belässt dem ersuchenden Staat die Entscheidungshoheit über die nicht vertrauliche Erledigung, wenn der ersuchte Staat der Vertraulichkeit nicht entsprechen kann.

F. «Beschleunigtes Verfahren» (Abs. 9)

- 35 Abs. 9 sieht für «dringende Fälle» die Weiterleitung von Ersuchen ohne unmittelbare Beteiligung der zentralen Behörden gemäss Abs. 2 vor. Die Kommunikation verläuft entweder direkt zwischen den ausführenden Behörden (lit. a und d) oder über Interpol (lit. b). Die Schweiz hat jedoch von

234. Zu letzterem Popp, § 17 Rn. 465.

235. BSK-Heimgartner/Niggli, Art. 80b IRSG N. 14 ff.; OK-Dangubic/Stelzer-Wieckowska, Art. 80b IRSG N. 37 ff.

236. BGE 130 II 505; BGE 136 IV 16.

237. So aber Botschaft 2010, S. 4733 ff.

der in lit. e vorgesehenen Möglichkeit Gebrauch gemacht und bestimmt, dass eingehende Ersuchen – entsprechend dem Wortlaut des Übereinkommens «aus Gründen der Effizienz» – **ausschliesslich an die zentrale Behörde**, das Bundesamt für Justiz, zu richten sind. Damit werden die ausführenden Behörden in der Schweiz von der sofortigen Bearbeitung eingehender Ersuchen entlastet.²³⁸ Für ersuchende ausländische Staaten tritt eine Vereinfachung (nur) insofern ein, als sie nicht über ihre zentrale Behörde kommunizieren müssen. Vielmehr kann eine nachgeordnete ausländische Behörde ein Ersuchen an das Bundesamt für Justiz richten oder das Ersuchen kann diesem über Interpol zugeleitet werden.²³⁹

Zweck des Art. 27 CCC ist es, zwischen den Vertragsstaaten ein über die 36 vertraglose Rechtshilfe hinausgehendes Minimalverfahren zu etablieren. Keinesfalls soll der ersuchende Staat schlechter gestellt werden als bei einem Vorgehen nach dem nationalen IRSG. Ersuchen nach Art. 27 CCC können daher auch auf den **Kommunikationswegen des Art. 29 IRSG** erfolgen. Dies beinhaltet ein Vorgehen nach Art. 29 Abs. 2 Alt. 2 IRSG, nach dem das Ersuchen zwar nicht direkt an die nachgeordnete Behörde gerichtet, dieser aber zumindest zeitgleich mit dem Ersuchen an das Bundesamt für Justiz ein Doppel zugestellt werden kann.

Abs. 9 lit. e enthält **keinen Gegenseitigkeitsvorbehalt**. Nachgeordnete 37 Schweizer Behörden können also nach der CCC ausgehende Ersuchen unmittelbar an nachgeordnete Behörden anderer Staaten übermitteln, soweit diese Staaten nicht ihrerseits eine Erklärung nach Abs. 9 lit. e abgegeben haben. Dem üblichen Vorgehen in der Schweiz entspricht dies (vorbehältlich im Geltungsbereich staatsvertraglicher Regelungen) jedoch nicht.²⁴⁰

IV. RECHTSSCHUTZ

Für den Bürger, der von den ersuchensgegenständlichen Massnahmen 38 betroffen ist, richten sich die Rechtsschutzmöglichkeiten gemäss Art. 25 Abs. 4 CCC nach dem **nationalen Recht des ersuchten Staates**. Wird die Schweiz ersucht, ist also gemäss Art. 21 IRSG unter Umständen ein

238. Für das Bundesamt für Justiz entsteht demgegenüber ein zusätzlicher Aufwand, Botschaft 2010, S. 4743.

239. Botschaft 2010, S. 4730.

240. Vgl. Ambos/König/Rackow-Meyer, 6. Teil Rz. 643.

Rechtsbeistand zu bestellen und es besteht gegen die Schlussverfügung die Beschwerdemöglichkeit gemäss Art. 80e IRSG.²⁴¹ Ersucht die Schweiz einen anderen Staat um Rechtshilfe, richtet sich der Rechtsschutz gegen die Massnahmen als solche nach dem dortigen Verfahrensrecht. Gegen das schweizerische Ersuchen ist die Beschwerde für den Betroffenen nur unter den Voraussetzungen des Art. 25 Abs. 2 IRSG möglich, welche im Anwendungsbereich des Art. 27 CCC nicht vorliegen werden.

- 39 Zwischen ersuchendem und ersuchtem Staat ist Art. 27 CCC verbindlich und schafft bei Vorliegen der Voraussetzungen eine **Pflicht zur Erledigung des Rechtshilfeersuchens**. Die Durchsetzung erfolgt nach Massgabe des Art. 45 CCC, der vorrangig eine Lösung auf diplomatischer Ebene und subsidiär die Entscheidung durch einen zwischen den jeweiligen Parteien festzulegenden Spruchkörper vorsieht, nämlich durch das European Committee on Crime Problems (CDPC), ein Schiedsgericht oder den Internationalen Gerichtshof.

LITERATURVERZEICHNIS

Dangubic Miro, Kommentierung zu Art. 25 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter <https://onlinekommentar.ch/de/kommentare/ccc25>, besucht am 5.4.2024.

Dangubic Miro/Stelzer-Wieckowska Marta, Kommentierung zu Art. 80b IRSG, in: Staffler Lukas/Glassey Maria Ludwiczak (Hrsg.), Onlinekommentar zum Bundesgesetz über internationale Rechtshilfe in Strafsachen, abrufbar unter <https://onlinekommentar.ch/de/kommentare/irsg80b>, besucht am 27.2.2025.

Donatsch Andreas/Heimgartner Stefan/Simonek Madeleine, Internationale Rechtshilfe, 3. Aufl., Zürich 2024.

Gercke Marco, Kommentierung zum Übereinkommen über die Cyberkriminalität, in: Grützner Heinrich/Pötz Paul-Günther/Kress Claus/Gazeas Nikolaos/Brodowski Dominik, Internationaler Rechtshilfeverkehr in Strafsachen, 3. Aufl., Heidelberg 2022 (zit. Grützner/Pötz/Kress/Gazeas/Brodowski-Gercke).

241. Ambos/König/Rackow-Meyer, 6. Teil Rz. 648.

Gless Sabine, Überblick über die Rechtshilfe in Strafsachen, in: Schomburg Wolfgang/Lagodny Otto, Internationale Rechtshilfe in Strafsachen, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Gless).

Heimgartner Stefan/Niggli Marcel Alexander, Kommentierung zu Art. 80b IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan, Basler Kommentar Internationales Strafrecht, Basel 2015 (zit. BSK-Heimgartner/Niggli).

Meyer Frank, Ergänzende Kommentierung Schweiz, in: Ambos Kai/König Stefan/Rackow Peter, Rechtshilfe in Strafsachen, 2. Aufl., Baden-Baden 2020 (zit. Ambos/König/Rackow-Meyer).

Popp Peter, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel 2001.

Trautmann Sebastian, Kommentierung zu Art. 27 CCC, in: Schomburg Wolfgang/Lagodny Otto, Internationale Rechtshilfe in Strafsachen, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Trautmann).

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.admin.ch/opc/de/federal-gazette/2010/4697.pdf>, besucht am 5.4.2024 (zit. Botschaft 2010).

Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23.XI.2001, abrufbar unter <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>, besucht am 5.4.2024 (zit. Explanatory Report).

KOMMENTIERUNG ZU

Art. 28 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Julian Mausbach

ZITIERVORSCHLAG

Julian Mausbach, Kommentierung zu Art. 28 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Mausbach, Art. 28 CCC N. XXX.

Art. 28 Vertraulichkeit und Beschränkung der Verwendung

¹ Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so findet dieser Artikel Anwendung. Liegen ein solcher Vertrag, eine solche Übereinkunft oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung, wenn die betreffenden Vertragsparteien übereinkommen, an Stelle des Vertrags, der Übereinkunft oder der Rechtsvorschriften die Absätze 2–4 ganz oder teilweise anzuwenden.

² Die ersuchte Vertragspartei kann die Überlassung von Informationen oder Unterlagen in Erledigung eines Ersuchens von der Bedingung abhängig machen, dass sie:

a. vertraulich behandelt werden, wenn das Rechtshilfeersuchen ohne diese Bedingung nicht erledigt werden könnte; oder

b. nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet werden.

³ Kann die ersuchende Vertragspartei einer Bedingung nach Absatz 2 nicht entsprechen, so setzt sie die andere Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob die Informationen dennoch zur Verfügung gestellt werden sollen. Nimmt die ersuchende Vertragspartei die Bedingung an, so ist sie daran gebunden.

⁴ Jede Vertragspartei, die Informationen oder Unterlagen unter einer in Absatz 2 genannten Bedingung zur Verfügung stellt, kann von der anderen Vertragspartei verlangen, dass sie in Zusammenhang mit dieser Bedingung Angaben über die Verwendung der Informationen oder Unterlagen macht.

GLIEDERUNG

I. Ausrichtung.....	240
II. Anwendungsbereich (Art. 28 Abs. 1)	241
III. Beschränkende Bedingungen (Art. 28 Abs. 2).....	242
IV. Unmöglichkeit der Bedingungsentsprechung (Art. 28 Abs. 3).....	244
V. Verwendungsinformation (Art. 28 Abs. 4)	244
Materialienverzeichnis.....	245

I. AUSRICHTUNG

- 1 Art. 28 bezweckt die Sicherstellung der Rechtshilfe bei gleichzeitiger Gewährung von **Beschränkungen für die Verwendung von Informationen oder Material**. Auf diese Weise wird die ersuchte Partei in dies Lage versetzt, besonders sensible Informationen oder besonders sensibles Material nur geschützt zur Verfügung zu stellen. Dieser Schutz kann sich darin erstrecken, dass die Informationen nur für den Zweck verwendet werden dürfen, für den die Unterstützung gewährt wird, oder der Empfängerkreis definiert wird, indem die zur Verfügung gestellten Informationen oder Materialien nicht über die Strafverfolgungsbehörden der ersuchenden Partei hinaus verbreitet werden dürfen. In diesem Sinne ist Art. 28 von seiner Ausrichtung her als klassisch vermittelnde Norm zu verstehen, die zum einen dem Grundzweck der Rechtshilfe und zum anderem den berechtigten Interessen am (Daten-)Schutz der gegenständlichen Informationen und Materialien verpflichtet ist.
- 2 Der vermittelnde Ansatz wird dabei dadurch sichergestellt, dass in Art. 28 eine **Vertraulichkeitspflicht** zu lesen ist. Danach muss die empfangende Behörde Informationen, die sie von einem anderen Staat erhalten haben, vertraulich behandeln. Dies bedeutet, dass die Informationen nicht öffentlich gemacht oder an unbefugte Dritte weitergegeben werden dürfen.
- 3 Des Weiteren besteht der **Grundsatz der zweckgebundenen Nutzung**. Diesem folgend, darf der empfangende Staat die Informationen nur für die Zwecke verwenden, für die sie ursprünglich übermittelt wurden. Das bedeutet, dass Informationen nicht ohne Zustimmung des übermittelnden Staates für andere Zwecke oder in anderen Verfahren verwendet werden dürfen.
- 4 Ergänzt wird dies wiederum dadurch, dass **Ausnahmen von der Zweckbindung** ihrerseits wiederum der Zustimmung bedürfen. Beabsichtigt der empfangende Staat die Informationen für andere Zwecke als jene, die von der Zweckbindung erfasst sind, zu nutzen, ist er darauf angewiesen, dass der übermittelnde Staat dieser Zweckerweiterung zustimmt. Es kommt mithin zu einer Sicherstellung, dass die Kontrolle über die Verwendung der

Informationen in der Hand des Staates verbleibt, der sie ursprünglich bereitgestellt hat.

Art. 28 kann damit als ein zentraler Bestandteil der internationalen 5 Zusammenarbeit zur Bekämpfung der Cyberkriminalität verstanden werden. Er sichert, dass Informationen, die zwischen Staaten ausgetauscht werden, vertraulich behandelt und nur für den vorgesehenen Zweck genutzt werden. Art. 28 schafft mithin eine Basis für den vertrauensvollen internationalen Informationsaustausch und unterstützt die Einhaltung nationaler und internationaler Datenschutzrichtlinien.

II. ANWENDUNGSBEREICH (ART. 28 ABS. 1)

Art. 28 findet nur Anwendung, wenn **kein Rechtshilfevertrag** oder eine 6 Vereinbarung auf der Grundlage einheitlicher oder gegenseitiger Rechtsvorschriften zwischen der ersuchenden und der ersuchten Partei besteht. Die bestehenden Übereinkommen und Rechtshilfeverträgen, mit Blick auf die Beweiserhebung namentlich das Übereinkommen vom 8. November 1990 über Geldwäscherei sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten, das Europäische Übereinkommen vom 20. April 1959 über die Rechtshilfe in Strafsachen oder das Zweite Zusatzprotokolls vom 8. November 2001 zum Europäischen Übereinkommen über die Rechtshilfe in Strafsachen sind mit Blick auf Abs. 1 zu beachten und führen dazu, dass Art. 28 für nicht wenige Rechtshilfeverfahren von diesen verdrängt wird.

Sofern ein solcher Vertrag oder eine solche Vereinbarung in Kraft ist, so gelten 7 deren Bestimmungen über Vertraulichkeit und Verwendungsbeschränkungen anstelle von Art. 28. Dies jedenfalls, sofern die Parteien nicht ausdrücklich die Anwendung von Art. 28 Abs. 2 bis 4 vereinbart haben. Für die Mehrzahl der Rechtshilfeverfahren mit Beteiligung der Schweizer Behörden ist dabei davon auszugehen, dass die Rechtshilfe im Sinne von Abs. 1 nach den entsprechenden Übereinkommen und Rechtshilfeverträgen abgewickelt wird.

Ob und in welcher Weise ansonsten eine Vereinbarung zwischen der Schweiz 8 und anderen Staaten nicht an den genannten Rechtshilfevereinbarungen beteiligten Staaten gegeben ist, die die Anwendbarkeit von Art. 28 ausschliesst, eigene Vertraulichkeitsregelungen aufstellt oder doch auf Art. 28 Abs. 2 bis Abs. 4 rekurriert, ist ansonsten anhand jeweils länderspezifisch zu

prüfen. Die seitens des Bundesamtes für Justiz vorgehaltenen Liste bilateraler und multilateraler Verträge im Bereich der internationalen Rechtshilfe in Strafsachen bietet sich hierzu an.²⁴²

- 9 Sofern eine Regelung zwischen den Parteien vorhanden ist, gilt ausschliesslich diese. Überschneidungen mit anderen bestehenden bilateralen und multilateralen Rechtshilfeverträgen und ähnlichen Vereinbarungen werden auf diese Weise durch die klare Vorgabe des Abs. 1 vermieden, so dass sich die Zuständigen in der Praxis an die übliche Regelung halten können und es keiner Auseinandersetzung zum Verhältnis konkurrierender oder gar widersprüchliche Übereinkünfte bedarf.²⁴³

III. BESCHRÄNKENDE BEDINGUNGEN (ART. 28 ABS. 2)

- 10 Abs. 2 gestattet der ersuchten Vertragspartei zwei Arten von Bedingungen zu stellen. Sie kann zunächst die Informationen oder Unterlagen unter der Bedingung zur Verfügung stellen, dass diese **vertraulich** bleiben, wenn und sofern dem Ersuchen ansonsten nicht entsprochen werden kann (lit. a; vergleichbar mit der vertraulich zu behandelnden Identität eines Informanten).²⁴⁴
- 11 Des Weiteren kann die Bedingung aufgestellt werden, dass die übermittelten Informationen oder Unterlagen **nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet** werden dürfen (lit. b).
- 12 Die Beschränkung der Verwendung der übermittelten Informationen und Unterlagen muss dabei von der ersuchten Vertragspartei ausdrücklich verlangt werden. Dies muss in gleicher Weise im Übrigen auch für die Bedingung des vertraulichen Behandeln gelten, wie sich bereits aus dem Wortlaut der Norm ergibt, wenn dieser davon spricht, dass die Übersendung von einer Bedingung abhängig gemacht wird und damit eine Aktivität der ersuchten Partei erwartet wird.

242. Abrufbar unter: <https://www.bj.admin.ch/bj/de/home/sicherheit/rechtshilfe/strafsachen/rechtsgrundlagen.html>, zuletzt aufgerufen am 19.2.2025.

243. Siehe hierzu Explanatory Report, Ziff. 276.

244. Siehe hierzu Explanatory Report, Ziff. 277.

Kommt es daher nicht zu einer ausdrücklichen Erklärung der Bedingung, 13 besteht für die ersuchende Partei keine solche Beschränkung.

Insbesondere mit der zweiten Bedingung wird der in Artikel 67 IRSG 14 verankerte Grundsatz der Spezialität, welcher in der Praxis von zentraler Bedeutung ist, auch in Art. 28 abgebildet. Nach diesem Grundsatz dürfen übermittelte Schriftstücke und Auskünfte im ersuchenden Staat in Verfahren wegen Taten, in denen Rechtshilfe nicht zulässig ist, weder für Ermittlungen benutzt noch als Beweismittel verwendet werden. Dieses Verbot erstreckt sich in der Schweiz auch und insbesondere auf Taten, die nach schweizerischer Auffassung politischen, militärischen oder fiskalischen Charakter haben.²⁴⁵

Im Rahmen der Verhandlungen zur Cybercrime Convention wurden **zwei** 15 **Ausnahmen** von der Möglichkeit, die Verwendung einzuschränken, anerkannt. Diese sind daher implizit in den Bestimmungen des Absatzes enthalten und in diesem Sinne ihrerseits beschränkend, als diese Ausnahmen eine Verwendungsbeschränkung nicht tragen.²⁴⁶

Die erste Beschränkung ergibt sich aus den grundlegenden Rechtsprinzipien 16 vieler Staaten, welche verlangen, dass Informationen und Material, bei denen es sich um Beweise handelt, die einen Angeklagten entlasten, **der Verteidigung oder einer Justizbehörde offengelegt werden müssen**. Handelt es sich daher bei den zur Verfügung gestellten Informationen oder dem zur Verfügung gestellten Material um solche Beweise, kann kein Verstoss gegen grundlegende Rechtsprinzipien erwartet oder verlangt werden.²⁴⁷

In vergleichbarer Weise erstreckt sich eine Begrenzung auch nicht auf 17 **öffentliche Gerichtsverfahren**. Material, das im Rahmen von Rechtshilferegeln übermittelt wird und für die Verwendung in einem Gerichtsverfahren bestimmt ist, das normalerweise öffentlich ist, kann nicht Gegenstand einer entsprechenden Verwendungsbeschränkung sein.

245. Vgl. Art. 3 Abs. 1 und 3 IRSG. Als Tat mit fiskalischem Charakter gilt dabei eine Tat, die auf eine Verkürzung fiskalischer Abgaben gerichtet erscheint oder Vorschriften über währungs-, handels- oder wirtschaftspolitische Massnahmen verletzt.

246. Botschaft CCC, S. 4731, und Explanatory Report, Ziff. 278.

247. Botschaft CCC, S. 4731.

IV. UNMÖGLICHKEIT DER BEDINGUNGSENTSPRECHUNG (ART. 28 ABS. 3)

- 18 Abs. 3 wiederum legt eine Pflicht der ersuchenden Partei fest, unmittelbar auf eine Bedingung zu reagieren, sofern sie dieser nicht entsprechen kann. Die ersuchende Partei hat diesen Umstand der ersuchten Partei **umgehend mitzuteilen**. Dieser wiederum steht es zu, zu prüfen und zu entscheiden, ob sie die Informationen dennoch und damit in Kenntnis der Unmöglichkeit der Bedingungseinhaltung, also letztlich bedingungslos zur Verfügung stellen will. Hierbei wird man ein Festhalten an den Grundsätzen der Rechtshilfe verlangen wie voraussetzen dürfen, was mit Blick auf die Entscheidung bedeutet, dass es unter dem Gedanken der Verdaulichkeit der ersuchten Partei zusteht, einen vorhandenen Ermessenspielraum auch in diesem Gedanken anzuwenden.²⁴⁸
- 19 Sofern hinsichtlich einer Bedingung nicht umgehend mitgeteilt wird, dass dieser nicht entsprochen werden kann, ist diese Bedingung, wie auch im Fall einer ausdrücklichen Annahme der Bedingung, als verpflichtende Bedingung in Kraft.

V. VERWENDUNGSINFORMATION (ART. 28 ABS. 4)

- 20 Abs. 4 bildet eine **Kontrollstufe** ab. Es wird der informations- bzw. materialsendenden Partei ermöglicht, sich ein Bild davon zu verschaffen, wie die Informationen und Materialien verwendet wurden, die unter eine Bedingung des Abs. 2 zur Verfügung gestellt wurden. Um dies zu gewährleisten, kann seitens der ersuchten Partei von der ersuchenden Vertragspartei verlangt werden, dass Angaben zur Verwendung der Informationen oder Unterlagen gemacht werden. Diese müssen es hinsichtlich Dichte und Umfang dabei mindestens gestatten, die Einhaltung der Bedingungen überprüfen zu können.²⁴⁹
- 21 Im Ergebnis dient dies nicht nur der Kontrolle der ersuchenden Partei, sondern gewährleistet auch, dass die ersuchte Partei ihr obliegenden Pflichten einhalten kann – hier insbesondere die Pflicht sicherzustellen, dass es nicht zu einem Verstoß gegen Art. 67 IRSG kommt.

248. Siehe hierzu Explanatory Report, Ziff. 279.

249. Siehe hierzu Explanatory Report, Ziff. 280.

MATERIALIENVERZEICHNIS

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, zuletzt besucht am 19.2.2025 (zit. Botschaft CCC).

Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001, <https://rm.coe.int/16800cce5b>, zuletzt besucht am 19.2.2025 (zit. Explanatory Report).

KOMMENTIERUNG ZU

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

Eine Kommentierung von Simon Bächtold

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	251
A. Multinational-arbeitsteilige Strafverfolgung bei Cyberkriminalität	251
B. Praktische Bedeutung und verwandte Artikel	251
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)	254
III. Sicherung und Erhebung von Daten im Ausland	255
A. Einen Preservation Request stellen	255
1. Die ersuchende Behörde (lit. a.)	255
2. Die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung (lit. b.)	256
3. Die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat (lit. c.)	256
4. Alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standorts des Computersystems (lit. d.)	257
5. Die Notwendigkeit der Sicherung (lit. e.) und die Absicht der Vertragspartei, ein Rechtshilfeersuchen zu stellen (lit. f.)	257
B. Weiterleitung und Verarbeitung des Preservation Requests	257
C. Abgrenzung zum Information Request	258
D. Prosequierung mittels Rechtshilfeersuchen	260
E. Best Practices für Rechtshilfeersuchen an die USA	260
IV. Ausführen von Preservation Requests durch Schweizer Behörden	262
A. Verfahrensablauf und Zuständigkeiten	262
B. Umsetzung mittels Schweizer Recht	263
Literaturverzeichnis	267
Materialienverzeichnis	267

I. EINLEITUNG

A. Multinational-arbeitsteilige Strafverfolgung bei Cyberkriminalität

Kriminelle verwenden das **Internet** zur Begehung von Straftaten vor allem ¹ 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.).

Entsprechend der Natur des Internets als weltweites Kommunikationsnetz, ² 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.

Wer im Cyber-Bereich ermittelt, kommt ausserhalb des Bagatellbereichs in ³ der Regel am Art. 29 CCC (Preservation Request / umgehende Sicherstellung von Daten) nicht vorbei.

B. Praktische Bedeutung und verwandte Artikel

Art. 29 CCC zählt zusammen mit Art. 32 lit. b CCC zu den praktisch ⁴ 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 Ausland²⁵⁰ gespeichert sind, Rechtshilfeverfahren jedoch regelmässig sehr langwierig sind.²⁵¹ 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.²⁵²
- 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 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,

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

251. 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).

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

sondern richtet sich nach dem Recht des angefragten Staates (Art. 25 Abs. 4 CCC).²⁵³ 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.²⁵⁴ Faktisch muss ein Preservation Request daher analog einer **straftprozessualen Zwangsmassnahme** behandelt werden.²⁵⁵ 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).²⁵⁶ In solchen Ausnahmefällen darf die Polizei Ersuchen nach Art. 29 CCC auch autonom stellen.

Zu erwähnen ist auch Art. 16 CCC, welcher von den Mitgliedsstaaten verlangt, ⁸ 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

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

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

255. 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).

256. 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.

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 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.²⁵⁷ 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

257. 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.

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

Aus Schweizer Sicht ist Art. 29 CCC vor allem für die Erhebung von 11
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

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

1. Die ersuchende Behörde (lit. a.)

Hierbei wird es sich in der Praxis regelmässig um eine **Staatsanwaltschaft** 13
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.²⁵⁸ 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 CCC²⁵⁹). 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.

258. 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).

259. 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»²⁶⁰ bzw. nicht «offensichtlich untauglich»²⁶¹ 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.²⁶² 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

260. BGE 101 IV 364 E. 2.

261. BGE 142 IV 207 E. 7.1.5.

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

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.)

Hier dürfte in der Regel schlicht das **Unternehmen** bezeichnet werden, ¹⁶ welchem das konkrete Adressierungselement zugeordnet ist. Also etwa Google für @gmail-Mailadressen, Meta (für Facebook, Instagram und WhatsApp) etc.²⁶³

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

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

B. Weiterleitung und Verarbeitung des Preservation Requests

Unabhängig vom Wortlaut der Cybercrime Convention, gibt es in der Praxis ¹⁸ **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).

Aus Effizienzgründen (Vermeidung von Medienbrüchen, Automatisierung) ¹⁹ sind aber viele grosse Anbieter von internetbasierten Kommunikationsdiensten dazu übergegangen, eigene Law Enforcement Request Systeme (LERS) zu betreiben, worüber die Strafverfolgungsbehörden

263. 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.

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.²⁶⁴ 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.²⁶⁵ Die Koordinationsstelle des fedpol kann zudem angefragt werden, ob andere Schweizer Strafverfolgungsbehörden schon denselben Preservation Request gestellt haben,²⁶⁶ 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

264. 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.

265. 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.

zu Art. 32 CCC verwiesen.²⁶⁷ Kurz gesagt geht es beim Information Request um die **freiwillige Herausgabe** von Daten an einen CCC-Partnerstaat direkt durch den Dienstanbieter. Die «Freiwilligkeit» bezieht sich dabei in der Praxis auf den Dienstanbieter 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 gefragt.²⁶⁸ 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.

Wenngleich die Cybercrime Convention diese Einschränkung nicht kennt, 22 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»).²⁶⁹ 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.²⁷⁰ Oft werden Information und Preservation Requests auch zeitgleich gestellt, da unsicher ist, welche Daten die Dienstanbieter überhaupt freiwillig zur Verfügung stellen.

In der Praxis werden Information Requests sehr viel niederschwelliger 23 gestellt, weil sich dadurch die Staatsanwaltschaft nicht zu einem Rechtshilfeersuchen verpflichtet. Ein solches ist auch nicht notwendig, weil

266. 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.

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

268. 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.

269. 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).

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

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.²⁷¹
- 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 «Practical Guide for Requesting Electronic Evidence Across Borders», herausgegeben von UNODC, CTED und IAP, sowie auf eigenen Erfahrungen.

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

An ausländische Behörden gerichtete Rechtshilfeersuchen in Cybercrime- 27
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).

Zur Erhältlichmachung von Inhaltsdaten von US-Dienstanbietern muss das 28
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»,²⁷² Art. 35 CCC). Gemäss Erklärung der Schweiz ist dies primär das Bundesamt für Justiz.²⁷³ Für Belange der Cybercrime Convention, insbesondere für Preservation Requests, ist jedoch die

272. CoE 24/7 Network.

Bundeskriminalpolizei (fedpol) zuständig (das Bundesamt für Justiz leitet diesbezügliche Anfragen an das fedpol weiter). Fedpol erhält pro Jahr gegen **200 Anfragen**²⁷⁴ aus dem Ausland, die es wiederum zur Verarbeitung an die kantonalen Polizeikörpers weiterleitet.

B. Umsetzung mittels Schweizer Recht

Der Prozess, wie ein ausländischer Preservation Request in der Schweiz ³² verarbeitet wird, ist **nicht gesetzlich geregelt**. Bemerkenswert ist, wie wenig die Botschaft zur Umsetzung der Cybercrime Convention sich mit verfahrensrechtlichen und praktischen Fragen auseinandersetzt.²⁷⁵ Erwähnt wird lediglich, dass die Vertragsstaaten nicht verpflichtet sind, nebst der Beschlagnahme und Edition weitere rechtliche Instrumente zu schaffen.²⁷⁶

Das Schweizer Strafprozessrecht kennt **keine «Preservation Orders»** im ³³ Sinne der Cybercrime Convention.²⁷⁷ 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

273. 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.

274. 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).

275. Vgl. BBl 2010 4718.

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

277. 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.

Vorratsdatenspeicherung im Fernmeldebereich auf vergleichbare Weise umgesetzt. So sind es die Fernmeldediensteanbieter selbst, welche die Registrierungs- und 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).²⁷⁸

- 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 Diensteanbieter 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.²⁷⁹
- 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 Rechtshilferechts). 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 ist²⁸⁰). Die hiesige Ausführung des Preservation Requests ist nicht hinreichend bestimmt, weshalb – wie oben erwähnt – auf die Rechtsinstitute des nationalen

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

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

280. BGE 138 II 42 E. 3.1.

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).²⁸¹ 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.

Der Dienstanbieter selbst hat gemäss der aktuellen Rechtslage bei der Edition ³⁶ als Gewahrsamsinhaber der Daten ein eigenes Siegelungsrecht (vgl. Art. 248 Abs. 1 StPO).²⁸² 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 Rechtshilfeverfahren verzichtet.²⁸³ 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.²⁸⁴ Werden Daten von Dienstanbietern erhoben, bei denen aufgrund der Natur ihres Dienstes regelmässig mit geheimnisgeschützten Daten zu rechnen ist,

281. Vgl. Graf, Rz. 142.

282. BGE 140 IV 28 E. 3.2.

283. 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.

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

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.²⁸⁵ 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.²⁸⁶ 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, Dienstanbieter auch ausserhalb des Anwendungsbereichs des BÜPF, anstelle der Herausgabe, zur blossen Vorhaltung bestimmter Daten zu verpflichten.²⁸⁷ Dies würde viele der zuvor andiskutierten Probleme mit der Edition entschärfen und wäre daher zu befürworten. Eine echte **Effizienzsteigerung**

285. 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.

286. 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. 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.

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.

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

287. Das Argument wäre, dass wenn ein Dienstanbieter 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 Dienstanbieter 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.

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).

KOMMENTIERUNG ZU

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

Eine Kommentierung von Damian K. Graf

ZITIERVORSCHLAG

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

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

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

Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei:

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

rechtmässig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.

GLIEDERUNG

I. Allgemeines.....	274
A. Einleitung, Entstehungsgeschichte, Zweck und Kritik.....	274
B. Völkerrechtliches Fundament: Territorialitäts- und Souveränitätsprinzip (Art. 31 CCC) sowie deren Durchbrechung (Art. 32 CCC)Die Ausführungen dieses Kapitels finden sich bereits in Graf, Strafverfolgung 2.0, Rz. 21 ff.....	279
C. Materialien und Auslegung.....	282
D. Rechtsnatur.....	283
E. Geltungsbereich	284
F. Praxisrelevanz	288
II. Zugriff auf in einem anderen Vertragsstaat gespeicherte öffentlich zugängliche Daten («open source») (lit. a)	289
A. Öffentlich zugängliche Daten	289
B. Rechtsnatur: Qualifikation als Grundrechtseingriff?	292
C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht	295
III. Zugriff auf anderweitige, in einem anderen Vertragsstaat gespeicherte Daten (lit. b)	296
A. Rechtmässige und freiwillige Einwilligung der Person, die rechtmässig befugt ist, die Daten weiterzugeben.....	296
1. Weitergabeberechtigung.....	296
2. Einwilligung.....	300
B. Folge einer rechtsgültigen Einwilligung	302
C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht	303
IV. Über Art. 32 CCC hinausgehende Beweissicherung nach dem ZugriffsprinzipDie Ausführungen dieses Kapitels finden sich bereits in Graf, Strafverfolgung 2.0, Rz. 26 ff.	307
V. Folgen der Verletzung ausländischen Souveränitätsrechts	312
VI. Reformbedarf	314
Literaturverzeichnis	315
Materialienverzeichnis.....	321

I. ALLGEMEINES

A. Einleitung, Entstehungsgeschichte, Zweck und Kritik

- 1 In Anbetracht der stetig zunehmenden Verlagerung der Kommunikation auf Internetdienste (wie E-Mails, soziale Medien und Internettelefonie) sowie der technologischen Entwicklung weg vom lokalen Speicher hin zu «Cloud Computing» hat sich auch der Ermittlungsfokus der Strafverfolgungsbehörden gewandelt. Deren Arbeit wird durch diese **Beweisverlagerung in die digitale Welt** zunehmend komplexer. Diese Komplexität ist zum einen darauf zurückzuführen, dass Daten von flüchtiger Natur sind, problemlos grenzüberschreitend verschoben werden können (was bspw. aus Gründen besserer Auslastung der Rechnersysteme auch automatisch geschehen kann)²⁸⁸ sowie einer Verschlüsselung zugänglich sind. Zum anderen operieren führende Anbieter von kaum mehr wegzudenkenden Internetdiensten (wie etwa Google, Facebook bzw. Meta, WhatsApp, X oder Microsoft) gewöhnlicherweise vom Ausland aus (vor allem den USA) und bieten ihre Dienstleistungen von dort aus natürlichen und juristischen Personen in der Schweiz an, während deren Nutzerdaten im Ausland gespeichert werden. Dies führt dazu, dass die Ermittlungsbehörden ihre Aufmerksamkeit selbst in Binnensachverhalten regelmässig über die nationalen Grenzen hinaus richten müssen. In den EU-Mitgliedstaaten wird bereits in über 50 Prozent aller strafrechtlichen Ermittlungen ein grenzüberschreitendes Ersuchen gestellt, um elektronische Daten erhältlich zu machen.²⁸⁹ Das stellt die Strafverfolgungsbehörden vor einige Herausforderungen, nicht zuletzt völkerrechtlicher Natur, da die extraterritoriale Beweiserhebung prima vista einen Eingriff in die Souveränität des anderen Staates darstellt (vgl. nachstehend, N. 10 ff.).
- 2 In diesem grenzüberschreitenden Kontext müssen den Behörden **effektive Eingriffsbefugnisse** zur Verfügung gestellt werden, die es ihnen ermöglichen, die für inländische Strafverfahren erforderlichen Beweismittel sicherzustellen.²⁹⁰ Die Rechtshilfe als traditioneller Mechanismus

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

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

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

internationaler Zusammenarbeit gilt derweil als ineffizient und träge, gerade wenn es um flüchtige oder ohne besondere Mühe verschiebbare, löschbare oder manipulierbare Daten geht.²⁹¹ Regelmässig ist den Ermittlern auch nicht bekannt, in welchem Staat die Daten gespeichert sind oder, je nachdem, bei welchem Internet-Service-Provider die Daten überhaupt aufbewahrt werden, womit sie im Zeitpunkt des Zugriffs oft weder beurteilen können, ob sie dabei die «digitale Staatsgrenze» überschreiten, noch für sie erkennbar ist, in welchem Staat überhaupt um Rechtshilfe ersucht werden soll – und selbst wenn die Ermittler einen Staat identifiziert haben, benötigen sie für die erfolgsversprechende Begründung eines Rechtshilfeersuchens ein Minimum an Informationen (bspw. ein Nutzerkonto oder eine IP-Adresse), was sich zuweilen ebenfalls als schwierig erweisen kann.²⁹²

Die **Notwendigkeit einer grenzüberschreitenden Beweissicherung** ³ wurde bereits in den Neunzigerjahren erkannt, und am 11.9.1995 – zu einem Zeitpunkt, als die heutigen technischen Möglichkeiten erst in mancher Populärliteratur absehbar waren – verabschiedete der Europarat die Empfehlung Nr. R (95) 13 zu den Problemen des Strafverfahrensrechts im Zusammenhang mit Informationstechnologien. Deren Rz. 17 lautet wie folgt: «The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.»²⁹³ In Umsetzung dieser Empfehlung begannen daraufhin Verhandlungen über ein Übereinkommen über die Cyberkriminalität. Die Beschleunigung internationaler Kooperation sowie eine allfällige Einräumung grenzüberschreitender Befugnisse bar des Souveränitätsprinzips gehörten dabei zu den Kernthemen.

Der letztlich beschlossene Art. 32 der Cybercrime Convention («CCC»)²⁹⁴ ⁴ erlaubt, in Durchbrechung staatlicher Souveränität, in zwei Konstellationen

291. Seger, S. 74.

292. Seger, S. 74.

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

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

den Zugriff auf in anderen Vertragsstaaten gespeicherte Daten, ohne dass ein an die Behörden des anderen Staates gerichtetes Rechtshilfeersuchen erforderlich wäre: Zum einen, wenn öffentlich zugängliche Daten betroffen sind (lit. a), sowie zum anderen, wenn die berechtigte Person ihre Einwilligung in den Zugriff erteilt hat (lit. b). Art. 32 CCC erlaubt in diesen Fällen mit anderen Worten eine **direkte Sicherstellung von im Ausland gespeicherten Daten**, ohne dass zuvor die Einwilligung des betroffenen Staates eingeholt und ohne dass vor oder nach Erhebung der (steinige) Rechtshilfeweg beschritten werden müsste. Der administrative Ballaststoff fällt gänzlich weg, da der andere Staat über die Beweiserhebung nicht informiert werden muss.²⁹⁵ Sind die Voraussetzungen von Art. 32 CCC nicht erfüllt, namentlich falls die berechtigte Person nicht kooperiert, oder ist eine Erhebung technisch nicht möglich oder aus anderen Gründen nicht durchsetzbar, so ist in Anwendung von Art. 31 CCC **subsidiär der ordentliche Rechtshilfeweg** zu beschreiten, gegebenenfalls verbunden mit einem Ersuchen um unverzügliche Beweissicherung i.S.v. Art. 29 CCC, falls ein Beweisverlust einzutreten droht.

- 5 Im Vernehmlassungs- und Gesetzgebungsprozess zur Umsetzung der CCC in der Schweiz gab Art. 32 CCC, trotz der darin verwendeten auslegungsbedürftigen Begriffe und des damit einhergehenden Souveränitätseingriffs, zu keinerlei Bemerkungen Anlass.²⁹⁶
- 6 Die Stossrichtung des Art. 32 CCC ist andernorts **nicht unkritisiert** geblieben, einerseits wegen der damit einhergehenden Aufhebung des durch die territoriale Souveränität gewährleisteten Grundrechtsschutzes, ohne dass die inländischen Behörden überhaupt von solchen Grundrechtseingriffen Kenntnis erlangen.²⁹⁷ Art. 32 CCC erlaube insoweit unkontrollierte ausländische Hoheitshandlungen auf eigenem Staatsgebiet, was in verfassungsmässige Rechte der betroffenen Personen sowie Dritter eingreife,

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

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

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

²⁹⁸ unverhältnismässig²⁹⁹ sowie heikel sei, gerade hinsichtlich Staaten mit einer getrübbten Menschenrechtssituation. Die mit Art. 32 CCC einhergehende Erleichterung in der strafprozessualen Beweiserhebung ist in der Verfolgung von Straftaten mit einer digitalen Komponente indes nicht mehr wegzudenken: Unser Leben – und mithin dasjenige tatverdächtiger Personen – ist digital geworden und spielt sich zunehmend nicht im dem schweizerischen Territorium zurechenbaren digitalen Raum ab. Wohl verfügen heutzutage die meisten elektronischen Geräte noch über einen eigenen, oft grosszügigen lokalen Speicher, der, sofern das Gerät in der Schweiz sichergestellt werden kann, gestützt auf die allgemeinen strafprozessualen Regeln sichergestellt, durchsucht (Art. 246 StPO) und beschlagnahmt (Art. 263 StPO) werden kann. Der Trend geht indes weg vom lokalen Speicher hin zu cloudbasierten oder dislokalen Lösungen, deren Speicherort irgendwo auf der Welt, jedenfalls nur zu einem Bruchteil in der Schweiz liegen wird (mit Ausnahme besonderer Industrien wie des Banken- und Beratungswesens). Auch die Kommunikation erfolgt heutzutage regelmässig über soziale Medien und vergleichbare Internet-Services, wobei die Inhalte zuweilen nicht einmal mehr lokal auf dem eigenen Gerät gespeichert werden. Indem es Art. 32 CCC den inländischen Strafverfolgungsbehörden eines Vertragsstaates insbesondere erlaubt, ausländische Internet-Service-Provider direkt und unter Vermeidung des Rechtshilfewegs um Herausgabe von Daten zu ersuchen (vgl. nachstehend, N. 48, 55), wird mindestens teilweise sichergestellt, dass die materielle Wahrheitsfindung im Falle von Straftaten mit einer digitalen Komponente nicht gänzlich illusorisch wird.

Andererseits erachten insbesondere Strafverfolgerkreise den Art. 32 CCC als ⁷ zu restriktiv: Art. 32 CCC stelle als «kleinster gemeinsamer Nenner»³⁰⁰ einen letztlich wenig revolutionären Kompromiss dar. Diskussionen über die Zulässigkeit von über Art. 32 CCC **hinausgehenden grenzüberschreitenden Beweiserhebungen** scheiterten indes am fehlenden Konsens innerhalb des Europarats.³⁰¹ Auch in den seither weitergeführten Diskussionen fand sich weitgehend kein Einvernehmen,

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

299. BVerfGE 142, 234, Rz. 7.

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

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

obschon die Beweisverlagerung über die Staatsgrenzen hinaus von der Mehrheit der Staaten als eine der zentralen Herausforderungen territorialstaatlicher Strafverfolgung qualifiziert wird. Auch mit dem am 12.5.2022 verabschiedeten und bereits von zwei Staaten ratifizierten sowie 40 weiteren Staaten unterzeichneten (Stand: Oktober 2023) II. Zusatzprotokoll zur Cybercrime Convention («ZP II-CCC») blieb der grosse Wurf aus – immerhin soll es danach erlaubt sein, Dienstleister im Ausland direkt und ohne Umweg über die Rechtshilfe verbindlich aufzufordern, Registrierungsinformationen zu Domainnamen sowie Bestandesdaten³⁰² herauszugeben (Art. 6 und 7 ZP II-CCC). Von der Schweiz wurde das ZP II-CCC noch nicht unterzeichnet oder ratifiziert, was gemäss Quellen im Bundesamt für Justiz auch in naher Zukunft nicht geschehen soll – zum einen, weil die neue Regelung wiederum das Souveränitätsprinzip tangiere, und zum anderen, weil auf Stufe der Vereinten Nationen Diskussionen zu dieser Thematik geführt würden, die abzuwarten wären. In der Tat befinden sich die Beratungen zu einer United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes («UN Treaty on Cybercrime») in einem fortgeschrittenen Stadium. Der von der Mehrheit mitgetragene aktuelle Entwurf sieht aber keine grenzüberschreitende Beweiserhebung vor,³⁰³ weshalb ein Zuwarten mit der Unterzeichnung und Ratifizierung des ZP II-CCC nicht sachgerecht erscheint.

- 8 Einen Schritt weiter als Art. 32 CCC geht die unlängst in der EU verabschiedete Verordnung (EU) 2023/1543 über Europäische Herausgabebeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren vom 12.7.2023 («**e-Evidence-Verordnung**»), wonach Justizbehörden eines Mitgliedstaats elektronische Beweismittel direkt von einem Diensteanbieter in einem anderen Mitgliedstaat anfordern dürfen (Art. 1 Abs. 1 e-Evidence-Verordnung) und die Diensteanbieter rechtlich verpflichtet sind, die Daten innert 10 Tagen bzw. der angesetzten Frist zu edieren (Art. 10 e-Evidence-Verordnung). Art. 32 CCC setzt dagegen auf die Freiwilligkeit ausländischer Diensteanbieter –

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

303. United Nations, Consolidated Negotiating Document (vgl. immerhin die Minderheitsvorschläge in Art. 45 Abs. 1^{bis} und Art. 45 Abs. 1 lit. b).

kommen sie dem Ersuchen nicht oder nicht vollständig nach, ist der Rechtshilfeweg zu beschreiten, selbst bei willkürlicher, undurchsichtiger oder unbegründeter Kooperationsverweigerung. Wohl sieht Art. 18 Abs. 1 lit. b CCC zumindest vor, dass derjenige Internet-Service-Provider, der seine Dienste «im Hoheitsgebiet der Vertragspartei anbietet», Bestandesdaten im Zusammenhang mit diesen Diensten auf Verlangen hin herauszugeben hat. Das Bundesgericht erlaubt aber keine Editionsverfügung auf der Grundlage von Art. 18 Abs. 1 CCC an einen ausländischen Provider bzw. erachtet eine solche maximal dann als rechtmässig, wenn sie an dessen schweizerischen Ableger adressiert ist, sofern dieser die Daten entweder besitzt oder kontrolliert.³⁰⁴

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

B. Völkerrechtliches Fundament: Territorialitäts- und Souveränitätsprinzip (Art. 31 CCC) sowie deren Durchbrechung (Art. 32 CCC)³⁰⁵

Das **Territorialitätsprinzip** stellt eine der völkerrechtlichen Souveränität entfließende Schranke staatlichen Handelns dar. Es dient nicht nur der Begrenzung der Anwendbarkeit innerstaatlichen Strafrechts auf ausländische Sachverhalte – wovon freilich Ausnahmen existieren –³⁰⁶, sondern limitiert zugleich staatliches Handeln auf das eigene Hoheitsgebiet.³⁰⁷ Gänzlich verboten ist die Vornahme amtlicher Handlungen auf fremdem Territorium zwar nicht.³⁰⁸ Sofern derartiges Verhalten aber nicht ausdrücklich durch

304. BGer 1B_142/2016 vom 16.11.2016 E. 3.6; BGE 141 IV 108 E. 6.4; s.a. Explanatory Report, Rz. 173; T-CY, Cloud, Rz. 56; Forster, S. 619 f.; Roth, Rz. 50 ff.; a.M. Schweingruber, Rz. 21 ff.

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

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

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

308. Vgl. BGer 1B_87/2007 vom 22.6.2007 E. 2.7.

internationale (Rechtshilfe-)Abkommen, bilaterale Verträge oder zumindest ad hoc-Genehmigungen erlaubt ist, stellt es einen unzulässigen Eingriff in die staatliche Souveränität dar und kann nach ausländischem Recht gegebenenfalls entsprechend geahndet werden. Unbewilligte amtliche Handlungen auf fremdem Territorium werden auch nach schweizerischem Recht sanktioniert (Art. 299 StGB; vgl. auch Art. 271 StGB). In Verletzung des Territorialitätsprinzips erhobene Beweise können zudem im innerstaatlichen Strafverfahren gegebenenfalls nicht verwertet werden (vgl. nachstehend, N. 69 ff.).

- 11 Insbesondere **«eigenmächtige Handlungen mit Zwangs- und Eingriffscharakter auf fremdem Hoheitsgebiet»**³⁰⁹ verletzen die staatliche Souveränität und sind daher völkerrechtswidrig. Somit sind, sofern dafür nicht die Rechtshilfe des fremden Staats in Anspruch genommen wird, etwa Verhaftungen von Personen im Ausland durch schweizerische Beamte ebenso unzulässig wie die Durchführung von Einvernahmen, die Vornahme von Augenscheinen oder die direkte Vollstreckung von Urteilen.³¹⁰ Dasselbe gilt gemäss Bundesgericht für den Versand von Vorladungen an im Ausland domizilierte beschuldigte Personen, die nicht mit Zwangsandrohungen versehen sein dürfen, mithin als blosser Einladungen auszugestalten sind.³¹¹ Klar erscheint damit, dass die Strafverfolgungsbehörden nicht physisch im Ausland Beweise erheben oder dort Verfahrenshandlungen vornehmen dürfen, ohne den Rechtshilfeweg zu beschreiten resp. ohne dass solche Handlungen in einem Abkommen explizit erlaubt wären. Eigenmächtige Hausdurchsuchungen oder die Sicherstellung und Durchsuchung von elektronischen Geräten oder Unterlagen auf fremdem Staatsgebiet sind damit zweifellos untersagt.
- 12 Nicht anders gelagert sind Beweisbeschaffungssituationen, in denen sich die Strafbehörden zwar nicht physisch auf ausländischem Staatsgebiet aufhalten, aber in der Schweiz Untersuchungshandlungen vornehmen, die sich auf die fremde Gebietshoheit auswirken. Darunter fällt bspw. die Observation von Personen auf der deutschen Uferseite des Rheins durch schweizerische Polizisten von Schaffhausen aus, genauso wie die Video-Einvernahme eines im Ausland befindlichen Beschuldigten durch ein schweizerisches Gericht.

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

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

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

Solches Verhalten verletzt das Völkerrecht ebenfalls, da es in seinen Wirkungen einem Hoheitsakt direkt auf fremdem Staatsgebiet gleichkommt.
312

Auch der Zugriff auf Computersysteme im Ausland von einem Standort in der Schweiz aus und damit die **Sicherstellung von im Ausland gespeicherten Daten** sind als solche extraterritorialen Hoheitsakte zu qualifizieren.³¹³ Die Staatengemeinschaft beansprucht auch hinsichtlich auf eigenem Territorium stationierter Datenverarbeitungsanlagen und der dort gespeicherten Daten Souveränität.³¹⁴ Nationale Durchsuchungsbefugnisse können derartige Eingriffe in fremde Souveränitätsrechte nicht legitimieren.³¹⁵ Das ist vom Bundesgericht einmal grundsätzlich anerkannt worden³¹⁶ (vgl. indes nachstehend, N. 63 ff.) und wird insbesondere auch in den (intensiven) Diskussionen zum Inhalt bzw. zur Fortentwicklung der CCC abgebildet.³¹⁷ 13

Sobald in einem solchen Sinne in die Souveränität eines ausländischen Staates eingegriffen werden soll, muss dieser infolgedessen einwilligen, entweder indem er auf individuelles Ersuchen hin Rechtshilfe leistet oder internationalen Partnern staatsvertraglich oder ad hoc die Berechtigung einräumt, entsprechend tätig zu werden. Anwendungsbeispiele für die partielle Aufgabe der Souveränität der Schweiz finden sich in Abkommen mit Nachbarländern zur polizeilichen «Nacheile»³¹⁸ oder, beschränkt, im Kontext 14

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

313. Zusammenfassung von BGE 141 IV 108 E. 5.3 und 5.12 in BGer 1B_29/2017 vom 24.5.2017 E. 4.7; so auch BGE 143 IV 21 E. 3.2; ferner Roth, Rz. 30; Dombrowski, S. 12.

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

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

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

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

der Cybercrime Convention. Denn durch die Schaffung von Art. 32 CCC wurde in zwei Konstellationen auf die Notwendigkeit eines Rechtshilfeersuchens verzichtet: Einerseits ist der Zugriff auf öffentlich zugängliche gespeicherte Computerdaten zulässig, gleichwohl, wo sich die Daten geographisch befinden (lit. a). Andererseits – und im Vergleich zu anderen Rechtshilfeakkorden sehr weitgehend – darf eine Vertragspartei gemäss Art. 32 lit. b CCC «auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmässige und freiwillige Zustimmung der Person einholt, die rechtmässig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.» Das legitimiert nicht nur eine direkte Anfrage bei ausländischen Providern zur Herausgabe von Informationen, sondern auch den eigenhändigen Zugriff der Behörden über bestehende Benutzerkonten (vgl. nachstehend, N. 55). In der CCC wird für die Vertragsstaaten mit anderen Worten verbindlich festgelegt, unter welchen Umständen Behörden direkt auf im Ausland befindliche Daten zugreifen können (i.e. unter den Voraussetzungen von Art. 32 CCC) und wann sie ein förmliches Rechtshilfebegehren zu stellen verpflichtet sind (in allen anderen Fällen; Art. 31 CCC). Daraus erhellt, dass der **Zugriff auf ausländische Daten** unabhängig davon, dass sich Mitglieder der Strafverfolgungsbehörden bei derartigen Beweissicherungsmaßnahmen nicht physisch auf ausländischem Gebiet aufhalten, als **prinzipieller Eingriff in die Souveränität** gewertet wird. Im Rahmen der Ausarbeitung der CCC stellte sich denn auch gerade heraus, «dass kein Konsens erreicht werden konnte für weitergehende Regeln, unter welchen Voraussetzungen ein unilateraler Zugriff eines Staates auf Daten, die sich in einem anderen Vertragsstaat befinden, ohne Genehmigung desselben erfolgen kann.»³¹⁹

C. Materialien und Auslegung

- 15 Die von Art. 32 CCC verwendeten Begriffe und die davon erfassten Konstellationen wurden im **Explanatory Report zur CCC** – sinngemäss die «Botschaft» des Europarats zur CCC – nur teilweise näher erläutert, was das

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

319. BBl 2010 4737.

Risiko birgt, dass die Behörden der Vertragsstaaten diese unterschiedlich auslegen. Das scheint aber ein bewusster Entscheid gewesen zu sein.³²⁰ Immerhin hat eine Arbeitsgruppe zum grenzüberschreitenden Zugriff auf Daten («T-CY Transborder Group») des Komitees der Vertragsparteien («Cybercrime Convention Committee, «T-CY») am 3.12.2014 eine **Leitlinie («Guidance Note») zum grenzüberschreitenden Zugriff auf Daten unter Art. 32 CCC** erlassen, die als Auslegungshilfe herangezogen werden kann. Die Voraussetzungen des Art. 32 CCC – etwa die Frage, wer berechtigt ist, die Zustimmung nach Art. 32 lit. b CCC zu erteilen – sind aber letztlich nach inländischem Recht zu bestimmen (vgl. nachstehend, N. 41 f.); insoweit sind eine innerstaatliche Begriffsbestimmung und damit allfällige unterschiedliche Auffassungen zwischen den Vertragsstaaten unvermeidlich.

Gemäss Bundesrat soll die Bestimmung eng ausgelegt werden, «um der Gefahr des Missbrauchs unter Umgehung der Rechtshilfe oder in Verletzung der Privatsphäre Dritter entgegenzuwirken.»³²¹ Berücksichtigt man allerdings die mit Art. 32 CCC angestrebte Wirkung – die Verfahrensbeschleunigung bzw. die vereinfachte Beweiserhebung –, so gibt das Freiraum für **praxisnahe und praxistaugliche Auslegungen**.¹⁶

D. Rechtsnatur

Art. 32 CCC ist eine **«self-executing» völkerrechtliche Norm**,³²² die mit Ratifizierung direkt Anwendung findet. Die Vertragsparteien räumen den anderen Vertragsstaaten dadurch das Recht ein, in Umgehung des Rechtshilfewegs direkt auf Daten in ihrem Hoheitsgebiet zuzugreifen. Mit anderen Worten normiert die Bestimmung einen «Verzicht auf das innerstaatliche Verfahren im ersuchten Staat.»³²³ Die Strafverfolgungsbehörden der Vertragsstaaten können sich unmittelbar auf Art. 32 CCC abstützen, und zwar sowohl im innerstaatlichen Strafprozess, um entsprechende Beweiserhebungen im Ausland zu legitimieren (wobei sie weiterhin die inländischen prozessualen Regeln einzuhalten haben, vgl. nachstehend, N. 56) – Art. 32 CCC stellt insoweit keine originäre¹⁷

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

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

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

323. Walder, S. 542.

Zwangsmassnahme dar –³²⁴, als auch können sie sich im Verhältnis zum betroffenen Vertragsstaat darauf berufen, dass keine widerrechtliche Beeinträchtigung ausländischer Souveränität vorliegt. Im Verhältnis zum IRSG gehen die Bestimmungen der CCC denjenigen des IRSG jedenfalls vor (Art. 1 Abs. 1 IRSG).³²⁵

E. Geltungsbereich

- 18 Art. 32 CCC erlaubt die Sicherstellung von Computerdaten, die in einem anderen Vertragsstaat gespeichert sind.
- 19 Als **Computerdaten** gelten nach Art. 1 lit. b CCC sämtliche Darstellungen «von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschliesslich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann.» Durch Art. 32 CCC erfasst ist damit der Zugriff auf **Bestandes-, Verkehrs- bzw. Randdaten wie auch Inhaltsdaten**, die entweder gespeichert sind oder sich im Zeitpunkt des Zugriffs im Übermittlungsstadium befinden. Aufgrund seiner rechtlichen Qualifikation als elektronischer Datenbestand kann bspw. auch Kryptovermögen in Anwendung von Art. 32 lit. b CCC sichergestellt werden, sofern die berechtigten Personen ihre Ermächtigung dazu erteilen.³²⁶
- 20 Art. 32 CCC stellt ausdrücklich auf den **Speicherort** der konkret envisagierten Daten ab (Art. 32 lit. b CCC: «[...] gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden»; vgl. auch Art. 31 CCC: «[...], die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der ersuchten Vertragspartei befindet»). Bei Daten, die an mehreren Orten gespeichert sind, ist der Speicherort des Datensatzes massgebend, der konkret sichergestellt werden soll. Ein Zugriff in Anwendung dieser Bestimmung ist folglich nur dann zulässig, wenn die CCC am **Ort der Datenhaltung** anwendbar ist.³²⁷ Zumal keiner der 68 Vertragsstaaten einen

324. Vgl. auch Walder, S. 542.

325. OGer ZH SB140420 vom 2.5.2015 E. 3.3.3.

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

Vorbehalt zu Art. 32 CCC angebracht hat, kann sich die Prüfung darauf beschränken, ob der Staat am zu tangierenden Speicherort Vertragspartei der Cybercrime Convention ist, diese mithin unterzeichnet und ratifiziert hat.

Nicht anwendbar ist Art. 32 CCC auf **rein innerstaatliche Verhältnisse**:²¹ Sind die Daten lokal auf einem sich in der Schweiz befindenden und hier sichergestellten Endgerät oder Server gespeichert, so ist diesbezüglich schweizerisches Landesrecht anwendbar (vorab Art. 246, Art. 263 und Art. 265 StPO, für Randdaten siehe Art. 273 StPO).³²⁸ Das ist auch dann der Fall, wenn sich ausländische Datensätze im Zeitpunkt des Zugriffs im Zwischenspeicher des hier sichergestellten Geräts befinden. Wird das Gerät indes als «Schlüssel» bzw. «Einfallstor» verwendet, um Zugang zu Services zu erhalten, die ihre Daten im Ausland gespeichert haben (bspw. Cloud, Webmail, etc.), ohne dass diese lokal auf dem Gerät gespeichert wären, handelt es sich diesbezüglich um einen transnationalen Datenabgriff und Art. 32 CCC ist zu beachten (vgl. allerdings nachstehend, N. 63 ff.). Das schweizerische Landesrecht ist auch dann anwendbar, wenn ausländische Provider schweizerische Tochtergesellschaften oder Partner haben, die die Daten in der Schweiz speichern.³²⁹ Diesfalls kann der Zugriff bei letzteren erfolgen. Datencenter werden allerdings regelmässig nicht dazu zählen, da die bei ihnen gelagerten Daten oft verschlüsselt sind und diese ohne Mitwirkung oder zwangsweise Erhebung bei den datenberechtigten Personen kaum ausgelesen werden können. Die ausländischen Personen müssen dann entweder in Anwendung von Art. 32 lit. b CCC oder subsidiär rechtshilfweise um die Herausgabe der Daten oder Schlüssel ersucht werden. Art. 32 lit. b CCC ist auch dann anwendbar, wenn inländische Tochtergesellschaften oder Partner ausländischer Provider von der Staatsanwaltschaft angewiesen werden, Daten auszuhändigen, die sie im Ausland gespeichert haben.³³⁰ Korrekterweise darf eine inländische Person nicht unter Zwangsandrohung aufgefordert werden, für die Strafverfolgungsbehörden im Ausland verfügbare Beweismittel zu beschaffen, auch wenn es sich dabei um Daten handeln sollte, hinsichtlich derer sie zugriffsberechtigt ist.³³¹ Das Bundesgericht hielt dazu fest, eine Editionsverfügung gemäss Art. 265 StPO an einen schweizerischen Ableger eines Internet-Service-Providers sei zulässig, wenn sie hinsichtlich der

327. Bär, Rz. 29.

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

329. Forster, Fn. 14.

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

gegenständlichen Daten über eine Zugriffsmöglichkeit sowie eine Zugriffsberechtigung verfüge («pouvoir de disposition, en fait et en droit, sur ces données»).

³³² Das beisst sich nicht mit den soeben erfolgten Ausführungen, da die Editionsverfügung noch keine Zwangsmassnahme darstellt³³³ und sie in diesem Kontext als Ersuchen nach Art. 32 CCC um freiwillige Herausgabe verstanden und gewürdigt werden kann.

- 22 Hinsichtlich von **Drittstaaten**, die sich der Konvention nicht angeschlossen haben, muss im Umkehrschluss davon ausgegangen werden, dass die staatliche Souveränität hier jedweden Online-Zugriff auf (nicht-öffentliche, vgl. nachstehend, N. 35) Daten verbietet und daher einzig die Beschreitung des Rechtshilfewegs in Frage kommt.³³⁴
- 23 Das **Abstützen auf den Speicherort** ist zwar naheliegend, weil sich die Staaten auch hinsichtlich der sich auf ihrem Territorium befindenden IT-Infrastruktur auf das Souveränitätsprinzip zu berufen vermögen.³³⁵ Problematisch ist indes, dass im Zeitpunkt des Zugriffs nicht selten weder für die Strafverfolgungsbehörde noch für den Datenberechtigten oder gar für den Datengewahrsamsinhaber bekannt ist, wo die Daten in jedem Moment gespeichert sind. So speichern Internet-Service-Provider die Daten ihrer Kundinnen und Kunden zuweilen nicht in ihrem Sitzstaat, sondern anderswo. Der Speicherort kann sich aufgrund von technischen Umstrukturierungen oder Verlagerung an andere (billigere) Standorte über die Zeit auch ändern. Jedenfalls kann der Speicherort im Zeitpunkt des Datenabgriffs oft nicht abschliessend eruiert werden.³³⁶ Es stellt sich damit die Frage, wie mit dem

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

332. BGer 1B_142/2016 vom 16.11.2016 E. 3.6; BGE 143 IV 21 E. 3.4.2.

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

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

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

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

Standardfall umzugehen ist, in welchem für die Strafverfolgungsbehörde im Zeitpunkt der beabsichtigten Sicherstellung nicht bestimmbar ist, ob die Daten in einem CCC-Vertragsstaat, einem Drittstaat oder gar im eigenen Land gespeichert sind. Die Materialien zu Art. 32 CCC befassen sich nicht abschliessend damit; die T-CY Guidance Note sieht nur, aber immerhin, vor, dass die Vertragsstaaten in Situationen, in denen der Speicherort unbekannt oder unsicher ist, die Rechtmässigkeit des Zugriffs im Lichte des innerstaatlichen Rechts, der einschlägigen völkerrechtlichen Grundsätze oder mit Rücksicht auf internationale Beziehungen selbst beurteilen sollen («[...] Parties may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations»³³⁷). Bei **unbekanntem Speicherort** drängt sich was folgt auf: Würde für die Anwendbarkeit von Art. 32 CCC die sichere Kenntnis verlangt, dass der Speicherort in einem Vertragsstaat liegt, verlöre Art. 32 lit. b CCC seine Bedeutung und wäre die Sicherstellung von Cloud-Daten ad absurdum geführt.³³⁸ «Allein die Möglichkeit eines Standorts in einem Drittstaat kann auch keine Rechtshilfeverpflichtung auslösen, zumal gar nicht feststeht, an welches Land man sich richten dafür soll.»³³⁹ Detaillierte Abklärungen zum Speicherort sind vor dem Zugriff oft unmöglich oder nehmen zu viel Zeit in Anspruch – freilich: falls keine Dringlichkeit vorliegt und der Speicherort ohne besonderen Aufwand technisch festgestellt werden kann, sollte man sich darum bemühen.³⁴⁰ Angesichts des Beschleunigungsgedankens der CCC wäre ein generelles Zuwarten bis zur sicheren Kenntnis aber nicht angezeigt, zumal dann, wenn Beweisverlust droht. Sollte sich im Nachhinein herausstellen, dass der Speicherort tatsächlich in einem Drittstaat lag, wird auf dem Rechtshilfeweg eine nachträgliche Genehmigung des Datenzugriffs einzuholen sein (vgl. nachstehend, N. 71).

Im Verhältnis zu den grossen **Social Media-Providern** stellt sich die 24 Sachlage noch etwas komplizierter dar. Diese haben ihren Hauptsitz in den USA, ihren Europasitz aber oft in Irland und gemäss eigenen (angesichts des U.S. Cloud Act aber nicht unbedingt korrekten) Angaben einzig von Irland aus Zugriff auf die Daten europäischer und schweizerischer Kundinnen und

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

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

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

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

Kunden (was die Provider mit der europäischen Datenschutz-Grundverordnung vom 27.4.2016 [«DSGVO»] begründen), wobei die Daten wiederum regelmässig in anderen Staaten (bspw. Schweden) gespeichert sind.³⁴¹ Irland hat die CCC allerdings bislang nicht ratifiziert. Entsprechend stellt sich die Frage, ob Ersuchen nach Art. 32 lit. b CCC für europäische Daten zuhänden der irischen Ableger überhaupt zulässig und die erhobenen Daten verwertbar sind. Muss alternativ Schweden als möglicher Speicherort adressiert werden, wenngleich die Daten dort zwar allenfalls abgegriffen werden können, diese aber verschlüsselt und damit unbrauchbar sein dürften? Oder ist die amerikanische Muttergesellschaft zu tangieren, die die Daten bei ihrer europäischen Tochtergesellschaft beschaffen soll? In der Praxis wird die Brisanz dieser Frage dadurch abgeschwächt, dass die Auskunftersuchen über von den Internet-Service-Providern bereitgestellte «Law Enforcement Portals» gestellt werden können – von welcher Gruppengesellschaft aus die Provider die ersuchten Daten den Behörden dann zur Verfügung stellen bzw. wie sie sich intern organisiert haben, ist ihnen überlassen und muss nicht weiter geprüft werden, zumal die Strafverfolgungsbehörden ohnehin keine Möglichkeit haben, zu überprüfen, wo die edierten Daten effektiv gespeichert gewesen sind und welche Gruppengesellschaft genau darauf Zugriff gehabt hat.

- 25 Angesichts all dieser Schwierigkeiten macht der Speicherort als massgebendes Kriterium wenig Sinn. De lege ferenda sollte daher für Art. 32 CCC auf das Anknüpfungsmerkmal des Speicherorts verzichtet und vielmehr an den **Sitz oder Aufenthaltsort** derjenigen Person geknüpft werden, die **auf die Daten rechtmässig Zugriff** hat. Alternativ (der e-Evidence-Verordnung der EU³⁴² und Art. 18 Abs. 1 lit. b CCC entsprechend) kann man auch ausreichen lassen, dass das jeweilige Unternehmen seine **Dienste im betreffenden Staat anbietet**.³⁴³

F. Praxisrelevanz

- 26 Art. 32 CCC hat sich als **unverzichtbares Mittel** zur Verfolgung von Kriminalität mit einer digitalen Komponente entwickelt. Schweizerische Strafverfolgungsbehörden stützen sich regelmässig auf Art. 32 CCC, sei es

341. Siehe auch Seger, S. 77.

342. Dazu Pfeffer, Ziff. III.

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

durch die Sammlung von Open Source Information («OSINF») in Anwendung von Art. 32 lit. a CCC, sei es durch den Zugriff auf Daten bei freiwilliger Bekanntgabe der Login-Daten durch die schweizerische datenberechtigte Person gemäss Art. 32 lit. b CCC oder insbesondere durch direkte Anfragen («Information Requests») an ausländische Internet-Service-Provider zur Bekanntgabe von Bestandes-, Rand- oder Inhaltsdaten (wobei in der Praxis zumeist nur Bestandes- und Randdaten geliefert werden und für Inhaltsdaten der Rechtshilfeweg, allenfalls in Kombination mit einem «Preservation Request» nach Art. 29 CCC, beschritten werden muss). Die Zahlen direkter Auskunftersuchen sind bemerkenswert: Im ersten Halbjahr 2022 hat Google allein über 422'000 direkte Anfragen erhalten, darunter 1'357 von schweizerischen Strafverfolgungsbehörden, wovon 90 % gutgeheissen wurden.³⁴⁴ Die Provider sind allerdings keine Rechenschaft schuldig, wenn sie eine Anfrage ablehnen; sie können die Bedingungen für eine Herausgabe eigens festlegen, verändern diese auch immer wieder und zudem variieren die Bedingungen je nach Anbieter beträchtlich.³⁴⁵ Das ist unter dem geltenden Regime hinzunehmen, da Art. 32 CCC auf Freiwilligkeit beruht.

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

A. Öffentlich zugängliche Daten

Das Sammeln und Auswerten von «open source information» wird im nachrichtendienstlichen Sektor als «**OSINT**» («**Open Source Intelligence**») bezeichnet. Die Nutzung öffentlich zugänglicher Daten hat sich auch in der

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

345. Seger, S. 77.

Strafverfolgung als nützliche und nicht-invasive Ermittlungsmethode entwickelt. Unterstützt wird dies durch die Tech-Industrie, die Tools entwickelt hat, mit welchen die Daten nicht mehr händisch zusammengetragen werden müssen, sondern dies automatisiert erfolgt: Etwa durch Bereitstellen einer Software, mit der sämtliche öffentlich zugänglichen Informationen aus Facebook herausgezogen und in Beziehungsbäumen sowie auf der Zeitachse dargestellt werden können, oder technische Hilfsmittel, um den Geldfluss von Kryptowährungen (deren Blockchain öffentlich zugänglich ist) nachvollziehen zu können. Auch der Einsatz von künstlicher Intelligenz ist keine Zukunftsmusik mehr.

- 28 Öffentlich sind Daten dann, wenn sie **via eine Datenverarbeitungsanlage frei zugänglich**³⁴⁶ und nicht durch besondere Sicherheitsvorkehrungen dem allgemeinen Zugriff entzogen sind.³⁴⁷ Es reicht dabei aus, wenn sie einem unbestimmten Kreis von Nutzern zugänglich gemacht sind, selbst wenn ein Login erforderlich sein sollte, «dieses aber grundsätzlich jedem Nutzer erteilt wird, wenn ein entsprechendes Anmeldeformular ausgefüllt wurde.»³⁴⁸ Ein System kann auch bloss teilweise öffentlich sein.³⁴⁹ Daten, auf die «nur mittels einer Schnittstelle eines im – nicht öffentlich zugänglichen – Durchsuchungsobjekt befindlichen Endgeräts zugegriffen werden kann», sind dagegen nicht «open source».³⁵⁰
- 29 Als öffentlich zugängliche Daten gelten **beispielhaft** – im Sinne einer nicht abschliessenden Aufzählung – frei zugängliche Massenmedien (Printmedien [selbst wenn mittels Paywall geschützt], Rundfunk), sämtliche im Internet (Clearnet wie auch Darknet) auffindbaren Informationen, webbasierte Anwendungen (wie Google Earth), Informationen auf der öffentlich

346. Vgl. TPF 2018 68 E. 4.3.2 (zu Art. 320 StGB). Massgebend ist, dass «eine hohe Wahrscheinlichkeit der (redlichen) Kenntnisnahme durch Dritte besteht, mithin kein grosses Hindernis überwunden werden muss, um sie zu erfahren», BGE 6B_56/2014 vom 16.12.2014 E. 7.1.

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

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

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

350. Grassle/Hiéramente, S. 193, m.w.H.

einschbaren Blockchain (bspw. bei Bitcoin), auf dem Webauftritt unter der Domainadresse einer Firma oder einer Verwaltung öffentlich abrufbare Daten,³⁵¹ frei zugängliche Webcams, eine jedem Interessenten offen stehende Mailingliste,³⁵² auf einer Sharing-Plattform frei verfügbare Daten,³⁵³ das Abgreifen technischer Daten ab einem Webserver, die Ermittlung von Domaininformationen über «WhoIs»-Datenbanken, im Ausland frei oder gegen Entgelt zugängliche Schuldner-, Grundbuch-, Handelsregister- und Einwohnerkontrollauskünfte oder verfügbare Aufzeichnungen aus Straf-, Verwaltungs- und Zivilverfahren, das Beobachten öffentlicher Chats,³⁵⁴ offener Internet-Foren³⁵⁵ und öffentlich geschalteter sozialer Netzwerke (die Verwendung von öffentlichen Daten, Fotos und Beziehungen auf Facebook, Informationen ab X, Instagram, LinkedIn etc.).³⁵⁶ Auch ein Post in einer geschlossenen Gruppe (Online-Forum, Facebook o.Ä.) kann bei Gruppen mit einer hohen Mitgliederanzahl bzw. mit faktisch unbeschränktem Zugang als öffentlich qualifiziert werden, es sei denn, der Personenkreis sei bestimmt abgegrenzt und die Personen wären persönlich untereinander verbunden.³⁵⁷ Entsprechend nicht mehr als öffentlich können «geschlossene user groups» bezeichnet werden, in denen durch Administratoren der Seite eine Einzelfallprüfung der Identität der Nutzer erfolgt und ein Ermittlungsbeamter beispielsweise nur durch Vortäuschen einer Legende Zugang erhalten würde.»³⁵⁸

Je nach den Umständen können nicht nur Inhaltsdaten (Personen- oder 30 andere Daten), sondern auch Bestandesdaten (bspw. Registrierungsinformationen aus «WhoIs»-Datenbeständen) oder (selten) auch Randdaten öffentlich sein und folglich in Anwendung von Art. 32 lit. a CCC erhoben werden.

Für die Qualifikation als öffentlich zugängliche Daten spielt es keine Rolle, ob 31 die Daten unbefugt oder mit Einwilligung der datenberechtigten Person

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

352. BVerfGE 142, 234, Rz. 31.

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

354. BVerfGE 142, 234, Rz. 31.

355. BGE 141 IV 108 E. 5.8.

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

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

veröffentlicht wurden. Ist die **Veröffentlichung rechtswidrig** erfolgt (bspw. durch Verletzung gesetzlicher Geheimhaltungsverpflichtungen), so sind die Daten im innerstaatlichen Strafverfahren dann verwertbar, wenn sie von den Strafverfolgungsbehörden rechtmässig hätten erlangt werden können und eine Interessenabwägung für deren Verwertung spricht.³⁵⁹ Es gilt folglich für das erste Kriterium abzuklären, ob die Daten hypothetisch auch hätten sichergestellt werden können, wenn sie nicht öffentlich gewesen wären – also ob sie i.A.v. Art. 32 lit. b CCC oder via den Rechtshilfegeweg hätten erlangt werden können.

B. Rechtsnatur: Qualifikation als Grundrechtseingriff?

- 32 Fraglich ist, inwieweit das Sammeln und Auswerten öffentlich zugänglicher Daten als Grundrechtseingriff und in der Konsequenz als Zwangsmassnahme i.S.v. Art. 196 StPO zu qualifizieren sind. Die Beantwortung dieser Frage ist zentral, zum einen um festzulegen, inwieweit auch auf öffentliche Daten, die in einem Drittstaat liegen, zugegriffen werden kann, und zum anderen weil bejahendenfalls eine hinreichend konkrete gesetzliche Grundlage bestehen muss (Art. 197 Abs. 1 lit. a StPO). Letzteres ist durch Art. 95 StPO (Beschaffung von Personendaten) allerdings bereits verwirklicht.³⁶⁰
- 33 Als Zwangsmassnahmen werden gemäss Art. 196 StPO Verfahrenshandlungen der Strafbehörden definiert, die u.a. dazu dienen, Beweise zu sichern, soweit sie in die Grundrechte der betroffenen Personen eingreifen. Art. 196 StPO setzt damit (im Widerspruch zum Wortlaut [«Zwangs»-Massnahme]) nicht notwendigerweise Zwang voraus, sondern stützt vielmehr entscheidend darauf ab, ob die Massnahme als Eingriff in die Grundrechte der betroffenen Personen zu werten ist.³⁶¹ Im Vordergrund steht dabei, neben dem Recht auf persönliche Freiheit und der Eigentumsgarantie, der Schutz der Privatsphäre nach Art. 13 BV und Art. 8 EMRK³⁶² bzw. konkreter das darin verankerte

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

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

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

361. BGE 145 IV 42 E. 3.

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

Recht auf informationelle Selbstbestimmung.³⁶³ Als Eingriffe in dieses verfassungsmässige Recht kommen u.a. die Telefonüberwachung,³⁶⁴ die Erhebung von Fernmeldedaten,³⁶⁵ die Abnahme und Analyse von DNA und Fingerabdrücken,³⁶⁶ die Observation (inkl. systematischer Überwachung durch Privatdetektive),³⁶⁷ Videoaufnahmen durch die Polizei,³⁶⁸ das Einsetzen eines IMSI-Catchers³⁶⁹ und die passwortgeschützte Onlinerecherche resp. Sicherstellung von Chat-Nachrichten³⁷⁰ in Betracht.

Zur automatisierten Verkehrsüberwachung hielt das Bundesgericht einmal ³⁴ fest, der Schutz der Privatsphäre beschränke sich nicht auf private Räumlichkeiten, sondern erstrecke sich auch auf den privatöffentlichen Bereich; von Art. 13 BV erfasst würden auch Lebenssachverhalte mit persönlichem Gehalt, die sich im öffentlichen Raum ereignen.³⁷¹ Mit dem deutschen Bundesverfassungsgericht kann der Zugriff auf «im Internet verfügbare Kommunikationsinhalte und Informationen, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richtet», indes richtigerweise noch nicht als Eingriff in das Recht auf informationelle Selbstbestimmung charakterisiert werden.³⁷² Wohl sind Inhalte, die auf Blogs, Foren oder in sozialen Medien einem bestimmten Nutzerkreis vorbehalten

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

364. BGE 109 Ia 273 E. 4a.

365. BGer 1B_26/2016 vom 29.11.2016 E. 4.2.

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

367. BGE 143 IV 387 E. 4.2.

368. BGE 145 IV 42 E. 4.

369. BGer 1B_252/2017 vom 21.2.2018 E. 6.6.

370. BGer 1B_29/2017 vom 24.5.2017 E. 7.6.

371. BGE 146 I 11 E. 3.1.1.

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

und damit an durch persönliche Beziehungen oder besonderes Vertrauen geprägtes Umfeld richten, der Privatsphäre i.S.v. Art. 13 Abs. 1 BV zuzurechnen und deren Abgriff als Grundrechtseingriff zu werten. Daten, die für jeden Internetnutzer voraussetzungslos zugänglich oder für alle auf einer Plattform registrierte Nutzer (unabhängig eines Näheverhältnisses zur informationspreisgebenden Person) einsehbar sind, können derweil unbesehen des Inhalts nicht mehr als «privat» eingestuft werden.³⁷³ An Informationen, die bereits öffentlich bekannt sind, besteht richtigerweise kein schützenswertes Interesse mehr (mit Ausnahme des datenschutzrechtlichen «Rechts auf Vergessen»).

- 35 Ist der Zugriff auf allgemein zugängliche Daten keine Zwangsmassnahme, bedeutet das zugleich, dass Art. 32 lit. a CCC nicht konstitutiver, sondern rein **deklaratorischer Natur** ist.³⁷⁴ Wenn der Zugriff auf öffentliche Quellen mangels eigentlicher Zwangsausübung die Staatensouveränität nicht verletzt, bedarf es auch keiner zwischenstaatlichen Vereinbarung. Demgemäss können auch **öffentlich zugängliche Daten aus Drittstaaten**, die die CCC nicht ratifiziert haben, problemlos abgegriffen werden. Letzteres wird zuweilen auch damit begründet, dass es sich beim transnationalen Zugriff auf «open source data» um Völkergewohnheitsrecht handelt, als derart unbestritten gelten solche Ermittlungshandlungen.³⁷⁵
- 36 Selbst wenn dem nicht in dieser Absolutheit gefolgt würde, könnte in jedem Fall das Abgreifen **freiwillig offengelegter Daten** – etwa von Kommunikationsinhalten in den sozialen Medien – nicht als Grundrechtseingriff charakterisiert werden. Denn durch die bewusste Entscheidung, persönliche Informationen zu teilen, verzichten die betroffenen Personen in Bezug auf diese spezifischen Daten auf ihre informationelle Selbstbestimmung, oder in anderen Worten: durch die Freigabe in den öffentlichen Bereich haben sie ihre informationelle Selbstbestimmung gerade ausgeübt. Dasselbe gilt für die durch eigene Inputs hinterlassene öffentliche Datenspur, etwa mit Bitcoin getätigten Transaktionen, die auf der öffentlichen Blockchain nachverfolgbar sind. Sodann sind Daten, die nicht unmittelbar einer bestimmten Person zugerechnet werden können, unter keinem grundrechtlichen Titel

373. Cartner/Schweingruber, S. 992.

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

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

schützenswert. Dazu gehört etwa die Verwendung von «Google Earth» oder technischer Daten, die ein Webserver preisgibt. Folglich fällt maximal das Abgreifen und Auswerten nicht freiwillig offenbarter personenbezogener Informationen als Zwangsmassnahme in Betracht; hier könnte berechtigterweise geltend gemacht werden, die Betroffenen hätten keine Kontrolle darüber, welche Informationen über sie im Internet verfügbar sind. Allerdings wäre auch dann zu berücksichtigen, dass OSINT ein vergleichsweise wenig invasiver und damit verhältnismässiger Eingriff ist, da er sich auf Informationen beschränkt, die ohne spezielle Zugangsbeschränkung von jedermann abgerufen werden können.³⁷⁶

C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht

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

Aufgrund des fehlenden Grundrechtseingriffs sind «open source»-Ermittlungen nicht als Zwangsmassnahmen i.S.v. Art. 196 ff. StPO einzustufen (vgl. vorstehend, N. 32 ff.). Als Folge dessen sind weder die formellen und materiellen Vorschriften zur Durchsuchung (Art. 246 ff. StPO) noch zur Beschlagnahme (Art. 263 StPO) anwendbar. «OSINF» bzw. «OSINT» gilt vielmehr als eine gestützt auf Art. 95 StPO zulässige Erhebung von Beweismitteln i.S.v. Art. 139 Abs. 1 StPO.³⁷⁷ ³⁸

Das Einloggen durch Angehörige von Strafverfolgungsbehörden unter einer falschen Identität in den sozialen Medien oder in einem Chat, um Zugang zu den dort veröffentlichten Inhalten erhält, ist nicht als **verdeckte Fahndung** (Art. 298a StPO) oder verdeckte Ermittlung (Art. 285a StPO) einzustufen, da hier kein direkter Kontakt mit der Zielperson aufgebaut wird.³⁷⁸ Anders sähe es aus, wenn der Ermittler der Zielperson aktiv eine Freundschaftsanfrage o. ³⁹

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

377. Cartner/Schweingruber, S. 996 f.

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

dgl. schicken würde, um dessen (privaten) Beiträge ebenfalls zur Kenntnis nehmen zu können, oder wenn er sich durch Anlegen einer Legende Zutritt zu einem nicht allgemein zugänglichen Chat oder Forum erschleicht.

- 40 Der **Beweiswert** von öffentlich verfügbaren Daten gilt es im Rahmen der freien Beweiswürdigung (Art. 10 Abs. 2 StPO) im Detail zu prüfen.³⁷⁹ Dabei spielen diverse Überlegungen eine Rolle, vorab die Herkunft des Beweises, dessen Authentizität und Verlässlichkeit,³⁸⁰ das Verhältnis dessen Verfassers zu den Verfahrensparteien, vor allem aber auch, ob die Quelle anonym oder bekannt ist, zumal die Zweifel bei unbekannter Herkunft gross und Daten relativ einfach manipulierbar sind.³⁸¹ Bedeutend ist sodann auch, dass die Daten nach dem aktuellen Stand der Technik forensisch gesichert werden, da sich aus Metadaten allfällige Rückschlüsse auf den Beweiswert ziehen lassen; das blosses Anfertigen von Screenshots wird hierfür kaum genügen.

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

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

1. Weitergabeberechtigung

- 41 Art. 32 CCC regelt lediglich die völkerrechtliche Zulässigkeit des Datenzugriffs; «die innerstaatlichen Vorschriften, an denen die Datenübermittlung zu messen ist, nach denen also zu entscheiden ist, ob die Zustimmung zu der Übermittlung rechtmässig durch eine dazu befugte Person erteilt worden ist, werden von dem Übereinkommen nicht berührt.»³⁸² Der

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

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

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

Europarat hat darauf verzichtet, den Begriff der Weitergabeberechtigung in der CCC näher zu definieren. Im Explanatory Report wird dazu ausgeführt, wer sein Einverständnis erklären könne, «may vary depending on the circumstances, the nature of the person and the applicable law concerned.»³⁸³

Die Frage, wer «rechtmässig befugt ist, die Daten [...] weiterzugeben»,⁴² bestimmt sich nach dem **inländischen Recht des ersuchenden Staates**, also demjenigen, in dem die Ermittlungen stattfinden.³⁸⁴ Dies erscheint auch deshalb sinnvoll, weil eine genaue Lokalisierung der Daten vor dem Zugriff oft nicht oder nicht ohne grossen Aufwand möglich ist.³⁸⁵ Es wäre zudem nicht praktikabel und mit dem Beschleunigungsgedanken der CCC unvereinbar, von den schweizerischen Behörden die Prüfung der Berechtigungssituation für jeden Vertragsstaat separat zu verlangen, bevor sie eine Datensicherung vornehmen dürften.

Erforderlich ist die **Berechtigung, Daten weiterzugeben**. Notwendig, aber⁴³ auch hinreichend ist die Einwilligung einer Person, die rechtmässig befugt ist, diese den Strafverfolgungsbehörden zu offenbaren.³⁸⁶ Die Berechtigung kann **gesetzlicher oder obligatorischer Natur** sein.

Entgegen der Botschaft³⁸⁷ ist es keine zusätzliche Voraussetzung, dass die⁴⁴ Zustimmung «einer Person im Inland» vorliegen muss; Art. 32 lit. b CCC kennt kein derartiges einschränkendes Kriterium, das zudem dem Sinn und Zweck der Konvention zuwiderlaufen würde.³⁸⁸

Der Explanatory Report und die Botschaft nennen als einwilligungsfähig⁴⁵ beispielhaft Personen, die ihre E-Mails bei einem Service-Provider in einem anderen Staat oder anderweitige Daten im Ausland gespeichert haben.³⁸⁹ In der Literatur wird bei auf Cloud-Servern gespeicherten Daten der den

382. BVerfGE 142, 234, Rz. 39.

383. Explanatory Report, Rz. 294.

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

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

386. BBl 2010 4738.

387. So aber BBl 2010 4738.

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

Speicherplatz mietende Kunde als berechtigte Person bezeichnet,³⁹⁰ bei Daten über Finanztransaktionen die Bank,³⁹¹ für den geschäftlichen E-Mail-Account der Arbeitgeber³⁹² und bei juristischen Personen die dafür intern als zuständig erklärten Personen, bei Fehlen ebensolcher innerbetrieblicher Regelungen der Verwaltungsrat (AG) bzw. die Geschäftsführung (GmbH); Administratoren oder sonstigen Zugangsberechtigten dürfte diese Berechtigung regelmässig abgehen.³⁹³

- 46 Ein im Explanatory Report nicht abschliessend erörterter Aspekt beschlägt die Frage, ob die Einwilligung stets durch die betroffenen Personen erteilt werden muss (**Datenherrinnen**) oder die Ermächtigung anderer Stellen, die die personenbezogenen Daten bearbeiten (allen voran der Internet-Service-Provider als **Datengewahrsamsinhaber**), ausreicht.³⁹⁴ Eine Ausweitung auf Internet-Service-Provider wird kritisch beäugt, denn diese würden bloss das Datengewahrsam ausüben und befänden sich daher nicht in der Position, um rechtsgültig einzuwilligen zu können.³⁹⁵
- 47 Die Frage der Weitergabeberechtigung ist im breiteren Kontext zu betrachten, dass in der Schweiz nach geltender Rechtslage kein eigentumsähnliches Recht an Daten existiert: Das Eigentumsrecht nach Art. 641 ZGB erstreckt sich einzig auf die «Sache», worunter die Lehre «ein körperlicher, von anderen abgegrenzter Gegenstand, der tatsächlicher und rechtlicher Beherrschung zugänglich ist»,³⁹⁶ versteht. Da Daten immaterielle Güter darstellen, kann an ihnen (wohl aber an Datenverarbeitungsanlagen oder Datenträgern) kein

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

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

391. Brodowski, S. 478.

392. Graf, Strafverfolgung 2.0, Rz. 46.

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

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

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

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

Eigentum i.S.v. Art. 641 ZGB begründet werden.³⁹⁷ Auch das Urheberrecht erstreckt sich einzig auf geistige Schöpfungen mit individuellem Charakter in Datenform und ist nur ausnahmsweise anwendbar.³⁹⁸ Immerhin ist im Datenschutzrecht ein Zugangsrecht zu Daten anerkannt, jedenfalls in Bezug auf Personendaten,³⁹⁹ hinsichtlich derer in Art. 25 des Bundesgesetzes über den Datenschutz vom 25.9.2020 («DSG», SR 235.1) ein Auskunftsrecht normiert ist. Art. 28 DSG räumt den betroffenen Personen bei Vorliegen bestimmter Voraussetzungen zudem das Recht auf Datenherausgabe und -übertragung von Personendaten ein (Datenportabilität), sofern sie diese Daten den Verantwortlichen bekanntgegeben haben. Ferner dürfen Personendaten «nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist» (Art. 6 Abs. 3 DSG). Die Herausgabe von Personendaten an die Strafverfolgungsbehörden stellt dabei eine Form der Datenbearbeitung dar (vgl. Art. 5 lit. d DSG). Will heissen: Die berechtigte Person kann in die Weitergabe durch die datenbearbeitende Person einwilligen.

Die Schweiz, im Einklang mit anderen Vertragsstaaten, lässt deshalb die **Einwilligung von Internet-Service-Provider** als Folge ihres privatrechtlichen Verhältnisses mit der betroffenen Person genügen, wenn die Diensteanbieter sich in ihren Allgemeinen Nutzungsbedingungen bzw. Datenverwendungsrichtlinien ein Weiterleitungsrecht an ausländische Strafverfolgungsbehörden ausbedungen haben.⁴⁰⁰ Die Mehrheit der Internet-Service-Provider sieht in ihren User Agreements vor, dass Daten nicht nur bei Vorliegen eines gültigen Gerichtsbeschlusses, sondern auch auf einfache Anfrage durch Strafverfolgungsbehörden hin herausgegeben werden können

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

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

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

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

bzw. dass die Provider mit Strafverfolgungsbehörden kooperieren.⁴⁰¹ Eine Weitergabe ist in diesen Fällen rechtskonform.

2. Einwilligung

- 49 Dass eine betroffene ausländische Providerfirma in beschriebenem Sinne grundsätzlich berechtigt wäre, ihre Zustimmung zu einer direkten Datenherausgabe zu erklären, reicht (nach dem klaren Wortlaut von Art. 32 lit. b CCC) für einen grenzübergreifenden Zugriff noch nicht aus: Vielmehr ist weiter zu prüfen, ob die anfragende Strafverfolgungsbehörde eine rechtswirksame «rechtmässige und freiwillige Zustimmung» eingeholt hat.⁴⁰²
- 50 **Einwilligungsfähig** ist, wie besehen, die juristische oder urteilsfähige⁴⁰³ natürliche Person, die aufgrund gesetzlicher oder obligatorischer Berechtigung über die Daten verfügen und Dritten Zugriff darauf gewähren darf (vgl. auch vorstehend, N. 43 ff.). Bei mehreren weitergabeberechtigten Personen ist die Einwilligung einer Person ausreichend. Liegt beispielsweise die Ermächtigung der Kontoinhaberin vor, bedarf es seitens der ausländischen Providerfirma keiner zusätzlichen Zustimmung.⁴⁰⁴ Umgekehrt reicht es aus, wenn der ausländische Provider, gestützt auf eine entsprechende Ermächtigung des Kunden in den Allgemeinen Nutzungsbedingungen, die Daten herausgibt (zur Einwilligung durch Internet-Service-Provider vgl. vorstehend, N. 46 ff.).⁴⁰⁵
- 51 Die Einwilligung kann nach allgemeinen strafprozessualen Grundsätzen entweder **ausdrücklich** erklärt werden (wofür kein Formerfordernis gilt) **oder konkludent** erfolgen.⁴⁰⁶ Letzteres liegt namentlich dann vor, wenn die von den Strafverfolgungsbehörden angefragte Person – bspw. ein

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

402. BGE 141 IV 108 E. 5.10.

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

404. Forster, Fn. 14.

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

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

Diensteanbieter oder der Inhaber des betreffenden Kontos – die Daten auf Anfrage hin herausgibt.⁴⁰⁷

Das bedeutet zugleich, dass entsprechende **«Information Requests» ins 52 Ausland** gestellt werden dürfen, und zwar ohne dass dies als unzulässige Handlung in einem fremden Staat zu qualifizieren wäre. Direkte Anfragen an ausländische Provider haben sich in der Praxis denn auch international zu einem Standard entwickelt, die entweder über von den Providern eigens betriebene Strafverfolgungsportale eingegeben oder, im Falle von anderen (kleineren) Providern, auch auf dem Polizeiweg (via Interpol) zugestellt werden können. Verschiedene Staatsverträge erlauben eine direkte Zustellung amtlicher Dokumente ins Ausland zudem mindestens dem Grundsatz nach, allen voran Art. 52 Abs. 1 des Schengener Durchführungsübereinkommens vom 19.6.1990 («SDÜ»). Dieser sieht aber vor, dass jeder Staat eine Erklärung darüber abgeben kann bzw. abzugeben hat, welche Urkunden an Personen in seinem Staatsgebiet übersendet werden dürfen.⁴⁰⁸ Es gilt hier folglich prinzipiell für jeden Vertragsstaat gesondert zu prüfen, ob und bejahendenfalls inwieweit eine direkte Zustellung erlaubt ist. Sofern die Angeschriebenen darauf hingewiesen werden, dass jegliche Mitwirkung freiwillig ist und an eine verweigerte Mitwirkung keine direkten negativen Folgen geknüpft sind, ist allerdings nicht ersichtlich, inwieweit darin überhaupt eine Verletzung fremder Gebietshoheit und damit ein Anwendungsfall von Art. 52 Abs. 1 SDÜ erblickt werden kann – es handelt sich um blosser Einladungen ohne Zwangsandrohung und ohne an eine allfällige Kooperationsverweigerung geknüpfte negativen Folgen.⁴⁰⁹ Es würde denn auch wenig Sinn machen, wenn durch die Ausnahmeregelung des Art. 32 lit. b CCC eine Effizienzsteigerung zum beschwerlichen formellen Rechtshilfeweg eingeführt werden sollte, dies aber zeitgleich durch das Erfordernis torpediert würde, auf ebendiesem formellen Rechtshilfeweg die Bereitschaft der betroffenen

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

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

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

Personen zur freiwilligen Mitwirkung abklären zu müssen. Art. 32 lit. b CCC geht insoweit Art. 52 SDÜ vor.⁴¹⁰

- 53 Die Einwilligung muss **freiwillig** erfolgen; die betroffene Person darf nicht getäuscht oder durch Zwang zur Datenherausgabe gebracht werden.⁴¹¹ Wohl besteht oft eine indirekte Drucksituation, weil die Staatsanwaltschaft im Weigerungsfall die rechtshilfweise Sicherstellung und Überstellung der betreffenden Daten verlangen dürfte. Das reicht indes für eine Beeinträchtigung der Willensbildung noch nicht aus. Dasselbe gilt bspw. im Falle einer Haftsituation, wo sich die beschuldigte Person aufgrund der Umstände subjektiv dazu gezwungen sehen könnte, zu kooperieren und die im Ausland gespeicherten Daten zur Verfügung zu stellen, um möglichst schnell aus der Haft entlassen zu werden. Doch auch eine derartige allgemein gehaltene Drucksituation hindert sie nicht an der Abgabe einer rechtskonformen Einwilligung. Untersagt ist dagegen freilich die konkrete Androhung allfälliger weiterer Nachteile. Entsprechend kann auch eine in der Schweiz domizilierte Person nicht unter Zwangsandrohung dazu verpflichtet werden, im Ausland gespeicherte Daten, auf die sie Zugriff hat, zu produzieren.⁴¹² Freilich kann sie aber mittels Editionsverfügung (Art. 265 StPO) darum ersucht werden.
- 54 Schliesslich ist die Einwilligung jederzeit widerrufbar, wobei der **Widerruf** bloss ex nunc gilt. Ein Widerruf nach erfolgter Datensicherung ist daher unbeachtlich.

B. Folge einer rechtsgültigen Einwilligung

- 55 Gibt die verfügbungsberechtigte Person ihre Login-Daten zu ausländischen abgeleiteten Internetdiensten freiwillig preis resp. willigt in die Online-Durchsuchung ein, steht es den Strafverfolgungsbehörden in Anwendung von Art. 32 lit. b CCC offen, direkt durch Nutzung der Zugangsdaten auf die Informationen zuzugreifen und diese sicherzustellen.⁴¹³ Auch steht es jeder

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

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

412. Vgl. Seitz, S. 45.

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

Privatperson frei, die eigenen, bei einem ausländischen Provider gespeicherten Daten (etwa E-Mails oder Chat-Nachrichten) den Strafverfolgungsbehörden in Kopie zur Verfügung zu stellen.⁴¹⁴ Ebenfalls zulässig ist es, wenn die Strafverfolgungsbehörde einen im Ausland domizilierten Internet-Service-Provider direkt um Herausgabe von Daten ersucht (vgl. vorstehend, N. 48, 51 f.).

C. Voraussetzungen für einen zulässigen Datenzugriff nach schweizerischem Strafprozessrecht

Der Zugriff auf nicht-öffentliche Daten in der Schweiz ist nicht voraussetzungslos möglich. Handelt es sich um Inhaltsdaten, so sind die Daten sicherzustellen (etwa durch eine Editionsverfügung [Art. 265 StPO] oder anlässlich einer Hausdurchsuchung [Art. 244 StPO]), zu durchsuchen (Art. 246 StPO) und anschliessend, soweit beweisrelevant, zu beschlagnahmen (Art. 263 StPO). Für Verkehrsdaten ist eine rückwirkende Randdatenerhebung (Art. 273 StPO) zu verfügen und vom Zwangsmassnahmengericht genehmigen zu lassen (Art. 274 StPO). Art. 32 lit. b CCC stellt nun keine eigenständige Beweissicherungs- oder Beweiserhebungsmassnahme dar, die die innerstaatlichen Voraussetzungen überflügeln würde. Die Bestimmung regelt einzig, dass bei Vorliegen einer rechtsgültigen Einwilligung auf ein Rechtshilfeverfahren verzichtet werden kann.⁴¹⁵ Der Datenzugriff, auch wenn er transnational erfolgt, stellt daher eine **innerstaatliche Zwangsmassnahme** dar, die den innerstaatlichen Gesetzlichkeiten zu genügen hat. Die Sicherstellung von Daten im Ausland muss damit – zusätzlich zur beschriebenen Einwilligung – als notwendige Bedingung dieselben Voraussetzungen erfüllen, wie wenn die Daten in der Schweiz gespeichert gewesen wären.⁴¹⁶ Ein «Information Request» an einen Internet-Service-Provider ist mithin als Editionsverfügung i.S.v. Art. 265 StPO zu qualifizieren.

Zunächst folgt daraus, dass grundsätzlich die **Eröffnung einer Strafuntersuchung** i.S.v. Art. 309 Abs. 1 StPO und damit ein hinreichender Tatverdacht vorausgesetzt sind, wobei ein noch nicht formell eröffnetes Strafverfahren mit dem Datenabgriff automatisch als eröffnet gilt (Art. 309

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

415. Walder, S. 542.

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

Abs. 1 lit. b StPO). Im selbständigen polizeilichen Ermittlungsverfahren darf nicht auf Art. 32 lit. b CCC abgestützt werden. Auch Nachrichtendienste können sich nicht darauf berufen.

- 58 Die CCC dient der Erhebung von in elektronischer Form vorhandenem Beweismaterial für eine Straftat (vgl. Art. 25 Abs. 1 und Art. 14 Abs. 2 lit. c CCC).⁴¹⁷ Der **hinreichende Tatverdacht** kann sich damit grundsätzlich auf eine beliebige Straftat erstrecken, sofern mindestens der kriminologische Verdacht besteht, dass diese mit einem technischen Hilfsmittel begangen wurde. Die Deliktsschwere ist unerheblich: Der transnationale Datenzugriff steht grundsätzlich für Verbrechen, Vergehen wie auch Übertretungen offen (in Bagatellfällen mag allerdings die Verhältnismässigkeit des Datenzugriffs zur Diskussion stehen).
- 59 Für die Sicherstellung von **Inhaltsdaten** ist erforderlich, dass zu vermuten ist, dass sich darin Informationen befinden, die der Beschlagnahme unterliegen (Art. 246 StPO). Gemäss Art. 263 Abs. 1 lit. a StPO können Gegenstände einer beschuldigten Person oder einer Drittperson namentlich dann beschlagnahmt werden, wenn sie als Beweismittel gebraucht werden. Für die Sicherstellung und Durchsuchung von Aufzeichnungen genügt damit eine **potentielle Beweiserheblichkeit**, die dann gegeben ist, wenn die Daten zur Aufklärung der vorgeworfenen Straftaten «von Bedeutung sein können»⁴¹⁸ bzw. nicht «offensichtlich untauglich»⁴¹⁹ erscheinen. Die Rechtsprechung stellt daran keine hohen Anforderungen.⁴²⁰ Die Sicherstellung und Durchsuchung muss schliesslich **verhältnismässig** (Art. 197 Abs. 1 lit. c und d StPO) und damit geeignet, erforderlich und angemessen sein. Gerade bei der Verfolgung von Übertretungen kann die Verhältnismässigkeit fraglich sein.⁴²¹ In formeller Hinsicht ist die Sicherstellung und Durchsuchung durch die Staatsanwaltschaft im Regelfall in einem schriftlichen Befehl zu verfügen (Art. 241 Abs. 1 StPO). Für die Erhebung von **Bestandesdaten** reicht es dagegen als einzige Voraussetzung aus, dass der Verdacht besteht, dass eine Straftat über das Internet begangen worden ist (Art. 22 Abs. 1 des Bundesgesetzes

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

418. BGE 101 IV 364 E. 2.

419. BGE 142 IV 207 E. 7.1.5.

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

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

betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18.3.2016 [«BÜPF»; SR 780.1]).

Werden die **IP-History/Logdaten** oder sonstige **Randdaten** im Ausland 60 erhoben, stellt sich die Frage, ob die Staatsanwaltschaft diese Aufzeichnungen in eigener Kompetenz erhältlich machen darf oder ob in Anwendung von Art. 273 Abs. 2 StPO eine Genehmigung durch das Zwangsmassnahmengericht einzuholen ist. Das Bundesgericht hielt einmal fest, Art. 273 StPO ermögliche lediglich eine rückwirkende Randdatenerhebung des Fernmeldeverkehrs «gegenüber dem schweizerischen Recht unterworfenen, in der Schweiz domizilierten Fernmeldedienst-Anbieterinnen bzw. Internet-Zugangsprovidern.»⁴²² Dessen Anwendbarkeit auf internationale Sachverhalte schloss es damit aus, mit der Folge, dass für die Erhebung keine Genehmigung durch das Zwangsmassnahmengericht notwendig sein sollte; Art. 32 lit. b CCC erlaube mit anderen Worten «einen erleichterten internationalen Austausch von Randdaten.»⁴²³ In einem anderen Entscheid wies das Bundesgericht ein Genehmigungsgesuch der Staatsanwaltschaft allerdings mit der Begründung ab, die Voraussetzungen von Art. 32 lit. b CCC seien vorliegend nicht erfüllt gewesen, wobei es nachschob, der direkte grenzüberschreitende Zugriff wäre vom Zwangsmassnahmengericht nach Art. 273 StPO zu bewilligen gewesen.⁴²⁴ Mehr noch, es konstatierte in einem weiteren Urteil ausdrücklich, auch für bei ausländischen Providern abgefragte IP-Histories müsse eine Genehmigung des Zwangsmassnahmengerichts eingeholt werden und weil dies im konkreten Fall nicht erfolgt sei, seien die aus den Anfragen stammenden Erkenntnisse absolut unverwertbar.⁴²⁵ Dass sich das Bundesgericht hier mit Art. 273 StPO beschäftigt hat, mag auf den ersten Blick nachvollziehbar erscheinen, wenn man sich die Rechtsnatur von Art. 32 lit. b CCC vergegenwärtigt, der einzig den transnationalen Zugriff völkerrechtlich für zulässig erklärt, die innerstaatlichen Vorschriften, gerade was die Kompetenz zur Datenerhebung anbelangt, dagegen nicht berührt. Allerdings ist zu berücksichtigen, dass die Vorschriften über die rückwirkende Randdatenerhebung nicht allein durch die Art der zu erhebenden Daten (Verkehrs- bzw. Randdaten) aktiviert werden, sondern die Daten müssen bei einem Fernmeldeanbieter beschafft werden bzw. durch das Fernmeldegeheimnis geschützt sein (Art. 321^{ter} StGB

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

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

424. BGE 141 IV 108 E. 5.12.

425. BGer 6B_656/2015 vom 16.12.2016 E. 1.4.3; vgl. die Kritik bei Hansjakob, S. 252 ff.

und Art. 43 des Fernmeldegesetzes vom 30.4.1997 [«FMG»; SR 784.10]).⁴²⁶ Das Fernmeldegeheimnis gilt aber (soweit hier interessierend) nur für Anbieter, die einen Internetzugang bzw. eine fernmeldetechnische Übertragung anbieten.

⁴²⁷ Internet-Service-Provider bzw. Anbieter abgeleiteter Kommunikationsdienste,⁴²⁸ die keinen Internetzugang, sondern einzig Dienstleistungen anbieten, die über das Internet erbracht werden («Over-the-Top-Dienste»), gelten nicht als Fernmeldeanbieter.⁴²⁹ Aus diesem Grund unterliegt weder die Sicherstellung von Randdaten bei solchen Unternehmen im Inland noch im Ausland einer Genehmigungspflicht. Vielmehr reicht auch hierfür eine Editionsverfügung zuhanden des Internet-Service-Providers aus (Art. 265 StPO). Werden folglich im Ausland gestützt auf Art. 32 lit. b CCC IP-Histories und andere Randdaten bei Nicht-Fernmeldeanbietern erhoben, ist **keine Genehmigung des Zwangsmassnahmengerichts** einzuholen.

- 61 Es stellt sich schliesslich die Frage, inwieweit die **übrigen Voraussetzungen der Rechtshilfe**, namentlich Ablehnungsgründe und die Notwendigkeit einer doppelten Strafbarkeit, auch für Art. 32 lit. b CCC gelten. Art. 25 Abs. 4 CCC sieht, unter dem 3. Titel («Allgemeine Grundsätze der Rechtshilfe»), vor, dass, soweit die CCC nicht ausdrücklich etwas anderes vorsieht, «die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen einschliesslich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann», unterliegt.⁴³⁰ Nun erlaubt Art. 32 lit. b CCC aber einen der Rechtshilfe vorgehenden direkten Zugriff; eines «Ersuchens» an den anderen Vertragsstaat, wie es Art. 25 Abs. 4 CCC zugrunde liegt, bedarf es hier gerade nicht. Für den freiwillig eingeräumten Zugriff bedarf es folglich weder einer doppelten Strafbarkeit noch sind weitere Bedingungen einzuhalten, die sonst im Rechtshilfeverfahren gelten würden.⁴³¹ Diese Aufweichung rechtfertigt sich

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

427. BGer 2C_544/2020 vom 29.4.2021 E. 4.2.

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

429. BGer 2C_544/2020 vom 29.4.2021 E. 4.2 und 5; vgl. auch BBl 2013 2707; Biaggini, Rz. 17.

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

zum einen durch die Freiwilligkeit der einwilligenden Personen und zum anderen angesichts der Rechtsnatur von Art. 32 lit. b CCC, der den territorialen Arm der Strafverfolgungsbehörden verlängert, während es sich weiterhin um eine inländische Beweissicherungsmassnahme handelt. Scheitert der Versuch, die Aufzeichnungen gestützt auf Art. 32 lit. b CCC sicherzustellen, so ist freilich der ordentliche Rechtshilfeweg einzuschlagen, für welchen die entsprechenden Limitationen wieder gelten.

Gegen die direkte Sicherstellung als solche oder die Providieranfrage kann sich die betroffene Person nicht wehren; immerhin steht ihr gegen die Durchsuchung der Rechtsbehelf der **Siegelung** (Art. 248 StPO) offen, soweit sie ein Beschlagnahmeverbot (Art. 264 StPO) glaubhaft machen kann. Die Siegelung bewirkt, dass die Strafverfolgungsbehörden die Aufzeichnungen einstweilen nicht durchsuchen dürfen, bis das Zwangsmassnahmengericht über die Zulässigkeit der Datenerhebung und Durchsuchung befunden hat.⁴³² 62

IV. ÜBER ART. 32 CCC HINAUSGEHENDE BEWEISSICHERUNG NACH DEM ZUGRIFFSPRINZIP⁴³³

In Friktion zum Territorialitätsprinzip, das auf den Lagerungsort der Beweismittel und damit bei Daten auf den physischen Speicherort abstützt,⁴³⁴ erlaubt das Bundesgericht einen Zugriff selbst bei **fehlender Einwilligung**, und zwar unabhängig davon, wo die Daten im Zeitpunkt des Zugriffs gespeichert sind; entscheidend sei, dass die Daten von der Schweiz aus abgerufen werden könnten: «Wer über einen Internetzugang im Inland einen abgeleiteten Internetdienst benutzt, der von einer ausländischen Firma angeboten wird, handelt nicht im Ausland. Auch der blosser Umstand, dass die elektronischen Daten des betreffenden abgeleiteten Internetdienstes auf Servern (bzw. Cloud-Speichermedien) im Ausland verwaltet werden, lässt eine von der Schweiz aus erfolgte gesetzeskonforme Online-Recherche nicht als unzulässige Untersuchungshandlung auf ausländischem Territorium (im Sinne der dargelegten Praxis) erscheinen [...]»⁴³⁵ 63

431. Kritisch Seger, S. 79.

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

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

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

- 64 Gegenstand der Beurteilung war der Zugriff auf den Facebook-Account einer wegen qualifizierten Betäubungsmittelhandels beschuldigten Person, deren Zugangsdaten die Strafverfolgungsbehörden erhältlich gemacht hatten. Die Staatsanwaltschaft liess daraufhin das Facebook-Konto unter Verwendung der ermittelten Login-Daten sichten und beweisrelevante Chat-Nachrichten sicherstellen.⁴³⁶ Der Speicherort dieser Daten lag damals – und liegt auch heute – nicht in der Schweiz. Das Bundesgericht hielt im zitierten Urteil fest, dass direkt auf Konten von Beschuldigten oder Dritten bei ausländischen Internetdiensten zugegriffen werden darf, wenn die allgemeinen Voraussetzungen einer Durchsuchung nach schweizerischer StPO⁴³⁷ erfüllt sind und die Ermittler «von in der Schweiz befindlichen Computern, Servern und IT-Infrastrukturen aus»⁴³⁸ agieren, mithin physisch in der Schweiz verbleiben.
- 65 Die Praxis hat diese Rechtsprechung dankend aufgenommen. Sie ist nicht nur auf Facebook anwendbar, sondern auf eine Vielzahl von in- und ausländischen Diensten wie Host-Provider, Kommunikationsdienste, Cloud-Services, Anbieter von Datenoutsourcing, Chat-Foren, Plattformen zum Austausch von Dokumenten, Shopping-Portale und E-Mail-Dienst-Anbieter. Auch Kryptovermögen, das in einer Hot Wallet gehalten wird, kann in Anwendung dieser Rechtsprechung sichergestellt (d.h. üblicherweise auf ein Wallet der Strafverfolgungsbehörde transferiert) werden. Die bundesgerichtliche Rechtsprechung gewinnt auch immer mehr an Bedeutung. Der allgemeine Trend für elektronische Geräte lautet: Weg von individuellem Speicher hin zur Sicherung in der Cloud. Gerade Mobiltelefone werden heute von Nutzern für verschiedene Services oft nur noch als «Schlüssel» verwendet, wobei die betreffenden Daten nicht mehr auf dem physischen Gerät gespeichert sind. Wird entsprechend ein Mobiltelefon oder ein Tablet

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

436. BGE 143 IV 270 Sachverhalt A.

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

438. BGE 143 IV 270 E. 7.10.

anlässlich einer Hausdurchsuchung oder einer polizeilichen Anhaltung sichergestellt und stellt sich dabei heraus, dass die Daten nicht auf dem Gerät, sondern in der Cloud gespeichert sind, oder finden sich Apps von Kommunikationsdiensten oder Web-E-Mail-Anbietern auf dem Gerät, können gestützt auf die bundesgerichtliche Rechtsprechung all diese Daten sichergestellt werden. Erleichtert wird dieses Vorgehen in der Praxis dadurch, dass Nutzerinnen und Nutzer aus Bequemlichkeitsgründen ihre Login-Daten zu Internetdiensten oft im Passwortmanager oder in einem Internet-Browser abspeichern oder aber für verschiedene Dienste dasselbe Passwort verwenden. Auch anlässlich von Hausdurchsuchungen bei Unternehmen trifft man zunehmend an, dass diese ihre Daten nicht mehr am Sitz bzw. Ort der Geschäftsführung selber hosten bzw. gespeichert haben, sondern dass sie die Datenverarbeitung und -aufbewahrung an externe Dienstleister outgesourced haben. In derartigen Situationen hilft der zitierte Bundesgerichtsentscheid ebenfalls, da er die Datensicherung auch in solchen Fällen erlaubt.

Implizit hat sich das Bundesgericht im zitierten Entscheid auf das sog. **«Zugriffsprinzip»** berufen.⁴³⁹ Danach wird bei Computerdaten nicht auf den Standort des Datenträgers, auf dem die Informationen gespeichert sind, abgestützt, sondern darauf, wer von wo aus Zugriff auf die verfahrensrelevanten Daten hat. Die Herrschaft über die Daten liege bei derjenigen Person, die über die Zugriffsberechtigung verfüge, und nicht bei derjenigen, die im physischen Besitze des Datenträgers sei.⁴⁴⁰ Das führen einzelne Autoren als Begründung an, weshalb in der Durchsuchung und Beschlagnahme von im Ausland gespeicherten Daten durch schweizerische Behörden in der Schweiz keine Souveränitätsverletzung zu sehen sei.⁴⁴¹ Die Zulässigkeit des Online-Zugriffs soll danach mit anderen Worten allein von der Rechtmässigkeit der inländischen Ermittlungshandlung abhängen.⁴⁴² 66

Wird nun aber auf nicht öffentlich zugängliche, insbesondere passwort- oder durch sonstige Barrieren geschützte ausländische Quellen zugegriffen, wirkt sich das mit hoher Intensität auf das ausländische («digitale») Hoheitsgebiet aus. Verschiedentlich wird daher der Zugriff durch Ermittlungsbehörden auf 67

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

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

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

442. So auch Wicker, S. 768.

Daten im Ausland als **Eingriff in die Souveränität des betreffenden Staates** gewertet;⁴⁴³ an derartige Beweismittel könne man nur über die internationale Rechtshilfe bzw. bloss dann auf direktem Weg gelangen, falls dies in internationalen Übereinkommen explizit so vorgesehen sei.⁴⁴⁴ In der Tat ändert das Zugriffsprinzip nichts an den Auswirkungen staatlicher Online-Zugriffe auf die fremde Souveränität, wo der eigentliche Erfolg der Massnahme eintritt.⁴⁴⁵ Zwar dürfte das fehlende physische Tätigwerden von Beamten auf fremdem Staatsgebiet die durch Art. 299 StGB gezogenen Grenzen noch nicht überschreiten. Sie treten jedoch, was ihre Eingriffsintensität betrifft, keineswegs hinter die äquivalenten physischen Ermittlungstätigkeiten (die Durchsuchung des Speicherträgers im Ausland durch schweizerische Beamten) zurück, die eindeutig unzulässig wären.⁴⁴⁶ Dazu kommt, dass durch den Online-Abruf Datenverarbeitungsvorgänge im Ausland ausgelöst werden;⁴⁴⁷ der Zugriff hinterlässt im Zielstaat nachvollziehbare Spuren. Der ermittelnde Beamte kann sich dort schlimmstenfalls je nach nationaler Gesetzgebung wegen unbefugten Eindringens in ein Datenverarbeitungssystem, unbefugter Datenbeschaffung oder der Missachtung fremder Hoheitsrechte strafbar machen.⁴⁴⁸ Digitale Beweisaufnahmen von der Schweiz aus erfolgen für den ausländischen Staat darüber hinaus heimlich, was sie – angesichts der Nachrichtendienst-Skandale der jüngeren Vergangenheit – aus dessen Sicht noch gefährlicher macht.⁴⁴⁹ Bemerkenswerterweise lässt das nationale Recht diverser Staaten gemäss einer UN-Studie dessen ungeachtet eine Art direkten Zugriff auf im Ausland gespeicherte Daten zu, während der Anteil an Staaten, die einen solchen direkten Zugriff durch ausländische Strafverfolgungsbehörden erlauben, gemäss derselben Studie doch merklich kleiner ist.⁴⁵⁰ Das völkerrechtliche Sensorium scheint folglich grösser zu sein, wenn die eigene Souveränität betroffen ist, als wenn man selbst auf die Beweisbeschaffung im

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

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

445. Marberth-Kubicki, § 43 Fn. 386.

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

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

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

449. Marberth-Kubicki, § 43 Fn. 386.

450. UNODC, S. 219 f.

Ausland angewiesen ist. Jedenfalls erlaubt die Cybercrime-Konvention den direkten Zugriff auf ausländische Daten in Art. 32 CCC bereits in beschränkter Weise; eine darüber hinausgehende Beweisbeschaffung – zumindest im Verhältnis der Konventionsstaaten untereinander – ist *e contrario* als Eingriff in die staatliche Souveränität zu werten.⁴⁵¹ Nicht umsonst hat der Europarat den subsidiären Art. 31 CCC mit dem Titel «Rechtshilfe beim Zugriff auf gespeicherte Daten» ausdrücklich vorgesehen. Ein von EU-Mitgliedsstaaten im Kontext der Verhandlungen eingebrachter Vorschlag, wonach in dringenden Fällen eine transnationale Online-Durchsuchung zulässig sein soll,⁴⁵² wurde denn auch nicht aufgenommen – man verzichtete mangels Konsens darauf, derartige Situationen zu regeln.⁴⁵³ Auch die seither wieder aufgenommenen Bestrebungen sind bis anhin weitgehend fruchtlos geblieben; das 2. Zusatzprotokoll zur CCC ist in dieser Hinsicht ebenfalls kein grosser Wurf. Der direkte transnationale Zugriff auf Daten ohne Einwilligung einer berechtigten Person ist damit weiterhin nicht von einem internationalen Konsens abgedeckt, verstösst gegen die Souveränität des betreffenden Staats und ist damit **völkerrechtswidrig**,⁴⁵⁴ solange keine Weiterentwicklung der aktuellen bi- oder multilateralen Übereinkommen stattgefunden hat.

Dieses Resultat ist **unbefriedigend**. Erstens gerade dann, wenn die Gefahr 68 besteht, dass die Daten ohne sofortiges Tätigwerden verlustig gehen können. Es ist deshalb vorstellbar, in Ausnahmekonstellationen die vorläufige transnationale Sicherstellung von Daten bei Vorliegen von Kollusionsgefahr bzw. der Gefahr des Beweisverlusts zuzulassen, wenn selbst ein «Preservation Request» i.S.v. Art. 29 CCC zu spät erfolgen würde.⁴⁵⁵ Diesfalls wären die

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

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

453. Explanatory Report, Rz. 293.

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

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

V. FOLGEN DER VERLETZUNG AUSLÄNDISCHEN SOUVERÄNITÄTSRECHTS

- 69 Werden die Befugnisse der CCC überschritten, die Rechtshilfe in Strafsachen durch den direkten Zugriff auf ausländische Datenträger umgangen und damit das Territorialitäts- bzw. Souveränitätsprinzip verletzt, so stellt sich die Frage der Unverwertbarkeit so erlangter Beweismittel. Die Umgehung des Rechtshilfewegs kann im inländischen Strafprozess grundsätzlich gerügt werden.⁴⁵⁶
- 70 Kantonale Gerichte haben sich bislang für ein relatives **Verwertungsverbot** i.S.v. Art. 141 Abs. 2 StPO ausgesprochen, womit die betreffenden Beweise verwertet werden dürfen, soweit sie zur Aufklärung einer schweren Straftat erforderlich sind.⁴⁵⁷ Fraglich ist derweil, ob das völkerrechtliche Territorialitätsprinzip und das Erfordernis des Beschreitens des

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

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

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

Rechtshilfewegs tatsächlich bloss als Gültigkeitsvorschriften einzustufen sind oder ob angesichts ihrer Wichtigkeit nicht vielmehr von einem absoluten Verwertbarkeitsverbot ausgegangen werden muss (bspw. in der Gestalt eines Verstosses gegen den Ordre public). Das Bundesgericht hat in diese Richtung entschieden, als es eine geheime Überwachungsmassnahme (GPS-Tracker und Abhörgeräte in einem Fahrzeug, mit welchem auch Fahrten ins Ausland erfolgt waren) mit Bezug auf die Auslandsfahrten als absolut unverwertbar erachtete.⁴⁵⁸ Möglich und sinnvoll erscheint hier indes die Übernahme der in Deutschland vertretenen Auffassung, wonach es für die Frage der Verwertbarkeit darauf ankommt, ob die Ermittlungsperson im Zeitpunkt der Datenerhebung erkannt hat, dass der Zugriff nicht in Übereinstimmung mit internationalem Recht erfolgen würde.⁴⁵⁹ War ihr das nicht bewusst, muss die Möglichkeit bestehen, für die (objektiv in rechtswidriger Weise erlangten) Beweismittel ein **nachträgliches förmliches Rechtshilfeverfahren** (im Sinne eines Genehmigungsverfahrens) durchführen zu lassen, um die Unverwertbarkeit der Beweise abzuwenden.⁴⁶⁰

Letzteres ist insbesondere auf jene Fälle anwendbar, in denen nicht von 71
Vornherein klar ist, wo die Daten gespeichert sind: Kann ein Speicherort im Inland nicht ausgeschlossen werden, so muss ein Zugriff zur Beweissicherung erlaubt sein; eine positive Kenntnis des Speicherorts ist nicht vorauszusetzen. «Allein die Möglichkeit eines Standorts im Ausland kann keine Rechtshilfeverpflichtung auslösen, zumal in diesen Fällen nicht bestimmbar ist, welches Land davon eigentlich betroffen sein wird.»⁴⁶¹ Sollte sich hernach (bspw. auch auf entsprechende Rügen der Verteidigung hin) herausstellen, dass die abgegriffenen Daten nicht im Inland und auch nicht in einem Vertragsstaat gespeichert waren, wird im betreffenden Staat eine nachträgliche Genehmigung auf dem Rechtshilfeweg einzuholen sein.⁴⁶²

458. BGE 146 IV 36 E. 2.3.

459. BeckOK-Graf, § 100a StPO N. 263.

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

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

VI. REFORMBEDARF

- 72 Der Europarat erkannte die Notwendigkeit der Aufweichung territorialer Grundsätze aufgrund der technischen Entwicklung früh und erliess in Art. 32 CCC eine im Vergleich zu traditionellen Rechtshilfeübereinkommen fortschrittliche Regelung. Weitergehende verfolgte Ideen waren ebenso visionär wie aufgrund des doch stark verankerten Souveränitätsgedankens (noch) nicht mehrheitsfähig. Will die Staatengemeinschaft indes eine effektive Strafverfolgung, die auch im 21. Jahrhundert ihre Aufgaben wahrnehmen können soll, erscheint es nötig und sinnvoll, **die Souveränität mit Bezug auf vernetzte Daten vollumfänglich aufzugeben**. Denn es geht heute nicht mehr bloss um die grenzüberschreitende Kriminalität, die für nationale Strafverfolgungsbehörden seit jeher nur schwer greifbar gewesen ist, sondern auch reine Binnensachverhalte können als Folge der Beweismittelverlagerung über die Landesgrenzen hinaus bald nicht mehr, schon gar nicht mehr in einer angemessenen Kosten-Nutzen-Relation, aufgeklärt werden.
- 73 Zugegebenermassen scheint es erfolgsversprechender zu sein, vorerst kleinere Brötchen zu backen: Erstens soll die Schweiz das **2. Zusatzprotokoll zur CCC**, auch wenn es sich dabei nicht um den ganz grossen Wurf handelt, möglichst rasch unterzeichnen und ratifizieren. Zweitens wäre schon viel getan, wenn man im Kontext von Art. 32 lit. b CCC mit der Rechtswirklichkeit Schritt halten und nicht mehr nur an den Speicherort, sondern vielmehr (auch) an den **Sitz der zugriffsberechtigten Person** oder daran anknüpfen würde, dass ein Unternehmen seine Dienste im betreffenden Staat anbietet (vgl. vorstehend, N. 25). Drittens sollte sich die Schweiz um eine **Assoziierung an das e-Evidence-System der EU** bemühen (wenngleich dies politisch schwierig umzusetzen sein wird). Viertens sind die wiederkehrenden Diskussionen zu einem **unilateralen Zugriff** auf Daten im Ausland wiederaufzunehmen und einem Abschluss zuzuführen. Mindestens sollte inskünftig ein **Zugriffsort im Inland** als hinreichend erachtet werden, um den Datenzugriff nicht mehr als die Souveränität des Staates am Speicherort verletzend einstufen zu müssen.⁴⁶³

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

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

Dabei könnten gerade auch Schutzmassnahmen und Garantien (bspw. eine Informationspflicht über den Zugriff an den betroffenen Staat, die Notwendigkeit einer nachträglichen Genehmigung, Anforderungen an die Rechtsstaatlichkeit und die Wahrung von Grundrechten etc.) miteingeflochten werden, um die Akzeptanz einer solchen Lösung zu erhöhen.⁴⁶⁴

LITERATURVERZEICHNIS

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

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

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

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

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

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

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

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

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

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

Burgermeister Daniel, Beweiserhebung in der Cloud, Luzern 2015, abrufbar unter https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/staak/MAS_Forensics/dok/Masterarbeiten_MAS_5/Burgermeister_Daniel.pdf, besucht am 17.10.2023.

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

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

De Busser Els, Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You, Groningen Journal of International Law 2/2 (2014): Privacy in International Law, S. 90 ff., abrufbar unter https://www.researchgate.net/publication/328962642_Open_Source_Data_and_Criminal_Investigations_Anything_You_Publish_Can_and_Will_Be_Used_Against_You, besucht am 17.10.2023.

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

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

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

Forster Marc, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 613 ff.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MATERIALIENVERZEICHNIS

Botschaft des Bundesrates an die Bundesversammlung zu einem Bundesgesetz über internationale Rechtshilfe in Strafsachen und einem Bundesbeschluss über Vorbehalte zum Europäischen Auslieferungsübereinkommen

vom 8.3.1976, BBl 1976 II 444 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1976/2_444_430_443/de, besucht am 17.10.2023.

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

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

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

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

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

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

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

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

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

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

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

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

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

United Nations, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, Consolidated negotiating document on the general provisions and the provisions on

criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes vom 21.1.2023, abrufbar unter https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf, besucht am 17.10.2023 (zit. United Nations, Consolidated Negotiating Document).

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

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

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 33 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Nicolas Bottinelli / Julien Wenger

ZITIERVORSCHLAG

Nicolas Bottinelli/Julien Wenger, Kommentierung zu Art. 33 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Bottinelli/Wenger, Art. 33 CCC N. XXX.

Art. 33 Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit

¹ Die Vertragsparteien leisten einander Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit in Zusammenhang mit bestimmten Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt werden. Vorbehaltlich des Absatzes 2 unterliegt die Rechtshilfe den nach innerstaatlichem Recht vorgesehenen Bedingungen und Verfahren.

²Jede Vertragspartei leistet zumindest in Bezug auf die Straftaten Rechtshilfe, bei denen die Erhebung von Verkehrsdaten in Echtzeit in einem gleichartigen inländischen Fall möglich wäre.

GLIEDERUNG

I. Einleitung	328
II. Begriffe	329
III. Umsetzung im Schweizer Recht	332
A. Art. 18b IRSG	332
1. Historischer Hintergrund	332
2. Definitionen	332
3. Verfahren	333
4. Einige materielle Abgrenzungen	337
B. Unterscheidungen	337
Literaturverzeichnis	339
Materialienverzeichnis	340

I. EINLEITUNG

- 1 Art. 33 CCC, der in Kapitel III des Übereinkommens über Cyberkriminalität mit dem Titel "Internationale Zusammenarbeit" erscheint, ist die erste von zwei Bestimmungen des Übereinkommens, die sich mit den Verpflichtungen der Vertragsstaaten zur Zusammenarbeit bei der Erhebung und Übermittlung von Kommunikationsdaten befassen. Diese Bestimmung bezieht sich auf Verkehrsdaten, im Gegensatz zu Art. 34 CCC, der sich mit Daten über den Inhalt der Kommunikation befasst.
- 2 Die ratio legis dieser Bestimmung besteht darin, dass Ermittler sehr häufig nicht sicher sein können, dass sie die Quelle einer Nachricht anhand der Aufzeichnungen früherer Übertragungen zurückverfolgen können, da entscheidende Verkehrsdaten von einem Diensteanbieter im Übertragungsweg automatisch gelöscht worden sein können, bevor sie aufbewahrt werden können; es wurde daher als notwendig erachtet, dass Ermittler jeder Vertragspartei die Möglichkeit haben müssen, in Echtzeit Verkehrsdaten über Nachrichten zu beschaffen, die von einem Computersystem im Hoheitsgebiet anderer Vertragsparteien übertragen werden.
- 3 Die Schweizer Praxis bestätigt diesen Bedarf angesichts der Zunahme von Messaging- und E-Mail-Plattformen, die Anonymisierungsdienste anbieten, nicht nur durch die Verwendung einer End-to-End-Verschlüsselung der Daten (end-to-end encryption), die manchmal mit einer Null-Zugriffs-Verschlüsselung (zero-access encryption) gekoppelt ist, sondern auch durch die fehlende Speicherung von Verbindungsprotokollen (Logs), so dass weder eine rückwirkende Überwachung der Verkehrsdaten noch die Durchsuchung gespeicherter Daten die Identifizierung des Nutzers des Dienstes ermöglichen kann. Das Abfangen von Daten in Echtzeit ermöglicht - ggf. über den in Art. 30 CCC vorgesehenen Mechanismus - die Rückverfolgung zur Quelle der Kommunikation.
- 4 Art. 33 Abs. 2 CCC sieht die Verpflichtung der Vertragsstaaten vor, Rechtshilfe "zumindest in Bezug auf Straftaten zu leisten, bei denen die Echtzeit-Erhebung von Verkehrsdaten in einem ähnlichen Fall innerstaatlich zur Verfügung stehen würde". Es ist also das nationale materielle Strafrecht (insbesondere der Straftatenkatalog), das den Mindestrahmen für die

Verpflichtungen jeder Vertragspartei festlegt. Diese Lösung hat den Vorteil, dass die Klippen der Erstellung einer Liste von Straftaten, für die in dieser Konstellation Rechtshilfe geleistet werden müsste, umschifft werden, was angesichts der unterschiedlichen Kulturen und Rechtssysteme sicherlich zu einem Aufschrei vieler Staaten geführt hätte. Umgekehrt sollen die Vertragsparteien ermutigt werden, möglichst umfassende Rechtshilfe zu leisten, d.h. auch in Situationen, in denen die verfolgten Straftaten eine solche Überwachungsmaßnahme im nationalen Strafverfahren nicht rechtfertigen würden - eine Lösung, für die sich die Schweiz nicht entschieden hat.

Gerade auf der Ebene des nationalen Verfahrensrechts verpflichtet die CCC ⁵ die Vertragsstaaten, gesetzgeberische Maßnahmen zu ergreifen, die sich als notwendig erweisen, um ihre zuständigen Behörden zu ermächtigen, einerseits in ihrem Hoheitsgebiet in Echtzeit Verkehrsdaten zu sammeln oder aufzuzeichnen, die mit bestimmten Kommunikationen verbunden sind, die in ihrem Hoheitsgebiet mithilfe eines Computersystems übermittelt werden, und andererseits die Diensteanbieter zu verpflichten, diese Daten selbst zu sammeln oder aufzuzeichnen oder die Behörden dabei zu unterstützen (Art. 20 CCC).

II. BEGRIFFE

Unter "Verkehrsdaten" versteht die Konvention "alle Daten, die sich auf eine ⁶ über ein Computersystem laufende Kommunikation beziehen, von diesem als Teil der Kommunikationskette erzeugt werden und Ursprung, Ziel, Route, Uhrzeit, Datum, Größe und Dauer der Kommunikation oder die Art des zugrunde liegenden Dienstes angeben" (Art. 1 lit. d CCC). Diese Daten werden von Computern erzeugt, die zur Kommunikationskette gehören, um den Inhalt einer Nachricht von ihrem Ursprung bis zu ihrem Ziel zu transportieren. Sie sind also Hilfskräfte der Kommunikation selbst. Mit "Ursprung" ist eine Telefonnummer, eine IP-Adresse oder ein ähnliches Mittel zur Identifizierung eines Kommunikationsgeräts gemeint, für das ein Dienstanbieter Dienste erbringt. Mit "Ziel" ist ein vergleichbarer Hinweis auf ein Kommunikationsgerät gemeint, zu dem Kommunikationen übertragen werden. Der Ausdruck "Art des zugrunde liegenden Dienstes" bezieht sich auf die Art des Dienstes, der innerhalb des Netzwerks genutzt wird: Dateiübertragung, E-Mail oder Instant Messaging. Zusammenfassend lässt sich sagen, dass Verkehrsdaten Informationen über Absender und Empfänger

sowie über Zeitpunkt, Umfang, Dauer, Art und Route einer Kommunikation liefern.

- 7 Die eigentliche Definition der "Verkehrsdaten" wurde vom Schweizer Gesetzgeber im Rahmen der Umsetzung des Übereinkommens nicht ausdrücklich übernommen (insbesondere in Art. 18b IRSG; vgl. unten III.A.). Der Bundesrat war damals der Ansicht, dass die Definition durch Lehre und Praxis ausreichend beschrieben sei, nämlich: "Verkehrsdaten umfassen insbesondere die Adressierungsressourcen des Ursprungs des Zugriffs, das Datum und die Uhrzeit des Beginns und des Endes der Verbindung, die für das Identifikationsverfahren (Login) verwendeten Daten und die Art der Verbindung". Seit dem 1. September 2016 definiert das Schweizer Recht "sekundäre Telekommunikationsdaten" (Art. 273 StPO mit Verweis auf Art. 8 lit. b BÜPF) als "Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person in Verbindung stand oder steht, sowie die technischen Merkmale der betreffenden Verbindung". Wenn dieser Begriff der Sekundärdaten auch auf die Telekommunikation im Allgemeinen - und nicht nur auf den Computerverkehr - anwendbar ist, umfasst er den Begriff der Verkehrsdaten. Dieser Begriff steht im Gegensatz zu dem Begriff der Inhaltsdaten (vgl. Kommentar zu Art. 34 CCC).
- 8 Art. 33 CCC zielt auf das Sammeln von Verkehrsdaten in Echtzeit ab. Es geht darum, diese Daten bereits heute und für die Zukunft abzufangen, wenn Kommunikation ein- oder ausgeht. Dieser Begriff steht im Gegensatz zum Sammeln bereits vorhandener, aufgezeichneter bzw. auf einem Datenträger (Server, Cloud o. Ä.) gespeicherter Daten, selbst wenn es sich um Verkehrsdaten von bereits erfolgten Kommunikationen handelt. Diese direkte Zeitlichkeit bedeutet, dass die überwachte Person keinen Einfluss auf diese Daten hat. Mit anderen Worten: Die überwachte Person hat typischerweise nicht die Möglichkeit, die Daten vor dem Abfangen zu löschen. Das "Abfangen" dieser Daten erfolgt in der Regel bei einem Drittanbieter (Internet- und/oder Telefonanbieter, abgeleitete Telekommunikationsanbieter wie Unternehmen, die Kommunikationsanwendungen betreiben). Unserer Ansicht nach deckt Art. 33 CCC insbesondere nicht das Abfangen von Daten direkt bei der überwachten Person mittels einer Software vom Typ Trojanisches Pferd (Govware) ab. Hingegen scheint ein Abfangen des Datenverkehrs durch ein spezielles technisches Überwachungsgerät vom Typ IMSI-Catcher nicht ausgeschlossen zu sein (siehe unten III.A.3).

Die abgefangenen Daten müssen "bestimmten Kommunikationen zugeordnet" 9 sein. Die Verwendung des Plurals erklärt sich aus der Tatsache, dass es notwendig sein kann, Verkehrsdaten zu mehreren Kommunikationen zu sammeln, um die Identität der Person festzustellen, die die Kommunikation initiiert hat und/oder an die sie gerichtet ist. Der Begriff "spezifiziert" bedeutet, dass die CCC die Vertragsstaaten nicht dazu verpflichtet, eine allgemeine oder systematische Überwachung und Sammlung einer großen Menge an Verkehrsdaten einzurichten. Diese Bestimmung kann daher nicht als Rechtfertigung für eine unbestimmte Suche nach Beweismitteln ("fishing expedition") dienen. Nach Ansicht der Autoren sind auch die Protokolle der Verbindungen zu einem E-Mail-Postfach (Logs und zugehörige IPs) im Sinne dieser Bestimmung "mit einer spezifischen Kommunikation verbunden". Denn auch wenn die Verbindung zu einer E-Mail-Box nicht notwendigerweise zum Senden oder Empfangen einer Nachricht führt, stellt sie doch eine notwendige Voraussetzung dafür dar. Dieser Ansatz scheint der vom Schweizer Recht gewählte zu sein; wie bereits erwähnt, stützte sich der Bundesrat in der CCC-Botschaft auf eine Definition der Doktrin, die die Adressierungsressourcen einschließlich der Daten und Zeiten der Verbindung und Trennung einschließt. Art. 18b IRSG übernimmt im Übrigen diesen Begriff der "spezifizierten Kommunikation" nicht, was insbesondere den Weg für die Echtzeiterfassung und die vorzeitige Übermittlung von Verbindungsprotokollen öffnet (vgl. unten III.A.4.).

Darüber hinaus muss die spezifizierte Kommunikation im Hoheitsgebiet einer 10 Vertragspartei stattfinden. Dieser Aspekt könnte potenziell problematisch sein, da die Verwendung von Cloud-Technologie es nicht mehr erlaubt, einen Speicherort mit einem bestimmten Staat in Verbindung zu bringen. In der Praxis hat das Kriterium des Ortes, an dem die Daten gespeichert werden, an Bedeutung verloren, zugunsten des Kriteriums des Ortes, an dem sich die (natürliche oder juristische) Person befindet, die über eine effektive Kontrolle über die Daten verfügt. Nach Ansicht der Autoren findet Art. 33 CCC auch in dieser neuen Konstellation Anwendung.

Die Bestimmung verpflichtet die Vertragsparteien, einander bei der Echtzeit- 11 Erhebung dieser Daten Amtshilfe zu leisten. Wenn der Begriff "Sammlung" beim ersten Lesen den Begriff "Übermittlung" einschließt - da diese Sammlung auf Ersuchen und für die Zwecke einer ausländischen Behörde erfolgt -, werden wir sehen, dass der Schweizer Gesetzgeber im Rahmen der

Umsetzung von Art. 33 CCC zwischen diesen beiden Begriffen unterschieden hat (siehe unten III.).

- 12 Schließlich ist das Übereinkommen als solches nicht auf die klassische Telekommunikation (analoge Telefonie) anwendbar, da die Daten mithilfe eines Computersystems übertragen werden müssen. Das Aufkommen des digitalen Telefons und generell die Konvergenz der Telekommunikationstechnologien verwischt jedoch die Unterscheidungen zwischen Telekommunikation und Telematik und die Besonderheiten ihrer Infrastrukturen. Daher gilt die Konvention - insbesondere Art. 20 und 33 CCC - für spezifizierte Kommunikationen, die mithilfe eines Computersystems übertragen werden, wobei die Kommunikation über ein Telekommunikationsnetz übertragen werden kann, bevor sie von einem anderen Computersystem empfangen wird.

III. UMSETZUNG IM SCHWEIZER RECHT

A. Art. 18b IRSG

1. Historischer Hintergrund

- 13 Art. 18b IRSG wird im Zuge der Ratifizierung der CCC durch die Schweiz eingeführt. Die CCC-Botschaft erinnert daran, dass Echtzeit-Überwachungsmassnahmen den überwachten Personen grundsätzlich unbekannt bleiben müssen; dieses Postulat lässt sich nur schwer mit dem Grundprinzip des IRSG vereinbaren, wonach keine Informationen aus der Geheimsphäre einer Person an das Ausland weitergegeben werden dürfen, ohne dass diese zuvor die Möglichkeit hatte, sich dagegen zu wehren. Art. 18b IRSG ermöglicht es somit, die Anforderungen von Art. 33 CCC zu erfüllen.

2. Definitionen

- 14 Nach Art. 18b Abs. 1 IRSG kann die mit der Behandlung eines Rechtshilfeersuchens betraute Bundes- oder Kantonsbehörde vor Abschluss des Rechtshilfeverfahrens die Übermittlung von Daten über den Computerverkehr ins Ausland anordnen, wenn aus den vorläufigen Massnahmen hervorgeht, dass sich die Quelle der Mitteilung, die Gegenstand des Rechtshilfeersuchens ist, im Ausland befindet (Abs. 1 lit. a) oder wenn diese Daten von der Vollzugsbehörde aufgrund einer genehmigten Anordnung

zur Echtzeitüberwachung gesammelt werden (Art. 269-281 StPO; Abs. 2 lit. b). Während die Annahme in lit. a die Ausführungsgesetzgebung zu Art. 30 CCC darstellt, setzt lit. b die internationalen Verpflichtungen der Schweiz um, die sich aus Art. 33 CCC ergeben. Dennoch sichert diese Bestimmung noch nicht die Gewährung der Rechtshilfe, da Abs. 2 die Verwendung dieser Daten als Beweismittel verbietet, bevor der Entscheid über die Gewährung und den Umfang der Rechtshilfe (Art. 80d IRSG) rechtskräftig geworden ist. Die auf Art. 18b IRSG gestützte Verfügung, die der ersuchenden Behörde einen raschen Zugriff auf die Daten ermöglicht, ist eine Zwischenverfügung, die dann den Weg für das nach schweizerischem Recht erforderliche klassische Rechtshilfeverfahren ebnet. Insofern hat der Gesetzgeber darauf geachtet, die Erhebung der Daten und ihren raschen Zugriff durch die ersuchende Behörde von der Rechtshilfe selbst zu unterscheiden und damit die schweizerische Rechtsordnung mit den internationalen Verpflichtungen in Einklang zu bringen.

3. Verfahren

Art. 18b Abs. 1 lit. b IRSG verweist auf die Art. 269 bis 281 StPO und damit insbesondere, wenn es um die Überwachung von sekundären Telekommunikationsdaten geht, auf Art. 273 StPO. Letzterer sieht insbesondere vor, dass nur ein dringender Verdacht der Begehung von Verbrechen und Vergehen (Art. 10 Abs. 2 und 3 StGB) es der Staatsanwaltschaft erlaubt, sekundäre Fernmeldedaten zu beschaffen. Somit wollte der Schweizer Gesetzgeber den Anwendungsbereich von Art. 33 CCC nicht auf Straftaten ausdehnen, die die Anwendung dieser Massnahmen nach Schweizer Recht nicht erlauben würden, wie dies in Art. 33 Abs. 2 CCC vorgeschlagen wird. 15

Art. 18b Abs. 1 lit. b IRSG stellt eine Abweichung vom klassischen Rechtshilfesystem dar, wonach vor jeder Übermittlung von Beweismitteln ins Ausland das rechtliche Gehör der von einer Rechtshilfemaßnahme betroffenen Person gewährleistet und eine ordnungsgemäß zugestellte und rechtskräftige Schlussverfügung erlassen werden muss (Art. 80d IRSG). Vor Inkrafttreten dieser Bestimmung konnte die Schweiz solche Daten aus einer geheimen Überwachung nicht ohne vorgängige Information der betroffenen Person (sofern diese in der Schweiz wohnhaft ist oder hier ein Zustellungsdomizil hat; vgl. Art. 80m IRSG) ins Ausland liefern, was die 16

Massnahme für das ausländische Verfahren oft nutzlos machte oder dieses sogar gefährden konnte.

- 17 Neu wird die Vollzugsbehörde nach dem Eintreten (Art. 80a IRSG) die Überwachungsmassnahme über den Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF; Art. 273 StPO i.V.m. Art. 60 ff. VÜPF) anordnen.
- 18 Anschließend muss sie die Maßnahme innerhalb von 24 Stunden nach der Anordnung durch das Zwangsmassnahmengericht genehmigen lassen (Art. 274 Abs. 1 StPO). Zu beachten ist, dass das Bundesgericht bezüglich der in Art. 273 StPO aufgestellten Bedingung des Vorliegens eines "dringenden Verdachts" zu Recht darauf hingewiesen hat, dass gemäss den Rechtshilferegeln und der ständigen Rechtsprechung die Art. 14 EUeR, 28 IRSG und 10 IRSV die ersuchende Behörde verpflichten, zu erklären, worin ihr Verdacht besteht, nicht aber, ihn zu beweisen oder auch nur glaubhaft zu machen. Vorbehaltlich des Verbots von Sondierungsgesuchen muss der Verdacht der ersuchenden Behörde daher nicht besonders schwerwiegend oder präzise sein. Denn auch wenn das innerstaatliche Recht anzuwenden ist, wenn es für die Zusammenarbeit günstiger ist als das Vertragsrecht, darf es hingegen keine materiellen Bedingungen für die Rechtshilfe aufstellen, die im Vertragsrecht nicht vorgesehen sind.
- 19 Das Zwangsmassnahmengericht entscheidet innerhalb von fünf Tagen (Art. 274 Abs. 2 StPO). Wird die Überwachung abgelehnt, müssen die gesammelten Unterlagen und Aufzeichnungen sofort vernichtet werden (Art. 277 Abs. 1 StPO). Wird die Bewilligung erteilt, ist zu beachten, dass Art. 279 StPO, der die Mitteilung an den Beschuldigten oder den Dritten, der Gegenstand der Überwachung ist, vorsieht und diesen sowie dem überwachten Fernmeldedienst ein Beschwerderecht einräumt (Art. 279 Abs. 3 StPO), trotz des Verweises in Art. 18b Abs. 2 lit. a auf die Art. 269 bis 281 StPO keine Anwendung findet. Die im Bereich der internationalen Rechtshilfe in Strafsachen anwendbaren Übereinkommen und Gesetze weichen nämlich vom üblichen System der StPO ab, die nur dann Anwendung findet, wenn sie für die Zusammenarbeit günstiger ist als diese anwendbaren Übereinkommen und Gesetze (Günstigkeitsprinzip). Dies hat insbesondere zur Folge, dass die Parteistellung, das Recht auf Zustellung und die Rechtswege durch die spezifischen Rechtshilfebestimmungen geregelt werden. Gemäss Art. 80m Abs. 1 IRSG ist die Pflicht zur Zustellung von Rechtshilfeentscheiden auf

Personen beschränkt, die in der Schweiz wohnhaft sind oder hier ihren Wohnsitz haben. Allfällige gegenteilige Hinweise seitens des TMC, sei es durch Hinweis auf das Gesetz oder durch Anbringen von Bedingungen im Sinne von Art. 274 Abs. 2 StPO, wären somit ungültig, da das TMC nicht für diesen Aspekt des Verfahrens zuständig ist. Es wird Aufgabe der Vollzugsbehörde sein, im Rahmen des Rechtshilfeverfahrens - also gegebenenfalls nach der in Art. 18b IRSG vorgesehenen vorzeitigen Übermittlung - für die Einhaltung dieser anwendbaren Übereinkommen und Gesetze zu sorgen und lediglich die in Art. 80m IRSG vorgesehenen Zustellungen vorzunehmen.

Nach Erhalt der Daten aus der Überwachung kann die Vollzugsbehörde eine 20 auf Art. 18b IRSG gestützte Zwischenverfügung erlassen, um die vorzeitige Übermittlung der Daten an die ersuchende Behörde anzuordnen. Die Verfügung sowie die Anordnung und Bewilligung der Überwachung werden dem BJ mitgeteilt (Art. 18b Abs. 3 IRSG). Wenn die Überwachung langfristig angelegt ist und regelmäßig Daten gesammelt werden, kann die Anordnung alle künftigen Daten aus der genehmigten Überwachung abdecken, so dass die Vollstreckungsbehörde (oder gegebenenfalls die Polizei) die Daten nach Eingang weiterleiten kann. Da die betroffene Person in diesem Stadium nicht benachrichtigt wird und in Anbetracht der durch Art. 18b Abs. 2 IRSG auferlegten Grenzen, verletzt ein solches Vorgehen nicht die Rechte der Parteien des Rechtshilfeverfahrens und muss zugelassen werden können.

Allerdings sollte bei jeder vorzeitigen Übermittlung an die ersuchende 21 Behörde daran erinnert werden, dass diese Daten nicht als Beweismittel verwendet werden dürfen, bevor der Entscheid über die Gewährung und den Umfang der Rechtshilfe rechtskräftig geworden ist (Art. 18b Abs. 2 IRSG). Dadurch wird der Rechtsschutz im Nachhinein gewährleistet. Es ist auch wesentlich, eine Aufzeichnung - zumindest in Form einer Liste - der vorzeitig übermittelten Daten aufzubewahren, damit die Vollzugsbehörde am Ende des Rechtshilfeverfahrens genau weiß, auf welche Daten sich die endgültige Schlussverfügung beziehen muss.

In der Praxis kann die Vollzugsbehörde, wenn die von der 22 Überwachungsmaßnahme betroffene Person unbekannt ist, keinen Wohnsitz oder Aufenthalt in der Schweiz hat oder sogar eine falsche Identität verwendet, die Verwendung der Daten als Beweismittel rasch durch eine Schlussverfügung bestätigen. Da die Schlussverfügung nur dem BJ zugestellt

wird (Art. 80h lit. a IRSG), bleibt das Geheimnis über das Bestehen der Massnahmen gewahrt.

- 23 Wenn die von der Überwachungsmassnahme betroffene Person in der Schweiz wohnhaft ist oder hier ihren Wohnsitz hat, muss ihr das rechtliche Gehör gewährt werden (Art. 80m Abs. 1 IRSG in Verbindung mit Art. 80b IRSG), was bedeutet, dass sie vor Erlass der Schlussverfügung über die Massnahme informiert werden muss und Gelegenheit haben muss, sich schriftlich zu äussern. Art. 18b IRSG erlaubt es gerade, die Information der betroffenen Person und die Gewährung des rechtlichen Gehörs so lange hinauszuschieben, wie es für das Verfahren im Ausland notwendig ist. In der Praxis wird die Vollzugsbehörde regelmässig bei der ersuchenden Behörde nachfragen müssen, ob es für das Verfahren im Ausland notwendig ist, die in der Schweiz angeordnete Überwachungsmassnahme geheim zu halten.
- 24 Die Schlussverfügung kann beim Bundesstrafgericht angefochten werden (Art. 80e IRSG). Die Zwischenverfügung über die vorzeitige Übermittlung von Verkehrsdaten gemäss Art. 18b IRSG kann zusammen mit der Schlussverfügung angefochten werden (Art. 80e Abs. 1 IRSG). Eine sofortige Beschwerde gegen die Zwischenverfügung scheint möglich, wenn die Vollzugsbehörde nicht die notwendigen Vorsichtsmassnahmen getroffen hat, um sicherzustellen, dass die Vorlagen in Art. 18b Abs. 2 IRSG eingehalten werden. Eine Beschwerde an das Bundesgericht bleibt unter den restriktiven Bedingungen von Art. 84 BGG (besonders wichtiger Fall) möglich. Ein Teil der Lehre argumentiert, dass bei Gutheissung der Beschwerde die übermittelten Informationen aus der ausländischen Akte entfernt werden müssen. Dies ist sicherlich der Fall, wenn sich die ausländische Behörde dazu verpflichtet hat, obwohl diese Verpflichtung nicht in Art. 18b IRSG enthalten ist.
- 25 Der sehr weite Wortlaut von Art. 18b Abs. 1 lit. b IRSG scheint auch die vorzeitige Übermittlung von Computerverkehrsdaten zu erlauben, wenn diese mittels IMSI-Catcher (Art. 269bis StPO), Govware (Art. 269ter StPO) oder anderen technischen Überwachungsvorrichtungen (Art. 280 StPO) abgefangen wurden, obwohl Art. 33 CCC eine solche Verpflichtung nicht vorsehen würde.

4. Einige materielle Abgrenzungen

Im Gegensatz zum Wortlaut von Art. 33 CCC ist Art. 18b IRSG nicht auf ²⁶ "spezifizierte Kommunikationen" beschränkt. So kann das Verbindungsprotokoll (Logs) zu einer E-Mail-Box mittels Echtzeitüberwachung erhalten und im Voraus an die ersuchende Behörde übermittelt werden, auch wenn keine Kommunikation stattfindet (z.B. keine gesendete E-Mail während dieser Verbindungssitzung oder keine empfangene E-Mail).

Das Bundesgericht hatte Gelegenheit zu bekräftigen, dass Art. 18b IRSG eine ²⁷ Rechtsgrundlage darstellt, die die vorzeitige Übermittlung von Verkehrsdaten aus einer Echtzeitüberwachung ermöglicht, wobei Inhaltsdaten mangels einer gesetzlichen oder vertraglichen Grundlage ausgeschlossen sind.

Im gleichen Urteil öffnete das Bundesgericht die vorzeitige ²⁸ Datenübermittlung im Sinne von Art. 18b IRSG für Telefonverkehrsdaten. Demnach sind Sekundärdaten aus der aktiven Überwachung eines Telefonanschlusses (z.B. angerufene oder anrufende Nummern, Dauer des Telefongesprächs oder auch aktivierte Antenne) Daten, die auf der Grundlage von Art. 18b IRSG vorzeitig an eine ausländische Behörde weitergegeben werden können sollten. Unserer Ansicht nach ist diese Auslegung des Bundesgerichts alles in allem logisch angesichts der allgemeinen Digitalisierung der Telekommunikationssysteme und damit des zunehmend hinfälligen und künstlichen Charakters der Unterscheidung zwischen einem klassischen Telekommunikationssystem einerseits und einem Computersystem andererseits.

Art. 18b IRSG hat einen weiteren Vorteil: Wenn die Sammlung von frühzeitig ²⁹ übermittelten Verkehrsdaten ergibt, dass eine weitere Überwachungsmaßnahme auf einem anderen Konto, einer anderen Leitung usw. in der Schweiz oder im Ausland gerechtfertigt ist, kann die ersuchende Behörde sofort die Durchführung einer solchen Massnahme beantragen.

B. Unterscheidungen

Die in Art. 18b IRSG vorgesehene vorzeitige Übermittlung von Informationen ³⁰ im Zusammenhang mit dem Computerverkehr ist von der spontanen Übermittlung von Beweismitteln und Informationen (Art. 67a IRSG) zu unterscheiden, die ebenfalls eine Ausnahme von dem Grundsatz darstellt,

dass vor einer Übermittlung ins Ausland eine rechtskräftige Schlussverfügung erforderlich ist. Im Unterschied zum System von Art. 67a IRSG greift Art. 18b IRSG notwendigerweise im Zusammenhang mit der Ausführung eines ausländischen Rechtshilfeersuchens zur Erlangung dieser Beweismittel ein. Art. 18b IRSG sieht nämlich keineswegs eine "spontane" vorzeitige Übermittlung von Verkehrsdaten vor. Darüber hinaus verbietet Art. 67a IRSG die Übermittlung von Beweismitteln, sobald sie den Geheimbereich berühren (Art. 67 Abs. 4 IRSG). In diesem Fall dürfen nur Informationen an eine ausländische Behörde geliefert werden (Art. 67a Abs. 5 IRSG).

- 31 Die in Art. 18b IRSG vorgesehene vorzeitige Übermittlung von Informationen im Zusammenhang mit dem Computerverkehr ist auch von der dynamischen Rechtshilfe (Art. 80dbis IRSG), die ausnahmsweise eine vorzeitige Übermittlung von Informationen oder Beweismitteln erlaubt, (a) wenn ausländische Ermittlungen in Fällen von organisierter Kriminalität oder Terrorismus ohne diese Rechtshilfemaßnahme übermäßig erschwert würden, insbesondere wegen der Gefahr von Kollusion, oder weil die Vertraulichkeit des Verfahrens gewahrt werden muss, oder (b) um eine ernste und unmittelbare Gefahr abzuwenden, insbesondere die Begehung eines terroristischen Akts. Die Einführung dieser neuen Bestimmung im Jahr 2021 - zusammen mit neuen Regeln für die gemeinsame Ermittlungsgruppe - wurde als wichtiger erster Schritt hin zu flexibleren Regeln und einer schnelleren und reaktionsschnelleren, auf internationalem Vertrauen basierenden Rechtshilfe angesehen. Was den sachlichen Anwendungsbereich betrifft, so kennt Art. 18b IRSG keine Einschränkungen, während Art. 80dbis IRSG sich - außer bei ernster und unmittelbarer Gefahr - auf die organisierte Kriminalität und den Terrorismus beschränkt. Umgekehrt sieht Art. 80dbis IRSG vor, dass jede Art von Beweismitteln oder Informationen auf diesem Weg vorzeitig übermittelt werden kann, während der Anwendungsbereich von Art. 18b IRSG auf Daten über den Computerverkehr beschränkt ist, wobei jedoch daran erinnert werden muss, dass das Bundesgericht den Weg für eine analoge Anwendung von Art. 18b IRSG in Bezug auf die Telefonüberwachung geebnet hat. Schließlich sieht Art. 18b IRSG - zumindest ausdrücklich - keine vorherige Verpflichtung der ersuchenden Behörde vor, da die Vollstreckungsbehörde die ersuchende Behörde darüber informieren muss, dass die vorzeitig übermittelten Daten nicht als Beweismittel verwendet werden dürfen, bevor die Entscheidung über die Gewährung und den Umfang

der Rechtshilfe rechtskräftig geworden ist (Art. 18b Abs. 2 IRSG). In diesem Punkt ist Art. 80dbis IRSG formalistischer (vgl. Art. 80dbis Abs. 4 IRSG).

Schließlich scheint eine vorzeitige Übermittlung im Sinne von Art. 18b IRSG ³² im Rahmen einer gemeinsamen Ermittlungsgruppe (GEG; oder Joint Investigation Team, JIT; Art. 80dter-80dduodecies IRSG); tatsächlich ist der eingeschränkte materielle Anwendungsbereich von Art. 80dbis IRSG nach Ansicht der Autoren trotz des unglücklichen Verweises in Art. 80docties IRSG auf die Voraussetzungen von Art. 80dbis IRSG nicht auf gemeinsame Ermittlungsteams anwendbar.

Die Autoren haben den vorliegenden Beitrag in persönlicher Eigenschaft verfasst. Die dargestellten Einschätzungen und Meinungen sind ihre eigenen und binden die Bundesanwaltschaft nicht.

LITERATURVERZEICHNIS

Böhi Simon, commentaire de l'art. 18b EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1^{ère} édition, Bâle 2015.

Dangubic Miro/Clerc Yves, Art. 80d^{bis} IRSG – ein Überblick, *forumpoenale* 4 (2022) p. 287.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2e édition., Zurich et al. 2015.

Glutz Alexander M., commentaire de l'art. 67a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1^{ère} édition, Bâle 2015.

Hansjakob Thomas/Pajarola Umberto, commentaire de l'art. 272 CPP, in : Donatsch Andreas/Lieber Viktor/ Summers Sarah/Wohlers Wolfgang (édit.), Kommentar zur Schweizerischen Strafprozessordnung StPO, 3^e édition, Zurich 2020.

Isenring Bernhard/Maybud Roy D./Quiblier Laura, Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick, *SJZ* 115 (2019) p. 439.

Ludwiczak Glassey Maria/Bonzanigo Francesca, L'artificielle distinction entre « informations » et « moyens de preuve » en entraide pénale internationale, *Revue Pénale Suisse* 140/2022 p. 402-427.

Ludwiczak Maria, L'entraide pénale internationale 'dynamique' en bref. Le projet, les débats, le compromis, *Pratique juridique actuelle*, 1 (2021) p. 71–75.

Zimmermann Robert, *La coopération judiciaire internationale en matière pénale*, 5^e édition, Berne 2019.

MATERIALIENVERZEICHNIS

Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013, FF 2013 2379, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2013/512/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2013-512-fr-pdf-a.pdf>, consulté en janvier 2024 (cité : Message LSCPT).

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité du 18 juin 2010, FF 2010 4275, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2010/813/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2010-813-fr-pdf-a.pdf>, consulté en janvier 2024 (cité : Message CCC).

Rapport explicatif de la Convention sur la cybercriminalité du 23 novembre 2001, Conseil de l'Europe, Série des traités européens – no 185, consultable sous <https://rm.coe.int/16800ccea4>, consulté en janvier 2024 (cité : Rapport explicatif du Conseil de l'Europe).

ACHTUNG: Diese Version des Kommentars ist eine automatische maschinelle Übersetzung des Originals. Die Originalversion ist französisch. Die Übersetzung wurde mit www.deepl.com durchgeführt. Nur die Originalversion ist autoritativ. Die übersetzte Form des Kommentars kann nicht zitiert werden.

KOMMENTIERUNG ZU

Art. 34 CCC (Übereinkommen über die Cyberkriminalität [Cybercrime Convention])

Eine Kommentierung von Nicolas Bottinelli / Julien Wenger

ZITIERVORSCHLAG

Nicolas Bottinelli/Julien Wenger, Kommentierung zu Art. 34 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar zum Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Kurzzitat: OK-Bottinelli/Wenger, Art. 34 CCC N. XXX.

Art. 34 Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit

Die Vertragsparteien leisten einander Rechtshilfe bei der Erhebung oder Aufzeichnung von Inhaltsdaten bestimmter Kommunikationen, die mittels eines Computersystems übermittelt werden, in Echtzeit, soweit dies nach ihren anwendbaren Verträgen und innerstaatlichen Rechtsvorschriften zulässig ist.

GLIEDERUNG

I. Einleitung 343

II. Begriffe 343

III. Umsetzung im Schweizer Recht 346

 A. Das Abfangen von Inhaltsdaten im Schweizer Recht 346

 B. Unterscheidungen und Sonderfälle 349

 1. Vorzeitige Übermittlung von Inhaltsdaten? 349

 2. Unterscheidung zwischen einer Hinterlegungsanordnung (Art. 265 StPO) und einer Überwachungsmaßnahme (Art. 269 ff. StPO), insbesondere im Hinblick auf E-Mail-Postfächer. 350

 3. Verwendung einer falschen Identität 351

Literaturverzeichnis 352

Materialienverzeichnis..... 352

I. EINLEITUNG

Art. 34 CCC, der in Kapitel III der Cybercrime Convention mit dem Titel "Internationale Zusammenarbeit" enthalten ist, befasst sich mit der internationalen Zusammenarbeit im Zusammenhang mit Inhaltsdaten, im Gegensatz zu Verkehrsdaten, die in Art. 33 CCC behandelt werden.

Die CCC erkennt die Bedeutung der Möglichkeit der Überwachung von Inhaltsdaten für nationale Strafverfahren an (Art. 21 CCC): Die Erhebung von Telekommunikationsinhaltsdaten war schon immer ein nützliches Ermittlungsinstrument, um festzustellen, ob die Kommunikation illegal ist, und um Beweise für vergangene oder zukünftige Straftaten zu erbringen. Computergestützte Kommunikation kann die gleiche Art von Straftat darstellen oder beweisen, bietet aber durch die Übertragung großer Datenmengen (Text, Bilder und Ton) umfassendere Möglichkeiten. Es ist nicht möglich, die schädigende und illegale Natur dieser Kommunikation in Echtzeit festzustellen, ohne den Inhalt der Nachricht abzufangen. Wenn die Strafverfolgungsbehörden nicht in der Lage wären, Straftaten zum Zeitpunkt ihrer Begehung festzustellen und zu verhindern, wären sie darauf beschränkt, längst vergangene Straftaten zu untersuchen, bei denen der Schaden bereits eingetreten ist. Daraus folgt, dass die Echtzeit-Überwachung von Daten über den Inhalt von Computerkommunikationen mindestens, wenn nicht sogar wichtiger ist als die Echtzeit-Überwachung der Telekommunikation.

Art. 34 CCC verpflichtet die Vertragsstaaten jedoch nicht, bei der grenzüberschreitenden Sammlung dieser Daten kooperieren zu können; höchstens verweist der Erläuternde Bericht des Europarats auf die bewährten Praktiken in der Empfehlung von 1985 über die Anwendung des EUeR auf die Überwachung des Fernmeldeverkehrs. Das Zweite Zusatzprotokoll zum CCC vom 12. Mai 2022 befasst sich nicht mit dieser Maßnahme, ebenso wenig wie die vorbereitenden Arbeiten zum Dritten Zusatzprotokoll zum EUeR.

II. BEGRIFFE

Art. 34 CCC sieht vor, dass die Vertragsparteien einander in diesem Rahmen Rechtshilfe leisten, "soweit dies nach ihren anwendbaren Verträgen und innerstaatlichen Gesetzen zulässig ist". Im Gegensatz zu Art. 33 CCC in Bezug auf Computerverkehrsdaten erlegt Art. 34 CCC den Vertragsstaaten keine

strikten Verpflichtungen auf, wenn es um die Rechtshilfe beim Abfangen von Daten geht, die sich auf den Inhalt der Computerkommunikation beziehen. Die Entscheidung, sich auf innerstaatliche Regelungen und Gesetze zu verlassen, ist durch den sehr einschneidenden Charakter des Abhörens und die noch in den Kinderschuhen steckende Praxis der Rechtshilfe in diesem Bereich gerechtfertigt.

- 5 Der Begriff "Inhaltsdaten" wird in der Konvention nicht definiert. Er bezieht sich auf den Informationsgehalt der Kommunikation, d. h. die Bedeutung der Kommunikation oder die durch die Kommunikation übermittelte Nachricht oder Information (mit Ausnahme von Verkehrsdaten). Konkret bedeutet "Inhaltsdaten" die eigentliche Kommunikation, ihren eigentlichen Gegenstand, d. h. insbesondere den Text einer E-Mail (einschließlich der schweizerischen Gestaltung der Rubrik "Betreff"), einer Instant Message, etwaige Anhänge oder auch die übertragene Datei oder den Audio- und/oder Videostrom. Dieser Begriff steht im Gegensatz zum Begriff "Verkehrsdaten", der im Wesentlichen die Elemente der Kommunikationskette umfasst (Ursprung, Ziel, Route, Uhrzeit, Datum, Größe und Dauer der Kommunikation oder die Art des zugrunde liegenden Dienstes; Art. 1 lit. d CCC). Diese Unterscheidung ist bei Überwachungsmaßnahmen von grundlegender Bedeutung und hat direkte Auswirkungen auf die Gewährung internationaler Rechtshilfe. So erlaubt die Schweiz unter bestimmten Voraussetzungen die rasche und vorzeitige Übermittlung von Computerverkehrsdaten auf der Grundlage von Art. 18b IRSG, was bei Inhaltsdaten ausgeschlossen ist (vgl. unten III.B.1.).
- 6 Art. 34 CCC deckt das "Abfangen in Echtzeit" ab, ein Begriff, der im Gegensatz zur Durchsuchung von Daten steht, die auf einem Computermedium (Server, Cloud oder andere) aufgezeichnet bzw. gespeichert sind. Diese unmittelbare Zeitlichkeit bedeutet, dass die überwachte Person keinen Einfluss auf diese Daten hat. Mit anderen Worten, diese verfügt nicht über die Möglichkeit, sie vor dem Abfangen zu löschen. Das "Abfangen" dieser Daten erfolgt in der Regel bei einem Drittanbieter (Internet- und/oder Telefonanbieter, Anbieter von abgeleiteten Kommunikationsdiensten [im Folgenden: CSD], wie z. B. Unternehmen, die Kommunikationsanwendungen betreiben). Unseres Erachtens deckt Art. 34 CCC insbesondere nicht das Abfangen von Inhaltsdaten direkt beim Ermittlungsverdächtigen mittels Trojaner-Software (Govware) ab; es ist

jedoch nicht ausgeschlossen, dass Art. 34 CCC als Grundlage für das Abfangen von Kommunikation mittels eines IMSI Catchers dienen kann.

Die Bestimmung sieht vor, dass die Rechtshilfe für das "Sammeln oder 7 Aufzeichnen" von Daten in Echtzeit gewährt wird. Unserer Ansicht nach, auch wenn die Unterscheidung zwischen diesen beiden Begriffen unsicher erscheint, umfasst die Sammlung den ursprünglichen Akt des Sammelns der Daten, während die Aufzeichnung ihre Aufbewahrung im Hinblick auf ihre Übermittlung an die ersuchende Behörde bzw. ihre Verwendung im Rahmen der strafrechtlichen Ermittlungen betrifft. Diese beiden Begriffe stellen somit zwei aufeinanderfolgende Schritte dar, die für die Durchführung der Überwachung erforderlich sind, aber ihre Unterscheidung ist kaum von praktischer Bedeutung. Außerdem werden wir sehen, dass der Schweizer Gesetzgeber zwischen den Begriffen "Erhebung" und "Aufzeichnung" und "Übermittlung" unterschieden hat, da diese Erhebung auf Ersuchen und für die Zwecke einer ausländischen Behörde erfolgt, wenn man sie auf den ersten Blick liest. Die in Ausführung eines ausländischen Rechtshilfeersuchens gesammelten Daten unterliegen nämlich nicht dem üblichen Rechtshilfeverfahren vor jeder Übermittlung des Beweismittels ins Ausland (vgl. insbesondere infra III.A. zu Art. 18a IRSG).

Die abgefangenen Daten müssen sich auf "spezifische Kommunikationen" 8 beziehen. Dieser Begriff ist so zu verstehen, dass das Übereinkommen die allgemeine oder systematische Überwachung und Sammlung großer Mengen inhaltsbezogener Daten (Massenüberwachung) weder verlangt noch zulässt. Das Übereinkommen erlaubt auch keine "Fishing Expedition", bei der man hofft, kriminelle Aktivitäten zu entdecken, was etwas ganz anderes ist als die Untersuchung von konkreten Fällen illegaler Handlungen. Natürlich bedeutet dieser Begriff nicht, dass es notwendig ist, die spezifische zukünftige Kommunikation zwischen verschiedenen Computersystemen zu überwachen, da es nur selten möglich ist, zukünftige Kommunikationen zu antizipieren. Was jedoch zu beachten ist, ist, dass der Gegenstand der Überwachung (E-Mail-Adresse, Benutzerkennung einer E-Mail-Anwendung usw.) genau bestimmt werden muss.

Schließlich ist das Übereinkommen als solches nicht auf die klassische 9 Telekommunikation (analoge Telefonie) anwendbar, da die Daten mithilfe eines Computersystems übertragen werden müssen. Das Aufkommen des digitalen Telefons und generell die Konvergenz der

Telekommunikationstechnologien verwischt jedoch die Unterscheidungen zwischen Telekommunikation und Telematik und die Besonderheiten ihrer Infrastrukturen. Daher gilt die Konvention - insbesondere die Art. 21 und 34 CCC - für spezifizierte Kommunikationen, die mithilfe eines Computersystems übertragen werden, wobei die Kommunikation über ein Telekommunikationsnetz übertragen werden kann, bevor sie von einem anderen Computersystem empfangen wird.

III. UMSETZUNG IM SCHWEIZER RECHT

A. Das Abfangen von Inhaltsdaten im Schweizer Recht

- 10 Während Art. 33 CCC die Einführung von Art. 18b IRSG bewirkte, der eine vorzeitige Übermittlung (d.h. vor Rechtskraft einer Abschlussverfügung) von Computerverkehrsdaten an die ersuchende Behörde ermöglicht, führte Art. 34 CCC - zumindest direkt - zu keiner Änderung der schweizerischen Gesetzgebung im Bereich des Abfangens von Inhaltsdaten. Es gelten daher, mit einigen Vorbehalten, die üblichen Regeln des schweizerischen Strafprozessrechts (Art. 269 ff. StPO), die in Art. 18a IRSG verankert sind.
- 11 Art. 18a IRSG ist die Top-Bestimmung für die Überwachung des Post- und Fernmeldeverkehrs im Bereich der Rechtshilfe. Daraus geht im Wesentlichen hervor, dass auf ausdrückliches Ersuchen einer ersuchenden Behörde die Staatsanwaltschaft - in bestimmten Fällen sogar das Bundesamt für Justiz - eine solche Überwachung anordnen kann (Abs. 2) und dass die Anordnung der Zustimmung des zuständigen Zwangsmassnahmengerichts bedarf (Abs. 3). Im Übrigen verweist Art. 18a IRSG auf die Art. 269 bis 279 StPO sowie auf das Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Dieser Verweis auf Art. 269 ff. StPO - insbesondere auf den Straftatenkatalog in Art. 269 StPO - entspricht dem "Spektrum schwerer Straftaten", das die Vertragsparteien in ihrem innerstaatlichen Recht definieren müssen, um das Abfangen von Inhaltsdaten zu ermöglichen (Art. 21 und 34 CCC). Der allgemeine Verweis auf die Bestimmungen des IRSG erlaubt es auch, davon auszugehen, dass Art. 18a IRSG sowohl auf gewöhnliche Kommunikation (klassische analoge Telefonie) als auch auf Kommunikation im Zusammenhang mit einem Computersystem anwendbar ist (vgl. not. Art. 2 lit. c IRSG).

In der Praxis wird die Vollzugsbehörde nach dem Eintreten (Art. 80a IRSG) 12 die Überwachungsmassnahme über den Dienst Überwachung Post- und Fernmeldeverkehr (nachfolgend: Dienst ÜPF; Art. 269 StPO i.V.m. Art. 55 ff. VÜPF) anordnen. So wird es möglich sein, die Echtzeit-Überwachung von Inhalten und Sekundärdaten von Netzzugangsdiensten (Art. 55 VÜPF), die Echtzeit-Überwachung von Inhalten und Sekundärdaten von Telefon- und Multimediadiensten (Art. 57 VÜPF) oder die Echtzeit-Überwachung von Inhalten und Sekundärdaten von E-Mail-Diensten (Art. 59 VÜPF) anzuordnen.

Die Vollzugsbehörde muss die Massnahme dann innerhalb von 24 Stunden 13 nach der Anordnung durch das Zwangsmassnahmengericht genehmigen lassen (Art. 274 Abs. 1 StPO). Zu beachten ist, dass das Bundesgericht bezüglich der in Art. 269 Abs. 1 lit. a StPO aufgestellten Bedingung des Vorliegens eines "dringenden Verdachts" zu Recht darauf hingewiesen hat, dass gemäss den Rechtshilferegeln und der ständigen Rechtsprechung Art. 14 EUeR, 28 IRSG und 10 IRSV die ersuchende Behörde verpflichtet, zu erklären, worin ihr Verdacht besteht, nicht aber, ihn zu beweisen oder auch nur glaubhaft zu machen. Vorbehaltlich des Verbots von Sondierungsgesuchen muss der Verdacht der ersuchenden Behörde daher nicht besonders schwerwiegend oder präzise sein. Denn auch wenn das innerstaatliche Recht Anwendung finden muss, wenn es für die Zusammenarbeit günstiger ist als das Vertragsrecht, darf es hingegen keine materiellen Bedingungen für die Rechtshilfe aufstellen, die nicht im Vertragsrecht vorgesehen sind.

Das Zwangsmassnahmengericht entscheidet innerhalb von fünf Tagen (Art. 14 274 Abs. 2 StPO). Wird die Überwachung abgelehnt, müssen die gesammelten Unterlagen und Aufzeichnungen sofort vernichtet werden (Art. 277 Abs. 1 StPO). Wird die Bewilligung erteilt, ist zu beachten, dass Art. 279 StPO, der die Mitteilung an den Beschuldigten oder den Dritten, der Gegenstand der Überwachung ist, vorsieht und diesen sowie dem überwachten Fernmeldedienst ein Beschwerderecht einräumt (Art. 279 Abs. 3 StPO), trotz des Verweises von Art. 18a Abs. 4 IRSG auf die Art. 269 bis 279 StPO keine Anwendung findet. Die im Bereich der internationalen Rechtshilfe in Strafsachen anwendbaren Übereinkommen und Gesetze weichen nämlich vom üblichen System der StPO ab, die nur dann Anwendung findet, wenn sie für die Zusammenarbeit günstiger ist als diese anwendbaren Übereinkommen und Gesetze (Günstigkeitsprinzip). Dies hat insbesondere zur Folge, dass die

Parteistellung, das Recht auf Zustellung und die Rechtswege durch die spezifischen Rechtshilfebestimmungen geregelt werden. Gemäss Art. 80m Abs. 1 IRSG ist die Pflicht zur Zustellung von Rechtshilfeentscheiden auf Personen beschränkt, die in der Schweiz wohnhaft sind oder hier ihren Wohnsitz haben. Allfällige gegenteilige Hinweise seitens des TMC, sei es durch Hinweis auf das Gesetz oder durch Anbringen von Bedingungen im Sinne von Art. 274 Abs. 2 StPO, wären somit ungültig, da das TMC nicht für diesen Aspekt des Verfahrens zuständig ist. Es wird Aufgabe der Vollzugsbehörde sein, im Rahmen des Rechtshilfeverfahrens für die Einhaltung dieser Übereinkommen und anwendbaren Gesetze zu sorgen und lediglich die in Art. 80m IRSG vorgesehenen Zustellungen vorzunehmen.

- 15 Nach Erhalt der Überwachungsdaten muss die Vollzugsbehörde das Recht auf Anhörung der von der Überwachungsmassnahme betroffenen Person gewährleisten (Art. 80b IRSG). Es wird sich zeigen, dass bei Inhaltsdaten eine vorzeitige Übermittlung, d.h. vor Rechtskraft einer Abschlussverfügung, grundsätzlich ausgeschlossen ist (siehe unten III.B.1.). Da die fragliche Zwangsmassnahme ihrem Wesen nach geheim ist, kann sich eine Offenlegung gegenüber der betroffenen Person als folgeschwer für das Verfahren im Ausland erweisen. Dabei sind zwei Fälle zu unterscheiden:

1. Wenn die von der Massnahme betroffene Person keinen Wohnsitz oder kein Zustellungsdomizil in der Schweiz hat, muss ihr die Verfügung der Behörde nicht zugestellt werden (Art. 80m Abs. 1 IRSG). Die Abschlussverfügung wird somit nur dem BJ zugestellt (Art. 80h lit. a IRSG), was eine Übermittlung des Ergebnisses der Überwachung an die ersuchende Behörde ermöglicht, ohne dass die betroffene Person tatsächlich darüber informiert wurde. Wenn sich die betroffene Person bei der Vollzugsbehörde meldet, indem sie vor der Rechtskraft der Abschlussverfügung einen Wohnsitz in der Schweiz begründet hat, muss ihr selbstverständlich das Recht auf Teilnahme am Verfahren und auf Akteneinsicht garantiert werden (Art. 80b Abs. 1 in Verbindung mit Art. 80m Abs. 2 IRSG).

2. Hat die Person, gegen die die Massnahme gerichtet ist, ihren Wohnsitz in der Schweiz oder hat sie hier ihren Wohnsitz gewählt, muss die Vollzugsbehörde ihr das Recht auf Teilnahme am Verfahren und auf Akteneinsicht garantieren (Art. 80b Abs. 1 IRSG; vorbehaltlich des Sonderfalls der Verwendung einer falschen Identität, siehe unten III.B.3), bevor das Beweismittel ins Ausland übermittelt wird. Nichtsdestotrotz ist die

ersuchende Behörde nicht verpflichtet, der betroffenen Person dieses Recht nach Beendigung der Überwachungsmaßnahme zu gewähren. Die Maßnahme kann so lange geheim bleiben, wie dies für das Verfahren im Ausland erforderlich ist. Die Vollzugsbehörde muss sich bei der ersuchenden Behörde vergewissern, wann die Existenz der Überwachungsmaßnahme offengelegt werden kann, um die Fortsetzung des Rechtshilfeverfahrens zu ermöglichen.

Am Ende des Verfahrens erlässt die Vollzugsbehörde eine Schlussverfügung, die beim Bundesstrafgericht angefochten werden kann (Art. 80e IRSG). Eine anschliessende Beschwerde an das Bundesgericht bleibt unter den restriktiven Bedingungen von Art. 84 BGG (besonders wichtiger Fall) möglich. 16

B. Unterscheidungen und Sonderfälle

1. Vorzeitige Übermittlung von Inhaltsdaten?

Unter bestimmten Voraussetzungen erlaubt Art. 18b IRSG die vorzeitige Übermittlung - d.h. vor Erlass einer Schlussverfügung - von Daten über den Computerverkehr, die aufgrund einer bewilligten Anordnung zur Echtzeitüberwachung gesammelt wurden. Art. 18b IRSG stellt die Umsetzung der Verpflichtungen aus Art. 33 CCC dar. Da es sich jedoch um Inhaltsdaten handelt, hatte das Bundesgericht Gelegenheit zu bestätigen, dass Art. 18b IRSG nicht anwendbar ist und dass daher eine vorzeitige Übermittlung, d.h. vor Rechtskraft einer Abschlussverfügung, auf der Grundlage dieser Bestimmung ausgeschlossen ist. Damit wird der Schweiz ein wichtiges Instrument im Kampf gegen die internationale Kriminalität, insbesondere die organisierte Kriminalität und den Terrorismus, vorenthalten. Es ist auch fraglich, ob Art. 18a IRSG mit dieser Auslegung des Bundesgerichts noch über eine tatsächliche praktische Bedeutung und Nützlichkeit verfügt. 17

Dennoch hat der Gesetzgeber 2021 neue Bestimmungen eingeführt, die diesen Mangel teilweise beheben und einen wichtigen Schritt in Richtung flexiblerer Regeln und einer schnelleren und reaktiveren, auf internationalem Vertrauen basierenden Rechtshilfe darstellen. Art. 80dbis IRSG (dynamische Rechtshilfe) ermöglicht ausnahmsweise eine vorzeitige Übermittlung von Informationen oder Beweismitteln, wenn (a) ausländische Ermittlungen in Fällen von organisierter Kriminalität oder Terrorismus ohne diese Rechtshilfemassnahme übermässig erschwert würden, insbesondere wegen der Gefahr von Kollusion, oder weil die Vertraulichkeit des Verfahrens 18

gewahrt werden muss, oder (b) um eine schwere und unmittelbare Gefahr abzuwenden, insbesondere die Begehung eines terroristischen Akts. Diese Bestimmung soll in dringenden und begründeten Fällen (z. B. Geiselnahme oder Terroranschlag) eine wirksame Prävention ermöglichen, indem eine zu späte Reaktion auf geplante Straftaten vermieden wird, wobei der Vertraulichkeit in diesem Zusammenhang eine große Bedeutung zukommt. In materieller Hinsicht sieht Art. 80dbis IRSG im Gegensatz zu Art. 18b IRSG, der die vorzeitige Übermittlung auf Daten des Computerverkehrs und sogar auf Sekundärdaten der klassischen Telekommunikation beschränkt, vor, dass jede Art von Beweismitteln oder Informationen auf diesem Weg vorzeitig übermittelt werden kann. In formeller Hinsicht verlangt Art. 80dbis Abs. 4 IRSG, dass die Vollzugsbehörde vor jeder vorzeitigen Übermittlung bestimmte zusätzliche Verpflichtungen von der ersuchenden Behörde einholt, insbesondere die Informationen oder Beweismittel nur zu Ermittlungszwecken und keinesfalls zur Beantragung, Begründung oder zum Erlass einer Endentscheidung zu verwenden (lit. a) und die vorzeitig übermittelten Informationen oder Beweismittel aus den Akten des ausländischen Verfahrens zu entfernen, wenn die Rechtshilfe verweigert wird (lit. c). Wenn alle diese Bedingungen erfüllt sind, steht einer vorzeitigen Übermittlung von Inhaltsdaten über und unter den Bedingungen von Art. 80dbis IRSG nichts im Wege.

- 19 Darüber hinaus kann eine vorzeitige Übermittlung von Inhaltsdaten durchaus im Rahmen und nach den Regeln einer gemeinsamen Ermittlungsgruppe (GEG; oder Joint Investigation Team, JIT; Art. 80dter-80dduodecies IRSG) erfolgen. In diesem Fall kann sie auch dann tätig werden, wenn die Voraussetzungen nach Art. 80dbis Abs. 1 lit. a und b oder Abs. 2 IRSG nicht erfüllt sind.

2. Unterscheidung zwischen einer Hinterlegungsanordnung (Art. 265 StPO) und einer Überwachungsmaßnahme (Art. 269 ff. StPO), insbesondere im Hinblick auf E-Mail-Postfächer.

- 20 Das Fernmeldegeheimnis ist eine Verfassungsgarantie, die in Art. 13 Abs. 1 BV verankert ist. Dieses Recht stellt einen wesentlichen Aspekt des Rechts auf Achtung des Privatlebens dar. Die Überwachung der Korrespondenz sowie der durch die Post und die Telekommunikation hergestellten Beziehungen stellt einen schweren Eingriff in dieses Grundrecht dar. Daher ist es wichtig zu

unterscheiden, was unter diese Garantie fällt und was nicht. Zu diesem Zweck werden traditionell zwei Kriterien angewandt, um zwischen Fällen, in denen die Informationen direkt durch einen Produktionsauftrag erlangt werden können, und solchen, in denen ein BÜPF-Antrag erforderlich ist, zu unterscheiden:

- das erste entscheidende Kriterium ist der Bezug zur Fernmeldekorrespondenz ;
- das zweite Kriterium ist die Frage, ob die verlangten Daten unter das Grundrecht auf das Fernmeldegeheimnis fallen, das durch Art. 13 Abs. 1 BV geschützt wird.

Das Zusammentreffen der beiden Kriterien impliziert die Anwendung des 21
BÜPF.

In der Praxis wird es in den meisten Fällen um den Zugriff auf den Inhalt von 22
elektronischen Postfächern (E-Mail, E-mail) gehen. Um zwischen Daten, die unter das Fernmeldegeheimnis fallen, und Daten, die direkt von der Strafbehörde erlangt werden können (Hinterlegungsanordnung im Sinne von Art. 265 StPO), zu unterscheiden, hat das Bundesgericht das Kriterium des Zeitpunkts des letzten Zugriffs (Verbindung, Log) des E-Mail-Empfängers auf sein elektronisches Postfach aufgestellt. Das Bundesgericht hält fest, dass das Mitteilungsverfahren als zu dem Zeitpunkt beendet anzusehen ist, zu dem der Empfänger alleiniger Herr der Daten wird, d.h. zu dem Zeitpunkt, zu dem der Empfänger auf sein E-Mail-Postfach zugreift, und zwar unabhängig davon, ob er die erhaltenen E-Mails tatsächlich geöffnet und zur Kenntnis genommen hat. In der Praxis bedeutet dies, dass der Staatsanwalt den Inhalt der E-Mails vor dem letzten Login direkt vom Dienstanbieter erhalten kann (Art. 265 StPO), während er den Weg über den Dienst SCPT und das Zwangsmassnahmengericht gehen muss, um den Inhalt der E-Mails nach dem letzten Login zu erhalten (Art. 269 ff. StPO). Mit anderen Worten: Art. 31 CCC (Amtshilfe beim Zugriff auf gespeicherte Daten) und nicht Art. 34 CCC gilt für das Sammeln und Weiterleiten von E-Mails, die vor dem letzten Log entstanden sind.

3. Verwendung einer falschen Identität

Unserer Ansicht nach sollte demjenigen, der zur Begehung einer Straftat ein 23
Konto bei einer Plattform (E-Mail-Anwendung, E-Mail-Postfach usw.)

verwendet, die einen hohen Grad an Vertraulichkeit gewährleistet (Art End-to-End-Verschlüsselung der Daten [end-to-end encryption], manchmal gekoppelt mit einer Verschlüsselung vom Typ Null-Zugriff [zero-access encryption], keine oder nur wenige für die Registrierung erforderliche Daten usw.), nicht die Eigenschaft einer Partei im Rechtshilfeverfahren zuerkannt werden, wodurch seine Identifizierung für die Strafbehörden erschwert wird. Denn ohne eine anfängliche Identifizierung gibt es nur wenige Möglichkeiten, um zu überprüfen, ob die Person, die diese Eigenschaft vorgibt, tatsächlich der Nutzer dieser Ressource ist.

Die Autoren haben den vorliegenden Beitrag in persönlicher Eigenschaft verfasst. Die dargestellten Einschätzungen und Meinungen sind ihre eigenen und binden die Bundesanwaltschaft nicht.

LITERATURVERZEICHNIS

Aeppli Michael, commentaire de l'art. 18a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1^{ère} édition, Bâle 2015.

Dangubic Miro/Clerc Yves, Art. 80d^{bis} IRSG – ein Überblick, *forumpoenale* 4 (2022) p. 287-292.

Ludwiczak Glassey Maria/Bonzanigo Francesca, L'artificielle distinction entre « informations » et « moyens de preuve » en entraide pénale internationale, *Revue Pénale Suisse* 140 (2022) p. 402-427.

Ludwiczak Maria, L'entraide pénale internationale 'dynamique' en bref. Le projet, les débats, le compromis, *Pratique juridique actuelle*, 1 (2021) p. 71–75.

Zimmermann Robert, La coopération judiciaire internationale en matière pénale, 5^e édition, Berne 2019.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, *Internationale Rechtshilfe*, 2e édition., Zurich et al. 2015.

MATERIALIENVERZEICHNIS

Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013, FF 2013 2379, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/>

[eli/fga/2013/512/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2013-512-fr-pdf-a.pdf](#), consulté en janvier 2024 (cité : Message LSCPT).

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité du 18 juin 2010, FF 2010 4275, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2010/813/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2010-813-fr-pdf-a.pdf>, consulté en janvier 2024 (cité : Message CCC).

Message relatif à l'arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme et de son Protocole additionnel et concernant le renforcement des normes pénales contre le terrorisme et le crime organisé, FF 2018 6469 ss, consultable sous <https://www.fedlex.admin.ch/eli/fga/2018/2301/fr>, consulté en janvier 2024 (cité : Message terrorisme).

Rapport explicatif de la Convention sur la cybercriminalité du 23 novembre 2001, Conseil de l'Europe, Série des traités européens – no 185, consultable sous <https://rm.coe.int/16800ccea4>, consulté en janvier 2024 (cité : Rapport explicatif du Conseil de l'Europe).

Rapport explicatif relatif à la révision totale de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT; RS 780.11) du Service Surveillance de la correspondance par poste et télécommunication, consultable sous https://www.li.admin.ch/sites/default/files/2018-02/Rapport_explicatif_OSCPT.pdf, consulté en janvier 2024 (cité : Rapport explicatif OSCPT).

Recommandation n° R (85) 10 du Comité des Ministres aux États membres concernant l'application pratique de la convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications du 28 juin 1985, consultable sous : <https://rm.coe.int/09000016804e3071>, consulté en janvier 2024 (cité : Recommandation no R (85) 10).